

**ЕВН** България Електроразпределение ЕАД

**гр.Пловдив**

**ДОКУМЕНТАЦИЯ ЗА УЧАСТИЕ**

**в система за предварителен подбор на изпълнители**

**№ С-14-НМ-Д-123**

**с предмет**

**Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"**

**ПЛОВДИВ, 2014 г.**

**СЪДЪРЖАНИЕ**

1. Описание на етапите и правилата
2. Образец на заявление за включване в система за предварителен подбор на изпълнители
3. Търговски условия (Издание Юни.2014 г.)за Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"
4. Технически изисквания (Издание Юни.2014)за Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"
5. Въпросник за подбор
6. Декларация № 1 чрез лицата по Чл. 47, ал.6 за липса на обстоятелствата по чл.47, ал. 1, т.2, т.3; ал.2, т. 2а, т.3, т.4 и ал.5,т.2 от ЗОП
7. Декларация № 2 от лицата по Чл. 47, ал.4 за липса на обстоятелствата по чл.47, ал.1, т.1, ал. 2, т.5 и ал.5,т.1 от ЗОП
8. Декларация № 3 от лицата по Чл. 47, ал.6 за обстоятелствата по чл. 56, ал. 1, т. 11 и т.12 от ЗОП
9. Декларация № 4 чрез лицата по Чл. 47, ал.6 за обстоятелствата по чл. 56, ал.1, т.8 от ЗОП
10. Декларация № 5 от подизпълнител
11. Проект на договор
12. Банкова гаранция за добро изпълнение – мостра
13. Мерки за безопасност при работа на външни фирми на територията на Възложителя
14. Общи условия на закупуване
15. Клауза за социална отговорност
16. Решение № С-14-НМ-Д-123/Р01 на Възложителя
17. Обявление за квалификационна система №С-14-НМ-Д-123

**Описание на етапите и правилата**

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

**Кратко описание на предмета, етапите на подбор и правилата на система за предварителен подбор**  
**Кратко описание на предмета****РАЗДЕЛ А: Описание на етапите на подбор****Етап I: Подаване и разглеждане на заявления за участие**

След разглеждане на процедурната документация, за да бъдете включени в система за предварителен подбор, е задължително да подадете заявление за участие, което да бъде придружено от документите, изброени в т.1

„Задължителни изисквания към кандидатите“, по-долу:

**1. Задължителни изисквания към кандидатите**

Със заявлението за участие следва да бъдат представени, следните документи:

- 1.1. Списък с пълно и коректно изброяване на приложените към него документи, както и копие на документа за закупуване на документацията за участие
- 1.2. Подписани и подпечатани от участника: проекто-договор, ведно с търговски условия за Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери", технически изисквания за Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери", общи условия на закупуване на дружествата от групата на EVN и клауза за социална отговорност на дружествата от групата на EVN, приложения към проекто договор.
- 1.3. Детайлно техническо описание на предлаганите стоки и/или услуги.

**Изисквания за юридическото състояние**

- 1.4. Документи, удостоверяващи правосубектността на кандидата: копие от документа за регистрация или единен идентификационен код съгласно чл. 23 от Закона за търговския регистър, когато участникът е юридическо лице или едноличен търговец; копие от документа за самоличност, когато участникът е физическо лице; за чуждестранните лица - съответен еквивалентен документ за регистрация, издаден от съдебен или административен орган в държавата, в която е установен, който се представя в официален превод. Споразумение/договор за създаване на обединение (когато участникът е обединение, което не е юридическо лице) – Споразумението/договорът за създаване на обединение следва да бъде с нотариална заверка на подписите и да бъде представено в оригинал или нотариално заверено копие. В споразумението се посочва представляващият обединението. В случай, че обединението има регистрация в Регистър БУЛСТАТ, да се представи БУЛСТАТ на обединението, копие от документа за регистрация или единен идентификационен код съгласно чл. 23 от Закона за търговския регистър..
- 1.5. Декларация № 1 чрез лицата по Чл. 47, ал.6 за липса на обстоятелствата по чл.47, ал. 1, т.2, т.3; ал.2, т. 2а, т.3, т.4 и ал.5, т.2 от ЗОП
- 1.6. Декларация № 2 от лицата по Чл. 47, ал.4 за липса на обстоятелствата по чл.47, ал.1, т.1, ал. 2, т.5 и ал.5, т.1 от ЗОП
- 1.7. Декларация № 3 чрез лицата по Чл. 47, ал.6 за обстоятелствата по чл. 56, ал. 1, т. 11 и т.12 от ЗОП
- 1.8. Декларация № 4 от лицата по Чл. 47, ал.6 за обстоятелствата по чл. 56, ал.1, т.8 от ЗОП
- 1.9. Декларация №5 от подизпълнител, в случаите когато кандидатът ще използва подизпълнител

**Изисквания за технически възможности и квалификация**

- 1.10. Кандидатът трябва да представи попълнен „Въпросник за подбор“ - ,т.6 от въпросника, т.1 до 5 се попълват от Възложителя.
- 1.11. Кандидатът трябва да представи следните документи:
  - 1.11.1. Описание на системата
  - 1.11.2. Описание на компонентите
  - 1.11.3. Описание на изискванията към хардуера за всеки елемент (комуникационни сървъри, приложения, база данни), като е необходимо архитектурата, върху която ще бъдат инсталирани елементите, да бъде съгласувана с Възложителя
  - 1.11.4. Ръководство за потребителя
  - 1.11.5. Ръководство поддръжка Сертификати на отделните компоненти от системата (електромери, Концентратор на данни..)
- 1.12. Успешно преминал функционален тест на инсталиране и пускане в експлоатация на тестовия вариант на "Системата за дистанционно отчитане на електромери" на база протокол - Приложения 1 към

документа "Техническите изисквания" за успешно преминал функционален тест, удостоверяващ изпълнението на минималните технически изисквания на Възложителя съгласно „Техническата спецификация“ към системата за предварителен подбор на Изпълнители. Тестът на мострите се извършва при следните условия и последователност:

- 1.12.1. Комисията разглежда документалната част на постъпилите заявления за участие и въз основа на представените, съгласно изискванията, документи, удостоверяващи тяхното икономическо и финансово състояние, техническата им възможност и/или квалификация за участие в системата за предварителен подбор.
- 1.12.2. За провеждане на функционален тест с участието на Кандидата с цел потвърждаване на изискваните функционалности, кандидатите изпълняващи документално изисквания на Възложителя ще бъдат поканени да представят безвъзмездно мостра на , тестови вариант на „Система за дистанционно отчитане на електромери“, напълно съответстваща на "Техническите изисквания" на Възложителя, включваща минимум:
  - 1.12.2.1. Мостри на част от Системата, съгласно т. III.1. и т.IV.1. от документа „Технически изисквания“, Електромери: Позиция 1: Еднофазен електромер за директно свързване – 4 броя, Позиция 2: Трифазен електромер за директно свързване – 4 броя, Позиция 3: Трифазен електромер за индиректно свързване – 4 броя, Концентратор за данни: 2бр.);
  - 1.12.2.2. Софтуерът на тестовия вариант на Системата инсталиран на хардуер на Кандидата.

За предоставена мостра от Кандидата на Възложителя се подписва приемо-предавателен протокол, като приемо-предавателния протокол се добавя към документацията към заявлението за участие.

Мострите се предоставят безвъзмездно на Възложителя на адреси съгласно т. VII.3 от документа „Технически изисквания“ и се връща на Участника/ Кандидата, в случай че същия не е допуснат до участие в система за предварителен подбор на изпълнители или срока на валидност на система за предварителен подбор на изпълнители е изтекъл.

- 1.12.3. За провеждане на функционален тест на тестови вариант на Системата, Възложителя ще изпрати покана до Кандидата за ден и час на провеждането му, не по-късно от 1 месец считано от датата на на премо-предавателния протокол за предадени мостри
- 1.12.4. В случай, че предоставения тестови вариант на «Системата за дистанционно отчитане на електромери» не издържи теста, Кандидатът има право да представи нова мостра на системата след получаване на протокол за извършен функционален тест от Възложителя, но не по-късно от 4 месеца считано от датата на подаване на "Заявление за участие".
- 1.13. Внедрена система за контрол на качеството, сертифицирана по ISO 9001-2008 или еквивалентна на производителя/-ите на стоките – предмет на система за предварителен подбор на изпълнители. Съответствието с изискването се доказва с копие на валиден сертификат към момента на подаване на заявлението.
- 1.14. Доказателства за инсталация на поне 100 000 Електромера с Power Line Communication (PLC) управлявани от една система на територията на Европейския съюз.
- 1.15. Доказателства, че кандидатът е собственик на софтуера, който управлява системата или разполага с права от собственика на софтуера да прави корекции в него.
- 1.16. Доказателства, че кандидатът има сътрудници на трудов и граждански договор за осъществяване на поддръжката на софтуера и хардуера на системата. Представя се списък на сътрудници назначени на трудов и граждански договор.
- 1.17. Доказателства, че кандидатът има 24/7 часов онлайн служба за съобщения и телефон хелп деск (Help Desck) – предоставяне на информация за тестов достъп до система
- 1.18. Кандидатът трябва да е оторизиран за разпространение на оборудването на територията на България. В случай, че кандидатът не е производител на оборудването, то той трябва да представи актуален договор и/или оторизационно писмо от производителя на предлаганото оборудване, показващи права за разпространението им на територията на България.

#### **Изисквания за икономическо и финансово състояние**

- 1.19. Възложителя няма изисквания към кандидатите.
- 1.20. **Други задължителни изисквания**
  - 1.20.1. Декларациите, предоставени на бланка на Възложителя не се допуска да се пренаписват върху бланки на кандидата. В случай на повече от един представляващ кандидата и/или повече от един подизпълнител, то предварително се размножава бланката в необходимия брой копия.
  - 1.20.2. Не се допуска Кандидатът да използва участие на подизпълнители с цел покриване на Изискванията за икономическо и финансово състояние на кандидатите и изискванията за технически възможности и квалификация.
  - 1.20.3. Когато Кандидатът предвижда участие на подизпълнители за всеки подизпълнител се представят:
    - 1.20.3.1. Документите, удостоверяващи правосубектността на подизпълнителя

- 1.20.3.2. Декларация №1, Декларация №2, Декларация № 5
- 1.20.3.3. Доказателства за икономическо, финансово състояние и технически възможности, съгласно задължителните изисквания към кандидатите. Доказателствата се представят и прилагат съобразно вида и дела на участието.
- 1.20.4. Когато Кандидатът е обединение на физически и/или юридически лица, то:
- 1.20.4.1. Съгласно разпоредбите на Чл.25, ал.3, т.2, Възложителят изисква създаване на юридическо лице, в случай че Кандидатът е обявен за Изпълнител
- 1.20.4.2. Съгласно разпоредбите на Чл.25, ал.8, задължителните изисквания към кандидатите се прилагат към обединението участник, а не към всяко от лицата, включени в него, с изключение на съответна регистрация, представяне на сертификат или друго условие, необходимо за изпълнение на поръчката, съгласно изискванията на нормативен или административен акт и съобразно разпределението на участието на лицата при изпълнение на дейностите, предвидено в договора за създаване на обединението.
- 1.20.4.3. Всички лица, включени в обединението трябва да отговарят на условията на Чл.55, ал.6 от ЗОП, а именно едно физическо или юридическо лице може да участва само в едно обединение.
- 1.20.4.4. Документите, удостоверяващи правосубектност се представят за всяко едно лице, включено в обединението.
- 1.20.4.5. Декларация № 1 и Декларация № 2 се представят от всяко едно лице, включено в обединението.
- 1.20.4.6. Доказателства за икономическо, финансово състояние и технически възможности, съгласно задължителните изисквания към кандидатите се представят само от участниците, чрез които обединението доказва задължителните изисквания към кандидатите.
- 1.20.4.7. Декларация № 3 се представя от участниците в обединението, които ще представят услуги. Съгласно разпоредбите на Чл.77, ал.3, т.3, със заявлението на участие се представя документ, подписан от лицата в обединението, в който задължително се посочва представляващия.
- 1.20.5. Когато участникът в процедура е чуждестранно физическо или юридическо лице или техни обединения (i) офертата се подава на български език; (ii) документите, удостоверяващи регистрацията му, когато участникът е юридическо лице или обединение на юридически лица или копие от документа за самоличност, когато участникът е физическо лице се представят в официален превод; (iii) всички останали документи, които са на чужд език, се представят и в превод.
- 1.20.6. В случай на участие на обединение или сдружение, под формата на дружество по Закона за задълженията и договорите (ЗЗД), в заявлението за участие следва да се представи копие от нотариално заверен договор за създаване на дружеството.
- 1.20.7. В случай на избор на изпълнител, който е дружество по смисъла на ЗЗД, в срок до 15 календарни дни от датата на получаване на решението за избор на изпълнител, същият следва да регистрира дружеството, с което да бъде сключен договор.

**Неизпълнението на което и да е от задължителните изисквания към кандидатите води до невключване на кандидата в системата за предварителен подбор на изпълнители.**

## **2. Подаване на заявление за участие**

- 2.1. Окомплектованите заявления за участие се предават на адрес: „ЕВН България Електроразпределение ЕАД, гр. Пловдив 4000, ул. „Христо Г. Данов“ №37, стая 110 - "Деловодство". Задължително върху плика се изписва "Заявление за участие", номера на системата за предварителен подбор на изпълнители „С-14-НМ-Д-123“, и предмета „Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"", както и информация за обратна връзка с кандидата – адрес, телефон, имейл.
- 2.2. В случай, че заявлението се подписва от лице, което не представлява участника по закон следва да бъде представено нотариално заверено пълномощно, в което да е изрично предвидено пълномощникът да може да подписва заявлението и валидно да задължава с подписа си кандидата в конкретната процедура по възлагане на обществена поръчка.
- 2.3. Заявлението за участие в системата за предварителен подбор на изпълнители се изпраща в запечатан, непрозрачен плик, в срок, на адрес на Възложителя, посочен в обявлението. Заявления, пристигнали след указания срок и/или в плик с нарушена цялост няма да бъдат допускани до разглеждане за включване в системата за предварителен подбор и ще бъдат връщани на кандидатите.
- 2.4. Заявлението за участие трябва да съдържа всички документи, изброени в т.1. Кандидат с непълно заявление няма да разглежда за включване в системата за предварителен подбор.
- 2.5. Заявлението за участие може да съдържа предложение относно продуктите на един производител. В случай, че кандидат желае да бъде включен в система за предварителен подбор на изпълнители с двама или повече производители, то е необходимо да подаде отделно, независимо заявление с пълен набор документация за всеки отделен производител, който представлява.

2.6. Всички разходи на кандидата по окомплектоването и подаването на заявление за участие в процедурата са за негова сметка

### **3. Разглеждане на заявлението за участие**

- 3.1. Назначената от Възложителя комисия, разглежда подаденото заявление за участие от кандидата. Заявление за участие в система за предварителен подбор може да се подава по всяко време в срока на действие на системата. На база констатирано изпълнение на всички задължителни изисквания съгласно т.1 „задължителни изисквания към кандидатите“, с доклад до Възложителя, комисията предлага да включи или мотивирано да откаже включването на кандидата в системата за предварителен подбор на изпълнители.
- 3.2. Възложителят си запазва правото за извършване проверка на място на информацията, съдържаща се в представените от кандидата документи, за което кандидата ще бъде уведомен писмено, не по-малко от три дни преди това.
- 3.3. При констатиране на неверни декларираните данни и/или предоставени документи, с които се доказват изпълнение на задължителните изисквания към кандидатите, кандидатът няма да бъде допуснат до включване в система за предварителен подбор на изпълнители.
- 3.4. В шестмесечен срок от получаване на заявлението Възложителят, на базата на протокола на комисията, взема решение с което уведомява кандидата в 15-дневен срок от датата на решението за включването му в системата за предварителен подбор или за отказа си за това, като мотивира последното.
- 3.5. Кандидатите, включени в система за предварителен подбор на Изпълнители са задължени да уведомяват Възложителя в 14 (четиринадесет) дневен срок в случай на промяна на декларираните със заявлението за участие обстоятелства.

**Неизпълнението на което и да е от задължителните изисквания към кандидатите води до невключване на кандидата в системата за предварителен подбор на изпълнители.**

### **Етап II: Провеждане на договаряне с допуснатите участници**

4. При възникване на необходимост от доставка на материали/услуги, предмет на системата за предварителен подбор на изпълнители по определена позиция, Възложителят издава Решение за стартиране на процедура на договаряне с обявление по система за предварителен подбор на изпълнители.
5. Възложителят отправя писмена поканата за представяне на първоначална оферта до всички участници, включени в системата. Количества, които се посочват в поканата за първоначална оферта са прогнозни и служат само за изготвяне на ценовото сравнение. Първоначалната оферта трябва да бъде представена на хартиен носител, като хартиения носител следва да бъде подпечатан и подписан от упълномощено от фирмата участник лице.
6. В зависимост от прогнозната стойност на процедурата, Възложителят може да изиска от участниците да предоставят банкова или депозитна гаранция за участие, чийто размер ще бъде определен от Възложителя и посочен в поканата за предоставяне на първоначална оферта.
7. При калкулиране на цените в офертата, участникът трябва задължително да включи в тях всички транспортно-командировъчни разходи, разходи за нощувки, дневни и други разходи, необходими за изпълнението на възложените доставки. След подписване на договор, разходите, непредвидени при подаване на офертата са изцяло от и за сметка на Изпълнителя. Възложителят не се ангажира с поемането на допълнителни разходи.
8. Първоначалната оферта се състои от два запечатани, непрозрачни плика. Плик №1 с надпис „Гаранция за участие“ съдържа документ, удостоверяващ внесена гаранция за участие, Плик №2 с надпис „Ценово предложение“, съдържа началната оферта и финансовото предложение, изготвени на бланки на Възложителя. Първоначалната оферта се предава в надписан, запечатан и непрозрачен, на адрес: "ЕВН България Електроразпределение ЕАД", гр. Пловдив 4000, ул. „Христо Г. Данов“ №37, стая 110 - "Деловодство". Задължително върху плика се изписва "Начална оферта, номера на системата за предварителен подбор на изпълнители „С-14-НМ-Д-123“ и предмета "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"". Крайният срок за представяне на първоначалната оферта, както и срокът на валидност на офертите ще бъде посочен в поканата, отправена от Възложителя.
9. С цел да създаде прозрачни и равни условия за приемане на оферти, както и за избягване на спорове във връзка с реда на тяхното постъпване, Възложителят определя следните правила за тяхното подаване.
  - 9.1. Ред за подаване на оферти
    - 9.1.1. Заинтересованите лица имат право да използват всички способи, предвидени в ЗОП за подаване на оферти;
    - 9.1.2. В случаите когато представител или пълномощник на заинтересовано лице подава оферта в сградата по седалището и адреса на управление на Възложителя – гр. Пловдив, ул. „Христо Г. Данов“ № 37, представителят или пълномощникът на заинтересовано лице се задължава:
      - 9.1.2.1. да изтегли (получи) документ - билет от терминално устройство, разположено непосредствено пред стая с номер 110, находяща се на партерен етаж в сградата по седалището и адреса на управление на Възложителя;



- 9.1.2.2. да подаде офертата чрез депозирането ѝ в стая 110, където се намира деловодството на Възложителя, като при депозирането на офертата заинтересованото лице представя получения документ - билет, от съдържанието на който се виждат пореден номер; дата и час;
- 9.1.2.3. да удостовери със своя саморъчен подпис и изписване на лично и фамилно име върху документа – билет, че същият е прикрепен към външната опаковка – плик, съдържащ оферта.
- 9.1.2.4. да получи документ, съдържащ номер от входящия регистър на дружеството Възложител, отразяващ поредността на подаването на офертата.
- 9.1.2.5. Поредността, в която ще се счита, че са получени оферти, изпратени чрез лице, притежаващо необходимите по закон права да извършва куриерски услуги, ще бъде определян съобразно датата и часът, вписани върху товарителния запис и поредността на получаване на останалите оферти.
- 9.2. Допълнителни разяснения и примери
- Терминалното устройство на Възложителя предлага възможността за изтегляне на билет от терминалното устройство с предназначение за „Депозиране на оферта в процедура според условията на Закона за обществените поръчки (ЗОП)“. При изтегляне на билет, кандидатът получава фиш с пореден номер и следното съдържание:
- „Този документ, получен от терминално устройство, функциониращо в сграда по седалището на Възложителя, се издава, за да послужи за удостоверяване на реда, в който Възложителят приема документ(и) от заинтересованото лице по смисъла на и в случаите, предвидени от закона.
- Документът е валиден, само в случай че заинтересованото лице - държател на същия, официално и на хартиен носител подаде (в стая 110) според условията на ЗОП, в определения от Възложителя срок, съответно необходимите по конкретна обществена поръчка документи.“
- Пример:
- Кандидат „X“ изтегля билет от терминалното устройство, с пореден номер 1.
- Кандидат „Y“ изтегля билет от терминалното устройство, с пореден номер 2.
- Кандидат „Z“ изтегля билет от терминалното устройство, с пореден номер 3.
- В случай, че кандидатите или представители на кандидатите „X“, „Y“ и „Z“ се намират физически пред деловодството на Възложителя, с цел подаване на оферта, Възложителят е длъжен да приеме първо офертата на кандидат „X“, притежаващ билет с пореден номер 1, след това офертата на кандидат „Y“, получил билет с пореден номер 2 и накрая – офертата на кандидат „Z“, получил билет с пореден номер 3.
- В случай, че кандидат „X“, получил билет с пореден номер 1, е изтеглил своя билет, но след това не се намира пред деловодството и не предприеме действия за подаване на офертата си на хартиен носител, то изтегленият билет губи валидността си, и кандидат „Y“, с изтеглен пореден номер 2, може да подаде офертата си преди кандидат „X“, а Възложителят е длъжен да ги приеме. При липса на представител и на кандидат „Y“, право да подаде пръв офертата си, има кандидат „Z“, въпреки че е изтеглил билет с пореден номер 3.
- Когато кандидатът подава оферта в сградата по седалището и адреса на управление на Възложителя, определеният краен срок за подаване на оферта в деловодството на Възложителя, се счита спазен, в случай, че изтегленият документ - билет от терминално устройство е с генерирани ден и час преди или равен на посочените в документацията към процедурата за избор. В този случай, Възложителят е длъжен да приеме офертата на кандидат, притежаващ билет от терминалното устройство, с генерирани ден и час преди или равен на определения краен срок за подаване на оферта в документацията към процедурата за избор, само в случай, че същият се намира физически в стаята на деловодството, респективно пред нея, в ден и час преди или равен на определения краен срок за подаване на оферта в документацията към процедурата за избор.
- Когато кандидат е получил билет от терминалното устройство с генерирани ден и час на получаване преди или равен на определения краен срок за подаване на оферта в документацията към процедурата за избор, но не е предоставил офертата в деловодството на Възложителя до определения краен срок за подаване на оферта в документацията към процедурата за избор и не се намира физически в стаята на деловодството, в часа, определен като краен срок за подаване на оферта в документацията към процедурата за избор, Възложителят не приема и връща офертата на кандидата като отбелязва точния час и дата на представяне на офертата първо върху билета (ако бъде представен такъв), като отбелязва часа и датата на депозирането им в деловодството на Възложителя и върху плика на офертата.
- В случай, че в стаята на деловодството едновременно непосредствено преди изтичане на крайния определен срок за подаване на оферта, повече от едно заинтересовано лице заявява желание за подаване на оферти, за да се избегне субективността при определяне поредността на подаване на оферти, възложителят ще спазва поредността на номерата, получени от терминалното устройство.
- В случай че в стаята на деловодството се направи опит за подаване на оферта, без да е изтеглен билет от терминалното устройство, офертата няма да бъде приемана, а приносителят на офертата ще бъде информиран за реда за подаване на оферти към процедури за обществена поръчка, описани в настоящия документ.
- Присъствието на приносителя на офертата преди посочения краен срок за подаване на оферта, в деловодството на Възложителя не е достатъчно условие за приемане на документите от Възложителя, същите трябва да са придружени от билет от терминалното устройство.

Пример:

Час определен като краен срок за подаване на оферта в документацията към процедурата за избор: 16:00:00

Кандидат "X" изтегля билет от терминалното устройство, с час 15:59:00.

Кандидат "Y" изтегля билет от терминалното устройство, с час 16:00:00.

Кандидат "Z" изтегля билет от терминалното устройство, с час 16:02:00.

В случай, че кандидатите или представители на кандидатите „X“, „Y“ и „Z“ се намират физически в стаята на или пред деловодството на Възложителя, с цел подаване на оферта, Възложителят е длъжен да приеме офертата единствено на кандидат „X“ и кандидат „Y“. Офертата на кандидат „Z“ следва да бъде върната, тъй като билетът, изтеглен от този кандидат, е генериран от терминалното устройство след настъпване на крайния срок определен за получаване на оферти.

В случай, че например кандидат „X“ не се намира в стаята на или пред деловодството и не предприеме действия за подаване на офертата си на хартиен носител, то изтеглянето от него билет губи валидността си, а Възложителят приема единствено офертата на кандидат „Y“. При липса на представител и на кандидат „Y“ в стаята на или пред деловодството, Възложителят не приема офертата на никой от кандидатите.

10. След разглеждане на офертите от комисията, назначена от Възложителя, всички участници, представили коректна оферта ще бъдат поканени за участие в договарянето, което представлява и преговори с окончателен характер. Датата и часът на договарянето ще бъде посочен в поканата, отправена от Възложителя и определени съгласно разпоредбите на Чл.89, ал.2.

### **Етап III: Решение за избор на Изпълнител и сключване на договор**

11. След провеждането на договарянето/преговорите с окончателен характер, на основание на критерия **"най-ниска цена"**, със свое Решение, Възложителят на обществената поръчка, на базата на класирането в протокола на комисията, ще определи Изпълнителя на обществената поръчка. Възложителят изпраща решение за избор на Изпълнител до всички участници в договарянето.

12. Изисквания към Изпълнителя

Преди подписване на договора за обществена поръчка, Изпълнителят е задължен да представи документи от съответните компетентни органи и/или институции за удостоверяване на обстоятелствата, че:

12.1. Изпълнителят:

12.1.1. не е обявен в несъстоятелност;

12.1.2. не е в производство по ликвидация и не се намира в подобна процедура съгласно националните закони и подзаконовни актове.

12.1.3. няма задължения по смисъла на чл. 162, ал. 2, т. 1 от Данъчно-осигурителния процесуален кодекс към държавата и към община, установени с влязъл в сила акт на компетентен орган, освен ако е допуснато разсрочване или отсрочване на задълженията, или има задължения за данъци или вноски за социалното осигуряване съгласно законодателството на държавата, в която кандидатът или участникът е установен.

12.2. Лицата по Чл.47, ал 4 не са осъждани в влязла в сила присъда за:

12.2.1. престъпление против финансовата, данъчната или осигурителната система, включително изпиране на пари, по чл. 253 - 260 от Наказателния кодекс;

12.2.2. подкуп по чл. 301 - 307 от Наказателния кодекс;

12.2.3. участие в организирана престъпна група по чл. 321 и 321а от Наказателния кодекс;

12.2.4. престъпление против собствеността по чл. 194 - 217 от Наказателния кодекс;

12.2.5. престъпление против стопанството по чл. 219 - 252 от Наказателния кодекс.

12.2.6. престъпление по чл. 313 от Наказателния кодекс във връзка с провеждане на процедура за възлагане на обществена поръчка

12.3. Преди подписване на договора за обществена поръчка Изпълнителят е задължен да представи банкова/депозитна гаранция за изпълнение в размер на 3% от стойността на договора/поръчката за срока на действие на договора 4-ри календарни години заедно с опция за удължаване с 1+1+1 години, включително гаранционния срок, в лева без включен ДДС.

12.4. Сертификат за задължително издържан IT секюрити тест (Security Evaluation Smart Meter Infrastructure) издаден от Riscure B.V., Адрес: Delftechpark 49, 2628 XJ Delft Netherlands (Холандия), T:+31 15251 4090, [www. Riscure.com](http://www.Riscure.com), като необходимо условие за изпълнение на поръчката съгласно 3-Н Защита на личните данни. Таксата при изпълнителя на теста е за сметка на Възложителя..

### **РАЗДЕЛ Б: Кратко описание на правилата**

#### **1. Изключване от система за предварителен подбор**

##### **1.1. Изключване на участници**



- 1.1.1. Възложителят може да прекрати участието в система за предварителен подбор на участник, който е престанал да отговаря на обявените задължителни изисквания и критерии за допускане. Прекратяването става с мотивирано решение на Възложителя, което се изпраща до изключения участник в сроковете, предвидени в ЗОП.
- 1.1.2. Възложителят прекратява участието/изключва от система за предварителен подбор, участници които не отговарят на актуализираните критерии и правила за подбор, когато такива са обявени, след указания от Възложителя срок за да представяне на исканите доказателства.
- 1.2. Изключване на Изпълнители
  - 1.2.1. Изпълнението на договор, сключен чрез използване на предварителен подбор в рамките на СПП, се преценява от страна на Възложителя от гледна точка на това дали Изпълнителят е спазил всички условия от конкретния договор, включително:
    - 1.2.1.1. спазване на всички срокове;
    - 1.2.1.2. стриктно спазване на абсолютно всички Технически изисквания на Възложителя;
    - 1.2.1.3. недопускане на брак в рамките на доставката;
    - 1.2.1.4. навременно попълване и подписване на всички документи в рамките на взаимоотношенията с Възложителя;
    - 1.2.1.5. ненарушена опаковка на доставяните стоки;
    - 1.2.1.6. съдействие спрямо служителите на Възложителя при приемане и предаване на стоките;
    - 1.2.1.7. спазване на всички изисквания на Възложителя и българското законодателство за отчетност и фактуриране;
    - 1.2.1.8. други важни параметри на изпълнението, посочени в договора по конкретната процедура за възлагане на обществена поръчка;
  - 1.2.2. В случай, че Изпълнителят не изпълни качествено едно или няколко от посочените по-горе условия, то в зависимост от сериозността на нарушенията, Възложителят си запазва правото сключеният с Изпълнителя договор да бъде едностранно прекратен от Възложителя, съгласно предвидения за това ред, в Търговските условия към настоящата СПП.
  - 1.2.3. В случай, че Възложителят прекрати едностранно договор на Изпълнител и причината за прекратяване на договора има отношение към критериите за допускане и правилата за подбор на системата, то Възложителят си запазва правото да го изключи от системата за предварителен подбор, след мотивирано предложение от назначената за провеждане на СПП комисия.
  - 1.2.4. Възложителят може мотивирано да откаже включване и/или да изключи от система за предварителен подбор кандидати и/или изпълнители, които:
    - 1.2.5. са виновни за сериозно професионално нарушение, доказано с всяко средство, с което могат да си послужат възлагащите органи;
    - 1.2.6. не са изпълнили задълженията си, свързани с изпълнение на договори за обществени поръчки
2. **Промени в задължителните изисквания към кандидатите**
  - 2.1. Възложителят може да променя и актуализира системата за предварителен подбор. Актуализираните правила се изпращат до лицата, включени в системата за предварителен подбор.
  - 2.2. В случай, че Възложителят извърши промени (актуализира) в посочените задължителни изисквания към кандидатите в рамките на валидност на системата за предварителен подбор, то всички допуснати в системата участници, са длъжни да представят исканите доказателства във връзка с извършените промени в задължителните изисквания в указания от Възложителя срок.
  - 2.3. На база констатирано изпълнение на актуализираните задължителни изисквания от страна на допуснатите към момента на актуализацията в системата участници, комисията предлага с доклад до Възложителя, да потвърди участието в системата или мотивирано да изключи съответния участник от нея.
  - 2.4. На базата на доклада на комисията, Възложителят взема решение, с което уведомява кандидата в 15-дневен срок от датата на решението за потвърждаване на участието му в системата за предварителен подбор или за изключването му от нея, като мотивира последното.
3. **Ежегодна проверка на изпълнението на задължителните изисквания за включване в системата за предварителен подбор**
  - 3.1. През всяка календарна година от действието на системата, Възложителят е в правото си да изиска от всеки кандидат, включен в системата за предварителен подбор на Изпълнители, да изпрати попълнени с актуални данни Техническа спецификация, Техническа анкетна карта, Въпросник за подбор, в срок не по-късно от 10 (десет) календарни дни, считано от датата на получаване на искането от страна на Възложителя.
  - 3.2. Задължение за предаване на актуализирани Техническа спецификация, Техническа анкетна карта, Въпросник за подбор карта имат всички кандидати, включени в системата за предварителен подбор на изпълнители, без значение от датата на подаване на заявлението за участие, както и дали е бил изпълнител по процедура на договаряне с обявление, проведена на база на системата за предварителен подбор.

- 3.3.** Актуализирани Техническа спецификация, Техническа анкетна карта, Въпросник за подбор се предават в надписан, запечатан и непрозрачен плик на адрес: "ЕВН България Електроразпределение" ЕАД, гр. Пловдив 4000, ул. „Христо Г. Данов“ №37, стая 110 - деловодство. Задължително върху плика се изписва наименованието на документа (Техническа спецификация, Техническа анкетна карта, Въпросник за подбор) номера на системата за предварителен подбор на изпълнители „С-14-НМ-Д-123“ и предмета "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери".
- 3.4.** Възложителят си запазва правото да прекрати участието/изключи от системата за предварителен подбор на изпълнители кандидат, който не е предал актуализирани Техническа спецификация, Техническа анкетна карта, Въпросник за подбор в определените срокове, както и кандидат, за който се установи че е налична актуализация на данните, която има отношение към критериите и правилата за подбор на системата за предварителен подбор и не е обявена в определения за целта 14-дневен срок.
- 3.5.** Възложителят си запазва правото да извърши проверка на място на декларираните данни.

Част от документацията по процедурата за възлагане на обществена поръчка може да бъде изготвена в двуезичен вариант. В случай на противоречие между двата текста, то предимство има българският текст.

Част от документацията по процедурата за възлагане на обществена поръчка е изготвена в двуезичен вариант. В случай на противоречие между двата текста, то предимство има българският текст.

При възникване на въпроси, във връзка със системата за предварителен подбор на изпълнители, моля обръщайте се към следните лица за контакти:

Относно техническите изисквания:

Атанас Попов– 0700-1-777, вътр.34535

Относно търговските условия:

Бончо Георгиев– 0700-1-777, вътр.44297

ЕВН България Електроразпределение ЕАД, в качеството си на Възложител, желае на всички кандидати, закупили документация за участие в горесцитираната система, успешно и ползотворно сътрудничество.

ДО ЕВН България Електроразпределение ЕАД.  
гр. ПЛОВДИВ

**ЗАЯВЛЕНИЕ**  
ЗА УЧАСТИЕ В СИТЕМА ЗА ПРЕДВАРИТЕЛЕН ПОДБОР НА ИЗПЪЛНИТЕЛИ

**№ С-14-НМ-Д-123 с предмет:**

**“Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери”**”

от Кандидат .....  
Адрес за кореспонденция: п.к. .... град .....  
ул./бул./ж.к/№ .....  
Лице за контакт .....  
Тел. .... Факс .....  
Мобилен ..... Имейл .....

УВАЖАЕМИ ГОСПОЖИ И ГОСПОДА,

След получаването на документацията за включване в система за предварителен подбор, за която сте ВЪЗЛОЖИТЕЛ, долуподписаният ....., в качеството си на ..... заявявам, че представляваният от мен Кандидат желае да участва в обявената от вас система при условията и съгласно изискванията на ВЪЗЛОЖИТЕЛЯ,

Забележка: Заявлението заедно с всички приложени документи се представят на български език по реда на чл. 56, ал. 4 от ЗОП. Прилаганите документи се описват в отделен списък, като се представят подредени в посочената в списъка последователност и представляват неразделна част от настоящото заявление за участие.

.....  
(дата на подписване)

(печат, подпис)

.....  
Кандидат: (подпис и печат)

**Търговски условия**

(Издание Юни 2014)

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

**1. Дефиниции**

Изброените по-долу термини имат значението, посочено срещу тях, освен ако контекстът налага друго значение:

- 1.1. Договор означава договор, сключен между Възложителя и Изпълнителя, в който се определя предмета на доставката и условията за нейното изпълнение.
- 1.2. Доставка означава: (i) доставката на стоките; и/ или (ii) предоставянето на услугите, предмет на договора
- 1.3. Срок на действие е срокът, през който договорът действа между страните и създава валидни права и задължения за всяка от тях.
- 1.4. Срок на изпълнение е срокът, в който дадена доставка трябва да бъде изпълнена
- 1.5. Стойност на договора е максималната стойност, която Възложителят може да дължи на Изпълнителя в замяна на извършени доставки, заявени в срока на действие на договора.
- 1.6. Търговски условия е настоящият документ, който представлява неразделна част от договора, и определя общите условия, които ще се прилагат за всяка конкретна доставка, извършена през срока на действие на договора. В случай на разлика между предвиденото в търговските условия и договора, ще се прилага предвиденото в договора.
- 1.7. Технически изисквания е документ, в който Възложителят определя своите изисквания по отношение на доставката. Техническите изисквания представляват неразделна част от договора и са задължителни за изпълнение от Изпълнителя.
- 1.8. Общи условия за закупуване е документ, който определя общо-приложими условия за всички Изпълнители. Общите условия представляват неразделна част от договора и са задължителни за Изпълнителя, доколкото в договора не е предвидено друго.

**2. Ценови условия**

- 2.1. Всички договорени в процеса на възлагане на поръчката единични цени са окончателни, без включен ДДС, прилагат се за целия срок на действие на договора и не подлежат на актуализация, освен ако договора не предвижда друго.

**3. Място на изпълнение**

- 3.1. Мястото на изпълнение се посочва от Възложителя в договора.

**4. Срокове**

- 4.1. Срокът на действие на договора е до (i) посочения в договора срок на договора или (ii) усвояване стойността на договора, което настъпи по-рано.
- 4.2. Срокът за изпълнение на доставка/доставки по договора се определя в календарни дни след датата на сключване на договора и се посочва в договора/в отделните заявки за доставка към договора. В случай че, в договора не е предвиден конкретен срок за изпълнение на доставката, максималният срок за изпълнение е до 30 (тридесет) дни след подписване на договора и получаване на писмена Заявка за доставка от Възложителя, съдържаща точна спецификация на доставката.

**5. Собственост/ риск**

- 5.1. В случаите, когато предмет на договора е доставка на стоки, Изпълнителят е длъжен да прехвърли собствеността върху стоките, свободни от каквито и да е права на трети лица, както и да предаде на Възложителя всички документи във връзка с произхода и ползването на стоките.
- 5.2. Собствеността и риска от погиване и/или повреждане на стоките преминава върху Възложителя след подписване на приемо-предавателен протокол за приемане на доставката. Преди подписване на посочения протокол рискът се носи от Изпълнителя.

**6. Плащане**

- 6.1.** Плащанията се извършват от Възложителя по банков път, по посочена от Изпълнителя сметка. Възложителят не прави авансови плащания. Възложителят заплаща дължимите суми след изпълнение на всички изброени по-долу условия: (i) надлежно извършена доставка; (ii) подписване на двустранен приемо-предавателен протокол за приемане на доставката от оправомощени представители на страните; и (iii) получаване на оригинална фактура, отговаряща на изискванията на Възложителя и приложимите нормативни актове. Срокът за плащане започва да тече от датата, на която бъде изпълнено и последното от посочените по-горе условия.
- 6.2.** Извършване на плащане от страна на Възложителя не означава признаване на редовността на доставката и нейното приемане, нито отказ от право на: (i) неустойки и/или претенции (ii) гаранции; и (iii) обезщетения.
- 6.3.** При издаване на фактура се посочват (i) ЕИК номерът и идентификационният номер по ДДС на Възложителя и на Изпълнителя; (ii) приложимата ставка на ДДС и сумата на ДДС, в случай на самоначисляване или нулева ставка на ДДС, се посочва приложимото законодателство и (iii) номер на Заявката за доставка.
- 6.4.** Оригинален фактурен заедно с подписан приемо - предавателен протокол за извършване на доставка и копие от съответната Заявка за доставка се изпращат на вниманието на лицата за контакт на Възложителя, посочени в договора.
- 6.5.** Страните се съгласяват, че не се допуска в една и съща фактура да се фактурират доставки по различни договори, както и доставки по различни заявки към един и същ договор.
- 6.6.** В случай че договорът или част от него има за свой предмет извършване на услуга от Изпълнителя към Възложителя, и Изпълнителят е чуждестранно лице, за целите на избягване на двойно данъчно облагане чрез прилагане на международните Спогодби за избягване на двойно данъчно облагане /"СИДДО"/, за всяка календарна година поотделно Изпълнителят предоставя на Възложителя "Декларация за притежател на дохода" и "Сертификат за местно лице", които следва да бъдат представени до датата на издаване на първа фактура по договора и изпратени на имейл, както и в оригинал до лицата за контакт на Възложителя, представители на отдел „Снабдяване“, посочени на първата страница в договора. В случай че не бъдат представени горепосочените документи, Възложителят удържа при плащането на фактурите данък при източника съгласно приложимото българско законодателство, когато услугите са в обхвата на този данък.

## **7. Отговорност**

- 7.1.** Изпълнителят отговаря за точното изпълнение на възложената поръчка.
- 7.2.** Изпълнителят носи отговорност за всички действия, бездействия, неизпълнение или небрежност от страна на негов представител и/или персонал, както и на негови подизпълнители, в случай че има такива.
- 7.3.** Изпълнителят отговаря за всички вреди, причинени на Възложителя и/или трети лица при или по повод изпълнение на договора.
- 7.4.** В случай че, при изпълнение на договора настъпи застрахователно събитие, покрито от някой от застрахователните договори на Възложителя, Изпълнителят е длъжен да изпълнява стриктно инструкциите за действие, дадени от Възложителя. В случай че, за настъпило застрахователно събитие не бъде изплатено застрахователно обезщетение поради неправилно предприемане на действия от страна на Изпълнителя, последният отговаря пред Възложителя за пълния размер на претърпените в резултат на застрахователното събитие щети.

## **8. Права и задължения на Възложителя**

- 8.1.** Възложителят има право:
- 8.1.1.** Във всеки момент от срока на действие на договора да извършва проверки относно качеството на доставката, без с това да пречи на самостоятелността на Изпълнителя.
- 8.1.2.** Писмено и мотивирано да поиска от Изпълнителя да бъде отстранен някой от подизпълнителите, тъй като последният се смята за неподходящ или не отговаря на изискванията на Възложителя
- 8.2.** Възложителят е длъжен
- 8.2.1.** Да организира допускането на Изпълнителя до мястото на изпълнение на доставката.
- 8.2.2.** Да заплаща приетите доставки в предвидените срокове.
- 8.2.3.** Да оформя предвидените в договора документи във връзка с неговото изпълнение.
- 8.3.** Приемането на доставка от страна на Възложителя не представлява отказ от право, възникнало в съответствие с договора, и не освобождава Изпълнителя от задълженията и отговорността му,

свързани с неточното изпълнение на задълженията му по договора.

## **9. Права и задължения на Изпълнителя**

### **9.1. Изпълнителят има право:**

- 9.1.1. Да бъде допуснат до мястото на изпълнение на доставката.
- 9.1.2. Да получи дължимите плащания в предвидените за това срокове.

### **9.2. Изпълнителят е длъжен:**

- 9.2.1. Да извърши доставката съгласно условията на договора и в съответствие с изискванията на Възложителя.
  - 9.2.2. Да извършва всички действия, свързани с изпълнението на договора, с грижата на добър търговец, в съответствие с приложимото законодателство и изцяло в интерес на Възложителя, както и съобразно стандартите, определени от Възложителя и от приложимото право.
  - 9.2.3. В цялата си дейност по договора да спазва всички установени правила в областта на здравословни и безопасни условия на труда, опазване на околната среда, качество на доставката и другите приложими за дейностите по договора нормативи.
  - 9.2.4. Изпълнителят, включително неговият персонал и подизпълнители, се задължават да се въздържат от всякакви действия, които могат да имат отрицателен ефект върху икономическите и правните интереси на Възложителя или върху неговата репутация и добро име.
  - 9.2.5. Да опазва цялото имущество на Възложителя, до което има достъп във връзка с изпълнението на доставката.
  - 9.2.6. Да информира Възложителя незабавно в писмена форма за възникнали щети или повреди в съоръжения, инсталации, оборудване или друго имущество – собственост на Възложителя, при изпълнение на доставката, както и за непосредствено свързаните с това опасности.
  - 9.2.7. Да уведомява писмено Възложителя, когато съществува опасност от забава при изпълнението на доставката.
  - 9.2.8. Да осигурява на Възложителя достъп до всяко място и до всяка информация, свързани с изпълнението на договора.
  - 9.2.9. Да не нарушава чрез доставката защитените права на трети лица.
- 9.3. Без предварителното писмено разрешение на Възложителя, Изпълнителят няма право:**
- 9.3.1. Да използва правата на интелектуална собственост на Възложителя, като например търговски марки, промишлен дизайн и други.
  - 9.3.2. Да прави изявления, дава интервюта и/или подписва каквито и да е документи от името на Възложителя.
- 9.4.** Изпълнителят осигурява за своя сметка сключването и поддържането в сила на всички застрахователни договори по отношение на отговорността на Изпълнителя за вреди, причинени от действия на персонала на Изпълнителя на имуществото, живота и здравето на Възложителя, неговия персонал и/или трети лица.
- 9.5.** Изпълнителят се задължава да обезщети и предпазва Възложителя от претенции, съдебни дела или други действия, предприети срещу Възложителя от трети лица, доколкото те произтичат от причина, изхождаща от дейността на Изпълнителя във връзка с изпълнението на договора.
- 9.6.** С подписването на договора Изпълнителят изрично потвърждава, че договорът не е предназначен да, и не дава разрешение на Изпълнителя да използва по какъвто и да било начин, която и да е от търговските марки на Възложителя, освен в случаите, в които Възложителят изрично разрешава ползването им.

## **10. Гаранционен срок**

- 10.1. Изпълнителят поема гаранция за качеството на доставката и за годността ѝ за употреба.
- 10.2. Гаранционните срокове остават в сила, независимо от изтичане на срока на действие на договора или неговото предсрочно прекратяване.
- 10.3. Изпълнителят се задължава да отстрани за своя сметка всички повреди и отклонения от изискванията за качество, които са възникнали в рамките на гаранционния срок.
- 10.4. Изпълнителят гарантира съответствието на доставката и вложените материали с изискванията на Възложителя и приложимите български и международни стандарти, независимо от факта дали доставките произхождат от него или от негови доставчици.
- 10.5. При възникнали дефекти, поради повреда/несъответствие на качеството, гаранционният срок ще се удължи съответно с цялото време на престой.



## **11. Гаранция за изпълнение**

- 11.1. При подписване на договора Изпълнителят предоставя гаранция за изпълнение на договора, чийто размер се определя като % от стойността на договора без включен ДДС и се представя във формата на парична сума или банкова гаранция в лева. Гаранцията обезпечава изпълнението на договора, отстраняването на възникнали дефекти и задължението за плащане на каквито и да е парични суми от страна на Изпълнителя към Възложителя (като например плащане на неустойки, обезщетения или други подобни).
- 11.2. Срокът на валидност на предоставената гаранция за изпълнение се конкретизира в договора и включва срока на действие на договора и гаранционния срок на доставката/ите. Когато гаранцията за изпълнение на договора се представя във вид на парична сума, то тя се внася по сметка на Възложителя и се освобождава не по-късно от 30 дни след изтичане на срока на действие на договора включително гаранционния срок на доставката/ите. Всички банкови разходи, свързани с обслужването на гаранцията, включително при нейното възстановяване, са за сметка на Изпълнителя. Възложителят не дължи на Изпълнителя лихви или други обезщетителни плащания върху сумата по гаранцията
- 11.4. Когато гаранцията за изпълнение на договора е под формата на банкова гаранция, то тя е безусловна и неотменяема. Банковата гаранция е във форма, със съдържание и при условия, предварително одобрени от Възложителя. Всички разходи по поддържането на банковата гаранция са за сметка на Изпълнителя.
- 11.5. Възложителят задържа гаранцията за изпълнение на договора и в случаите когато в процеса на неговото изпълнение възникне спор между страните - до приключването му с влязло в сила решение на компетентния орган или чрез споразумение между страните.
- 11.6. В случай на удължаване на срока на договора на основанията предвидени в ЗОП, както и при промяна на друго основание на срока на договора или на гаранционния срок:
- 11.6.1. При банкова гаранция Изпълнителят е длъжен да предостави анекс към банковата гаранция или нова банкова гаранция в размера на неусвоената сума, покриваща и удължения срок;
- При депозитна гаранция- Възложителят има право да я задържи и за удължения

## **12. Неустойки**

- 12.1. Изпълнителят се задължава да изпълнява задълженията си по договора точно в качествено, количествено и времево отношение, като се съобразява с изискванията на Възложителя по отношение на доставката. Всяко отклонение от точното изпълнение на доставката се счита за неизпълнение от страна на Изпълнителя.
- 12.2. Предвидените неустойки имат обезщетителна функция за Възложителя и последният няма задължение да доказва претърпени вреди.
- 12.3. В случай че за Възложителя възникне право да получи неустойка или поради действие или бездействие на Изпълнителя, негов персонал и/или подизпълнители бъде наложена на Възложителя имуществена санкция от държавен и/или административен орган, или Възложителят бъде осъден да плати на трето лице обезщетение за претърпени вреди в следствие действие и/или бездействие на посочените по-горе в тази точка лица Възложителят има право да прихване размера на неустойката или имуществената санкция или обезщетението от плащането, дължимо на Изпълнителя. В тази връзка Възложителят изпраща на Изпълнителя съответно уведомление.
- 12.4. Всички разходи, възникващи през срока на действие на договора, които произтичат от нарушения на договорните и/или законовите задължения на Изпълнителя, са за сметка на Изпълнителя. В случай че Възложителят е заплатил подобни разходи, Изпълнителят се задължава да възстанови пълната им стойност на Възложителя. Възложителят има право да прихване стойността на разходите от дължимото на Изпълнителя плащане.
- 12.5. Неустойката се прихваща от задължението към доставчика след изпращане на уведомително писмо (документ за неустойка с обезщетителен характер) от ВЪЗЛОЖИТЕЛЯ.
- 12.6. Плащането на неустойка не лишава изправната страна от правото ѝ да търси обезщетение, когато претърпените вреди и пропуснатите ползи надвишават размера на неустойката.

## **13. Прекратяване на договора**

- 13.1. Договорът може да бъде предсрочно прекратен, освен в изрично посочените в него случаи, и по следните начини:
- 13.1.1. По взаимно писмено съгласие на страните, при намаляване на договорените количества или отпадане на дейности от предмета на поръчката или друг от предвидените от ЗОП случаи.
- 13.1.2. Едностранно от Възложителя с 30 (тридесет) дневно писмено предизвестие при намаляване на

договорените количества или отпадане на дейности от предмета на поръчката или друг от предвидените от ЗОП случаи.

13.1.3. Едностранно от Възложителя в случай на неизпълнение на задължение от страна на Изпълнителя. В този случай Възложителят изпраща уведомление до Изпълнителя с искане неизпълнението да бъде отстранено в срок от 5 дни от получаването на уведомлението. Ако Изпълнителят не отстрани неизпълнението в дадения срок, Възложителят има право да прекрати договора незабавно

13.1.4. Едностранно от Възложителя без предизвестие, в случай че срещу Изпълнителя е открито производство по несъстоятелност или ликвидация, както и ако върху имуществото му е наложен запор или възбрана

13.1.5. с изтичане на срока на договора

13.1.6. при усвояване на стойността на договора

13.2. В случаите на предсрочно прекратяване на договора по вина на Изпълнителя Възложителят има право да задържи цялата сума по гаранцията за добро изпълнение.

#### **14. Конфиденциалност**

14.1. Изпълнителят се задължава да разглежда като конфиденциална информация цялата търговска, правна и техническа информация и документация, която му е станала известна и не е публично достъпна, в хода на участие в процедурата за избор на изпълнител и последващото изпълнение на договора.

14.2. Изпълнителят се задължава да получава и да пази в тайна конфиденциалната информация, както и: (i) да съхранява и пази конфиденциалната информация от неправомерно използване, публикации или разкриване; (ii) да не използва конфиденциалната информация за други цели, освен за изпълнение на задълженията си по договора; (iii) да не използва каквато и да е конфиденциална информация, за осъществяване на нелоялна конкуренция; (iv) да ограничи достъпа до конфиденциалната информация на тези лица, които нямат нужда от такъв достъп с оглед изпълнението на договора; (v) да информира всяко от лицата, на които предоставя достъп до конфиденциална информация, че им е забранено да използват, публикуват или по друг начин да разкриват конфиденциалната информация..

14.3. Задълженията за опазване на конфиденциалната информация не се прилага спрямо информация, която е поискана от компетентен орган според действащото законодателство или е станала публично достояние не по вина на някоя от страните. Задълженията във връзка с опазване на конфиденциалната информация не са ограничени във времето. Нарушението на всяко едно от задълженията във връзка с опазване на конфиденциалната информация по време на срока на действие на договора или във всеки по-късен момент, дава право на Възложителя да получи от Изпълнителя неустойка в размер на 10% от стойността на договора за всеки отделен случай на нарушение.

#### **15. Форсмажорни обстоятелства**

15.1. Форсмажорни обстоятелства (непреодолима сила) е непредвидено или непредотвратимо събитие от извънреден характер, независимо от волята на страните включващо, но не ограничаващо се до: природни бедствия, генерални стачки, локаут, безредици, война, революция или разпоредби на органи на държавната власт и управление. Страната, която не може да изпълни свое задължение поради непреодолима сила, се задължава в 3 (три) дневен срок от възникване на форсмажорното обстоятелство да уведоми писмено насрещната страна, като посочи в какво се състои непреодолимата сила и как тя ще се отрази на изпълнението на договора. При неизпълнение на задължението за уведомяване, страната, която се позовава на непреодолима сила, не се освобождава от отговорност, респективно дължи предвидените неустойки и обезщетения в случаи на неизпълнение. В 14 (четиринадесет) дневен срок от началото на непреодолимата сила, същата следва да бъде потвърдена със сертификат от съответния компетентен орган. Докато трае непреодолимата сила страните не отговарят за неизпълнение, причинено от непреодолимата сила. Изпълнението на задълженията на страните спира за времето на непреодолимата сила, респективно страните не изпадат в забава и не дължат неустойки за забава. Страните, в случай на необходимост, съвместно определят нови срокове за изпълнение на договорните задължения. Ако непреодолимата сила трае повече от 15 (петнадесет) дни, всяка от страните има право да прекрати договора с 10 (десет) дневно писмено предизвестие.

**16. Общи разпоредби**

- 16.1. Страните се съгласяват, че в отношенията помежду им се изключва прилагането на общи условия на Изпълнителя.
- 16.2. В случай, че при изпълнение на доставката се образуват отпадъци с опасен и/или неопасен произход, ИЗПЪЛНИТЕЛЯТ е задължен да ги приеме, ако разполага с необходимите разрешителни и лицензии от компетентни органи (МОСМ, МЗ, МИЕ) или да предаде за приемане на лице, притежаващо съответните разрешителни, съгласно ЗУО и ЗООС.
- 16.3. В случай че, предмета на договора включва лицензии, то страните се съгласяват, че лицензиите са стандартен софтуер, които се записва на технически носител и са предназначени за общо ползване и не са взели предвид специфичните дейности на ползвателя/Възложителя. Възложителят има право да използва софтуера, в който е включен само копие от съответния софтуер и правата за копиране, възпроизвеждане, разпространение, промяна, публично представяне и други форми на комерсиална употреба не са налични/достъпни.
- 16.4. Страните се съгласяват, че договорът ще бъде изпълнен в съответствие с изискванията на чл. 31 от Регламент (ЕО) № 1907/2006 на Европейския парламент и на Съвета от 18 декември 2006 година, относно регистрацията, оценката, разрешаването и ограничаването на химикали (REACH)
- 16.5. В случай, че предмет на договора са стоки, подлежащи на рециклиране, страните се съгласяват, че те ще се приемат ИЗПЪЛНИТЕЛЯ за негова сметка, след писмено уведомление от страна на ВЪЗЛОЖИТЕЛЯ.
- 16.6. Сключването, изпълнението и тълкуването на договора се извършва съгласно приложимото българско законодателство.
- 16.7. Страните се съгласяват, че всякакво приложение на Конвенцията на ООН относно договорите за международна продажба на стоки от 11 април 1980 г. се изключва.
- 16.8. Договорът обвързва и съответните наследници и правопреемници на страните.
- 16.9. Ако някоя от разпоредбите на договора бъде обявена за недействителна или неприложима от компетентен орган, останалите разпоредби на договора, както и възникналите въз основа на тези останали разпоредби права и задължения на страните, запазват действието си. Недействителната или неприложима разпоредба следва да бъдат заместени от страните по добросъвестен начин от действителна, приложима разпоредба.
- 16.10. Всички съобщения, предизвестия и нареждания, разменяни между лицата за контакт Възложителя и Изпълнителя при изпълнение на договора са валидни, когато са изпратени по пощата с обратна разписка, предадени чрез куриер срещу подпис от приемащата страна или изпратени по факс с налично факс потвърждение за изпращане, освен ако в договора не са предвидени и други начини.
- 16.11. Всеки спор, противоречие или претенция, произтичащи от, или свързани с изпълнението, тълкуването, прилагането или прекратяването на договора, се уреждат по приятелски начин от страните. Ако страните не успеят да уредят отношенията си по приятелски начин, спорът се разрешава от компетентният съд по седалището на Възложителя.
- 16.12. Договорът се сключва въз основа и се тълкува в съответствие с българското законодателство.
- 16.13. В случай, че договорът е двуезичен, то при разминаване в текстовете като правно обвързващ се счита текста на български език

**С подписването на настоящите търговски условия Кандидатът гарантира за тяхното приемане, спазване и точно изпълнение.**

Фирмен печат:..... Подпис с правна сила: .....

**Технически изисквания**

(Издание Юни.2014 г.)

към система за предварителен подбор на изпълнители  
№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

**Техническа спецификация:****I. Technical requirements, regarding the Head End System****1. Description****1.1 Functional description:**

All data, collected until 00:00 a.m., must be received by the grid operator not later than 12:00 a.m. on the next calendar day.

Reading of the load profile must be possible, by setting periods – multiple times within a day. Any and all data, collected by 00:00 a.m. are stored, and in all future reading requests, only the values, which have not been read previously, are to be read.

The invoicing data readings and the logbooks are not subject to the requirement for daily reading and therefore the grid operator can plan an individual reading as well as various fixed reading requests.

For this purpose a time schedule is to be established and configured, for individual reading of the PUSH /data transmission/ and PULL / data reception/ modes.

In the PUSH mode, it should be possible to configure the time schedule for reading in the electricity meter.

In the PULL mode, the reading schedule is controlled by the Head End System. The reading schedule must specify the precise time of reading of each of the electricity meters.

**1.2 Initiator:**

For reading the electricity meters; according to the reading schedule

For configuration of the reading schedule:

The grid operator needs the data and for that purpose he determines the time schedule (if necessary the schedule is transferred to subordinate levels in the hierarchy).

**1.3 Result:**

For the reading of the electricity meters:

The grid operator has received all requested data.

For configuration:

A reading schedule is preset in the necessary system components.

**1.4 Service level:**

When starting the reading of the values, at 00:05 a.m., 99 % of all electricity meters must be read within 12 hours. A 4-hour reserve remains, and this is used for interference in case of missing readings.

**2. Ad hoc- reading**

2.1. Name: Spontaneous reading of the electricity meters or Immediate reading of electricity meters

2.2. Function description: The purpose is to obtain up-to-date electricity metering data upon the request by

**I. Технически изисквания към Система за дистанционно отчитане****1. Описание****1.1 Функционално описание:**

Всички данни, които са събрани до 00:00 ч., трябва да са при мрежовия оператор най-късно до 12:00 ч. на следващия календарен ден.

Товаровият профил трябва да може да се отчита посредством задаване на периоди - многократно в рамките на деня. Всички събирани до 00:00 ч. се съхраняват, при следващи заявки за отчитане това трябва да се отчетат само липсващи стойности.

Отчитанията на данните за фактуриране и дневниците не подлежат на изискването за ежедневно отчитане и затова мрежовият оператор може да планира индивидуално отчитане а така също и различни фиксирани заявки за отчитане.

За целта е необходимо да се определи респективно да се конфигурира времеви график за отчитане поотделно за режимите PUSH /предаване на данни/ и PULL /приемане на данни/.

При режим PUSH времевият график за отчитане трябва да може да се конфигурира в електромера.

При режим PULL графикът за отчитане се управлява от централната система. В графика за отчитане трябва да е определено кои електромери кога трябва да се отчетат.

**1.2 Инициатор:**

За отчитането на електромери: съгласно графика за отчитане

За конфигуриране на графика за отчитане:

Мрежовият оператор се нуждае от данните и за целта определя времеви график (при необходимост графикът се пренасочва към подчинени йерархични нива).

**1.3 Резултат:**

За отчитането на електромери:

Мрежовият оператор е получил всички изисквани данни

За конфигуриране:

В необходимите системни компоненти е заложен график за отчитане.

**1.4 Ниво на поддръжка:**

При стартиране на отчитането на стойностите към 00:05 ч. в рамките на около 12 часа трябва да са отчетени 99 % от всички електромери. Остава резерва от 4 часа, които се използват за намеса в случай на липсващи отчитания.

**2. Ad hoc- отчитане**

2.1. Наименование: Спонтанно отчитане на електромери или Незабавно отчитане на електромери

2.2. Описание на функцията: Целта е получаване на актуални електромерни данни при запитване от страна на оторизирани участници (спазване на

authorized participants (following the rules and provisions for data protection). This request is sent by the grid operator to the respective electricity meter in the form of a reading command. The scope of data may be defined (e.g. logbooks, invoicing data, load profile data)

In case the ad hoc-reading has been completed unsuccessfully several times, an on-site reading should be available.

The following applies to the combined methods:

Precondition: A two-way communication must be present with the combined meter or the electricity meter should store the latest metered value, provided by the combined meter.

The timeliness of the reported value depends on the interval, during which the combined meter transmits.

Throughout the transmission, the data is to be protected, in accordance with the concept of security.

The electricity meter receives encrypted data from the combined meter and retransmits it to the Head End System - preferably without decryption.

#### 2.3. Initiator:

- Change of client (differentiation when invoicing)
- If the planned periodic reading (multiple) has been unsuccessful
- Client complaints (inspection of authenticity)
- Maintaining the security of operation of the network

- During installation

#### 2.4. Result:

The required electricity meter data is received at the Head End System.

#### 2.5. Service level:

In 99 % of the cases  $\leq 5$  min.

### 3. On-Site Reading

#### 3.1. Name:

On-Site Reading

#### 3.2. Function description:

In general there must be an opportunity for reading the electricity meter on-site by means of a mobile terminal through the maintenance interface P0. In order to meet the strict provisions, regarding the data protection, an individual key/password is to be entered in the mobile terminal, which enables the reading of the respective electricity meter.

The data obtained in this manner, should be transferrable to the Head End System. Each reading must be incorporated in the access protocol.

The requirements in the area of security must be met.

#### 3.3. Initiator:

- unsuccessful planning reading
- (De-)installation

#### 3.4. Result:

The data is read and can be sent to the Head End System.

правата и на разпоредбите за защита на данните).

Това запитване мрежовият оператор изпраща на съответния електромер под формата на команда за отчитане. Обхватът на данните може да се дефинира (напр. дневници, данни за фактуриране, данни за товаров профил).

В случай, че ad hoc-отчитането многократно е завършило без успех, следва да има възможност за отчитане на място.

За комбинираните измервателни уреди е в сила следното:

Предпоставка: Да е налице двупосочна комуникация с комбинирания измервателен уред или електромерът да запамятава последната измервателна стойност, предадена от комбинирания измервателен уред.

Времето на отчетената стойност зависи от интервала, през който комбинираният електромер изпраща данни.

По време на целия пренос данните трябва да са защитени съгласно концепцията за сигурност.

Електромерът получава кодираните данни от комбинирания измервателен уред и ги препраща към централната системата - за предпочитане без разкодиране.

#### 2.3. Инициатор:

- Смяна на клиент (разграничаване при фактуриране)
- Когато планираното периодично отчитане (многократно) е било неуспешно
- Рекламация от клиента (проверка на верността)
- Поддържане на сигурността на експлоатацията на мрежата

- По време на монтаж

#### 2.4. Резултат:

Необходимите електромерни данни са получени в централната системата.

#### 2.5. Ниво на поддръжка:

В 99 % от случаите  $\leq 5$  мин.

### 3. Отчитане на място

#### 3.1. Наименование:

Отчитане на място

#### 3.2. Описание на функцията:

Принципно трябва да има възможност за отчитане на електромера на място посредством мобилен терминал през интерфейса за поддръжка P0. За да бъдат спазени строгите разпоредби относно защитата на данните, в мобилния терминал трябва да се въведе индивидуален ключ/ парола, който дава право да се отчете съответния електромер. Така получените данни трябва да могат да се предадат на централната система. Всяко отчитане трябва да се отбелязва в протокола за достъп.

Трябва да се спазват изискванията в областта на сигурността.

#### 3.3. Инициатор:

- неуспешно планирано отчитане
- (Де-)монтаж

#### 3.4. Резултат:

Данните са отчетени и могат да се изпратят до



3.5. Service level:  
insignificant

#### 4. Deactivation

For the deactivation, no group, or mass command (broadcast) must be used.

4.1 In case of client change

4.1.1 Name:

Power supply interruption, due to the fact, that the client leaves the real estate, which becomes uninhabited

4.1.2 Function description

The purpose is, the power supply of a certain site or facility, to be disconnected remotely (from the Head End System of the grid operator), because the property remains uninhabited. The deactivation takes place by opening the switch /Breaker/, situated in the electricity meter.

The Head End System of the grid operator sends to the respective electricity meter a command for deactivation. The intelligent electricity meter fulfills the command and sends a status back to the Head End System. This status must be clearly shown on the display of the electricity meter (e.g. OFF).

4.1.3 Initiator:

Erasing of an existing client

4.1.4 Result:

The power supply has been disconnected and the status "disconnected" is displayed on the electricity meter and in the Head End System.

4.1.5 Service level:

In 99 % of the cases  $\leq$  5 min

4.2 Payment-related disconnection

4.2.1 Name:

Disconnection within the payment collection process

4.2.2 Function description:

The grid operator may disconnect the facilities of clients with overdue payments.

The Head End System sends to the respective electricity meter a deactivation command. The electricity meter executes the respective command (the internal switch interrupts the power supply to the client facility) and sends back to the Head End System the relevant information, regarding the disconnection status. This status must be clearly shown on the display of the electricity meter.

After disconnection, there is no option for immediate reconnection on-site by the client.

4.2.3 Initiator:

The client fails to make a payment.

4.2.4 Result:

The switch in the electricity meter has disconnected the facility, visualized that on the display and has sent a message to the Head End System. The electricity meter IS NOT ready for immediate on-site reconnection.

централната системата.

3.5. Ниво на поддръжка:  
Несъществено

#### 4. Изключване

За изключванията не трябва да се използва групова респ. масова команда (Broadcast).

4.1. При смяна на клиент

4.1.1. Наименование:

Прекъсване поради това, че клиентът напуска имота, без да се нанесе нов клиент

4.1.2. Описание на функцията:

Целта е, електрозахранването на даден обект да бъде изключено дистанционно (от централната системата на мрежовия оператор), тъй като в обекта не се нанася друг клиент. Изключването се извършва чрез отваряне на прекъсвача /Breaker/, намиращ се в електромера.

Централната система на мрежовия оператор изпраща до желанния електромер команда за изключване. Интелигентният електромер изпълнява подадената от централната системата команда и изпраща обратно към централната системата статус. Този статус трябва също така да бъде ясно изобразен на дисплея на електромера (напр. OFF).

4.1.3 Инициатор:

Отписване на съществуващ клиент

4.1.4 Резултат:

Електрозахранването е прекъснато и статусът "прекъснат" е визуализиран на електромера и в централната системата.

4.1.5 Ниво на поддръжка:

В 99 % от случаите  $\leq$  5 мин

4.2 Прекъсване по причини, свързани с плащания

4.2.1 Наименование:

Прекъсване в рамките на процеса по събиране на плащания

4.2.2 Описание на функцията:

Мрежовият оператор може да изключи съоръженията на клиенти с просрочени задължения.

Централната системата изпраща до съответния електромер команда за изключване. Електромерът изпълнява подадената от централната системата команда (вътрешният прекъсвач изключва електрозахранването на клиентското съоръжение) и изпраща обратно до централната системата информация за статуса на изключването. Този статус трябва да бъде ясно изобразен на дисплея на електромера.

След прекъсване няма възможност за незабавно повторно включване на място от страна на клиента.

4.2.3 Инициатор:

Клиентът не извършва заплащане.

4.2.4 Резултат:

Прекъсвачът на електромера е изключил съоръжението, визуализиран е това на дисплея и е изпратил съобщение до централната системата. Електромерът НЕ е готов за незабавно повторно включване на място.



**4.2.5 Service level:**

In 99 % of the cases  $\leq$  5 min.

**4.3 On-site through the servicing interface****4.3.1. Name:**

Deactivation on-site through the servicing interface (P0)

**4.3.2 Function description:**

The electricity meter is switched off on-site by means of a mobile terminal through the servicing interface. In order to meet the strict provisions, regarding data protection, an individual key/password must be entered in the mobile terminal, enabling the disconnection of the respective electricity meter. Therefore, it should not be possible to deactivate several or all electricity meters by means of a single key. The key control must correspond to the security concept.

**4.3.3 Initiator:**

Working on the maintenance/ servicing of the client facility  
Disconnection, related to the collection of payments

**4.3.4 Result:**

The switch in the electricity meter has disconnected the facility, visualized that on the display and has sent a message about the changed status to the Head End System

**4.3.5 Service level:**

Immediately, upon sending a command by the mobile terminal

**5. Switching on****5.1 Connection-related with payment****5.1.1 Name:**

Permission for on-site switching on

**5.1.2 Function description:**

The electricity meter receives from the Head End System or through the maintenance interface, a command, activating (again) the on-site switching on. The switching on takes place in the following manner:

5.1.2.1 From the Head End System or through the maintenance interface an activation command is sent to the electricity meter. The electricity meter visualizes that status on the display. This status is reported to the Head End System.

5.1.2.2 From this moment on, the control mechanism of the electricity meter can be activated directly. The electricity meter must visualize this status change. This status is reported to the Head End System.

**5.1.3 Initiator:**

5.1.3.1 The client enters into possession in a facility with interrupted power supply and wants it to be reactivated.

5.1.3.2 The outstanding debts have been paid.

**5.1.4 Result:**

A) The electricity meter is activated /authorized/ for (another) switching on and this is visualized on the display. The status of the electricity can be shown in the Head End System.

B) The power supply has been restored, the visualization of the display and indication of the status at the Head End

**4.2.5 Ниво на поддръжка:**

В 99 % от случаите  $\leq$  5 мин.

**4.3 На място през интерфейса за обслужване****4.3.1. Наименование:**

Изключване на място през интерфейса за обслужване (P0)

**4.3.2 Описание на функцията:**

Електромерът се изключва на място посредством мобилен терминал чрез интерфейса за обслужване. За да бъдат спазени строгите разпоредби относно защитата на данните, в мобилния терминал трябва да се въведе индивидуален ключ/ парола, който дава право да се изключи съответния електромер. Следователно не трябва да е възможно изключване на няколко или на всички електромери от електромерното стопанство посредством един ключ. Управлението на ключовете трябва да съответства на концепцията за сигурност.

**4.3.3 Инициатор:**

Работи по поддръжка/ обслужване в клиентското съоръжение

Прекъсване свързано със събиране на плащания

**4.3.4 Резултат:**

Прекъсвачът на електромера е изключил съоръжението, визуализирал е това на дисплея и промененият статус е отразен в централната системата.

**4.3.5 Ниво на поддръжка:**

Непосредствено при подаване на командата от мобилния терминал

**5. Включване****5.1 Включване по причини, свързани с плащания****5.1.1 Наименование:**

Разрешение за включване на място

**5.1.2 Описание на функцията:**

Електромерът получава от централната системата или чрез интерфейса за поддръжка, команда, активираща (повторно) включване на място. Включването протича по следния начин:

5.1.2.1 От централната системата или чрез интерфейса за поддръжка се изпраща команда за активиране до електромера. Електромерът визуализира това състояние на дисплея. Това състояние се съобщава в централната системата.

5.1.2.2 От този момент може да се включи директно контролният механизъм на електромера.

Електромерът трябва да визуализира тази промяна в статус. Това състояние се съобщава в централната системата.

**5.1.3 Инициатор:**

5.1.3.1 Клиентът се нанася в обект с прекъснато съоръжение и желае то да бъде активирано.

5.1.3.2 Отворените задължения са заплатени.

**5.1.4 Резултат:**

A) Електромерът е активиран /разрешен/ за (повторно) включване и това е визуализирано на дисплея. Статусът на електромера може да се види също и в централната системата.

B) Електрозахранването е възстановено; визуализация на дисплея и отбелязване на статуса в централната

System.

5.1.5 Service level:

In 99 % of the cases  $\leq$  5 min. for activation

## 6. Date and time synchronization

6.1 Name:

Ensuring accurate system time for all end-devices

6.2 Function description:

Checking the actual time.

Behaviour in case of deviation in the time settings.

If the respective deviation is up to 2 seconds, no actions are required.

If the deviation is between 2 and 9 seconds, the time must be synchronized, no entry is made in the event logbook.

If the deviation exceeds 9 seconds, the time must be set and an entry in the event logbook must be made, as well as in the load profile if it is configured (displaying the date and time and an entry for the status).

The chronology ("numeration") of the metering activities must be stored.

The synchronization is performed from the Head End System through a WAN-interface. It must be possible to carry that out on-site through the servicing interface. The synchronization cycle must be capable of parameterization.

6.3 Initiator:

Parameterization cycle (Schedule)

6.4 Result:

The system time of all the end-devices is the same.

6.5 Service level:

99,9 % of the end devices have proper system time.

## 7. Firmware Download

7.1 Part, not subject to metrological inspection

7.1.1 Name:

Update of the firmware of a part, NOT subject to metrological inspection

7.1.2 Function description:

As with the electricity meter, the Head End System must support updates and, respectively, upgrades of a part, NOT subject to metrological inspection (the non-metrological part). Upon issuing a command, given by the grid operator, the updated software is loaded to the electricity meter. After loading, the electricity meter checks if the software has been fully downloaded and without any errors. After that the installation starts in the electricity meter. After the software is installed, the electricity meter must perform a self-check, which ensures the flawless functioning of the new software. Failing that, the previous version of the software will be restored automatically. The electricity meter sends to the Head End System an error message, indicating the failing attempt in the event logbook.

The previous version is restored automatically, when the electricity meter fails to establish contact with the Head

системата.

5.1.5 Ниво на поддръжка:

В 99 % от случаите  $\leq$  5 мин. за активиране

## 6. Синхронизиране на дата и час

6.1 Наименование:

Осигуряване на точно системно време на всички крайни устройства

6.2 Описание на функцията:

Проверява се актуалното време.

Поведение при отклонения в часа.

Ако констатираното отклонение е до 2 секунди, не трябва да се предприемат действия.

Ако отклонението е между 2 и 9 секунди, времето трябва да се синхронизира, не се предприема вписване в дневника на събитията.

Ако отклонението е по-голямо от 9 секунди, времето трябва да се определи и да се предприеме вписване в дневника на събитията и в товарния профил ако е конфигуриран (показание с дата и час и вписване за статуса).

Трябва да се запази хронологията ("номерацията") на измервателните стойности.

Синхронизирането се извършва от централната системата през WAN-интерфейс. Трябва да е възможно да се извърши също и на място чрез интерфейс за сервизно обслужване. Цикълът на синхронизиране трябва да може да се параметрира.

6.3 Инициатор:

Параметриран цикъл (Schedule)

6.4 Резултат:

Системното време на всички крайни устройства е еднакво.

6.5 Ниво на поддръжка:

99,9 % от крайните устройства имат правилно системно време.

## 7. Firmware Download

7.1 Част, Неподлежаща на метрологична проверка

7.1.1 Наименование:

Актуализация на фърмуера на Неподлежащата на метрологична проверка част

7.1.2 Описание на функцията:

Както електромерът, така също и централната система трябва да поддържат ъпдейт респ. ъпгрейт на Неподлежащата на метрологична проверка част (неметрологичната част). По команда, дадена от мрежовия оператор, актуализираният софтуер се зарежда в електромера. След зареждане, електромерът проверява дали софтуерът е прехвърлен изцяло и без грешки. След това стартира инсталирането в електромера. След като софтуерът бъде инсталиран в електромера трябва да се извърши самопроверка, която гарантира безпроблемното функциониране на новия софтуер. Ако не е така, предходната версия на софтуера трябва да се върне автоматично. Електромерът изпраща до централната система съобщение за грешка и отбелязва в неуспешния опит в дневника на събитията.

Предидната версия се връща автоматично също и тогава, когато електромерът не успее да се свърже с

End System within 72 hours.

An entry in the event logbook must also be made in case of successfully installed software.

#### 7.1.3 Initiator:

The electricity meter manufacturer provides a new firmware for the part, NOT subject to metrological inspection. Using a Head End System the grid operator sends through the electricity metering gate, an update to the electricity meter.

#### 7.1.4 Result:

The firmware in the electricity meter has been successfully updated. The electricity meter communicates that to the Head End System and makes an entry in its logbook.

#### 7.1.5 Service level:

99 % of all affected electricity meters within 30 days.

### 8. Sending an ALARM signal

#### 8.1 Name:

sending an ALARM

#### 8.2 Function description:

The electricity meters, data concentrator, may be exposed to tampering attempts, damages and technical issues. The alarms are events, defined by the grid operator. They must be sent spontaneously by the electricity meter to the Head End System. The alarm always results in certain actions (direct or indirect).

#### 8.3 Initiator:

A decentralized system component (electricity meter, Data Concentrator) identifies an event, configured as an alarm. Then the system component generates a clear alarm message and sends it independently and directly to the Head End System.

#### 8.4 Result:

The Head End System receives a clear alarm message and displays it to the grid operator in the respective form.

#### 8.5 Service level:

99 % within 5 minutes

### 9. EVENTS /events/

#### 9.1 Name:

EVENT creation and transfer

#### 9.2 Function description:

Unlike alarms, the events must be reported in an appropriate form by the respective system components, but these are not transmitted immediately to the Head End System. The Events are used to ensure the quality and are specified by the grid operator.

The components create clear event messages (event type; moment of occurrence and duration; moment of transmission ,... ), they record them in the events memory, /in the event logbook and transfer them to the Head End System during the periodic reading of the electricity meters or upon request.

#### 9.3 Initiator:

централната система в рамките на 72 часа.

Вписване в дневника на събитията трябва да се направи също и при успешно инсталиране на софтуера.

#### 7.1.3 Инициатор:

Производителят на електромера предоставя нов фърмуер за НЕподлежащата на метрологична проверка част. Чрез централна система мрежовият оператор изпраща през електромерния портал (гейт) ъпдейт към електромера.

#### 7.1.4 Резултат:

Фърмуерът в електромера е успешно актуализиран.

Електромерът съобщава това на централната системата и прави вписване в дневника на събитията си.

#### 7.1.5 Ниво на поддръжка:

99 % от всички засегнати електромери в рамките на 30 дни.

### 8. Изпращане на АЛАРМА

#### 8.1 Наименование:

изпращане на АЛАРМА

#### 8.2 Описание на функцията:

Електромерите, Концентраторите на данни, могат да са изложени на опити за манипулация, повреди и технически проблеми. Алармите са събития, дефинирани от мрежовия оператор. Те трябва да се изпращат спонтанно от електромера към централната система. Алармата задължително води след себе си действие респ. намеса (индиректна или директна).

#### 8.3 Инициатор:

Децентрална системна компонента (електромер, концентратор на данни) открива събитие, конфигурирано като аларма. След това системната компонента генерира еднозначно съобщение за аларма и го изпраща независимо и директно до централната система.

#### 8.4 Резултат:

Централната система получава еднозначното съобщение за аларма и го показва на мрежовия оператор в съответната форма.

#### 8.5 Ниво на поддръжка:

99% в рамките на 5 минути

### 9. СЪБИТИЯ / events /

#### 9.1 Наименование:

Създаване и пренасяне на СЪБИТИЯ

#### 9.2 Описание на функцията:

За разлика от алармите, събитията трябва да бъдат протоколирани в подходяща форма от съответните системни компоненти, но не се предават незабавно към централната система. Събитията служат за гарантиране на качеството и се специфицират от мрежовия оператор.

Компонентите създават еднозначни съобщения за събитие (вид на събитието; момент на поява и продължителност; момент на предаване ,... ), записват ги в паметта, предназначена за събития, / в дневника на събитията и ги прехвърлят към централната система по време на периодичното отчитане на електромерите или при поискване.

#### 9.3 Инициатор:

A decentralized system component (electricity meter, Data Concentrator) finds an occurrence, defined as an event. Then the system component generates a clear message of an event, records it and sends it to the Head End System during the respective reading.

#### 9.4 Result:

The Head End System receives a clear message about the event and displays it to the grid operator in the respective form.

#### 9.5 Service level:

99 % within 6 hours

Any additional functionality which is not defined in the current requirements must be defined in the offer.

#### Definition for Alarms and Events

Event	Alarm-> spontaneous message	Event-> In the readout data set	logbook / Event memory record
Terminal cover opening	Option: Yes	Yes	Yes
Meter main cover opening	Yes	Yes	Yes
Voltage interruptions (all 3 phases) U <5%	-		Time and duration
Phase failure detection U <5%		Yes	Yes
access Log			Yes
Unauthorized access attempt	Option: Yes	-	Yes
Critical Error (FF)	Yes	-	Yes
External magnetic field detection > 400 mT	Option: Yes	-	Yes
Current limit exceeded (per phase)	-	Yes	Yes
Overload	-	-	Yes
Disconnected device; Detected current flow	-	-	Yes
Last accepted	-	-	Yes

Децентрализирана системна компонента (електромер, концентратор на данни) открива случка, дефинирана като събитие. След това системната компонента генерира еднозначно съобщение за събитие, записва го и го изпраща към централната система по време на съответното отчитане.

#### 9.4 Резултат:

Централната система получава еднозначното съобщение за събитие го показва на мрежовия оператор в съответната форма.

#### 9.5 Ниво на поддръжка:

99 % в рамките на 6 часа

Всяка допълнителна функционалност, която не е дефинирана в настоящите изисквания следва да бъде описана в офертата

#### Определяне на Аларми и Събития Definition for Alarms and Events

Събитие	Аларма-> спонтанно съобщение	Събитие-> по време на отчитане	logbook / запис в памятта на събитията
Отваряне на клемна капачка	Опция: Да	Да	Да
Отваряне на основната капачка на електромера	Да	Да	Да
Отпадане на напрежение (всички 3 фази) U <5%	-		Време и продължителност
Отпадане на фазно напрежение U <5%		Да	Да
Осъществен достъп			Да
Опит за неоторизиран достъп	Опция: Да	-	Да
Критична грешка (FF)	Да	-	Да
Разпознаването на външно магнитно поле > 400 mT	Опция: Да	-	Да
Превишен лимит по ток (пофазно)	-	Да	Да
Претоварване	-	-	Да
Прекъснато устройство;	-	-	Да
Наличие на ток			
Последна	-	-	Да

command			
---------	--	--	--

приета команда			
-------------------	--	--	--

## II. System Requirements

### 1. Communication

#### 1.1 Data transfer requirements

The system must support the following simultaneous processes:

1. Sending consumption data
2. Automation of the client processes (e.g. disconnection and reconnection of the power-supply)
3. Automatic logging and identification of the end-devices
4. Online commuting commands
5. Remote configuration of system components
6. Spontaneous alarm transfer
7. Transfer of events and operational data upon request
8. Control of remote Firmwaredownload (from Data Concentrator), by means of the network of a mobile operator, end-devices,...)
9. For the various applications in system, the following priorities must be set:
  - 9.1 The spontaneous commands must be transmitted in such a manner, that their successful transmission and receiving feedback within 5 minutes are ensured.
  - 9.2 The spontaneous information must be transmitted to the Head End System within 5 minutes.
  - 9.3 The configurations of the system components must take place successfully within 5 minutes.
  - 9.4 The performance of mass readings within the legally established timeframe must be guaranteed.
  - 9.5 Not later than 24 hours after their installation (usually 15 minutes later) the end devices must be automatically registered in the Head End System.
  - 9.6 In case of remote Firmwaredownload it must be ensured that the new firmware will be rolled out to all system components within 30 days. It must be ensured that all of the above applications may work in parallel and be processed according to the current priorities.

Detailed requirements regarding:

#### 1.1.1. Remote reading of consumption data

The entire system must be dimensioned in such a manner

## II. Изисквания към системата

### 1. Комуникация

#### 1.1 Изисквания към преноса на данни

Системата трябва да се поддържа паралелно следните процеси:

1. Изпращане на данни за потреблението
2. Автоматизиране на клиентски процеси (напр. прекъсване и възстановяване на захранването)
3. Автоматично регистриране и идентифициране на крайни устройства
4. Online-команди за комутиране
5. Дистанционно конфигуриране на системни компоненти
6. Спонтанен пренос на аларми
7. Пренос на събития и оперативни данни при поискване
8. Управление на отдалечен Firmwaredownload (от концентратор на данни), посредством мрежата на мобилния оператор, крайни устройства,...)
9. За различните приложения в системата трябва да се зададат следните приоритети:
  - 9.1 Спонтанните команди трябва да се предават така, че да се гарантира успешно предаване на обратна информация в рамките на 5 минути.
  - 9.2 Спонтанната информация трябва да е предадена към централната система в рамките на 5 минути.
  - 9.3 Конфигурациите на системните компоненти трябва да се извършат успешно в рамките на 5 минути.
  - 9.4 Трябва да е гарантирано извършването на масови отчитания в рамките на законово определените срокове.
  - 9.5 Най-късно 24 часа след инсталирането им (обикновено след 15 минути) крайните устройства трябва автоматично да се регистрират в централната система.
  - 9.6 При отдалечен Firmwaredownload трябва да се гарантира, че новия фърмуер в рамките на 30 дни ще бъде зареден във всички системни компоненти. Трябва да се гарантира, че всички от гореспоменатите приложения ще работят едновременно и ще бъдат обработвани по приоритет.

Детайлни изисквания към:

#### 1.1.1. Дистанционно отчитане на данни за потреблението

Цялата система следва да се оразмери така, че да бъдат



that is met in all modes of operation. More specifically, the following is required:

1.1.1.1 Daily reading of all daily consumption values (active energy in both directions) not later than 12:00 a.m. (the reading starts at 0:05 a.m.)

1.1.1.2 Additional daily reading every 15 minutes of load profiles for electricity meter readings (active energy in both directions) of electricity meters,

1.1.1.2.1 which are required for billing purposes,

1.1.1.2.2 which are required for the operation of the network;

1.1.1.2.3 which are required for statistical purposes.

100 % transmission of the load profiles of all electricity meters is to be ensured. Within the aforesaid timeframe, 99 % of all the necessary data must be transmitted.

1.1.2. Client processes: Disconnection, reconnection and cash collection

The Client processes for disconnection and reconnection of the power-supply of client facilities (activation of the circuit breakers in the electricity meters), must take place successfully within 5 minutes and be confirmed in the Head End System (at least 99 % of all commands).

1.1.3. Registration and identification of end-devices

First of all, in the installation of electricity meters, but also in the replacement for metrological inspection, covering a vast territory, it must be possible to employ automatic identification and registration in the system of at least 1 000 end-devices per day. The end devices have to register at the Head End System within 15 minutes. It must be guaranteed that the maximum time for registration shall be 24 hours (for at least 99% of the end devices).

When transferring low-voltage lines (e.g. to another transformer station/ Data Concentrator) all the affected electricity meters must be automatically disconnected from the already inaccessible Data Concentrator within 24 hours and register with a new Data Concentrator (at least 99% of all affected electricity meters).

1.1.4. Remote configuration of system components

This remote configuration must be completed successfully within 5 minutes and confirmed in the Head End System. The system must be so dimensioned that 3% of all end-devices can be configured every month (at least 99% within the specified timeframe).

1.1.5. Transfer of alarms, events and messages

The alarms must be transmitted to the Head End System within 5 minutes (requirement: minimum 5% of all the end-devices per month).

The events and messages must be capable of spontaneous reading (individual reading). The operating modes must also be subject to remote reading. This transmission must take place successfully within 5 minutes (minimum 10% of

изпълнени при всички режими на работа. Поспециално се изисква:

1.1.1.1 Ежедневно отчитане на всички дневни стойности на потреблението (активна енергия в двете посоки) най-късно до 12:00 ч. (начало на отчитането в 0:05 ч.)

1.1.1.2 Допълнително ежедневно отчитане на всеки 15 минути на товари профили за електромерни показания (активна енергия в двете посоки) на електромери,

1.1.1.2.1 които са необходими за фактурирането,

1.1.1.2.2 които са необходими за експлоатацията на мрежата,

1.1.1.3 които са необходими за статистически цели.

Трябва да се гарантира пренасяне на 100 % от товарите профили на всички електромери. В рамките на горепосочения времеви интервал следва да се пренесат 99 % от необходимите данни.

1.1.2. Клиентски процеси: Прекъсване, възстановяване и инкасо

Клиентските процеси за прекъсване и възстановяване на клиентски съоръжения (задействане на прекъсвачите в електромерите), трябва да се извършат успешно в рамките на 5 минути и да се потвърдят в централната система (най-малко 99 % от всички команди).

1.1.3. Регистриране и идентифициране на крайни устройства

Преди всичко при монтаж на електромери, но също така и при подмяна за метрологична проверка, обхващаща голяма територия, трябва да е възможно автоматичното идентифициране и регистриране в системата на минимум 1 000 крайни устройства дневно. Крайните устройства по принцип трябва да се регистрират в централната система в рамките на 15 минути. Трябва да се гарантира, че максималното време за регистрация е 24 часа (за най-малко 99% от крайните устройства).

При прехвърляне на изводи НН (напр. към друг трафопост/концентратор на данни) всички засегнати електромери трябва в рамките на 24 часа автоматично да се изключат от вече недостъпния концентратор на данни и да се регистрират в новия концентратор на данни (най-малко 99% от всички засегнати електромери).

1.1.4. Дистанционно конфигуриране на системни компоненти

Дистанционното конфигуриране трябва да е успешно извършено в рамките на 5 минути и да бъде потвърдено в централната система. Системата трябва да е така оразмерена, че месечно да могат да бъдат преконфигурирани 3% от всички крайни устройства (най-малко 99% в рамките на зададеното време).

1.1.5. Пренос на аларми, събития и съобщения

Алармите трябва да бъдат пренесени до централната система в рамките на максимум 5 минути (изискване: минимум 5% от всички крайни устройства месечно).

Събитията и съобщенията трябва да могат да бъдат спонтанно отчетени (индивидуално отчитане).

Режимите на работа също трябва да могат да бъдат



all end-devices per month, 99 % within the specified time).

In case of mass readings, a maximum period of reading of 24 hours must be observed (at least 99% of all end-devices must be read within the specified time). E.g. the following data must be read from time to time, in the form of mass reading:

- 1.1.5.1. Power-supply interruptions
- 1.1.5.2. Error log
- 1.1.5.3. Access protocol
- 1.1.5.4. Logbooks for all end-devices

In order to maintain the operating control, as well as for the purposes of planning the development of the grid, for 99,9% of all infrastructure elements the following operational data must be submitted and recorded with the Head End System by 7:00 a.m. every day:

- ✓ In case of wired connection (Ethernet) of the data concentrator: the communication status of the switches/ Data Concentrator in the transformer stations in 15 minute intervals.

#### 1.1.6. Remote Firmwaredownload

The proposed system must enable the remote change of the firmware of all the system components. This Remote Firmwaredownload must be completed successfully within 30 days, which means that in the Head End System feedback, regarding the successful update of the firmware must have been received (requirement: minimum 99 % of all affected system components).

#### 1.1.7. Additional system requirements

1.1.7.1 At least once a day the system must check the system time. In case of deviations > 9 seconds, the system must set the time. Any and all processes of time setting must be registered in the logbook and transmitted to the Head End System.

1.1.7.2 The PLC-communication, must be protected, against the neighboring systems, so that in the operation of the neighboring systems it would be guaranteed that the above data will be transmitted to the requested availability.

1.1.7.3 For the PLC communication the possibility for changing the carrying frequency for communication or another fixed frequency must be declared, conforming to the available frequency for the modulation of the existing system and sufficiently different from the available system so that the communication sessions of the separate systems do not affect each other, so that the operation of two systems in a single grid is ensured.

1.1.7.4 The bandwidths of the system components must be dimensioned so that the additional requirements are met, in accordance with the security concept:

1.1.7.4.1 Encryption and authorization

1.1.7.4.2 Necessary changes to the keys (e.g. Session-Keys)

отчетени дистанционно. Този пренос трябва да бъде успешно извършен в рамките на 5 минути (минимум 10% от всички крайни устройства месечно, 99 % в рамките на зададеното време).

При масови отчитания трябва да се спазва максимално време за отчитане от 24 часа (най-малко 99% от всички крайни устройства трябва да бъдат отчетени в рамките на зададеното време). Напр. следните данни трябва да бъдат отчетени периодично под формата на масово отчитане:

1.1.5.1 Прекъсвания на напрежението

1.1.5.2 Регистър на грешките

1.1.5.3 Протокол за достъп

1.1.5.4 Дневници за всички крайни устройства

С цел поддържане на оперативното управление, както и на планирането на развитието на мрежата, за 99,9% от всички инфраструктурни елементи трябва до 7:00 всеки ден да се предават и записват в централната система следните оперативни данни:

- ✓ При свързаност посредством кабел (Ethernet) на Концентратор на данни: комуникационният статус на свичовете/ рутерите в трафопостовите през интервал от 15 минути.

#### 1.1.6. Отдалечен Firmwaredownload

Предложената система трябва да предоставя възможност за дистанционно променяне на фърмуера на всички системни компоненти. Този отдалечен Firmwaredownload трябва да приключи успешно в рамките на 30 дни, това означава, че в централната система трябва да е получена обратна информация за успешната актуализация на фърмуера (изискване: минимум 99 % от всички засегнати системни компоненти).

1.1.7. Допълнителни изисквания към системата

1.1.7.1 Системата трябва поне веднъж на ден да проверява системното време. Ако има отклонения > 9 секунди, системата трябва да настрои времето. Всички процеси за настройване на времето трябва да се впишат в дневника и да се предадат към централната система.

1.1.7.2 PLC-комуникацията трябва да е защитена срещу съседните й системи, така че при експлоатация на съседните системи да бъде гарантирано, че горепосочените данни ще бъдат пренесени с изискваната разполагаемост.

1.1.7.3 При PLC комуникация следва да се декларира възможността за промяна на носещата честота за комуникация или друга фиксирана честота съобразена с наличната честота за модулация на съществуваща система и отстояща от честота на наличната система така че комуникационните сесии на отделните системи да не влияят една на друга, за да се гарантира работа на две системи в една мрежа.

1.1.7.4 Широчините на честотните ленти на системните компоненти трябва да са така оразмерени, че да гарантират изпълнението на допълнително необходимите изисквания съгл. концепцията за сигурност:

1.1.7.4.1 Кодиране и оторизация

1.1.7.4.2 Необходими промени на ключовете (напр.

according to the level of the equipment.

1.1.7.4.3 Changes in the symmetrical keys of the interfaces at the electricity meter (in accordance with the level of equipment, always in case of change of residence)

1.1.8. Quantities

When hierarchic systems are concerned - Head End System - Data Concentrator- end-devices (electricity meters), the dimensioning of the entire system must take place, based on the following quantities/ numbers:

Depending on the size of the grid operator:

- i. At least 10 000 data concentrators to the Head End System.
- ii. At least 1 000 end-devices per data concentrator

1.1.9. Requirements, regarding the monitoring of the availability and time for execution the processes

The execution time (the time between the assignment of the order by the legacy systems and the transmission of a positive feedback to the legacy system of each separate command must be measured and recorded in the Head End System. The time for the execution of the mass commands (e.g. daily readings) must also be metered and recorded. The results from that monitoring must be presented on the interface for presentation of information (Webservice).

1.1.10. Special requirements when using hierarchic systems

#### Communication link between the Head End System and the data concentrator

The requested reaction and availability times throughout the system must be strictly observed also when using systems with Data Concentrator. The communication links of the Data Concentrator must be dimensioned so that all the reaction times are observed and the required availability is achieved.

In order to be able to discover the reason for errors in case of failure to observe the required values in the entire system, the availability of the separate connections for data transfer between the electricity metering portals and the Head End System must be metered and recorded, by means of functions for grid control and it must be made available through the information provision interface (Webservice).

When using public grids (e.g. ADSL, GPRS) the offer of the Head End System must specify the level of services, provided by the public providers, which is necessary for achieving the total availability.

When using landline communication connections (e.g. cables, optical cables), owned by the grid operator, the system components, specified by the grid operator must be allowed and – if necessary – requirements are to be defined, to be applicable to the provision of the total availability.

Session-Keys) според техническото ниво.

1.1.7.4.3 Промяна на симетричните ключове на интерфейсите при електромера (в съответствие с нивото на техниката, винаги при смяна на жилище)

1.1.8. Количества

Когато се касае за йерархични системи - централна система - Концентратор на данни- крайни устройства (електромери), оразмеряването на цялата система трябва да се извърши въз основа на следните количества/ бройки:

В зависимост от това, колко голям е мрежовият оператор:

- i. Най-малко 10 000 електромерни портали към централната система.
- ii. Най-малко 1 000 крайни устройства към един Концентратор на данни

1.1.9. Изисквания към мониторинга на разполагаемостта и на времената за изпълнение на процесите

Времето за изпълнение (времето между възлагането на поръчката от водещите системи и предаването на положителна обратна информация до водещата система, на всяка отделна команда трябва да се измери и запише в централната система. Трябва да се измерва и записва също и времето за изпълнение на масови команди (напр. ежедневните отчитания). Резултатите от този мониторинг трябва да се извеждат на интерфейс за предоставяне на информация (Webservice).

1.1.10. Специални изисквания при използване на йерархични системи

#### Комуникационна връзка между централната система и Концентратор на данни

Изисканите времена на реакция и разполагаемости в цялата система трябва да бъдат спазени и когато се използват системи с концентратор на данни. Комуникационната свързаност на концентратор на данните трябва да е така оразмерена, че да се спазват времената за реакция и да е гарантирана изисканата разполагаемост.

За да може да бъде открита причината за грешка в случай на неспазване на изисканите стойности в цялата система, разполагаемостта на отделните връзки за пренос на данни между електромерните портали и централната система трябва да се измери и запише посредством функционалност за управление на мрежата и да се предостави на разположение чрез интерфейс за предоставяне на информация (Webservice).

При използване на обществени мрежи (напр. ADSL, GPRS) оферента на централната система трябва да посочи нивото на обслужване от страна на обществените провайдъри, което е необходимо за постигане на общата разполагаемост.

При използване на линейни комуникационни връзки (напр. кабели, оптична връзка), които са собственост на мрежовия оператор, трябва да се разрешат зададените от мрежовия оператор системни компоненти и при необходимост да се дефинират изисквания, които са необходими за изпълнение на

Furthermore the mass methods, which are to be applied to this evidence, must be specified.

Note: The requirements, regarding planning, construction, commissioning and operation of telecommunication grids do not form part of this tender procedure.

Communication connections between the data concentrator and the end devices

#### 1.1.11. PLC

The PLC-system must be dimensioned so that with the aforesaid end-devices per one data concentrator and with simultaneous maximum data transfers, the required availability and certain reaction are observed. Particular attention is to be paid to the outlines for transformer stations with a total length of up to 1,5 km., as well as lines with up to 5 transfers from overhead line to another overhead line, consisting of several conductors with equal potentials or to a cable in a tube. The PLC system must be resistant to false signals, so that, despite the temporary reverse effects on the grid by the client facilities, the required availability and the specified reaction times are observed.

In case of interferences from electric appliances at the client facilities, it is necessary to ensure appropriate filters for reducing such interferences.

#### 1.2. Events and alarms

The integration in the Head End Systems for the control of alarms and events must be possible.

The respective event must be characterized by at least the following information:

- a. Clear identification of the origin
- b. Type of the event and information in clearly presented text
- c. Date/time of the event
- d. Time of transfer /of the central registration (if applicable)
- e. Event/Error category e.g.:
  - i. Informative
  - ii. Critical error: not removed,
  - iii. it is possible that other devices are also affected by that error,
  - iv. The error has not been ultimately validated.

All the readings of the electricity meters and events of all the system levels must be recorded in protocols and time-stamped (both for the original time of occurrence and the actual duration of the event). The time-stamp must always be combined with the report command and the information on the event.

The events/alarms must be recorded in all the decentralized components (electricity meters, circuit breakers, gates) as well as in the centralized system for a period of time, variable and specified for the respective Alarms and Events Group, as the minimum number of entries to be stored is 100.

Error analysis and optimization

общата разполагаемост.

Освен това следва да се посочат масовите методи, с които трябва да се приложи това доказателство.

Забележка: Изискванията към планирането, изграждането, въвеждането в експлоатация и експлоатацията на телекомуникационни мрежи не са част от настоящата тръжна процедура.

Комуникационни връзки между Концентратор на данни и крайните устройства

#### 1.1.11. PLC

PLC-системата трябва да е оразмерена така, че с по-горе упоменатия брой крайни устройства за един онцентратор на данни при едновременни, максимални трансфери на данни да бъдат спазени необходимата разполагаемост и определените времена за реакция. По специално трябва да бъдат разглеждани изводи на трафопостове с дължина до 1,5 км., както и линии с до 5 прехода от въздушна линия към друга въздушна линия, състояща се от няколко проводника с еднакъв потенциал, или към кабел в една тръба. Системата PLC трябва да е устойчива срещу погрешни сигнали, така че въпреки временни обратни въздействия върху мрежата от страна на клиентски съоръжения, да се спазят необходимата разполагаемост и определените времена за реакция.

В случай на смущения от електрически уреди в клиентски съоръжения е необходимо да бъдат осигурени подходящи филтри за намаляване на тези смущения.

#### 1.2 Събития и аларми

Интеграцията в централни системи за управление на аларми и събития трябва да е възможна.

Дадено събитие трябва да се характеризира поне със следната информация:

- a. Еднозначна идентификация на произхода
- b. Тип на събитието респективно информация в ясно формулиран текст
- c. Дата/Час на събитието
- d. Час на прехвърлянето/на централното регистриране (ако е приложимо)
- e. Събитие/Категория на грешката напр:
  - i. Информативна
  - ii. Критична грешка: не премахната,
  - iii. възможно е и други уреди да бъдат засегнати от тази грешка,
  - iv. Грешката не е окончателно валидирана.

Всички отчитания на електромери и събития на всички системни нива трябва да се протоколират и да им се добавят времеви печати (както за час така и за продължителност на събитието). Времевият печат трябва винаги да се комбинира с командата за отчет и с информацията за събитието.

Събитията/Алармите трябва да се запамятват във всички децентрализирани компоненти (електромери, прекъсвачи, гейтове) както и в централизираната система за период от време, променлив и настройван за дадена Група Аларми и Събития, но да се запамят минимум 100 записа.

Анализ на грешки и оптимизация

### 1.2.1. Information, regarding the events and the alarms

In order to process the critical situations, it is necessary that the centralized system is capable of interpreting events and alarms as well as to generate filters in order to prepare reports. The contents of such reports must be accessible for the users or to be stored in a recommended file format (e.g. \*.csv, .txt, .xls ...).

### 1.2.2. Configuration for the processing of events and alarms

The centralized system must document each and every event/alarm received, as for this purpose, it is possible that the relevant rules are freely selected (e.g. only to file protocols, create tickets etc. ) doing that, a temporary link between events/alarms is to be established

### 1.2.3. Report on the assets and the checked events and alarms

The centralized system must provide functionality for retrieving information regarding the active events and alarms and the history of various events/alarms.

There must be a capability for the events/ alarms to be sorted by different criteria, such as time roles, event/alarm type, electricity meter, electricity meter groups, etc. The centralized system must offer functionality for manual and automatic erasing of events/alarms.

### 1.2.4. Configuration of filters for various events/alarms

In order to determine which events/alarms must be referred to the centralized system, it should be possible to configure different filters.

It must be possible to make configurations for a single electricity meter, for a group of electricity meters as well as for all electricity meters.

These capabilities must also be available for the Data Concentrator.

The objective of the filter is to protect the centralized system against "overloading" through events/alarms.

The contractor must detail in the specification the filters, which can be defined.

The following reports must be provided for as a minimum:

- a. Automatically, according to the specified calendar schedule, reports are to be generated on the communication devices, lacking data or having no connection.
- b. Automatically, according to the specified calendar schedule for reading, reports are to be generated for the end devices, which lack data.
- c. Automatic, according to the specified calendar schedule,
- d. Analysis of the energy balance: The system must be capable of calculating the balance, based on parts of the network, defined by the operator – the amount of the reported energy, according to the commercial electricity meters with a similar or identical calendar schedule for reading and balancing electricity meter with the same schedule. Automatically, according to the specified

### 1.2.1. Информация относено събитията и алармите

За обработването на критични ситуации е необходимо централизираната система да е в състояние да интерпретира събития и аларми както и да генерира филтри с цел изготвяне на справки. Съдържанието на справките трябва да е достъпно за потребителите или да се съхранява в желан файлов формат (например \*.csv, .txt, .xls ...).

### 1.2.2. Конфигурация за обработването на събития и аларми

В централизираната система е необходимо всяко прието събитие/аларма да се документира, като за целта е възможно правилата за това свободно да се изберат (напр. само да се протоколират, създаване на тикети, и др. ) При това трябва да се създаде времева връзка между събития/аларми

### 1.2.3. Справка за активните и проверените събития и аларми

Централизираната система трябва да предлага функционалност за извеждане на информация относно активни събития и аларми и историята на различни събития/аларми.

Трябва да е налице възможност събитията/алармите да се сортират по различни критерии, като времеви период, тип на събитие/аларма, електромер, група от електромери, и др. Централизираната система трябва да предлага функционалност за ръчно и автоматично изтриване на събития/аларми.

### 1.2.4. Конфигурация на филтри за различни събития/аларми

За да се установи, кои събития/аларми трябва да се сигнализируют към централизираната система, трябва да е възможно конфигуриране на филтри.

Трябва да е възможно да се правят конфигурации за един електромер, за група електромери както и за всички електромери.

Тези възможности трябва да са налични и за Концентратор на данни.

Целта на филтъра е да се предпази централизираната система от "препълване" чрез събития/аларми.

Изпълнителят трябва да опише в спецификацията филтрите, които могат да бъдат дефинирани.

Следните справки следва минимално да бъдат възможни за изпълнение:

- a. Автоматично, съгласно зададения календарен график, да се генерират справки за комуникационните устройства, от които липсват данни или с които няма връзка.
- b. Автоматично, съгласно зададения календарен график за отчитане, да се генерират справки за крайните устройства, за които липсват данни.
- c. Автоматично, съгласно зададения календарен график,
- d. Анализ на енергийния баланс: Системата да има възможност за изчисляване на баланс по участъци от мрежата, дефинирани от оператор – сума от отчетената енергия от търговски електромери с еднакъв календарен график за отчитане и балансов електромер със същия график. Автоматично, съгласно зададения календарен график, да се генерират

calendar schedule, to generate files with the sections of the grid (outlets), where a disbalance of energy – outside the limits, preset by the operator.

- e. Metering data – for a period, latest data, automatic and manual generation of files, templates for formatting of files (data, time, serial number of the device, transformer station, outlet, address, data1, data2, data3 etc.), standard formats CSV,XLS

#### 1.2.5. Report on events/alarms and assigned filters

The centralized system must provide the capability of retrieving information regarding the relevant active filters, applicable to certain events/alarms. The capabilities for analyzing the filters, which, at a certain moment in time, were active, must be clearly detailed.

The centralized system must provide the capability for tracing the relevant filters, assigned to certain events/alarms. There should be a capability for preparing reports on the history of the active filters.

### III. Fully electronic electricity meter with manipulations recognition, an integrated modem and a load management relay

#### 1. Technical details

Position 1: Single-phase electricity meter for direct connection

Position 2: Three-phase electricity meter for direct connection

Position 3: Three-phase electricity meter for indirect connection

Consumption type:	Active and reactive power – A+, A-, Option: QI, QII, QIII, QIV
Current strength:	Positions 1 and 2: 5(60)A or 10(60)A Position 3: 5(10)A
Rated voltage:	Position 1: 230V Positions 2 and 3: 3x230/400V
Rated frequency:	50 Hz
Precision class:	Positions 1 and 2: 2 (MID A, according IEC Class 2) Position 3: 1 (MID B, according IEC Class 1)
Types of tariffs:	multi-tariff (at least 4 tariffs), currently preset with 2 tariffs, cyclical displaying of the data on a LCD-display. The stored billing values from previous periods must not be visualized on the display.
Tariff management :	by means of a built-in clock (with summer/winter switching)
Billing:	The billing, caused by the built-in clock, takes place at 00.00 a.m. on the date, defined by the system.

файлове с учащите от мрежата (изводи), където е измерен дебаланс на енергията – извън предварително зададени от оператора граници.

- e. Измервателни данни – за период, последни данни, автоматично и ръчно генериране на файлове, шаблони за форматиране на файловете (дата, час, сер.ном.на устройството, ТП, извод, адрес, данни1, данни2, данни3 и т.н.), стандартни формати CSV,XLS

#### 1.2.5. Справка за събития/аларми и причислени филтри

В централизираната система трябва да е възможно да се извежда информация относно това към кои събития/аларми какви активни филтри са причислени. Възможностите за анализиране относно филтрите, които в даден период от време са били активни, трябва да бъдат описани.

В централизираната система трябва да е възможно проследяването на това какви събития/аларми и какви филтри за били зададени. Трябва да е налице възможността да се изготвят справки за историята на активни филтри.

### III. Напълно електронен електромер с разпознаване на манипулации, интегриран модем и реле за управление на товара

#### 1. Технически данни

Позиция 1: Еднофазен електромер за директно свързване

Позиция 2: Трифазен електромер за директно свързване

Позиция 3: Трифазен електромер за индиректно свързване

Вид консумация:	Активна и реактивна енергия – A+, A-, Опция: QI, QII, QIII, QIV
Сила на тока:	Позиции 1 и 2: 5(60)A или 10(60)A, Позиция 3: 5(10)A
Номинално напрежение :	Позиция 1: 230V Позиции 2 и 3:
Номинална честота:	50 Hz
Клас на точност:	Позиции 1 и 2: 2 (MID A, съгласно IEC клас 2) Позиция 3: 1 (MID B, съгласно IEC клас 1)
Видове тарифи:	многотарифен (най-малко 4 тарифи), в момента параметризиран с 2 тарифи, с циклично показване на данните на LCD-дисплея. Запометените самоотчети (билинг стойности) от минали периоди не трябва да се визуализират на дисплея.
Управление на тарифите:	посредством вътрешен часовник (с лятно/зимно превключване)
Самоотчет (билинг):	Самоотчетът (билингът), предизвикан от вътрешния часовник, се извършва в 00.00 на



	There should be an option for remote defining of the date of the billing period
Data exchange channel:	IR - data exchange, PowerLine or GSM/GPRS – defining the interfaces, according to the block diagram
Control output:	Positions 1 and 2: Recommended 1000 Imp./kWh Position 3: Recommended 10000 Imp./kWh

## 2. General Requirements

The electricity meters must meet, in terms of technical specifications, the legal requirements, regarding metering in the Republic of Bulgaria.

Electricity meters, registered with the Governmental Register of Metering Devices, Approved for use in Bulgaria, may be used. A copy of the registration certificate (a type approval certificate) must be submitted.

Electricity meters, certified by the Measuring Instruments Directive (MID) may be used. A copy of the MID certificate, together with the type testing certificate, must be submitted.

A requisite precondition is the presence of a valid manufacturer's certificate, according to EN ISO 9001 or equivalent.

The electricity meters must be structurally designed and produced that no hazards would occur in fixed operational and normal conditions of work. More specifically, the following must be ensured:

- safety of people against electric shock
- safety of people against the effects of high temperatures
- security and resistance to heat and fire
- protection of the housing of the electricity meter against the penetration of hard objects, dust and water (at least IP51 or higher)
- protection of people, against events, being health hazards (vapours, sharp edges, ...).

Furthermore, the electricity meters (including the interfaces) must be protected against mechanical and electrical tampering.

In normal operating conditions, all parts of the electricity meters must be efficiently protected against corrosion. The protective layer must be strong enough, so that they cannot be damaged by weather conditions, under certain operating conditions.

### 2.1. Housing

Three openings on the box are required for the installation of the electricity meter on the installation panel, according to DIN 43857 part 1 for Position 1 and DIN 43857 part 2 for Positions 2 and 3. The dimensions must be met, irrespective of whether it is a fully integrated or modular solution.

The basic dimensions of the electricity meters, as well as the

	дефинирана от системата дата. Дефинирането на дата за край на билинг период следва да може да се задава дистанционно
Канал за обмен на данни:	IR - обмен на данни, PowerLine или GSM/GPRS – дефиниране на интерфейсите според блоковата схема
Контролен изход:	Позиции 1 и 2: Препоръчително 1000 Imp./kWh , Позиция 3: Препоръчително 10000 Imp./kWh.

## 2. Общи изисквания

Електромерите трябва да отговарят в техническото си изпълнение на законовите предписания за измерванията в Р. България.

Допускат се електромери, вписани в Държавния регистър на одобрените за използване в страната средства за измерване. Следва да се представи копие от вписването в държавния регистър – свидетелство за одобрен тип.

Допускат се електромери, сертифицирани съгласно Директива за измервателните уреди (MID). Следва да се представи копие от MID сертификат, заедно с типовото изпитание.

Необходимо е наличието на валиден сертификат на производителя по EN ISO 9001 или еквивалентен.

Електромерите трябва да са структурно проектирани и произведение така че при фиксирани експлоатационни и нормални условия на работа, да не възникват опасности. По-специално трябва да се осигури:

- безопасността на хората срещу токов удар
- безопасността на хората срещу ефектите на повишена температура
- сигурност и устойчивост на топлина и огън
- защитата на корпуса на електромера срещу проникване на твърди предмети, прах и вода (най-малко IP51 или по-висока)
- защита на хората срещу събития, засягащи здравето (изпарения, остри ръбове, ...).

В допълнение електромерите (включително и интерфейсите) трябва да имат защита срещу механични и електрически опити за манипулиране.

При нормална работа всички части на електромерите трябва да бъдат ефективно защитени от корозия. Защитните слоеве трябва да бъдат достатъчно здрави, така че да не могат да бъдат повредени от атмосферните влияния, при определените условия на работа .

### 2.1. Корпус

За монтирането на електромера към таблото за монтаж са необходими три отвора на кутията съгласно DIN 43857 част 1 за Позиция 1 и DIN 43857 част 2 за Позиции 2 и 3. Размерите трябва да се спазват, независимо от това дали е напълно интегрирано или модулно решение.

Основните размери на електромерите, а също и вида и



type and position of the fixtures must be recorded in tenderer's application, in case of deviations from the DIN requirements.

It must not be possible to open the housing without breaking it (e.g. it must be glued or welded), it is recommended that a sealing option is provided.

If the electricity meter can be opened without damaging it, there should be a contact, registering each and every opening of electricity meter's housing and it must be sealable.

The housing must be sealable in such a manner that the internal parts of the electricity meter must only be accessible, after breaking the seal/s.

The cover of the housing must only be removable with the use of tools.

The housing must be designed and positioned in such a manner, that in case of temporary deformation, the reliable operation of the electricity meter must not be affected.

It is recommended that the housings are made of reusable insulating material, in accordance with protection class II.

Any and all bolts must be made of metal and combined with a metal threaded bushing. Furthermore, the plate for the sealing wire must be cast together with the box or the terminal cover.

## 2.2. Terminals, connection block

Whenever the terminals are arranged in one or more connection blocks, they must have sufficient insulation and mechanical strength. In order to ensure that, the insulating material, designed for the production of the connecting terminals, must be checked, following the applicable rules.

The electricity meter must not have any calibration links on the connection block.

The material of the connection block must withstand the ISO 75-2 tests at a temperature of 135°C and pressure of 1,8 MPa (method A).

The inlets in the insulating material, leading to the terminals, must be large enough, so that the insulation of the conductor can also pass through them.

The method of fixing of the conductor in the terminals must ensure sufficient and proper contact. No loosening of the connection or overheating of the conductor must be possible. Screw terminals, used for the electric contact and the screws, which may be unscrewed and screwed multiple times, during operation of the electricity meter, must be supplied with a metal threaded bushing. The main connections must be designed as box couplings or frame terminals with one or two terminal with straight or Philips screws Pozidriv 2 for Positions 1 and 2 and Pozidriv 1 for Position 3. The respective screws must be Pozidriv-Kombi 2 for Positions 1 and 2 and Pozidriv 1 for Position 3.

Each electricity meter or connection block cover must have a label with standard symbols, indicating the electric

разположението на закрепващите елементи трябва да се запишат в заявлението за участие на кандидата, ако е налице отклонение от изискванията на DIN.

Отварянето на корпуса не трябва да е възможно без неговото разбиване (например да е залепен или заварен), желателно е да е налице възможност за пломбиране.

Ако електромерът може да се отваря без да се уврежда, то трябва да е налице контакт, регистриращ отварянията на корпуса на електромера и задължително да има възможност за пломбиране.

Корпусът трябва така да се пломбира, че вътрешните части на електромера да станат достъпни едва след счупване на пломбата/пломбите.

Отстраняването на капака на корпуса не бива да е възможно без използване на инструменти.

Корпусът трябва да е конструиран и разположен така, че при временна деформация да не се наруши надеждната работа на електромера.

Препоръчително е корпусите да се изработват от годен за повторна употреба изолационен материал в съответствие с клас на защита II.

Всички болтове трябва да са изработени от метал и да се комбинират с метална втулка с резба. Освен това пластината за телта на пломбата трябва да е отливка с кутията или с клемния капак.

## 2.2. Клеми, клемен блок

Когато клемите са подредени в един или повече клемни блокове, те трябва да имат достатъчно добра изолация и механична здравина. За да се гарантира това, изолационният материал, предвиден за производството на съединителните клеми, трябва да бъде проверен по съответния ред.

На клемния блок електромерът не трябва да има връзки за калибриране.

Материалът на клемния блок трябва да издържа изпитванията по ISO 75-2 при температура от 135°C и налягане от 1,8 MPa (метод A).

Входящите отвори в изолационния материал, които водят до клемите, трябва да бъдат достатъчно големи, че през тях да може да премине и изолацията на проводника.

Начинът на закрепване на проводника в клемите трябва да гарантира достатъчно добър и траен контакт. Не трябва да се допуска разхлабване на връзката или прекомерното загряване на проводника. Винтови свръзки, които осъществяват електрически контакт, и винтове, които могат да бъдат развивани и завивани многократно по време на експлоатацията на електромера, трябва да имат резбова втулка от метал. Основните клеми трябва да бъдат изработени като втулковидни клеми или рамковидни клеми с по един или два клемовидни винта за използването на прави и кръстатни отвертки Pozidriv 2 за Позиции 1 и 2 и Pozidriv 1 за Позиция 3. Като винтове трябва да се използват Pozidriv-Kombi 2 за Позиции 1 и 2 и Pozidriv 1 за Позиция 3.

На всеки електромер или капак на клемния блок трябва със стандартни символи да е трайно обозначена

connection diagram. The Employer will include a connection diagram. The precise connection method shall be determined by the Employer, by means of a sample.

The possibility for corrosion, as a result of the use of various conductive materials, must be minimized by means of proper selection of these work pieces.

The electric connections must ensure that the contact pressure is not transferred through the insulating material.

The terminal connections must ensure a permanent contact for the entire lifetime of the electricity meter.

Any dubious terminals of various potentials, arranged close to each other, must be secured against accidental short circuit.

### 2.3. Terminal cover

The terminals of the electricity meter, if placed in a connection block and not protected otherwise, must have a separate terminal cover, which can be sealed, independently from the main cover. The terminal cover must enclose the terminals, screws and connecting conductors, as well as their insulation at a proper length.

There must be no access to the terminals without breaking the seal of the terminal cover. The screws on the terminal cover must have the same heads, as those on the terminal screws.

The sealing option must be designed so that using more than one seal is possible, as long as the seals are permitted by the Bulgarian Metrology Institute.

It is recommended that the terminal cover is made of recyclable insulating material with protection class II.

The terminal cover must meet the provisions of DIN 43857.

### 2.4. Protection class

Solely electricity meters with insulated housing (incl. the connection block cover) with protection class II must be delivered. These electricity meters must have strong and durable housings and terminal covers, made of insulating material. The materials must have mechanical resistance and color resistance against ultraviolet radiation.

The housing must enclose all metal parts of the electricity meter, with the exception of small parts, such as the plate, bolts, rivets and other fasteners.

If such small parts outside the housing are accessible during installation or testing, in accordance with IEC 60529 they must be properly insulated, so that they cannot become energized in case of a failure in the main insulation. Insulation paint, enamel, ordinary paper, cotton, oxide film on the metal parts, self-adhesive foil or similar unstable materials, are insufficient for such additional insulation.

Reinforced insulation is required for the connection block and the terminal cover.

When sealing the meter, the sealing wire must not get in

електрическата схема за свързване. Възложителят ще приложи образец на схемата за свързване. Точния начин на закрепване ще се определи от Възложителя с помощта на мострата.

Възможността за корозирание в следствие използването на различни проводникови материали трябва да се снижи до минимум с подходящ подбор на тези заготовки.

Електрическите свързки трябва да са направени така, че контактното налягане да не се провежда през изолационния материал.

Клемните връзки трябва така да са изпълнени, че да се гарантира траен контакт за времето на експлоатационния срок на електромера.

Съединителните клеми с различен потенциал, които са подредени гъсто една до друга, трябва да са обезопасени срещу случайно късо съединение.

### 2.3. Клемен капак

Клемите на електромера, ако те са в клемен блок и не са защитени по друг начин, трябва да имат отделен клемен капак, който да може да бъде пломбиран независимо от основния капак. Клемният капак трябва да обхваща клемите, винтовете и присъединителните проводници, както и тяхната изолация на подходяща дължина.

Не трябва да има достъп до клемите без да бъде разпломбиран клемен капак. Винтовете на клемния капак трябва да бъдат изпълнени за същите глави като клемните винтове.

Възможността за пломбиране трябва да бъде проектирана така, че да е възможно пломбиране с една или повече пломби, разрешени от Българския Институт по Метрология.

Препоръчително е клемният капак да бъде произведен от рециклируем изолационен материал с клас на защита II.

Клемният капак трябва да отговаря на DIN 43857.

### 2.4. Клас на защита

Трябва да се доставят изключително и само електромери с изолиран корпус (вкл. капака на клемния блок) от клас на защита II. Тези електромери трябва да имат здрави и издръжливи корпуси и клемни капаци от изолационен материал. Материалите трябва да имат механична устойчивост и устойчивост на оцветяването срещу ултравиолетови лъчи.

Корпусът трябва да покрива всички метални части на електромера, с изключение на малки части като табелка, болтове, нитове и др. крепежни елементи.

Ако такива малки части извън корпуса са достъпни по време на монтаж или изпитване съгласно IEC 60529 те трябва да са подходящо изолирани срещу попадане под напрежение в случай на дефект на основната изолация. Изолационна боя, емайл, обикновена хартия, памук, оксид филм върху метални части, самозалепващо фолио или подобни нестабилни материали, не са достатъчни за тази допълнителна изолация.

За клемния блок и клемния капак се изисква подсилена изолация.

При пломбиране пломбажната тел не трябва да

contact with energized parts.

2.5. Protection against penetration of dust and water  
According to EN 60529 +A1 of 2000-10-01 the electricity meters must have the following protection, as a minimum:

2.6. Technical data plate

If the electricity meter is installed in the grid, the plate and the metrological seal must be clearly visible on the front.

If the meters are certified according to the requirements of Regulation of measuring instruments subject of metrological control nameplate must comply with the relevant requirements of the Ordinance.

If the meters are certified according to MID nameplate must meet the relevant requirements of MID

Each electricity meter must have the following labeling:

- 2.6.1. any and all labeling, as required by the MID
- 2.6.2. any and all warning signs, as required on national level
- 2.6.3. any and all labeling, required approvals and certificates
  - 1) Manufacturer's name or logo
  - 2) Type labels and sign for admission to operation. For MID electricity meters, the respective number of the notified body is also included.
  - 3) Number of phases and number of conductors, for which the electricity meter is designed (single- or three-phase). This data may be indicated, with the help of graphical symbols, in accordance with EN 62053-52 of 2006-10-01.
  - 4) Factory number and year of manufacturing. The factory number, as seen on the plate, must also be programmed in the software of the electricity meter. Whenever the technical data plate is a part of the cover of the housing, the factory number, specified on the plate must also be inscribed durably on the inside of the electricity meter. The plate cannot be placed on the terminal cover.
  - 5) Rated voltage: number of metered systems and voltage at the terminals.
  - 6) Rated current and maximum admissible current (e.g.: 0,5-10(60)A).
  - 7) Rated frequency: in Hz.
  - 8) Constant of the electricity meter, e.g. in Imp/kWh.
  - 9) Metering precision class 2 (MID A) for active and 2 for reactive values for Positions 1 and 2, metering precision class 1 (MID B) for active and 2 for reactive values in Position 3.
  - 10) Temperature range, in accordance with MID (-25°C to +55°C).
  - 11) Double protective insulation mark.
  - 12) Barcode

At Employer's request, a barcode is also to be affixed. The precise type of the barcode and its exact place on the technical data plate are determined, based on the sample.

13) Ownership labeling:

докосва части под напрежение.

2.5. Защита срещу проникване на прах и вода  
Електромерите трябва да разполагат със защита съгласно EN 60529 +A1 издание 2000-10-01:

2.6. Табелка с технически данни

Когато електромера е монтиран в мрежата табелката и метрологичната пломба трябва ясно да се виждат от предната страна.

В случай че електромерите, са сертифицирани съгласно изискванията на Наредба за средствата за измерване подлежащи на метрологичен контрол, табелката с техническите данни трябва да отговаря на съответните предписания на Наредбата.

В случай че електромерите, са сертифицирани съгласно MID табелката с техническите данни трябва да отговаря на съответните предписания на MID

Всеки електромер трябва да има следните означения:

- 2.6.1. всички маркировки, изисквани от MID
  - 2.6.2. всички необходими предупредителни знаци изисквани на национално ниво
  - 2.6.3. всички маркировки, необходими одобрения и сертификати
    - 1) Име на производителя или фирмен знак
    - 2) Означение на типа и знак за допускане за експлоатация. При MID електромери, се изобразява съответния номер на нотифицирания орган.
    - 3) Брой на фазите и брой на проводниците, за които е предвиден електромерът (едно- или трифазен). Тези данни могат да са означени с помощта на графични символи съгласно EN 62053-52 издание 2006-10-01.
    - 4) Заводски номер и година на производство. Заводският номер, както се вижда на табелката трябва да е програмиран и софтуерно в електромера. Когато табелката с техническите данни е част от капака на корпуса, отбелязаният върху табелката заводски номер трябва да е нанесен трайно и във вътрешната част на електромера. Поставянето на табелка върху клемния капак не е разрешено.
    - 5) Номинално напрежение: брой на измервателните системи и на напрежение на клемите.
    - 6) Номинален ток и максимално допустим ток (например: 0,5-10(60)A).
    - 7) Номинална честота: в Hz.
    - 8) Константа на електромера, напр. в Imp/kWh.
    - 9) Клас на измервателна точност 2 (MID A) за активни и 2 за реактивни величини за Позиции 1 и 2, клас на измервателна точност 1 (MID B) за активни и 2 за реактивни величини при Позиция 3.
    - 10) Температурен обхват съгласно MID (-25°C до +55°C).
    - 11) Знак за двойна защитна изолация.
    - 12) Баркод
- Изискване на възложителя е поставяне на баркод. Точният тип на баркода и мястото му на поставяне на табелката с техническите данни се определят чрез мострата.
- 13) Маркировка за собственост:



14) MID labeling (for MID-electricity meters).

15) CE – Labeling with the year of the MID calibration (e.g. M14 ) and notified body.

16) The counters, visualized on the display of the electricity meter, must be detailed on the technical data plate.

The entire information, specified above, must be specified on an UV-resistant plate, which must be durable, clear and readable from the outside.

It is permitted to use standardized symbols, according to CENELEC EN 60387, on the plate.

The plate design is agreed individually with the Employer.

2.7. Weather conditions – temperature range

Temperature range in operating mode:

- 25°C to +55°C

Temperature range during storage or transport: - 25°C to +70°C

The precision class must be preserved in the entire scope of the operating temperature.

### 3. Power supply

3.1. Consumed power in the voltage and current circuits

The power, consumed by each voltage and current circuit of the electricity meter, as well as the additional modules at the rated voltage, the rated temperature and rated frequency, including the consumption of the metering systems for active and complete power must not exceed the values, set out in EN 62053-21. This refers to both the fully integrated version and the modular version, as an aggregate of all modules, including the electricity meter. The own consumption with and without active communication of the electricity meter must be specified in the technical documentation of the product, enclosed to the application for participation.

3.2. Supply voltage

3.2.1. Grid voltage allowance range

The power supply of the electricity meter must be designed so that it can function properly in the following ranges:

→ rated voltage  $U_n=230V$

→ normal operating range:  $0,9U_n$  to  $1,10U_n$

→ operating range limits:  $0,8U_n$  to  $1,15U_n$

The tender must specify the minimum voltages, at which the electricity meter starts metering.

3.2.2. Rated voltages

Rated voltage: Position 1: 230V

Rated voltage: Positions 2 and 3: 3x230/400V

3.2.3. Frequency

The meters must be designed for a rated frequency of 50Hz.

14) Означаване според MID (при MID-електромери).

15) CE – Маркировка с година на MID калибриране (напр. M14 ) и нотифициран орган.

16) Броячите, които се визуализират на дисплея на електромера, трябва да са описани върху табелката с техническите данни.

Цялата информация, посочена по-горе, трябва да се съдържа върху UV - устойчива табелка, която трябва да бъде издръжлива, ясна и четлива отвън.

Разрешава се използването на стандартизирани символи според CENELEC EN 60387 на табелката.

Дизайнът на табелката е индивидуално договорена с Възложителя.

2.7. Климатични условия – температурен диапазон

Температурен диапазон при режим на работа:

- 25°C до +55°C

Температурен диапазон при съхранение и транспорт: - 25°C до +70°C

В целия диапазон на работната температура класът на точност трябва да се запази.

### 3. Захранване

3.1. Консумирана мощност в напреженовите и токовите вериги

Мощността, консумирана от всяка напреженова и токова верига на електромера, както и от допълнителните модули при номинално напрежение, номинална температурата и номинална честота, включително консумацията на измервателните системи за активна и пълна мощност не трябва да надвишава стойностите, определени в EN 62053-21. Това се отнася както за напълно интегрирана версия, така и за модулна версия като сбор от всички модули, включително електромера.

Собствената консумация с и без активна комуникация на електромера трябва да се посочат в техническата документация на изделието към заявлението за участие.

3.2. Захранващо напрежение

3.2.1. Допусково поле на мрежовото напрежение

Захранването на електромера трябва да бъде проектирано така, че да може да функционира правилно в следните диапазони:

→ номинално напрежение  $U_n=230V$

→ нормален работен обхват:  $0,9U_n$  до  $1,10U_n$

→ граничен работен обхват:  $0,8U_n$  до  $1,15U_n$

В офертата трябва да се посочват минималните напрежения, при която електромерът започва да измерва.

3.2.2. Нормирани номинални напрежения

Номинално напрежение: Позиция 1: 230V

Номинално напрежение: Позиции 2 и 3: 3x230/400V

3.2.3. Честота

Уредите трябва да са предназначени за номинална



They must be capable of working flawlessly in a two-pole field of  $\pm 2\%$  of the rated frequency.

### 3.3. Reverse effects on the grid

The supply grid block may be designed so that it does not allow any reverse effect by high-frequency oscillations in the grid.

The observation of EN 61000-3-2 +A2 edition 2005-11-01 must be guaranteed.

### 3.4. Protection against overvoltage

The test is conducted in accordance with EN 62052-11, chapter 7.3.2 pulse voltage test.

Pulse wave shape 1,2/50 microseconds, according to EN 60060-1.

Source impedance: 500Ohm + 500Ohm

Peak voltage value - 8kV.

### 3.5. Checking the resistance against pulse voltage

The products must meet the EN 61000-4-5 pulse effect test with a wave of 1,2/50 microseconds.

Pulse wave shape 1,2/50 microseconds, according to EN 60060-1.

Source impedance: 2 Ohm  $\pm$  10%

Peak voltage value - 6 kV.

### 3.6. Electromagnetic compatibility

The products must not be affected by any interference, according to CENELEC EN 55011 and CENELEC EN 55014.

The power supply must be resistant to external electric and magnetic field interference at the specified installation locations for the electricity meters.

The electricity meter must not be affected by GSM cell phones with a transmission power of up to 2Watt.

### 3.7. Resistance against transitive interference (Burst)

In this respect, the requirements of EN 61000-4-4 (test precision 4) must be met.

### 3.8. Magnetic interference by permanent magnets

If a permanent magnet, with a residual magnetization of 400mT is placed at the electricity meter, this should not result in either a metrical-technical or functional errors.

In case of higher fields (>400mT) and the meter is not protected against magnetic influences the electricity meter must record their occurrence. These must always be recorded in the Logbook. Sending an alarm signal to the system is optional.

### 3.9. Electromagnetic fields

In this respect the requirements as per EN 61000-4-3 must be met. According to chapter 5 a test precision of 4 is required. This corresponds to a test field strength of 30V/m.

### 3.10. Electrostatic discharge

In this respect, the requirements of EN 61000-4-2 must be met, test precision 4:

Contact discharge: 8kV

Aerial discharge: 15kV

### 3.11. Resistance to heat and fire

The connection block, the terminal cover and the housing of the electricity meter must be made of a non-combustible material, ensuring sufficient protection against the distribution of fire.

честота от 50Hz. Те трябва да могат да работят безпроблемно в допусково поле от  $\pm 2\%$  от номиналната честота.

### 3.3. Обратни въздействия върху мрежата

Захранващият мрежови блок трябва да е оформен така, че да не допуска обратни въздействия от високочестотни трептения по мрежата.

Трябва да се гарантира спазването на EN 61000-3-2 +A2 издание 2005-11-01.

### 3.4. Защита срещу пренапрежение

Тестът се извършва съгласно EN 62052-11, глава 7.3.2 тест импулсно напрежение.

Форма на вълната на импулса 1,2/50 микросекунди, съгласно EN 60060-1.

Импеданс на източника: 500Ohm + 500Ohm

Пикова стойност на напрежението от 8kV.

### 3.5. Проверка на устойчивостта срещу импулсно напрежение

Изделията трябва да са в съответствие с EN 61000-4-5 тест при импулсно въздействие с вълна 1,2/50 микросекунди.

Форма на вълната на импулса 1,2/50 микросекунди, съгласно EN 60060-1.

Импеданс на източника: 2 Ohm  $\pm$  10%

Пикова стойност на напрежението - 6 kV.

### 3.6. Електромагнитна съвместимост

Изделията не трябва да бъдат повлиявани от смущения съгласно CENELEC EN 55011 и CENELEC EN 55014. Не

трябва е възможно повлияване на захранванията от външни електрически и магнитни полета на предвидените места за монтаж на електромерите.

Електромерът не трябва да се повлиява от GSM мобилни апарати с мощност на излъчване до 2Watt.

### 3.7. Устойчивост срещу преходни смущения (Burst)

Тук трябва да се спазват изискванията по EN 61000-4-4 (точност на изпитването 4).

### 3.8. Магнитно повлияване от постоянни магнити

При поставянето на постоянен магнит с остатъчна намагнитеност 400mT електромерът не трябва да отчита нито измервателно-техническа, нито функционална грешка.

При по-високи полета (>400mT) електромерът трябва да регистрира поява им. Задължително е вписването им в дневника на събитията (LogBook). По желание, да се изпрати алармен сигнал към системата.

### 3.9. Електромагнитни радиочестотни полета

Тук трябва да се изпълнят изискванията по EN 61000-4-3. Съгласно глава 5 се изисква точност на изпитването

4. Това съответства на сила на тестовото поле от 30V/m.

### 3.10. Електростатично разреждане

Тук трябва да се изпълнят изискванията по EN 61000-4-2, точност на изпитването 4:

Контактен разряд: 8kV

Въздушен разряд: 15kV

### 3.11. Устойчивост на топлина и огън

Клемният блок, клемният капак и корпусът на електромера трябва да са изработени от самогасящ се материал, осигуряващ достатъчна защита срещу разпространението на огън.



The members of the personnel must not get burned when touching thermally overloaded parts. The standard tests, according to EN 62052-11 and IEC 60695-2-11, designed for this purpose must be observed.

### 3.12. Behavior in case of grid power failure and restoration

The supply of the three-phase electricity meter must, consists of three phases and in case of failure of one or two phases of the grid power supply, the electricity meter must preserve its complete functionality, of at least one phase amounts to  $UN \pm 10\%$ . In case of failure of the neutral conductor, the electricity meter must not be damaged permanently and no general data loss must occur. When the grid power supply is resumed, whether it is single-, double- or triple-phase, the electricity meter must resume its complete functionality within not more than 5 sec.

In case of power failure for within one metering period, no data is to be stored in the load profile, but it is necessary to identify the failure with an appropriate status. In case of longer power interruptions, the last (incomplete) data, regarding the load profile must be stored with an appropriate status (Power down). The first data after the restoration of the power supply must also be identified with an appropriate status (Power up).

## 4. Technical requirements

### 4.1. Rated and maximum current

Values (EN 50470-1)	Position 1	Position 2	Position 3
$I_{Ref}$ Referent current	5 or 10A	5 or 10A	5A
$I_{max}$ (maximum current for the respective precision class)	60A	60A	6A
Maximum current, which the electricity meter can withstand without any damages	80A	80A	10A

$I_{st}$  and  $I_{min}$  must be specified by the manufacturer. The minimum commutating current of the control relay must be at least  $I_{max}$ .

### 4.2. Metered values

Metering and storage of active energy:

- Total active energy +A (kWh)
- Total active energy -A (kWh)
- Load profile 15 min. +A: Generation of metered data (kWh) with date/time and status (e.g. power restoration)
- Load profile 15 min. -A: Generation of the metered data (kWh) with date/time and status (e.g. power restoration)

Не трябва да се стигне до опарване на персонала при докосване до термично претоварени части. Стандартни тестове според EN 62052-11 и IEC 60695-2-11, предвидени в това отношение трябва да бъдат изпълнени.

### 3.12. Поведение при отпадане и възстановяване на напрежението в мрежата

Захранването на трифазния електромер трябва да е трифазно изпълнено и при отпадането на една респективно на две фази на мрежовото напрежение електромерът трябва да запази пълната си функционална годност, ако поне едното фазово напрежение възлиза на  $UN \pm 10\%$ . При прекъсване на нулевия проводник електромерът не бива да се увреди трайно и не бива настъпи генерална загуба на данни. При възстановяване на мрежовото напрежение, независимо дали ще е едно-, дву- или трифазно, електромерът трябва най-късно след 5 сек. да е изцяло годен за функциониране.

При отпадане на напрежението за един период на измерване не трябва да се запамятват данни в товарния профил, но е необходимо да се идентифицира отпадането с подходящ статус. При по-дълги прекъсвания последните (непълни) данни за товарния профил трябва да бъдат запаменени с подходящ статус (Power down). Първите данни след възстановяване на напрежението трябва да бъдат идентифицирани с подходящ статус (Power up).

## 4. Технически изисквания

### 4.1. Номинален и максимален ток

Величини (EN 50470-1)	Позиция 1	Позиция 2	Позиция 3
$I_{Ref}$ Референтен ток	5 или 10A	5 или 10A	5A
$I_{max}$ (макс. ток за класа на точност)	60A	60A	6A
Максимален ток, който електромера може да понесе без да се повреди	80A	80A	10A

$I_{st}$  и  $I_{min}$  трябва да се обявят от производителя. Минималният комутиращ ток на релето за управление трябва да е най-малко  $I_{max}$ .

### 4.2. Измервани величини

Измерване и съхранение на активна енергия:

- Обща активна енергия +A (kWh)
- Обща активна енергия -A (kWh)
- Товарен профил 15 мин. +A: Формиране на измерените данни (kWh) с дата/час и статус (например възстановяване на напрежението)
- Товарен профил 15 мин. -A: Формиране на измерените данни (kWh) с дата/час и статус (например възстановяване на напрежението)

Option: Metering and storage of reactive energy:

- Total reactive power QI (kVAh)
- Total reactive power QII (kVAh)
- Total reactive power QIII (kVAh)
- Total reactive power QIV (kVAh)
- Load profile 15 min. QI: Generation of the metered data (kVAh) with date/time and status (e.g. power restoration)
- Load profile 15 min. QII: Generation of the metered data (kVAh) with date/time and status (e.g. power restoration)
- Load profile 15 min. QIII: Generation of the metered data (kVAh) with date/time and status (e.g. power restoration)
- Load profile 15 min. QIV: Generation of the metered data (kVAh) with date/time and status (e.g. power restoration)

Option: tariff registers

Apart from the aggregate logs (total energy) the electricity meter must also have at least four tariff registers for: +A, – A, Option: QI, QII, QIII, and QIV.

The activation of these logs must take place by means of an internal tariff table with hourly/daily/weekly/monthly/yearly and holiday programs, which may be configured from both the remote reading interface and the service port of the electricity meter.

Any and all changes to the tariff table must be registered with their actual date and time, in the event logbook.

#### 4.3. Identification of the metered values

For clear identification of the metered values, the OBIS code may be used (according to EN 62056-01: Object Identification System - OBIS).

The readings must be presented starting with zeroes. The grid operator should be able to determine which values are to be included in the list of these data.

Опция: Измерване и съхранение на реактивна енергия:

- Обща реактивна енергия QI (kVAh)
- Обща реактивна енергия QII (kVAh)
- Обща реактивна енергия QIII (kVAh)
- Обща реактивна енергия QIV (kVAh)
- Товаров профил 15 мин. QI: Формиране на измерените данни (kVAh) с дата/час и статус (например възстановяване на напрежението)
- Товаров профил 15 мин. QII: Формиране на измерените данни (kVAh) с дата/час и статус (например възстановяване на напрежението)
- Товаров профил 15 мин. QIII: Формиране на измерените данни (kVAh) с дата/час и статус (например възстановяване на напрежението)
- Товаров профил 15 мин. QIV: Формиране на измерените данни (kVAh) с дата/час и статус (например възстановяване на напрежението)

Опция: тарифни регистри

Електромерът трябва да притежава освен сумарните регистри (обща енергия) и най-малко четири тарифни регистри за: +A, –A; Опция: QI, QII, QIII, и QIV.

Активирането на тези регистри трябва да бъде направено чрез вътрешна тарифна таблица с часови/дневни/седмични/месечни/годишни и празнични програми, които да могат да се конфигурират както от интерфейса за дистанционно отчитане, така и през сервисния порт на електромера. Всякакви промени в тарифната таблица, трябва да се регистрират с дата и час в дневника на събитията.

4.3. Идентификация на измерваните величини  
За недвусмислено идентифициране на измерените стойности може да се използва OBIS код (според EN 62056-01: система OBIS – Object Identification System). Показанията трябва да са с водещи нули. Определянето кои величини да бъдат включени в списъка с данните трябва да може да се конфигурира от мрежовия оператор.

OBIS	Definition	Display/presentation of register	Interface P0 (IR)/ presentation of register	Interface P1 (PLC)/ presentation of register
*	Device ID, provided by the manufacturer	-	*	*
0.0.0	ID Number (Device serial No.)	-	20/0	20/0
F.F	Error register	Max. 8/0	Max.8/0	Max. 8/0
0.1.0	Reset counter	2/0	2/0	2/0
1.6.0	15min maximum demand (P+)	-	2/2 с 4 historical values	2/2 с 4 historical values
2.6.0	15min maximum power (P-)	-	2/2 с 4 historical values	2/2 с 4 historical values
1.8.0	Active energy register (A+)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
1.8.T	Active energy register (A+) T=1-4 – tariffs from 1 to 4	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
2.8.0	Active energy register (A-)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values

**5.8.0	Register reactive energy (QI)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
**6.8.0	Register reactive energy (QII)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
**7.8.0	Register reactive energy (QIII)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
**8.8.0	Register reactive energy (QIV)	6/2 без historical values	6/2 с 4 historical values	6/2 с 4 historical values
0.9.1	Current time [hh:mm:ss]	Hh:mm:ss	Hh:mm:ss	Hh:mm:ss
0.9.2	Current date [YYYY-MM-DD]	yy-mm-dd	yy-mm-dd	yy-mm-dd
31.25 (31.7)	Current L1	-	2/2	2/2
51.25 (51.7)	Current L2	-	2/2	2/2
71.25 (71.7)	Current L3	-	2/2	2/2
32.25 (32.7)	Voltage L1	-	3	3
52.25 (52.7)	Voltage L2	-	3	3
72.25 (72.7)	Voltage L3	-	3	3
*	Hardware identification	-	*	*
*	Firmware identification (under metrological seal)	-	*	*
*	Firmware identification (outside metrological seal)	-	*	*
*	Parameterization code ( tariff table, ...)	-	*	*
*	Time and date of last parameterization	-	*	*
Load profile data				
1.8.0	Energy profile (A+) with date and time, units of measurement and status	-	*	*
2.8.0	Energy profile (A-) with date and time, units of measurement and status	-	*	*
**5.8.0	Energy profile (QI) with date and time, units of measurement and status	-	*	*
**6.8.0	Energy profile (QII) with date and time, units of measurement and status	-	*	*
**7.8.0	Energy profile (QIII) with date and time, units of measurement and status	-	*	*
**8.8.0	Energy profile (QIV) with date and time, units of measurement and status	-	*	*
P.98	Event Logbook	-	*	*

\* To be approved by the grid operator.

\*\* Option

\* Трябва да се съгласуват от мрежовия оператор.

\*\* Опция

#### 4.4. Memory capacity

The electricity meter must store a load profile for each of the parameterized values (including information regarding the status, date and time) the last minimum 40 days.

#### 4.4. Обем на паметта

Електромерът трябва да съхранява за всяка от параметризираните стойности товаров профил (включително информация за състоянието, дата и час)

The memory of the event logbook must be capable of storing at least 100 events.

#### 4.5. Software architecture of the electricity meter

##### 4.5.1. General requirements

The structure must generally conform to the recommendations of the WELMEC Software Guide 7.2 (Measuring Instruments Directive 2004 / 22 / EC). In particular, it should be noted that a mandatory minimum requirement is that the firmware is separated into metrological (approved) and non-metrological (non-approvable). The metrological part of the firmware may only include the functions, detailed in 4.5.2. Any and all other functions may only be implemented in the non-approvable part.

##### 4.5.2. Metrological firmware

The metrological firmware must only include functions, which are directly required for metering purposes. The supplier must specify which are the metrological functions and sub-functions of the firmware.

##### 4.5.3. Software update/upgrade of the non-approvable part

Software update/upgrade in the non-metrological part must be possible to perform from the electricity meter and from the Head End System. After removing the electricity meter it should be checked if the entire software has been transferred. Only then can its installation begin. After the installation, the electricity meter carries out a self-check and checks if the new software has been properly installed, recording the relevant data in the event logbook.

If the update fails, the software is automatically restored to the previous version. The respective error must be recorded in the event logbook.

The procedure must take place in accordance with the requirements for "security of the electricity meter".

The firmware update of non-approvable part should not affect in any way of the current values of energy registers.

#### 4.6. Display

For displaying the data, using the external buttons of the electricity meter, displays, ensuring easy reading are to be used, as the delay in case of an environmental temperature of -25°C should not exceed 1 second.

For confidentiality purposes, displaying data for the load profile on the display, using the call button, is only allowed in special cases, this indicator is to be activated and deactivated additionally, using the WAN interface P1 for remote reading and through the service port (interface P0) for servicing and maintenance of the electricity meter (default setting – no data on the load profile is shown on the display).

The opening of the terminal cover must be shown on the display.

The electronic display must meet the following minimum requirements:

(Back)light

Capacity to display the following values:

за последните минимум 40 дни.

Паметта на дневника на събитията трябва да бъде най-малко 100 събития.

#### 4.5. Софтуерна архитектура на електромера

##### 4.5.1. Общи изисквания

Структурата по принцип трябва да се съобразява с препоръките на WELMEC Software Guide 7.2 (Measuring Instruments Directive 2004 / 22 / EC). По-специално следва да се отбележи, че като задължително минимално изискване е фърмуера да се раздели на метрологичен (одобрен) и неметрологичен (неодобряем). Метрологичната част на фърмуера може да включва само тези функции, които са описани в 4.5.2. Всички други функции могат да бъдат реализирани само в неодобряема част.

##### 4.5.2. Метрологичен фърмуер

Метрологичният фърмуер трябва да включва само тези функции, които са пряко необходими за измерване.

Доставчикът трябва да уточни кои са метрологичните функции и под-функции на фърмуера.

##### 4.5.3. Софтуерно обновяване/надграждане на неодобряемата част

Софтуерна актуализация/надстройка в неметрологичната част трябва да бъде изпълнима от електромера и централната система. След свалянето електромера трябва да провери дали пълният софтуер е бил прехвърлен. Само тогава може да започне инсталацията му. След инсталирането електромерът извършва самопроверка и проверка дали новият софтуер е правилно инсталиран, като записва съответните данни в дневника на събитията.

Ако актуализацията не е успешна трябва да се извърши автоматично връщане към предишната версия на софтуера. Трябва да се регистрира съответната грешка в дневника на събитията.

Процедурата трябва да бъде направена съгласно изискванията за "сигурност на електромера".

Промяната на неодобряемата част на фърмуера не трябва по никакъв начин да променя текущите стойности на енергийните регистри

#### 4.6. Дисплей

За изобразяване на данните, които се извикват с външните бутони на електромера, трябва да се използват дисплеи, с които лесно се отчита, като при температура на околната среда до -25°C забавянето трябва да е под 1 секунда.

Поради съображения за поверителност показването на данни за товарния профил на дисплея чрез бутона за повикване е разрешено само в специални случаи, този показател трябва да се активира и деактивира допълнително чрез WAN интерфейса за дистанционно отчитане P1 и посредством сервисния порт (интерфейс P0) за обслужване на електромера (настройка по подразбиране - да няма данни за товарния профил на дисплея).

Отварянето на клемния капак трябва да се изобрази на дисплея.

Електронният дисплей трябва да отговаря на следните минимални изисквания:

(Фоново) осветление

Възможност за изобразяване на следните величини:

- 4.6.1. Direct electricity meters
  - 4.6.1.1 8 digits with two digits after the decimal point (6/2) Minimum dimensions 8x3mm.
  - 4.6.1.2 Power with 8 digits and 3 digits after the decimal point (5/3)
- 4.6.2 Indirect electricity meters
  - 4.6.2.1 8 digits with three digits after the decimal point (5/3) Minimum dimensions 8x3mm.
  - 4.6.2.2 Power with 8 digits with 3 digits after the decimal point (5/3)
- 4.6.3 Main functions
  - 4.6.3.1 Units of measurement
  - 4.6.3.2 Code of the metered value (OBIS or another code)
  - 4.6.3.3 Energy indicator for +A, -A (Option: +R, -R), an arrow or a square diagram
  - 4.6.3.4 Phase indicators: Showing the presence of phase voltage and the direction of rotation of the field (e.g. blinking in case of reserve movement)
  - 4.6.3.5 Indicator for the absence of consumption
  - 4.6.3.6 Error code
  - 4.6.3.7 Status of the control relay
  - 4.6.3.8 Version of the firmware (approved and non-approved)
  - 4.6.3.9 Firmware checksums
  - 4.6.3.10 Date and time
  - 4.6.3.11 Displaying current values at request (e.g. current, voltage, power factor etc.)
  - 4.6.3.12 Option: Status indicators (freely adjustable) for:
    - 4.6.3.12.1 Connection of the device to the interface for external meters
    - 4.6.3.12.2 Active data transfer
    - 4.6.3.12.3 Status of the communication module
    - 4.6.3.12.4 Status of the control relay (e.g. OFF, stand-by...)
    - 4.6.3.12.5 Operating mode (Normal, Settings, Parameterization, Calibration)
    - 4.6.3.12.6 Tampering status
- 4.6.4 Additional functions
  - 4.6.4.1 Showing the active tariff
  - 4.6.4.2 Tariff table number
  - 4.6.4.3 Readings, regarding the aggregate reactive energy QI, QII, QIII and QIV
  - 4.6.4.4 Readings of all tariff registers

#### 4.7 Additional functions

The activation of the tariff registers (and their readings on the display) must be possible through the configuration table.

The electricity meter must be calibrated for the full range of metrological functions. It must always meter and store all the metered values.

In order to ensure the efficiency and usability, only the required tariff registers should be activated and displayed (e.g. single-tariff schedule with a single log).

The following parameters must be determined:

→ Allowing the reactive logs (5.8.0/6.8.0/7.8.0/8.8.0), as well as their displaying on screen.

- 4.6.1. Директни електромери
  - 4.6.1.1 8 цифри с два знака след десетичната запетая (6/2) Минимален размер 8x3mm.
  - 4.6.1.2 Мощност с 8 цифри с 3 знака след десетичната запетая (5/3)
- 4.6.2 Индиректни електромери
  - 4.6.2.1 8 цифри с два знака след десетичната запетая (5/3) Минимален размер 8x3mm.
  - 4.6.2.2 Мощност с 8 цифри с 3 знака след десетичната запетая (5/3)
- 4.6.3 Основни функции
  - 4.6.3.1 Мерни единици
  - 4.6.3.2 Код на измерваната величина (OBIS или друг код)
  - 4.6.3.3 Енергиен индикатор за +A, -A (Опция: +R, -R), стрелка или квадрантна диаграма
  - 4.6.3.4 Фазови индикатори: Показват наличието на фазните напрежения и посоката на въртене на полето (например мигане при обратна посока)
  - 4.6.3.5 Индикатор за липса на консумация
  - 4.6.3.6 Код за грешка
  - 4.6.3.7 Статус на релето за управление
  - 4.6.3.8 Версия на фърмуера (одобрен и неодобряем)
  - 4.6.3.9 Контролни суми на фърмуера
  - 4.6.3.10 Дата и час
  - 4.6.3.11 Показване на моментни величини по желание (напр. ток, напрежение, фактор на мощността и др.)
  - 4.6.3.12 Опция: Статусни индикатори (свободно настройваеми) за:
    - 4.6.3.12.1 Свързване на устройство към интерфейса за външни измервателни устройства
    - 4.6.3.12.2 Активен трансфер на данни
    - 4.6.3.12.3 Статус на комуникационния модул
    - 4.6.3.12.4 Статус на релето за управление (напр. ИЗКЛ., готов за включване...)
    - 4.6.3.12.5 Режим на работа (Нормален, Настройка, Параметризиране, Калибриране)
    - 4.6.3.12.6 Манипулационен статус
- 4.6.4 Допълнителни функции:
  - 4.6.4.1 Показване на активната тарифа
  - 4.6.4.2 Номер на тарифната таблица
  - 4.6.4.3 Показания за сумарна реактивна енергия QI, QII, QIII и QIV
  - 4.6.4.4 Показания на всички тарифни регистри

#### 4.7 Допълнителни функции

Активирането на тарифните регистри (и показанията им на дисплея) трябва да бъде възможно чрез конфигурационната таблица.

Електромерът трябва да бъде калибриран за пълен набор от метрологични функции. Той винаги трябва да измерва и съхранява всички измервани величини. За да се гарантира работоспособността и използваемостта само необходимите тарифни регистри трябва да бъдат активирани и показани на дисплея (напр. еднотарифен план с един регистър).

Трябва да се определят следните параметри:

→ Разрешаване на реактивните регистри (5.8.0/6.8.0/7.8.0/8.8.0), както и показването им на дисплея.



#### 4.8 Built-in clock and calendar

The built-in clock must meet the requirements of EN 62054-21 and EN 62052-21.

The control of the built-in clock must be quartz.

The built-in clock switch must have a complete calendar (date and time) with a summer/winter time switch and weekend and holidays switch.

Setting/synchronization of the date and time should be possible, using the WAN interface of the Head End System, as well as through the service interface on-site. The settings of the date and time, using the buttons on the electricity meter is forbidden for IT security reasons.

The change of summer/winter time (DST) must be parameterized, in accordance with the European standards. The switching times, valid in Bulgaria (UTC+2) must be taken into consideration, as well as all the leap years until 2050.

DST should be performed according next table:

DST time	DST:
Summer -> Winter	4:00 => 3:00 o'clock
Winter -> Summer	3:00 => 4:00 o'clock

The switching of the tariffs takes place in accordance with Regulator's Decision No. Ц-002/ 29.03.2002.

Tariff program	Tariff program active from:
Summer	00:00 01.04
Winter	00:00 01.11

The lifetime of the clock switch must be at least 20 years.

The precision must be within  $\pm 5$ ppm (a maximum daily deviation of 0,5 seconds per day).

Apart from that the clock switch must incorporate temperature compensation.

The switching of tariffs must take place in accordance with the following table:

Metered value	Tariff counter	Winter time	Summer time
P+	1.8.1 (nightly)	22:00 to 06:00	23:00 to 07:00
	1.8.2 (daily)	06:00 to 22:00	07:00 to 23:00

#### 4.9 Load control relay (Position 1 and 2)

There is a requirement for the presence of a switching off device, integrated in the electricity meter. The switching-off device must be capable of interpreting the following commands – both through the local interface, and remotely

- SWITCHING-ON RELAYS
- SWITCHING-OFF RELAYS

The formatted commands must be provided.

#### 4.8. Вътрешен часовник и календар

Вътрешният часовник трябва да отговаря на изискванията на EN 62054-21 и EN 62052-21.

Управлението на вътрешния часовник трябва да е кварцово.

Вътрешният часовников превключвател да разполага с пълен календар (дата и час) с превключване на лятно/зимно време и за почивните дни.

Настройка/синхронизиране на датата и часа трябва да са възможни чрез интерфейс WAN интерфейса на централната системата, както и чрез сервисния интерфейс на място. Настройката на дата и час чрез бутони на електромера не е позволено поради съображения за IT сигурност.

Смяната лятно/зимно време трябва да бъде параметризирана, съгласно европейския стандарт. Да се вземат предвид времената за превключване, валидни за България (UTC+2), както и всички високосни години до 2050.

Лятното часово време трябва да се извършва съгласно следващата таблица:

DST time	DST:
Лято -> Зима	4:00 => 3:00 o'clock
Зима-> Лято	3:00 => 4:00 o'clock

Превключването на тарифите се извършва съгл. Решение на Регулатора №Ц-002/ 29.03.2002.

Тарифна програма	Тарифна програма валидна от:
Лято	00:00 01.04
Зима	00:00 01.11

Продължителността на живот на часовниковия превключвател трябва да бъде най-малко 20 години.

Точността трябва да е в рамките  $\pm 5$ ppm (максимално дневно отклонение 0,5 секунди на ден).

Освен това часовниковият превключвател трябва да е с компенсиране на температурата.

Превключването на тарифите трябва да се извършва съгласно следната таблица:

Измервател на величина	Тарифен брояч	Зимно часово време	Лятно часово време
P+	1.8.1 (нощна)	22:00 до 06:00	23:00 до 07:00
	1.8.2 (дневна)	06:00 до 22:00	07:00 до 23:00

#### 4.9. Реле за управление на товара (Позиция 1 и 2)

Има изискване за наличие на интегрирано в електромера устройство за изключване. Устройството за изключване трябва да може да интерпретира следните команди – както през локален интерфейс, така и дистанционно:

- ВКЛЮЧВАНЕ НА РЕЛЕТАТА
- ИЗКЛЮЧВАНЕ НА РЕЛЕТАТА

Форматираните команди трябва да бъдат предоставени.

## Technical details

The switching-off device must meet the following minimum requirements:

Mechanical useful lifetime: 100 000 commutations  
 Mechanical useful lifetime, according to EN 62055-31, annex C: 10 000 commutations at 100 A,  $\cos\phi=1$   
 Maximum commutation voltage: 400 V (AC)  
 Maximum commutation current: 80 A  
 Short circuit < 10 ms as per EN 62053-21: 3 kA  
 Maximum commutation power: 25 kVA  
 Insulation capability: 4 kV with duration 1 minute

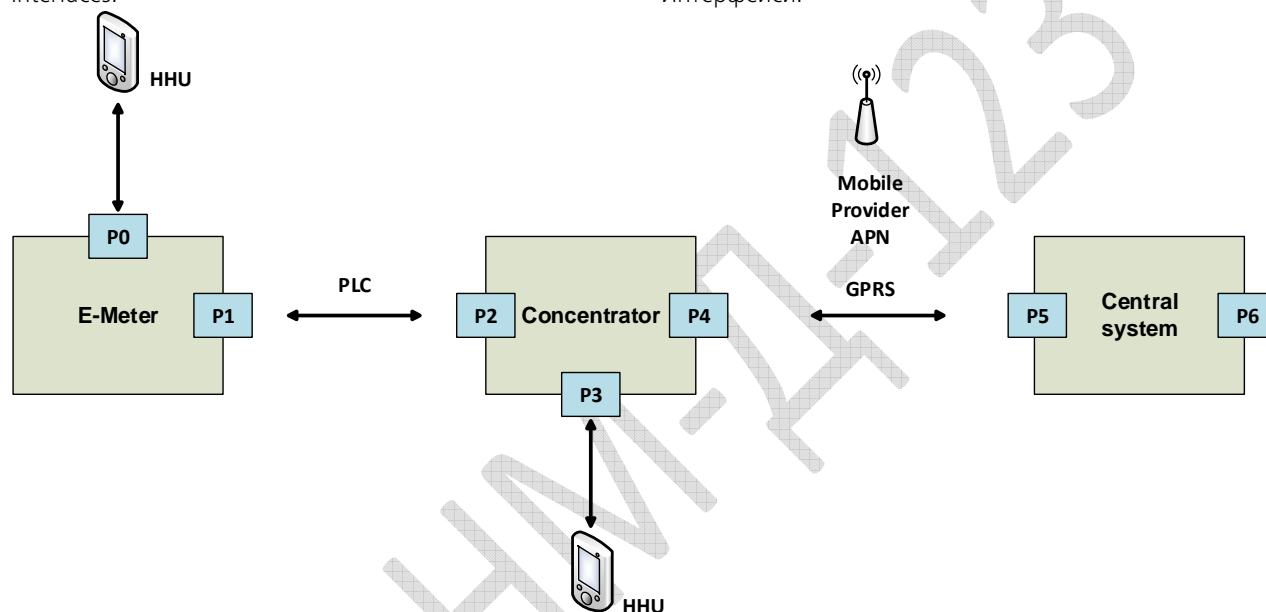
## Технически данни

Устройството за изключване трябва да покрива следните минимални изисквания:

Механичен полезен живот: 100 000 комутации  
 Механичен полезен живот съгл. EN 62055-31, анекс С: 10 000 комутации при 100 A,  $\cos\phi=1$   
 Максимално напрежение на комутиране: 400 V (AC)  
 Максимален комутиран ток: 80 A  
 Късо съединение < 10 ms според EN 62053-21: 3 kA  
 Максимална мощност на комутиране: 25 kVA  
 Изолационна способност: 4 kV с продължителност от 1 минута

## 5 Interfaces. Interface related Requirements

Interfaces:



## 5. Интерфейси. Изисквания към интерфейсите

Интерфейси:

### Interfaces description

Interface	Description
P0	Infrared (IR) interface through which external maintenance tasks can be performed of E-Meter with external device (HHU).
P1	WAN interface of the meter must be able to handle PLC communication
P2	PLC interface between data Concentrator and E-Meter.
P3	Interface through which external maintenance tasks can be performed of Concentrator with external device (HHU).
P4	Interface between data Concentrator and Head End System using GPRS communication environment.
P5	WAN interface of Head End System for communication with Concentrators.

### Описание на интерфейсите:

Интерфейс	Описание
P0	Инфрачервен (IR) интерфейс, чрез който външни дейности по поддръжка могат да бъдат извършвани с Е-електромера, с помощта на външно устройство (Преносим терминал).
P1	WAN интерфейса на електромера трябва да може да се справи с PLC комуникацията
P2	PLC интерфейсът между Концентратора на данни и Е-електромера.
P3	Интерфейс, чрез който могат да бъдат извършвани външни дейности по поддръжка с Концентратор с помощта на външно устройство (Преносим терминал).
P4	Интерфейс между Концентратора на данни и Централната система чрез използване на GPRS комуникация.
P5	WAN интерфейс на Централната система за комуникация с

P6	Interfaces for data exchange between Head End System and existing legacy systems or third party applications.
----	---

#### Electronic electricity meter

In general, the electricity meters must be designed, in a manner ensuring that any requests, sent to one interface cannot be retranslated through another interface (port insulation). This means that a single unauthorized access through the service interface cannot be used for burglary access to the WAN-interface, enabling the use of the WAN.

#### 5.1. Service interface (P0)

##### Physical layer

The service interface must be executed as an optical interface.

The communication speed must be at least 9600 boud.

##### Protocol layer

The service access to the electricity meter must be provided through DLMS/COSEM, IEC 62056-21 or another standard protocol. The eligible option must be determined by the grid operator.

##### Security

The security must be provided within the framework of the assignments of "Security of the electricity meter".

The access control must be provided by individual passwords. It is not necessary to code the data transmission, due to the exclusively local access

#### 5.2. WAN Interface (P1)

In order to ensure the quality of the communication channels data, such as signal level, signal-to-noise ratio and bit errors must be provided.

Optionally, the electricity meter must be designed integrated or modular.

The electricity meter/module must be supplied with indicators showing the communication status by means of LEDs:

- Presence of communication for PLC
- Status (normal operation status or error status)

#### 5.2.1. Integrated WAN Interface PLC (C)

##### Physical layer

The connection of the meters and the communication equipment to the grid must take place in accordance with the technical instructions of the manufacturer.

The manufacturer must propose a technical solution (e.g. interference suppression filter), in order to eliminate any possible interferences in the client equipment, caused by electric devices.

##### Application layer

Own protocols of the electricity meters are allowed.

##### Security

P6	Концентраторите. Интерфейси за обмен на данни между Централната система и съществуващите системи или приложения на трети страни.
----	---

#### Електронен електромер

По принцип електромерите трябва да се конструират така, че заявки до един интерфейс да не могат да се препредават чрез друг интерфейс (изолация на портовете). Това означава, че даден неоправомощен достъп през сервисния интерфейс да не може да бъде използван за взломен достъп във WAN-интерфейса и по този начин да може да се използва WAN-мрежата.

#### 5.1. Сервизен интерфейс (P0)

##### Физически слой

Сервизният интерфейс трябва да се изпълни като оптичен интерфейс.

Скоростта на комуникация трябва да е минимум на 9600 бода.

##### Протоколен слой

Сервизният достъп до електромера трябва да се осигури чрез DLMS/COSEM, IEC 62056-21 или друг стандартен протокол. Допустимата опция трябва да се определи от оператора на мрежата.

##### Сигурност

Сигурността трябва да се осъществи в рамките на заданията на „Сигурност на електромера“.

Контролът на достъпа трябва да се осъществява чрез индивидуални пароли. Не е необходимо кодирането на предаването на данни поради изключително локалния достъп

#### 5.2. WAN Интерфейс (P1)

За осигуряване на качеството на комуникационните канали трябва да се предоставят данни като ниво на сигнала, отношение сигнал-шум и грешки на битове.

Опционално, електромерът трябва да се изгради интегриран или модулен.

Електромерът/модулът трябва да разполага с индикатори показващи комуникационния статус посредством LED:

- Наличие на комуникация при PLC
- Статус (нормално работно състояние или състояние на грешка)

#### 5.2.1. Интегриран WAN Интерфейс PLC (C)

##### Физически слой

Свързването на измервателните уреди и комуникационното оборудване към мрежата трябва да бъде съгласно техническите предписания на фирмата производител.

Фирмата-производител трябва да предложи техническо решение (напр. филтър за подтискане на смущенията), за да се отстранят евентуални влияния в съоръженията на клиента от електроуреди.

##### Приложен слой

Допускат се собствени протоколи на електромерите.

##### Сигурност

The security must be provided within the assignments of "Security of the electricity meter".

#### 6. Permission for commissioning, initial and follow-up inspection

##### 6.1. Type approval and MID certification

For the MID electricity meters it is necessary to specify the place of manufacturing, the certifying body and the notified body for monitoring the inspection. The offer must contain a certificate from a type test, including temperature correlation of the metrological errors and a declaration of conformity, both for each delivery and in case of a change in the version of the product of the manufacturer.

The electricity meter may also be approved for use in Bulgaria, by means of registration in the commercial meters logs.

##### 6.2. Parameterization software

A license is required for the parameterization software, supplied with all the available functions of the proposed electricity meter. When supplying the electricity meter, it must be accompanied by the parameterization software, in order to ensure full compatibility and functionality with the various parameter options. The license must include all the software updates for the lifetime of the electricity meter.

The media, containing the installation files can be freely selected (CD, USB etc.).

If necessary, the supply shall include all due training in working with the software, setting the parameters and the necessary data processing.

A contact person must be specified.

The parameterization software must be designed in a manner, ensuring the access to the electricity meter through the service interface. Therefore attention is to be paid to the option for encryption of the connection with the electricity meters.

##### 6.3. Calibration (and option for entering the test mode)

The status of the test mode (ON or OFF) for the calibration must be clearly displayed on the electricity meter by means of the service interface and the display.

The following commands, which may be transmitted by the test device through the service interface and executed by the electricity meter, must be available:

- Test mode ON
- Test mode OFF
- Settings the time/date
- Increasing the LED constant (for the metrological inspection)
- Display test (optional)
- Switching the LED for active/reactive energy (optional)
- Billing (optional).
- Switching the tariffs for metering energy and power (optional)
- Control relay ON (Except option)
- Control relay OFF (Except option)

##### 6.3.1. LED

Сигурността трябва да се осъществи в рамките на заданията в „Сигурност на електромера“.

#### 6. Допускане в експлоатация, първоначална и последваща проверка

##### 6.1. Одобрение на типа и MID сертифициране

При MID електромери е нужно да се посочат мястото на производство, акредитиращият орган и нотифицираният орган за наблюдение на проверката. В офертата трябва да се представят сертификат от типово изпитание, включително температурната зависимост на метрологичните грешки и декларация за съответствие, както с всяка доставка така и при промяна на версията на продукта от производителя. Електромерът може да бъде и одобрен за ползване в България посредством списване в регистъра на средствата за търговско измерване.

##### 6.2. Параметризиращ софтуер

Нужен е лиценз за параметризиращ софтуер, снабден с всички налични функции на предложения електромер. Със закупуването на електромера е нужно да се предостави и параметризиращия софтуер, така че да е възможна пълна съвместимост и функционалност с различните версии на параметрите. Лицензът трябва да включва всички софтуерни актуализации за времето на живот на електромера. Носителят на инсталационните файлове може да е свободно избран (CD, USB и др.) носител.

При необходимост трябва да се проведе обучение относно работата със софтуера, задаване на параметрите и необходимата обработка на данните. Необходимо е да се посочи лице за контакт.

Параметризиращият софтуер трябва да бъде проектирана така, че достъпът до електромера през сервисния интерфейс да е възможен. Следователно да се обърне внимание на възможността на криптиране на връзката с електромерите.

##### 6.3. Калибриране (и възможност за влизане в тестов режим)

Статус на тестовия режим (вкл. или изкл.) за калибриране трябва да бъде видимо показан на електромера чрез сервисния интерфейс и дисплея. Необходими са следните команди, които да могат да бъдат подадени от тестовото устройство чрез сервисния интерфейс и изпълнени от електромера:

- Тестов режим ВКЛЮЧЕН
- Тестов режим ИЗКЛЮЧЕН
- Настройка на час/дата
- Увеличаване на константата на светодиода (за метрологична проверката)
- Тест на дисплея (опционално)
- Превключване на светодиода за активна/реактивна енергия (по желание)
- Самоотчет (по желание)
- Превключване на тарифи за измерване на енергия и мощност (по желание)
- Реле за управление ВКЛЮЧЕНО (Без Позиция 3)
- Реле за управление ИЗКЛЮЧЕНО (Без Позиция 3)

##### 6.3.1. Светодиод

A standard optical head should enable the reading of pulses at any time.

It is preferable to use red and green LEDs. The execution of the LED must ensure the flawless reading of pulses with optical heads, which can be activated from a distance of 30mm. This function must be guaranteed in case of referenced (closed) electricity meters. If there is only a single LED on the electricity meter, it should be possible to switch the pulses between active and reactive power and back through an IR command. Alternatively, there may be two LEDs (for active/reactive energy).

#### 6.3.2. Position of the LEDs and the IR-interface

In order to ensure the flawless automatic calibration of the electricity meter, the LED to be calibrated and the IR-interface must be positioned in such a manner, as to enable the simultaneous inspection, respectively calibration of the electricity meter using these two elements.

#### 6.3.3. Sensitivity requirements and error allowances

The requirements, regarding the warm-up times, the values for the effects and the error allowances are determined in accordance with the requirements of the BMI on the inspection of Electricity Meters.

The additional errors in case of a temperature rise must be specified in the test report.

The electricity meters must meet these requirements, especially with respect to adhering to the admissible error allowances.

The electricity meters must be manufactured in such a manner that to enable the automatic inspection of metering points with standard test equipment.

#### 6.3.4. Inspection of the behaviour in operating mode

In operating mode the electricity meter must meet EN 62053-21 and the relevant requirements established in the Bulgarian Metering and Measurement Act.

The electricity meters must be designed and manufactured so that it is possible to perform both automatic inspection of the operating mode (by means of a LED) with the respective testing equipment, as well as inspection by means of visual control (e.g. the arrow indicating the power flow direction on the display).

The LED constant must be designed so that during a start-up test, at least 2 pulses can be registered in 10 minutes.

#### 6.3.5. Inspection of the behavior of the electricity meter in idle mode

In idle mode, the electricity meter must meet EN 62053-21 and the relevant requirements, set out in the Bulgarian Metering and Measurement Act.

The minimum duration of the test is calculated, applying the formula below.

During that test, at the output of the electricity meter not

Със стандартна оптична глава трябва да е възможно снемането на импулси по всяко време.

За предпочитане е използването на червени и зелени светодиоди. LED-изпълнението трябва да гарантира безпроблемното снемане на импулси с оптични глави, които могат да бъдат задействани на разстояние от 30mm. Тази функция трябва да е гарантирана при еталонирани (затворени) електромери. Ако налице е само един светодиод върху електромера трябва да е възможно превключването на импулсите между активна и реактивна енергия и обратно чрез IR команда. Алтернативно, възможно е наличието на два светодиода (за активна/реактивна енергия).

#### 6.3.2. Разположение на светодиодите и IR-интерфейса

За да се създаде възможност, за безпроблемно автоматично калибриране на електромера, предвиденият за калибрирането светодиод от една страна и IR-интерфейса от друга страна трябва да бъдат така разположени, че да може да се извърши едновременно проверка, респективно калибриране на електромера чрез двата елемента.

#### 6.3.3. Изисквания за чувствителност и допустими граници на грешката

Изискванията към времената на затопляне, величините на влияние и допустими граници на грешките се определят съгласно изискванията на БИМ за проверка на СИ

Допълнителните грешки при краткотрайно затопляне трябва да бъдат посочени в протокола от изпитанието.

Електромерите трябва да отговарят на тези изисквания, особено на спазването на допустимите граници на грешките.

Електромерите трябва да бъдат изработени така, че да е възможна автоматична проверка на измервателни точки със стандардни средства за проверка.

#### 6.3.4. Проверка на поведението в режим на работа

В режим на работа електромерът трябва да отговаря на EN 62053-21 и съответно на утвърдените изисквания в българския Закон за Измерванията.

Електромерите трябва да са така изработени, че да е възможна, както автоматична проверка на режима на работа (посредством LED) със съответна изпитвателна техника, така и проверка чрез визуален контрол (напр. на стрелката за посоката на енергията върху дисплея).

Константата на светодиода трябва да бъде такава, че при стартов тест да е възможно регистрирането на минимум 2 импулса за 10 минути.

#### 6.3.5. Проверка на поведението на електромера в режим на самоход (празен ход)

В режим на самоход електромерът трябва да отговаря на EN 62053-21 и съответно на утвърдените в българския Изисквания на Закон за Измерванията.

Минималната продължителност на теста се изчислява по долупосочената формула. По време на този тест на изхода на електромера не трябва да се регистрира



more than one pulse is to be registered.

$$\Delta t \geq \frac{600 * 10^6}{k * m * U_n * I_{max}} = [\text{min}] \text{for Class 1}$$

$$\Delta t \geq \frac{480 * 10^6}{k * m * U_n * I_{max}} = [\text{min}] \text{For Class 2}$$

k = Constant of the pulse output

m = Number of metering systems

Un = Rated voltage

I<sub>max</sub> = Rated current

The electricity meter must be designed and manufactured so that it is possible to perform both automatic inspection of the idling (by means of a LED), as well as inspection by means of visual control of the electricity meter. The LED must always be on, when the electricity meter has no load.

#### 6.3.6. Stability of the pulses of the LED

The calibration of the electricity meters requires pulses, proportional to the power.

#### 6.3.7. Test mode

The electricity meter must have a calibration mode. In this mode, the energy counters must have 3 digits after the decimal point (for indirect electricity meters – 4 digits), and when reading the data, the increased resolution of the energy counters must be taken into consideration.)

The increased resolution in the test/calibration mode is required in order to ensure the increased efficiency of the inspection.

#### 6.4. Metering, grid connection

##### 6.4.1. Precision class

Direct connection: at least MID Class A

Indirect connection: at least MID Class B

Optional: for reactive energy Class 2

##### 6.4.2. Two-way metering

It is necessary that the forward and reverse energy is recorded in separate energy logs (as an aggregate and according to tariffs). This applies to both the active, and the reactive power.

##### 6.4.3. Metering, irrespective of the direction of the field

The metering cannot be affected by fields with different rotation directions, which sometimes occur in the grid.

##### 6.4.4. Functionality monitoring (self-diagnostics, watchdog)

The watchdog function is designed to avoid damages to the electricity meter due to software failures. Such damages are avoided as the software notifies from time to time the watchdog function, that it still functions properly. At watchdog's command, the software is restarted. If the precision of the energy logs is disturbed, it is necessary to restore the values from the last 15 minute period before the error. Each restart of the watchdog timer must be recorded in the event logbook. The restarting must not take more than 10 seconds.

повече от един импулс.

$$\Delta t \geq \frac{600 * 10^6}{k * m * U_n * I_{max}} = [\text{min}] \text{за Клас 1}$$

$$\Delta t \geq \frac{480 * 10^6}{k * m * U_n * I_{max}} = [\text{min}] \text{за Клас 2}$$

k = Константа на импулсия изход

m = Брой на измервателните системи

Un = Номинално напрежение

I<sub>max</sub> = Номинален ток

Електромерът трябва да бъде изработен така, че да е възможна, както автоматична проверка на самохода (посредством LED), така и проверка чрез визуален контрол на електромера. LED-диодът трябва да свети винаги когато електромерът няма товар.

#### 6.3.6. Стабилност на импулсите на светодиода За калибриране на електромерите са нужни импулси, пропорционални на мощността

#### 6.3.7. Тестов режим

Електромерът трябва да има режим за калибриране. В този режим енергийните броячи трябва да имат 3 знака след запетаята (при индиректни електромери – 4 знака), и при отчитането на данните, увеличената резолюция на енергийните броячи трябва да се отчита.)

Увеличената резолюция в режим на тест/калибриране е нужна с цел по ефективна проверка.

#### 6.4. Измерване, свързване към мрежата

##### 6.4.1. Клас на точност

Директно свързване: най-малко MID Клас A

Индиректно свързване: най-малко MID Клас B

По желание: за реактивна енергия Клас 2

##### 6.4.2. Двупосочно измерване

Нужно е енергията в права и обратна посока да се отчита в отделни енергийни регистри (сумарно и по тарифи). Това е валидно както за активната, така и за реактивната енергия.

##### 6.4.3. Измерване, независимо от посоката на въртене на полето

Измерването не трябва да се влияе от полета с различни посоки на въртене, които понякога се появяват с мрежата.

##### 6.4.4. Мониторинг на функционалността (самодиагностика, watchdog)

Чрез използването на watchdog функцията трябва да се предотврати повреда на електромера чрез отказ на софтуера. Тази повреда се избягва като софтуера периодично уведомява watchdog функцията, че все още работи правилно. По команда на watchdog функцията е необходимо да се направи рестарт на софтуера. Ако точността на енергийните регистри е нарушена е нужно да се върнат стойностите от последният 15 минутен период преди грешката. Всеки рестарт на watchdog таймера трябва да се запише в дневника на събитията. Рестартирането не трябва да трае повече от 10 секунди.

#### IV. Data Concentrator

##### 1. General requirements

##### 1.1. Definition

The data concentrator is a compact device, which performs two-way data communication through PLC resp. wireless connection (interface P1) and the transfer of data stored, through remote interface (interface P4). These interfaces are used to transfer all data, commands and signals between the Head End System and the end devices.

Apart from that the data concentrator has a local interface for maintenance (P3) for setting the parameters, configurations and reading data.

Table 1: General requirements regarding Data Concentrator

Technical details	Minimum requirements
Installation	<ul style="list-style-type: none"> <li>Capabilities for installation through a DIN-bus or a three-point connection to the connection block of the electricity meter</li> </ul>
External antenna	<ul style="list-style-type: none"> <li>Connection of the external antenna by means of a SMA-connector</li> </ul>
Protection	<ul style="list-style-type: none"> <li>Minimum IP 40 (according to EN 60529)</li> </ul>
Air humidity	<ul style="list-style-type: none"> <li>5% to 90% relative humidity (without condensate)</li> </ul>
Power supply	<ul style="list-style-type: none"> <li>3 x 230/400 V (wide range: 140 V to max 260 V)</li> <li>Safety with a max. 16 A-fuse</li> <li>Connection up to max 2,5 mm<sup>2</sup> cross section of the conductor</li> </ul>
PLC - communication method	<ul style="list-style-type: none"> <li>Transfer method, compatible with CENELEC volume A</li> <li>Connection of up to 1.000 end devices</li> </ul>
Software	<ul style="list-style-type: none"> <li>Firmware upgrade can be performed both through the remote, as well as through the local interface.</li> </ul>
Temperature range	<ul style="list-style-type: none"> <li>Operating range: - 25°C to 55°C</li> <li>Storage and transfer range: - 25°C to 70°C</li> </ul>
Device Interfaces	<ul style="list-style-type: none"> <li>P2: PLC,</li> <li>P3: RS 232, Ethernet</li> <li>P4: RS 232, Ethernet, interface to a modular GSM/GPRS/UMTS-modem (SMA – connector for connection of the external</li> </ul>

#### IV. Концентратор на данни

##### 1. Общи изисквания

##### 1.1. Дефиниция

Концентратор на данни е компактно устройство, което осъществява двупосочна комуникация на данни чрез PLC респ. безжична връзка (интерфейс P1) и прехвърлянето на съхранените данни чрез дистанционен интерфейс (интерфейс G4). Чрез тези интерфейси се трансферират всички данни, команди и сигнали между централната система и крайните устройства.

Освен това Концентратор на данни има локален интерфейс за поддръжка (P3) за настройка на параметрите, конфигурации и отчитане на данни.

Таблица 1: Общи изисквания към Концентратор на данни

Технически данни	Минимални изисквания
Монтаж	<ul style="list-style-type: none"> <li>Възможности за монтаж през DIN-шина или триточково закрепване за клемния блок на електромера</li> </ul>
Външна антена	<ul style="list-style-type: none"> <li>Свързване на външна антена посредством SMA-конектор</li> </ul>
Защита	<ul style="list-style-type: none"> <li>Минимум IP 40 (съгласно EN 60529)</li> </ul>
Влажност на въздуха	<ul style="list-style-type: none"> <li>5% до 90% относителна влажност (без конденз)</li> </ul>
Захранване с напрежение	<ul style="list-style-type: none"> <li>3 x 230/400 V (широк диапазон: 140 V до макс. 260 V)</li> <li>Обезопасяване с макс. 16 А-предпазител</li> <li>Свързване до макс. 2,5 mm<sup>2</sup> напречно сечение на проводника</li> </ul>
PLC - метод за комуникация	<ul style="list-style-type: none"> <li>Метод за прехвърляне, съвместим с CENELEC том А</li> <li>Подвързване на до 1.000 крайни устройства</li> </ul>
Софтуер	<ul style="list-style-type: none"> <li>Промяна на фърмуера може да се извършва както през дистанционния, така и през локалния интерфейс.</li> </ul>
Температурен диапазон	<ul style="list-style-type: none"> <li>Работен диапазон: - 25°C до 55°C</li> <li>Граничен диапазон за съхранение и трансфер: - 25°C до 70°C</li> </ul>
Интерфейси на устройството	<ul style="list-style-type: none"> <li>P2: PLC,</li> <li>P3: RS 232, Ethernet</li> <li>P4: RS 232, Ethernet, интерфейс към модул GSM/GPRS/UMTS-модем (SMA – конектор за</li> </ul>

	antennas) • Optional S: RS 232, Ethernet
Conformity with standards	• CE-certification • EN 61000-6-4 • EN 50065-1
Network protocols	• TCP/IP, HTTP, FTP, SCP •
Built-in clock module / Time base	• Possible synchronization with NTP (Network Time Protocol) server • Alternative: synchronization with the Head End System

	свързване на външни антени) • Опционално S: RS 232, Ethernet
Съответствие със стандарти	• CE-сертифициране • EN 61000-6-4 • EN 50065-1
Мрежови протоколи	• TCP/IP, HTTP, FTP, SCP
Вътрешен часовников модул / Часова база	• Възможна синхронизация с NTP (Network Time Protocol) сървър • Алтернативно: синхронизация с централната система

## 1.2 Constructive requirements

### 1.2.1. General provisions

Based on its structural design and manufacturing, the data concentrator must be designed so that under specific operating and normal conditions of use, no hazards can occur. The following is to be provided in particular:

- safety of people in case of energizing voltage(the current conducting parts must be properly insulated)
- safety of people under the effect of high temperature
- safety and resistance to heat and fire
- protection against the penetration of solids, dust and water.

All parts, exposed to corrosion under normal operating conditions, must be efficiently protected. The protective layers must have sufficient strength, so that under the specific operating conditions, cannot be damaged by the weather conditions. These requirements are of decisive significance for the selection of the protection class.

### 1.2.2 Housing

Optional: housing, which may be sealed, so that the internal parts of the device are only accessible after breaking the seal(s). The removal of the cover of the housing should not be possible without using tools.

### 1.2.3 Protection class

It is preferable that the housings are made of recyclable insulating material (resistant to UV-radiation, resistant to the vapours from solvents), corresponding to protection class II.

Protection against the penetration of dust and water.

The concentrator must be of protection class at least IP 51 according to IEC 60529:

#### 1.2.3.1 Weather conditions

The operating temperature and the environmental temperature must be between -20 °C to + 60 °C.

The temperature range during storage must be between -25 °C and + 65 °C.

#### 1.2.3.2 Power supply

## 1.2. Конструктивни изисквания

### 1.2.1. Общо положение

Въз основа на своя конструктивен дизайн и производство Концентратор на данни трябва да бъде така проектиран, че при определени експлоатационни и нормални условия на употреба да не могат да възникнат опасности. По-специално трябва да се подsigури следното:

- безопасност на лицата от попадане под напрежение(тоководещите части да са надежно изолирани)
- безопасност на лицата при въздействия от повишена температура
- безопасност и устойчивост на топлина и огън
- защита срещу проникване на твърди тела, прах и вода.

Всички части, изложени на корозия при нормални условия на употреба, трябва да бъдат ефективно защитени. Защитните слоеве трябва да бъдат толкова устойчиви, че при определените условия на работа да не могат да бъдат повредени от атмосферните условия. Тези изисквания са от решаващо значение за избора на клас на защита.

### 1.2.2 Корпус

Опционално: корпус, който може да се пломбира, така че вътрешните части на уреда да са достъпни само след счупване на пломбата(ите). Отстраняване на капачката на корпуса не бива да бъде възможно без използването на инструмент.

### 1.2.3 Клас на защита

За предпочитане е корпусите да бъдат изработени от рециклируем изолационен материал (устойчив на UV-светлина, устойчив на изпаренията от разворителите), съответстващ на клас на защита II.

Защита срещу проникване на прах и вода.

Концентраторът трябва да разполага с най-малко IP 51 клас на защита съгл. IEC 60529:

#### 1.2.3.1 Климатични условия

Работната температура и температурата на околната среда трябва да бъдат между -20 °C до +6 0 °C.

Диапазонът на температурата при съхранение трябва да е между -25 °C до + 65 °C.

#### 1.2.3.2 Захранване

Стандартизирано номинално напрежение: 3x230/400 V;

Standardized rated voltage: 3x230/400 V; 50 Hz

Range of the allowances of the power supply: The grid part with rated voltage  $U_n = 230$  V is to be designed in such a manner that it can operate flawlessly in the following voltage range:

230 +/- 20% Volts; 50 Hz

3-phase power supply with a maximum cross section of the conductor 2,5 mm<sup>2</sup>.

The power supply connections are also used to ensure PLC-communication with all 3 phases.

The type of connection of the conductors at the terminals must ensure sufficient and permanent contact. The loosening of the conductors or their excessive heating are to be prevented. Bolted connections, ensuring electric contact, and screws, which can be tightened and loosened many times, during the useful life of the data concentrator, must have a threaded metal bushing.

The risk of corrosion, due to the different contact materials, must be minimized by means of a proper selection of these materials.

The electric connections must be performed in such a manner that the contact pressure is not determined by the insulation material.

#### 1.2.4 Frequency

The concentrator must be designed for rated frequency 50 Hz. They must operate flawlessly in the range of the allowances of  $\pm 2\%$  of the rated frequency.

When connecting terminals with various potentials, near each other, these are to be secured against accidental short circuit.

#### 1.2.5 Reverse effects within the grid

The data concentrator (incl. network device and modem) must be designed so that no excessive reverse effects may occur in the grid as higher harmonics. The observation of EN 61000-3-2 must be ensured.

#### 1.2.6 Protection against power surges

The data concentrator must be inspected using a surge of peak voltage 1,2/50  $\mu$ s according to EN 61000-4-5 Control level of sensitivity 3 with a maximum value of 2 kV (the preferred sensitivity level is 4 at 6 kV).

#### 1.2.7 Electromagnetic compatibility

Must meet the requirements according to EN 61000-4-3.

The data concentrator must be capable of suppressing radio interferences. It must not affect the grid parts by external electric and magnetic fields, which can usually be expected at the operating locations.

#### 1.2.8 Technical data plate

At least the following information must be included, clearly visible when the device is installed – without the use of any other auxiliary devices:

1.2.8.1. Unique device number

1.2.8.2. Barcode in accordance with the grid operator's specifications

1.2.8.3. Labeling the manufacturer and type

50 Hz

Диапазони на допустимо отклонение на захранването: Мрежовата част с номиналното напрежение  $U_n = 230$  V за предпочитане трябва да бъде така проектирана, че да може да се експлоатира безупречно в следния диапазон на напрежение:

230 +/- 20% Волта; 50 Hz

3-фазно захранване с максимум 2,5 mm<sup>2</sup> напречно сечение на проводника.

Захранващите връзки служат и затова, PLC-комуникация да се осъществява във всички 3 фази.

Видът на закрепване на проводниците в клемите трябва да осигури достатъчен и постоянен контакт. Трябва да е предотвратено разхлабването на проводниците или прекомерното им загряване. Болтови връзки, които правят електрически контакт, и винтове, които могат да бъдат многократно затягвани и разхлабвани по време на полезния живот на Концентратор на данни трябва да имат втулка (буksa) с резба от метал.

Опасността от корозия поради различни контактни материали следва да бъде сведена до минимум чрез правилен подбор на тези материали.

Електрическите връзки трябва да бъдат изпълнени така, че контактното налягане да не се определя от материала на изолацията.

#### 1.2.4 Честота

Концентраторът трябва да бъде конструиран за номинална честота 50 Hz. Трябва да могат да се експлоатират безупречно в диапазона на допустимо отклонение от  $\pm 2\%$  от номиналната честота.

Присъединителни клеми с различни потенциали, които са поставени близо една до друга, трябва да бъдат обезопасени против случайно късо съединение.

#### 1.2.5 Мрежови обратни въздействия

Концентратор на данни (вкл. Мрежови уред и модем) трябва да бъде така проектиран, че в мрежата да не възникват недопустимо високи обратни въздействия под формата на висши хармоници. Следва да се гарантира спазването на EN 61000-3-2.

#### 1.2.6 Защита от ударно напрежение

Концентраторът трябва да се проверява с вълна на ударно напрежение 1,2/50  $\mu$ s съгл. EN 61000-4-5 Контролна степен на чувствителност 3 при максимална стойност от 2 kV (за предпочитане степен на чувствителност 4 при 6 kV).

#### 1.2.7 Електромагнитна съвместимост

Трябва да отговаря на изискванията съгласно EN 61000-4-3. Концентратор на данни трябва да може да подтиска радиосмущенията. Не бива да оказва влияние върху мрежовите части чрез външни електрически и магнитни полета, които обикновено могат да се очакват в местата на експлоатация.

#### 1.2.8 Фирмена табелка за технически данни

Върху уреда трябва да се нанесат минимум следните обозначения, които да бъдат добре четливи и в монтирано състояние на уреда - без използването на други помощни средства:

1.2.8.1. Уникален номер на уреда

1.2.8.2. Баркод в съответствие със спецификациите на мрежовия оператор

1.2.8.3. Обозначаване от производителя и типа

1.2.8.4. Description of LEDs with statuses

1.2.8.5. Manufacturing year

1.2.8.6. Connection diagram

1.3 Interfaces

1.3.1 WAN interface (P5)

1.3.1.1 GSM/GPRS/UMTS - modem

The GSM/GPRS/UMTS-modem is an integrated or modular replaceable communication unit. In general the modular/replaceable solution is preferred.

TABLE 2: MINIMUM REQUIREMENTS - MOBILE RADIO-MODEMS

Technical details	Minimum requirements
Operating voltage	230 +/- 20% Volts; 50 Hz
Functionality	GSM/GPRS/UMTS-module for GSM-grids

THE GSM/GPRS/UMTS-MODEM MUST AT LEAST HAVE THE FOLLOWING INDICATIONS:

- Unique device number
- Barcode in accordance with the grid operator's specifications
- Labeling the manufacturer and type
- Manufacturing year

1.3.1.1.1. Modem functionality

The GSM/GPRS/UMTS-module must be suitable for all the GPRS-grids, currently in operation in Bulgaria. The output power must be at least 2W. The sensitivity must be -108 dBm the data transfer through the GSM-grid, must take place, using a minimum of 9600 Baud (V.32bis). The data must be compressed.

1.3.1.1.2. SMA – connector

It is preferable to provide a SMA-coupling for connection of the external antennas to the data concentrator, resp. the GSM/GPRS/UMTS-modem.

1.3.1.1.3. Selection of the operator of the mobile network

In the borderline areas, where several operators of mobile radio networks intersect, it is necessary to select the operator of the mobile radio network (blocking international roaming). However, in general, the modem must select the operator of the mobile radio network with the strongest signal in the region.

1.3.1.1.4. Parameterization

The modem must provide software parameterization settings or a terminal program. The respective adjustments must be accessible remotely. The parameterization must not be lost in case of power failure or loss of voltage. It must be possible to configure minimum 2 different APN settings.

1.3.1.1.5. Resetting

The modem must also perform an automatic reset of the GSM/GPRS/UMTS- module after certain time, preset by the user, so that in case of failure of the modem, the connection can be established again. If there are other options, these must be specified in the tender.

1.2.8.4. Описание на LEDs със статуси

1.2.8.5. Година на производство

1.2.8.6. Схема на свързване

1.3 Интерфейси

1.3.1 WAN интерфейс (P5)

1.3.1.1 GSM/GPRS/UMTS - модем

Под GSM/GPRS/UMTS-модем се разбира интегрирана или модулно заменяема комуникационна единица. Принципно се предпочита модулно/ заменяемо решение.

ТАБЛИЦА 2: МИНИМАЛНИ ИЗИСКВАНИЯ МОБИЛНИ РАДИОМОДЕМИ

Технически данни	Минимални изисквания
Оперативно напрежение	230 +/- 20% Volts; 50 Hz
Функционалност	GSM/GPRS/UMTS-модул за GSM-мрежи

GSM/GPRS/UMTS-МОДЕМЪТ ТРЯБВА ДА ИМАТ ПОНЕ СЛЕДНИТЕ ОБОЗНАЧЕНИЯ:

- Уникален номер на уреда
- Баркод в съответствие със спецификациите на мрежовия оператор
- Обозначаване от производителя и типа
- Година на производство

1.3.1.1.1. Функционалност на модема

GSM/GPRS/UMTS-модулът трябва да е подходящ за всички GPRS-мрежи, намиращи се в експлоатация в България. Изходната мощност трябва да бъде максимум 2W. Чувствителността трябва да бъде -108dBm. Прехвърлянето на данни чрез GSM-мрежата трябва да се извърши с минимум 9600 Baud (V.32bis). Трябва да се извърши компресиране на данните.

1.3.1.1.2. SMA – конектор

За предпочитане е да се предостави SMA-буksа за свързване на външни антени към Концентратор на данния съотв. GSM/GPRS/UMTS-модем.

1.3.1.1.3. Избор на оператора на мобилната мрежа

В граничните райони, където се пресичат няколко оператора на мобилни радиомрежи, е необходимо да се избере операторът на мобилната радиомрежа (блокиране на международен роуминг). По принцип обаче модемът трябва да избере оператора на мобилна радиомрежа с най-силен сигнал в региона.

1.3.1.1.4. Параметризация

Модемът трябва да може се настройва със софтуер за параметризация или терминална програма. Това трябва да бъде възможно и от разстояние. Параметризацията не трябва да се загубва в случай на отпадане на напрежението или прекъсване на захранването. Трябва да бъде възможно конфигуриране едновременно на минимум 2 различни APN настройки.

1.3.1.1.5. Reset (нулиране)

Модемът също така трябва да извърши автоматичен Reset на GSM/GPRS/UMTS-модула след зададено от потребителя време, така че при сив на модема след това отново да може да се осъществи връзка. Ако има други възможности, те трябва да бъдат посочени и



### 1.3.2. Interface to end devices - Last Mile (C)F

In order to ensure the communication channels, data regarding the remote reading must be provided, such as signal level, signal-to-noise ratio, noise level, bit errors ratio, table of routes, non-reading electricity meters, at what phase a certain electricity meter is installed.

#### 1.3.2.1. PLC

Communications technique using high frequency signals to transmit data over. Typical interface technologies are narrowband PLC communication networks, local wired networks. Regardless of the network paths of the specific implementation, special care on the security of the C interface is necessary to prevent unauthorized monitoring or intervention (see also Clause 5 Privacy and Data security).

### 1.3.3. Service interface (P3)

The data concentrator must have an interface, allowing, in case of inactive remote interface (due to an issued with a supplier or technical problems), taking into consideration preset access rights, the following commands/actions to be performed on the data concentrator, as well as on the connected end devices:

- a. Reading data
- b. Setting the clocks of the subordinate devices - according to those of the data concentrator
- c. Configuring the devices
- d. Firmware update

#### 1.3.3.1. Ethernet interface

- 1.3.3.1.1. 10/100 Base-T standard.
- 1.3.3.1.2. LAN RJ-45 standard jack
- 1.3.3.1.3. For a connection of category 5 cables

### 1.4. Execution

#### 1.4.1 Commissioning

In general, after establishing the communication, the data concentrator must initialize and carry out self-identification and automated inspection of the authenticity with the Head End System, in accordance with the framework security conditions. The time for establishing the communication with the remote interface must not exceed one hour.

### 1.4.2 On-site operational inspection

The data concentrator must have indication capabilities, displaying the most important operating conditions of the electricity transmission line and remote communication by means of LED indicators. The plate must clearly differentiate, by using symbols or names, the PLC and the status displayed as a result of the remote communication, in order to avoid any confusion.

In case of GSM/GPRS/UMTS-communication the level of the signal and any error messages are to be displayed.

описани в офертата.

### 1.3.2. Интерфейс към крайни устояства Last Mile (C)

За гарантиране качеството на комуникационните канали трябва да се осигурят за дистанционно отчитане данни като например ниво на сигнала, съотношение сигнал-шум, ниво на шума, коефициент грешки в битове, таблици за маршрути, не отчитащи се електромери, на коя фаза е монтиран даден електромер.

#### 1.3.2.1. PLC

Комуникационни техники използващи високочестотни сигнали за пренос на данни. Типични технологии за интерфейс са теснолентовата PLC комуникационни мрежи. Независимо от мрежови пътища на конкретното изпълнение следва да се осигури специално внимание върху сигурността за превенция върху неоторизиран мониторинг или интервенция (виж също клауза 5 от част Сигурност и защита на данните).

### 1.3.3. Сервизен интерфейс (P3)

Концентраторът на данни трябва да разполага с интерфейс, който да позволява, при неактивен дистанционен интерфейс (поради проблем с доставчик или технически проблем), като се вземат предвид предварително зададени права за достъп, да се извършват следните команди/действия върху Концентратор на данни, както и на присъединените крайни устройства:

- a. Отчитане на данни
- b. Сверяване на часовниците на подчинените устройства- според тези на Концентратор на данни
- c. Конфигуриране на устройства
- d. Промяна фърмуера

#### 1.3.3.1. Ethernet интерфейс

- 1.3.3.1.1. 10/100 Base-T стандарт.
- 1.3.3.1.2. LAN RJ-45 стандартна бухса
- 1.3.3.1.3. За връзка с кабели категория 5

### 1.4. Изпълнение

#### 1.4.1 Въвеждане в експлоатация

По принцип Концентратор на данни след създаване на комуникационна връзка трябва да инициализира и извърши самоидентификация и автоматизирана проверка на автентичността с централната система в съответствие с рамковите условия за сигурност. Времето за създаване на комуникация на дистанционния интерфейс трябва да се извърши в рамките на един час.

### 1.4.2 Оперативна проверка на място

Концентратор на данни трябва да разполага с възможности за индикация, които могат да указват най-важните експлоатационни състояния на електропровода и дистанционна комуникация посредством LED индикатори. На табелката трябва да има ясно разделение чрез символи или наименования между PLC и статуса показания от дистанционната комуникация, за да се избегнат обърквания.

В случай на GSM/GPRS/UMTS-комуникация трябва да бъдат показани нивото на сигнала и съобщения за грешки.

#### 1.4.3 Execution

The PLC network is organized independently, according to the framework conditions, set by the respective PLC system. It is possible to carry out both the PUSH and PULL commands automatically or manually.

In order to reduce the online time of communication between the data concentrator and the Head End System, the order of execution of the requests must be, as follows:

- 1.4.3.1. Establishment of a communication link between the Head End System and the data concentrator
- 1.4.3.2. Transmission of the reading command to all the electricity meters, connected to the data concentrator
- 1.4.3.3. Closing the communication link between the Head End System and the data concentrator
- 1.4.3.4. The data concentrator establishes a communication link with the Head End System
- 1.4.3.5. Transfer of all data from the data concentrator to the Head End System. After the successful transfer, the data is erased from the memory of the Data concentrator.

#### 1.4.4. Firmware update

By means of a remote interface it is possible to replace some parts of the software or the firmware. This process must be fully transparent. The safety aspect and the related volume of the keys must function even during firmware download.

The acceptance of new firmwares shall take place after the automatic inspection, whether the hardware components are compatible with the planned download. The control processes and automatic tests are to be provided. Routine inspections for damages and self-tests are provided.

The restoration of the system to the previous software must take place automatically in case of errors. In this case the newly installed firmwares must be deleted. This is to be communicated to the central control system.

### **V. IT security requirements for distant meter reading and control system for EVN EP (EVN Bulgaria Elektrorazpredelenie EAD)**

Definitions of expressions:

E-Meter – Intelligent electricity meter, which is connected to the distribution grid and uses communication technologies for data exchange with central software platform. This is technical device which is measuring energy consumption and uses latest modern technologies for remote data transfer in both directions.

Central system - It is an aggregation expression of all systems which are responsible for the administration and management of E-Meters. In that aspect it can include Head End System (HES) for control and provisioning of electrometers, module for management of collected meter information data, technology for data validation and reporting, interfaces with existing legacy application stack of the Contractor and adequate module (service) for

#### 1.4.3 Изпълнение

PLC мрежата се организира самостоятелно според рамковите условия, които задава съответната PLC система. Възможно е автоматично или ръчно да се извършват както PUSH, така и PULL команди.

За да се намали онлайн-времето за комуникация между Концентратор на данни и централната система, редът на изпълнение на заявките трябва да бъде както следва:

- 1.4.3.1. Изграждане на комуникационна връзка между централната система и Концентратор на данни
- 1.4.3.2. Предаване на командата за отчитане към всички електромери, присъединени към Концентратор на данни
- 1.4.3.3. Приключване на комуникационната връзка между централната система и Концентратор на данни
- 1.4.3.4. Концентратор на данния изгражда комуникационна връзка към централната система
- 1.4.3.5. Прехвърляне на всички данни от Концентратор на данния към централната система. След успешно прехвърляне, данните се изтриват от паметта на Концентратор на данни.

#### 1.4.4. Смяна на фърмуера

Посредством дистанционния интерфейс е възможно да се заменят някои части на софтуера или фърмуера. Този процес трябва да бъде напълно прозрачен. Аспектът на безопасност и с това свързания обмен на ключове трябва да функционира дори и при фърмуер даунлоуд.

Приемането на новия фърмуер става само след автоматична проверка дали хардуерните компоненти са съвместими за планирания даунлоуд. Трябва да бъдат осигурени рутинни процедури за проверки и самостоятелни тестове.

Връщане към предишния софтуер трябва да се извършва автоматично в случай на грешка. В този случай новоинсталираният фърмуер трябва да бъде изтрит. Всяка грешка при промяна на фърмуера трябва да се отрази в централната системата.

### **VI. Изисквания за сигурност за дистанционно отчитане на електромери и системи за управление за EVN EP (EVN България Електроразпределение ЕАД)**

Дефиниции и изрази:

Е-електромер – Интелигентен електромер, свързан с разпределителната мрежа разпределителната мрежа и използващ комуникационни технологии за обмен на данни с централна софтуерна платформа. Това представлява техническо устройство, което измерва потреблението на електроенергия и ползва най-модерните технологии за дистанционен пренос на данни и в двете посоки.

Централна система – това е общ израз, касаещ всички системи, които отговарят за администрирането и управлението на Е-електромерите. В тази връзка, терминът може да включва Главна система /Head End System (HES)/ за управление и осигуряване на електромери, модул за управление на събраните данни с информация от електромерите, технология за валидиране и отчитане на данни, интерфейси със

managing the cryptographic techniques in order to guarantee the resistance towards the cyber-attacks in process of communication/data exchange with E-Meter and concentrator.

**Concentrator** – It is a device which is responsible for PLC (power line communication) with the E-Meter and supports the data transport through GPRS environment to the Central system in both directions.

**HHU** – Portable handheld unit which can be used for maintenance tasks of Concentrator or E-Meter.

**PLC** – Power line communication which is compatible with European regulations.(CELENEC)

**End-To-End Security** – means, that the whole communication between the endpoints (endpoints lay in the central system and the E-Meter) is secured. It must not be possible for an unauthorized person to read or manipulate the transferred information.

**Cryptographic Service** – Will be a part of the central system. The cryptographic service can be an additional application within the central system or the functionality can be provided by another application (e.g. by the HES). The cryptographic service should provide additional mechanism to support the end-to-end security within the distant meter reading and control system and should also provide mechanism for secure storing the used cryptographic keys.

**Cryptographic key** – is a string of bits used by a cryptographic algorithm to transform plain text into cipher text or vice versa. This key remains private and ensures secure communication. Cryptographic keys could be symmetric or asymmetric. Symmetric encryption requires only one key, which is used to encrypt and decrypt data. Asymmetric encryption uses two different keys: one for encryption and one for decryption.

1. General architecture of distant metering and control system:

1.1 The transfer environment of metering data from E-Meter must be realized with GPRS or PLC (power line communication). The technical module which is responsible for communication with E-Meter must be installed in the same corpus of E-Meter. In case of usage of PLC communication, a Concentrator must be a part of communication chain with the E-Meter which must be capable to transfer/collect data and communicate with many E-Meters and after that to transfer the data to the Central system. The Concentrator must be able to use GPRS communication environment or Ethernet connection for establishing transfer channel with the Central system. The Central system must provide a cryptographic service with which the data transfer to/from Concentrator and E-

съществуващите системи на изпълнителя и подходящи модули (обслужващи) за управление на криптографските техники, за да се гарантира устойчивостта срещу кибер атаки в процеса на комуникация/обмен на данни с Е-електромера и концентратора.

**Концентратор** – Това е устройство, което отговаря за Комуникацията по силовия кабел /PLC/ с Е-електромера и подпомага преноса на данни чрез GPRS среда до Централната система в двете посоки.

**Преносим терминал** – преносим ръчен уред, който може да се използва за извършване на дейности, свързани с поддръжката на Концентратора или Е-електромера.

**PLC** – Комуникация по силовия кабел, която е съвместима с европейските регламенти и нормативни разпоредби.(CELENEC)

**Безопасност от край до край** – означава, че е обезопасена цялата комуникация между крайните точки (крайните точки са в централната система и електромера). Не трябва да е възможно неопълномощени лица да отчитат или да манипулират пренесената информация.

**Криптографско обслужване** – ще бъде част от централната система. Криптографското обслужване може да бъде допълнително приложение в централната система или функционалността може да се осигури от друго приложение (напр. от HES).

Криптографското обслужване следва да предоставя допълнителен механизъм, който да поддържа сигурността от край до край в рамките на системата за дистанционно измерване и управление и също така следва да осигури механизъм за безопасно съхраняване на използваните криптографски ключове.

**Криптографски ключ** – е редица битове, използвани от криптографски алгоритъм за преобразуване на обикновен текст в шифрован и обратното. Този ключ остава таен и гарантира сигурна комуникация. Криптографските ключове могат да бъдат симетрични или асиметрични. Симетричното криптиране изисква само един ключ, който се използва за криптиране и декриптиране на данни. Асиметричното криптиране използва два различни ключа: един за криптиране и един за декриптиране.

1. Обща архитектура на системата за дистанционно измерване и управление:

1.1 Средата за пренос на данните от измерването, получени от Е-електромерите, трябва да се реализира посредством GPRS или PLC (комуникация по силов кабел). Техническият модул, който отговаря за комуникацията с Е-електромера, трябва да бъде монтиран в корпуса на Е-електромера. При използване на PLC комуникация, Концентраторът трябва да бъде част от комуникационната верига с Е-електромера, който трябва да може да пренася /събира данни и да комуникира с множество Е-електромери и след това да прехвърли данните до Централната система. Концентраторът трябва да може да използва комуникационната среда GPRS за установяване на канал за пренос на данни с

Meter to be encrypted. The central system must support the encrypted storage of the unique E-meter cryptographic keys.

Централната система. Централната система трябва да осигури криптографските услуги, чрез които преносът на данни до/от Концентратора и Е-електромера ще бъде криптиран. Централната система трябва да подпомага криптираното съхранение на уникалните ключове на Е-електромера.

## 2. Description of logical interfaces (see pic.1):

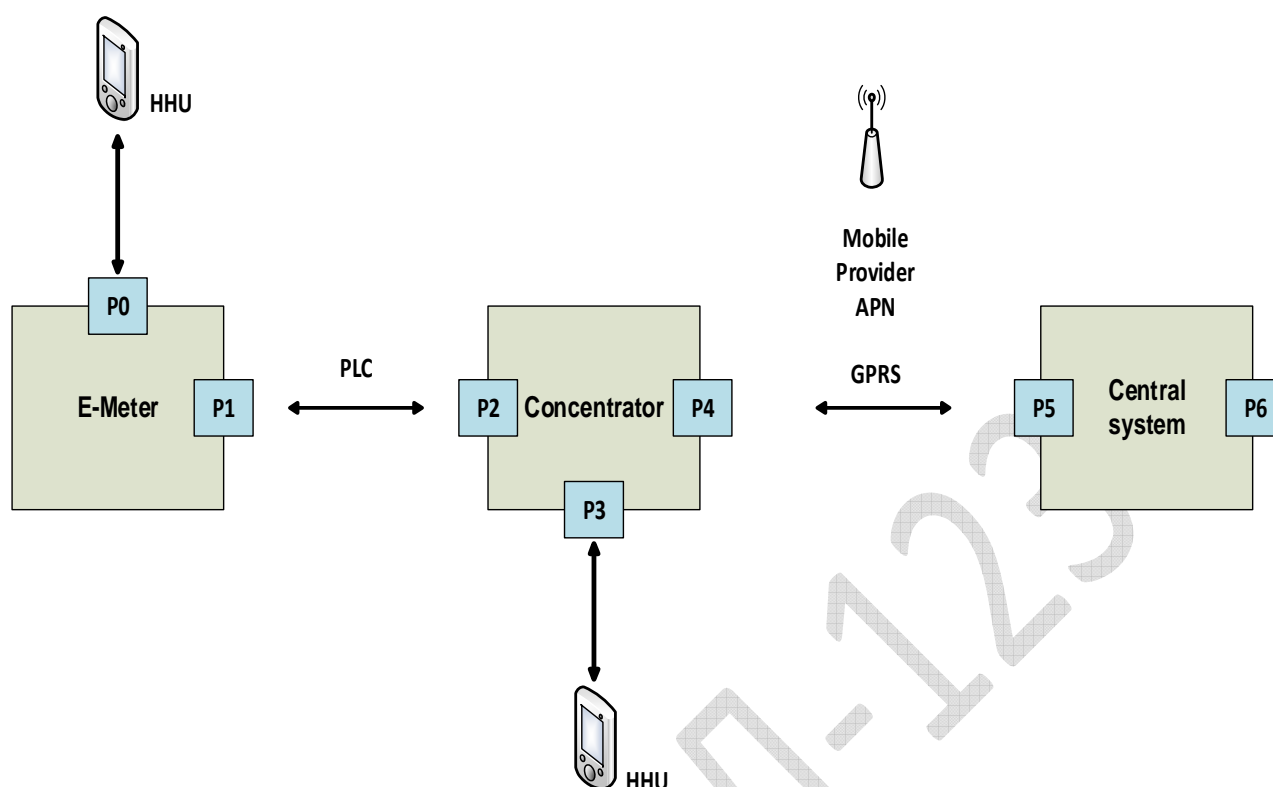
Interface	Description
P0	Infrared (IR) interface through which external maintenance tasks can be performed of E-Meter with external device (HHU).
P1	WAN interface of the meter must be able to handle PLC communication or GPRS communication when a GPRS meter will be used.
P2	PLC interface between data Concentrator and E-Meter.
P3	Interface through which external maintenance tasks can be performed of Concentrator with external device (HHU).
P4	Interface between data Concentrator and Central system using GPRS communication environment or Ethernet.
P5	WAN interface of Central system for communication with Concentrators.
P6	Interfaces for data exchange between Central system and existing legacy systems or third party applications.

pic.1

## 2. Описание на логическите интерфейси (виж илюстрация 1):

Интерфейс	Описание
P0	Инфрарчервен (IR) интерфейс, чрез който външни дейности по поддръжка могат да бъдат извършвани с Е-електромера, с помощта на външно устройство (Преносим терминал).
P1	WAN интерфейса на електромера трябва да може да се справи с PLC комуникацията или GPRS комуникация, когато се използва GPRS електромер.
P2	PLC интерфейсът между Концентратора на данни и Е-електромера.
P3	Интерфейс, чрез който могат да бъдат извършвани външни дейности по поддръжка с Концентратор с помощта на външно устройство (Преносим терминал).
P4	Интерфейс между Концентратора на данни и Централната система чрез използване на GPRS среда за комуникация или Ethernet.
P5	WAN интерфейс на Централната система за комуникация с Концентраторите.
P6	Интерфейси за обмен на данни между Централната система и съществуващите системи или приложения на трети страни.

Илюстрация 1



- |  |   |
|--|---|
| <p>3. Processing sensitive / personal data and IT security.</p> <p>3.1. Data information flow which is not needed must be not saved or recorded.</p> <p>3.2. Saved information which is not anymore important / needed must be deleted.</p> <p>3.3. Sensitive/personal data from E-Meter must be able maximum within 12 hours to be transferred and saved in Central system.</p> <p>3.4. Without permission, the unauthorized access to the data flow must be strictly prohibited.</p> <p>3.5. Unauthorized access to the protected channels (communication interfaces) must be not possible.</p> <p>3.6. The E-Meter must deliver reading out information from its registers if it is requested, with exception of alarms and defined critical events.</p> <p>3.7. In case of unexpected intervention in the data flow shown in pic.1 the grid operator must be alerted from a monitoring mechanism implemented in the central system.</p> <p>3.8. Passwords and cryptographic keys must be unique for each E-Meter in the process of exploitation from Central system.</p> | <p>3. Обработване на деликатни/лични данни и ИТ сигурност.</p> <p>3.1. Потокът на данни, които не са необходими, не трябва да бъде запазван или записван.</p> <p>3.2. Запазената информация, която вече не е важна/необходима трябва да бъде изтривана.</p> <p>3.3. Деликатни/лични данни от Е-електромер трябва да може в срок от не повече от 12 часа да се прехвърлят и запазват в Централната система.</p> <p>3.4. Без разрешение, неоторизирания достъп до данните трябва да бъде строго забранен.</p> <p>3.5. Всякакъв неоторизиран достъп до защитените канали (комуникационни интерфейси) трябва да е невъзможен.</p> <p>3.6. Трябва да е невъзможно получаването на непоискана информация отчетена от Е-електромерите, освен ако не става въпрос за аларми и предварително определени критични събития.</p> <p>3.7. В случай на неочаквана намеса в потока данни, както е показан на илюстрация 1 операторът на мрежата трябва да бъде предупреден чрез механизъм за контрол, вграден в Централната система.</p> <p>3.8. Паролите и криптографския механизъм (ключове) трябва да бъдат уникални за всеки Е-електромер в процеса на експлоатация на</p> |
|--|---|



## Централната система.

- 3.9. Commands for switch-off and switch-on for each E-Meter must be unique, encrypted and coded with the proper keys related to deployed cryptographic service.
- 3.10. IT security must be able to be managed from grid operator (distribution system operator).
- 3.11. The design and architecture of implemented IT security solution must be provided from bidder to EVN EP and also related processes in order to be able to be audited either from Contractor, or either from third party company. EVN EP will treat the received information with respected confidentiality.
4. The bidder (vendor) must support the audit of IT security of the whole system by EVN EP or by third party company in case of request from EVN EP.
- 4.1. In case of third party auditor, it must be independent from the bidder and will be chosen from EVN EP.
- 4.2. If necessary, the respective bidder must actively support the implementation of IT security audit by providing the necessary information and devices.
- 4.3. The bidder must provide human resources in the process of auditing the whole system from the contractor.
5. The following sensitive information must be solely transmitted with secured encrypted connection:
- 5.1. Personal information such as measurement data, etc.
- 5.2. Firmware updates.
- 5.3. Control commands (Switch on/off, set the Power limitation - if available).
- 5.4. Device settings and configurations.
6. All cryptographic keys must be located (stored) into the Central system, but only within a protected encrypted area or unexportable.
7. The Concentrator can store in it the cryptographic keys only for communication chain with the Central system and assigned E-Meters behind it. The cryptographic keys must be stored within a protected encrypted area or unexportable.
8. Each command from Central system to the E-Meter must be encrypted and must be executed only once
- 3.9. Командите за изключване и включване на всеки Е-електромер трябва да бъдат уникални, криптирани и кодирани с надлежните ключове, свързани с въведените криптографски услуги.
- 3.10. IT сигурността трябва да може да бъде управлявана от оператора на мрежата (оператора на електроразпределител-ната мрежа).
- 3.11. Конструкцията и архитектурата на приложеното решение за сигурност трябва да бъде предоставено от Участника на EVN EP, както и свързаните процеси, за да може да бъде подложен на одит от страна на Изпълнителя, или от трета страна. EVN EP третира всяка получена информация строго конфиденциално.
4. Участникът (продавачът) трябва да съдейства за одита на IT сигурността на цялата система, осъществяван от EVN EP или от трета страна, в случай, че EVN EP го поиска.
- 4.1. В случай, че трета страна е одиторът, тя трябва да е независима от участника и се избира от EVN EP.
- 4.2. Ако е необходимо, съответният участник трябва активно да подпомага въвеждането на одит на IT сигурността като предостави необходимата информация и човешки ресурси.
- 4.3 Участникът трябва да осигури човешки ресурси в процеса на одитиране на цялата система от страна на Изпълнителя.
5. Посочената по-долу деликатна информация трябва да се изпраща единствено по сигурна криптирана връзка:
- 5.1. Лична информация, като данни от измервания и т.н.
- 5.2. Актуализация на Фърмуер.
- 5.3. Контролни команди (Включване/изключване, определяне на ограничението за мощността – ако има такива).
- 5.4. Настройки и конфигурации на Устройството.
6. Всички Криптографски ключове трябва да бъдат съхранявани в Централната система, но само в рамките на защитената зона и да бъдат криптирани или неподлежащи на извличане.
7. Концентраторът може да се използва за съхраняване на Криптографските ключове, единствено за осъществяване на комуникационна верига с Централната система и съответните Е-електромери към нея. Криптографските ключове трябва да се съхраняват в рамките на защитена зона, криптирани или неподлежащи на извличане.
8. Всяка команда от Централната система към Е-електромера трябва да бъде криптирана и да се

towards the E-meter (Protection from Reply Attacks). Messages are accepted only from authenticated parties.

9. Cryptographic service within the central system:
- 9.1. All cryptographic methods used within the framework of the security solution (service) must be based on open and public available standards and must be considered by international organizations (like ENISA Document Algorithms Key Sizes and Parameter.
- 9.2. All used cryptographic algorithms need minimum to have cryptographic strength comparable to AES 128 (the cryptographic strength of an algorithm, for example, can be improved by increasing key length).
- 9.3. Unique cryptographic keys must be deployed in each E-Meter from the vendor.
- 9.4. For already installed E-meters the firmware update must be done in encrypted and secured communication channel. Guarantee must be available that firmware image was not manipulated and was issued by the vendor.
- 9.5. All passwords, which are implemented for E-Meter and data Concentrator, must meet the following minimum requirements:
- 9.5.1. Minimum length of 10 character
- 9.5.2. Composed of lowercase letters, uppercase letters and digit.
- 9.5.3. Randomly generated and not reproducible.
- 9.6. Passwords and cryptographic keys must be unique for each device (E-Meter or Concentrator), which are participating the process of encryption and decryption or messages for authentication.
- 9.7. Passwords and cryptographic keys, which can be used for encryption and decryption messages or for authentication of the communication data flow, must be generated with a cryptographically secure (pseudo) random number generator and not to be able to be reproduced. As an example of a possible implementation is made at this point to the following documents:
- 9.7.1. NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators.
- 9.7.2. BSI TR-02102 - Cryptographic module: recommendations and key lengths

This requirement must be obeyed on one hand for the initial installation and loading of E-Meters and on the other side in case of the regular exchange of keys that are in operation of already deployed E-Meters.

изпълнява само веднъж в посока Е-електромера (Защита от атаки чрез повторение). Съобщенията се приемат единствено от удостоверени страни.

9. Криптографски услуги в рамките на Централната система:
- 9.1. Всички криптографски методи, използвани в рамките на системата за сигурност, трябва да се основават на открити и обществено достъпни стандарти и трябва да бъдат разгледани от международни организации (като Размерите на ключовете и параметрите на алгоритми при криптиране на документи към ENISA).
- 9.2. Всички използвани криптографски алгоритми трябва да имат най-малко криптографската сила, сравнима с AES 128 (криптографската сила на алгоритъм, напр. може да бъде подобрен чрез увеличаване на дължината на ключа).
- 9.3. Уникални главни и оперативни ключове трябва да бъдат включени от търговеца към всеки Е-електромер.
- 9.4. За вече монтираните Е-електромерите, актуализацията на фърмуера трябва да се извършва чрез криптирани и сигурни комуникационни канали. Трябва да бъде дадена гаранция, че файлът с фърмуера не е манипулиран и е действително издаден от търговеца (дигитален подпис на файла с фърмуера, липса на неоторизирана промяна на ключа на търговеца в електромера).
- 9.5. Всички пароли, използвани за Е-електромер и Концентратора на данни, трябва да съответстват на следните минимални изисквания:
- 9.5.1. Минимална дължина - 10 символа.
- 9.5.2. Съставени от малки, главни букви и числа.
- 9.5.3. Генерирани произволно и не подлежащи на възпроизвеждане.
- 9.6. Паролите и Криптографските ключове трябва да бъдат уникални за всяко устройство (Е-електромер или Концентратор), което взема участие в криптирането и декриптирането или в съобщенията за валидиране.
- 9.7. Пароли и Криптографските ключове, които могат да бъдат използвани за съобщения за криптиране и декриптиране или за валидиране на комуникационните данни, трябва да бъдат генерирани произволно и да не подлежат на възпроизвеждане. Като пример за възможното използване, насочваме вниманието ви към следните документи:
- 9.7.1. NIST Специална публикация 800-90A – Препоръки за генериране на произволни числа, чрез използване на детерминистични генератори на произволни битове.
- 9.7.2. BSI TR-02102 - Криптографски модул: препоръки и дължина на ключовете
- Това изискване трябва да бъде спазвано при първоначалната инсталация и зареждане на Е-електромерите, като при редовна промяна на ключовете, за вече работещи Е-електромери.

- 9.8. All passwords which are participating the communication chain from Central system, Concentrator to E-Meter must be possible to be remotely changed from central system. Optional: if necessary, all operational cryptographic keys in the E-Meters could be changed on demand.
- 9.9. After installing the appropriate component (E-Meter or Concentrator), the initial used passwords must be changed. Optional if necessary all operational cryptographic keys in the E-Meters could be replaced on demand.
- 9.10. Secure backup and restore of data stored in the cryptographic service in central system must be possible.
- 9.11. Reporting and monitoring functions and representation of the current operating state of the cryptographic service must be available.
- 9.12. The cryptographic service should provide the following key management functions:
- 9.12.1. Import of the initial cryptographic keys from vendor, which for the operation of the cryptographic service are required.
- 9.12.2. Initial loading of cryptographic keys for encryption of communication for each E-meter in the central system database. All keys must be stored in encrypted and protected way into the environment of Central system.
- 9.12.3. Mutual authentication of E-Meter and Central System.
- 9.12.4. Encryption and decryption of messages.
- 9.12.5. Optional must be possible a process of renewing the operational cryptographic keys (key generation and distribution of operational cryptographic keys) from remote central system in case of necessity.
- 9.12.6 Support for a detailed investigation in case of defective E-Meters.
- 9.12.7 Operation and maintenance of cryptographic service.
- 9.12.8 Reporting and monitoring of system status.
- 9.12.9 Support a general key management procedure, which enables and supports safe operation of the Central system.
- 9.12.10 In case of successfully change of specific operational cryptographic key in E-Meter, all messages, news, commands which are secured with old key must no longer be accepted.
- 9.13 Transfer of cryptographic keys to the Concentrator and E-Meter must be done in a way that corresponds to the process of secured shipping (for example SSH, SCP, SFTP, HTTPS or other methods with minimum level of encryption AES 128). During the network
- 9.8. Всички пароли, които участват в кореспонденцията в рамките на Централната система, Концентратора и Е-електромера трябва да може да бъдат променяни дистанционно от централната система. Незадължителна характеристика: ако е необходимо, всички работни ключове в Е-електромерите могат да бъдат променени при поискване.
- 9.9. След монтаж на съответния елемент (Е-електромер или Концентратор), първоначално използваните пароли трябва да бъдат сменени. По желание, ако е необходимо, всички Криптографските ключове в Е-електромерите могат да бъдат заменени при поискване.
- 9.10. Трябва да е възможно сигурно съхранение на резервни копия и съответното възстановяване на данни, съхранявани криптографските части на централната система.
- 9.11. Трябва да има функции за докладване и контрол и представяне на текущото оперативно състояние на криптографските дейности.
- 9.12. Криптографската служба осигурява следните основни функции по управление на ключовете:
- 9.12.1. Въвеждане на първоначалните ключове, които се изискват за криптографските дейности.
- 9.12.2. Първоначално зареждане на основния и работните криптографски ключове за криптиране на комуникацията по всеки Е-електромер в базата данни на Централната система. Всички ключове трябва да се съхраняват в криптирана форма по защитен начин в базата данни на централната система.
- 9.12.3. Взаимно валидиране на Е-електромера и централната система.
- 9.12.4. Криптиране и декриптиране на съобщения.
- 9.12.5. По желание може да се включи и процес по подновяване на работните криптографски ключове (генериране на ключове и разпространение на работни Криптографските ключове) дистанционно от централната система при необходимост.
- 9.12.6 Съдействие за подробно разследване дефектни Е-електромери.
- 9.12.7 Работа с и поддръжка на криптографска услуга.
- 9.12.8 Отчитане и контрол на статуса на системата.
- 9.12.9 Съдействие за процедурите по общото управление на ключовете, което позволява и подпомага безопасната експлоатация на Централната система.
- 9.12.10 В случай, че успешно бъде променен конкретен експлоатационен криптографски ключ в Е-електромер, то не трябва повече да бъдат приемани никакви съобщения, новини, команди, обезопасени със стари ключове.
- 9.13 Прехвърлянето на Криптографските ключове в Концентратора и Е-електромера трябва да се осъществява по начин, който съответства на процеса по сигурното пазаруване (например SSH, SCP, SFTP, HTTPS или други методи с минимално равнище на

communication between the Central system, concentrators and E-meters must be established under method of authentication – password or certificate or public key or symmetric key can be used.

- 9.14 The cryptographic keys must be incorporated (imported) into the cryptographic service in advance defined process in order to be guaranteed the secure management of the keys.
- 9.15 Each E-Meter must be produced with embedded unique cryptographic keys and in the process of delivery a shipment file (list) must be delivered to EVN EP. The shipment file must contain the list of production information of E-Meters (serial number and etc.) and appropriate cryptographic keys for each E-Meter. The electronic delivery must occur in a defined format and must be transmitted to EVN EP via a secured channel. This delivery will be securely processed subsequently by the cryptographic service of the central system. That shipment file must be encrypted and can be decrypted only from the cryptographic service of Central system. Throughout the delivery process, it must be ensured that no unauthorized third party has an access to the cryptographic keys.
- 9.16 Optionally after commissioning and deployment of E-Meter, some of the factory embedded cryptographic keys could be replaced with new operational keys which are issued dynamically from the cryptographic service of Central system. The newly deployed keys must be used for operational communication with the E-Meter.
- 9.17 Optionally the cryptographic service must provide appropriate functions, which must randomly enable a generation of new E-Meter specific cryptographic operational keys, which can be used in the process of exploitation of E-Meter. In case of necessity the Central system (Cryptographic service) must be able to repeat the process of renewing the operational cryptographic keys for each E-Meter.
- 9.18 The following reporting functions must be available from the cryptographic service:
- 9.18.1 Periodic reporting must be possible about which key have been changed due to certain criteria in case of dynamic exchange of operational cryptographic keys for E-Meters.
- 9.19 If E-Meter is deinstalled (decommissioned) and if E-Meter and cryptographic service support a replacement process of operational cryptographic keys, all stored operational cryptographic keys must also be destroyed. Only authorized employees may be able to initiate such a deletion. Unused cryptographic keys must be no longer stored in E-Meter or Concentrator.
- криптиране AES 128). По време на мрежовата комуникация между Централната система, концентраторите и Е-електромерите може да се използва метод на валидиране – парола, сертификат, публичен ключ или симетричен ключ.
- 9.14 Криптографските ключове трябва да бъдат вградени в криптографската система чрез предварително определен процес, за да може да се гарантира сигурното управление на ключовете.
- 9.15 Всеки Е-електромер трябва да бъде произведен с вградени уникални Криптографски ключове и в процеса на доставка на EVN EP следва да се представи пътен лист. В пътния лист се съдържа информация за производството на Е-електромерите (сериен номер и т.н.) и съответните Криптографски ключове за всеки Е-електромер. Електронната доставка следва да се осъществи в предварително определен формат и трябва да бъде изпратена на EVN EP по сигурен канал. Тази доставка след това се обработва безопасно от криптографската система на Централната система. Този пътен лист трябва да бъде криптиран и може да бъде декриптиран единствено от криптографската система към Централната система. В рамките на целия процес по доставка трябва да се гарантира, че неоторизирани трети страни няма да имат достъп до Криптографските ключове.
- 9.16 По желание, след въвеждането в експлоатация и монтажа на Е-електромерите, някои от фабричните Криптографски ключове могат да бъдат заменени с нови работни ключове, които се издават динамично от криптографската система към Централната система. Нововъведените ключове трябва да се използват за оперативната комуникация с Е-електромера.
- 9.17 По желание криптографската система трябва да осигури необходимите функции, които произволно да осигуряват генерирането на нови специфични криптографски работни ключове за Е-електромерите, като тези ключове могат да се използват в процеса на експлоатация на Е-електромерите. При необходимост Централната система (Криптографската система) трябва да може да повтори процеса по подновяване на работните Криптографски ключове за всеки Е-електромер.
- 9.18 Криптографската система трябва да има възможност за изготвяне на следните отчети и доклади:
- 9.18.1 Трябва да е възможно изготвяне на периодични отчети за това, кои ключове са променени, поради определени критерии в случай на динамичен обмен на работните криптографски ключове за Е-електромерите.
- 9.19 Ако Е-електромерите бъдат демонтирани (изведени от експлоатация) и ако Е-електромерът и Криптографската система предлагат възможност за прилагане на процес по замяна на работните Криптографски ключове, всички запазени работни Криптографски ключове също трябва а бъдат унищожени. Единствено оторизирани служители имат право да инициират подобно унищожаване. Неизползваните Криптографски ключове не трябва да



9.20 If cryptographic service is allowing a replacement of operational cryptographic keys in the E-Meter, technical and organizational process measures must be possible to reduce the risk of accidental reset of cryptographic keys in E-Meter or Concentrator.

9.21 In case of availability of function for replacing of operational keys a unique process must be executed for deploying operational cryptographic key into a current E-Meter.

9.22 Cryptographic service is very critical for operation of whole Central system. Cryptographic service must be deployed with high availability architecture. The central system must provide a secure backup and restore capabilities for all stored cryptographic keys.

9.23 Cryptographic service should autonomously work without user interaction. Any operation upon sensitive information or operation of cryptographic service must be done in cooperation of two different employees. Separation of duties must be obeyed. All login attempts and user interactions have to be logged and generated protocol information must be protected against unauthorized manipulation. The log entries must be traceable to a unique user. The cryptographic service must further enable the implementation of different user roles.

9.24 Cryptographic service must generate an alarm in case of unauthorized use. It should provide appropriate reporting and monitoring functionality, which allows monitoring of current operating state.

9.25 The cryptographic service must provide at least the following information:

9.25.1 Current state of cryptographic service – for example initial delivery state, operational information, synchronization with redundant cryptographic service, discovering critical and not critical errors, discovered manipulation attempts as a result of occurred possible security incident, ... )

9.25.2 Detailed listing of all occurred during operation errors (like failed logon attempt with username ABC time XYZ)

9.25.3 Representation of all active cryptographic keys together with appropriate identification description and subsequently comparing mechanism whether redundant crypto module contains all keys too.

9.25.4 Representation of all authorized usernames with the respective designated permissions.

се съхраняват в Е-електромерите или Концентратора.

9.20 Ако Криптографската система може да заменя работните Криптографски ключове в Е-електромера, трябва да съществуват мерки, свързани с техническия и организационен процес, чрез които да се намали риска от случайно анулиране на Криптографските ключове в Е-електромера или Концентратора.

9.21 При наличие на функция за замяна на работните ключове, трябва да бъде приложен уникален процес, за прилагане на работни криптографски ключове спрямо действащите Е-електромери.

9.22 Криптографската система е от жизненоважно значение за функционирането на цялата Централна система. Криптографската система трябва да бъде изградена с архитектура, позволяваща висока производителност и достъпност. Централната система трябва да осигури сигурни механизми за запазване и възстановяване на резервни копия за всички запазени Криптографски ключове.

9.23 Ако се въведе криптографска услуга като допълнителна система, то тогава криптографската услуга би следвало да работи самостоятелно, без намесата на потребителя. Всякаква работа, по отношение на чувствителна информация или работа на криптографската услуга, трябва да се извършва съвместно от двама различни служителя. Задължително трябва да се спазва споделянето на задълженията. При опити за влизане в системата и работа с нея трябва да се реализират записи и да се генерират протоколи, които следва да бъдат защитени от неототоризирано манипулиране. Направените записи трябва да бъдат проследяеми до уникален потребител. Криптографската система трябва да позволява и прилагането на различни роли на потребителите.

9.24 Криптографската система трябва да генерира аларма в случай на неототоризирано използване. Тя трябва да предлага подходяща функционалност за отчетност и контрол, която да позволява контрол на текущото работно състояние.

9.25 Криптографската система трябва да осигурява най-малко следната информация:

9.25.1 Текущо състояние на криптографската система – например – състояние след първоначална доставка, оперативна информация, синхронизиране с допълнителни криптографски системи, откриване на критични и не-критични грешки, открити опити за манипулации в резултат на евентуален възникнал инцидент)

9.25.2 Подробен опис на всички възникнали грешки при работа (напр. успешно извършено запазване на резервно копие – час и дата XYZ, неуспешен опит за влизане в системата с потребителско име ABC – час и дата XYZ)

9.25.3 Представяне на всички активни Криптографски ключове, заедно със съответното описание за идентификация описание и последващо сравнение, за това дали резервния крипто модул също съдържа всички ключове.

9.25.4 Представяне на всички ототоризирани потребителски имена със съответните им



9.26 The access to the user interface (GUI) of the cryptographic service must be available only through defined and approved secure computers, if the cryptographic service is embedded as an additional system.

9.27 In the process of provisioning of new releases by the manufacturer (vendor) the following requirements must be fulfilled:

- 9.27.1 Support for all already used cryptographic methods also in the new release must be available;
- 9.27.2 Uninterrupted operation is secured in the process of update;
- 9.27.3 Delivery of documentation in which all new features and changes are documented.

9.27.4 EVN EP itself can decide whether and when a new release will be implemented or not.

9.27.5 Training must be provided for the new version

9.28 The Shipment file from the vendor, which must contain (master data of E-Meters, unique cryptographic keys for each E-Meter) must be signed with the private key of the meter manufacturer and encrypted. The received shipment file must be directly imported into the Central system and after that a decryption process to be started. See pic2.

разрешителни и права.

9.26 Достъпът до потребителския интерфейс (GUI) на криптографската услуга трябва да е възможен единствено чрез определени и доказано сигурни компютри, ако криптографската услуга е внедрена като допълнителна система.

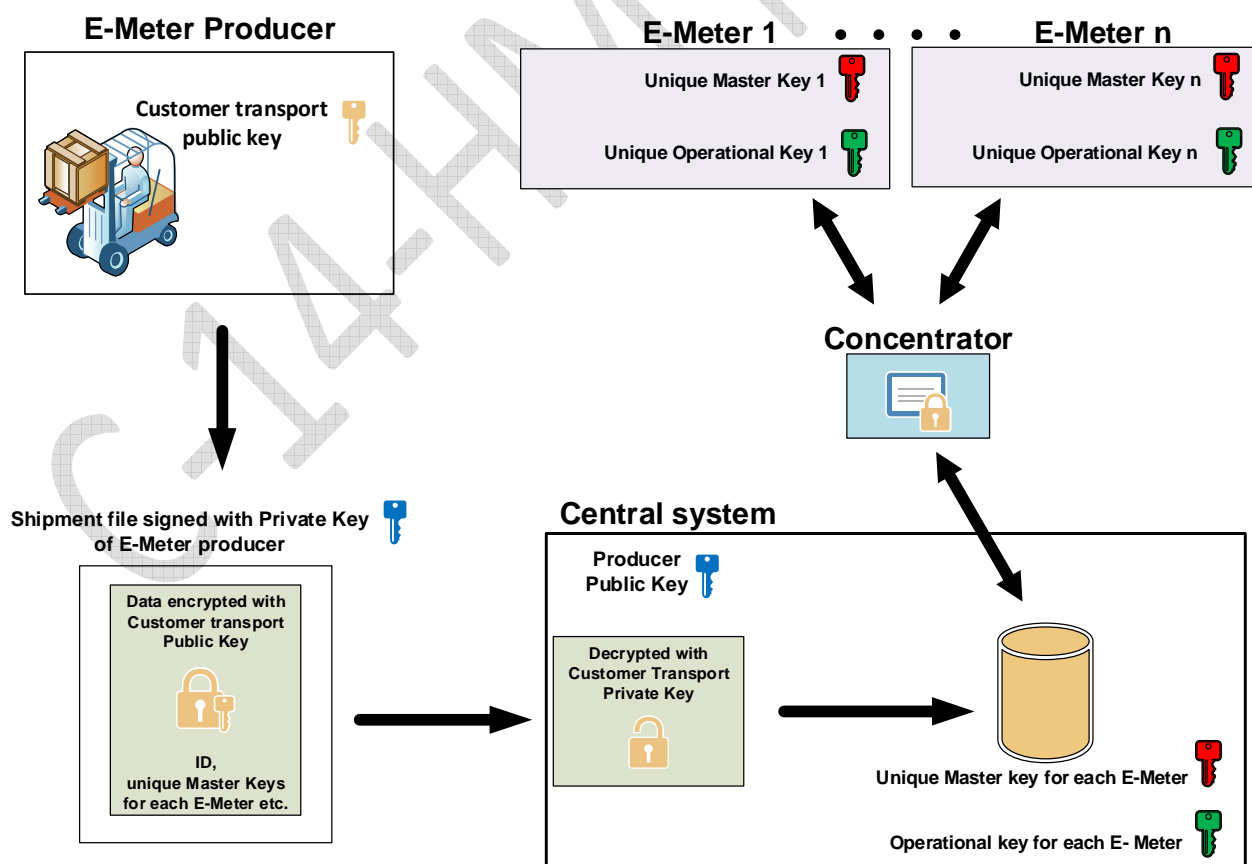
9.27 В процеса на прилагане на нови версии, предоставяни от производителя (продавача), трябва да бъдат изпълни следните изисквания:

- 9.27.1. Трябва да има поддръжка на всички вече използвани криптографски методи и в новата версия;
- 9.27.2. Непрекъснатото функциониране е обезпечено по време на процеса на актуализация;
- 9.27.3. Представяне на документация, в която са описани всички нови елементи, характеристики и промени.

9.27.4 EVN EP само може да вземе решение дали и кога да приложи определена нова версия.

9.27.5 Трябва да бъде осигурено обучение за работа с новата версия

9.28 Пътният лист от продавача, който трябва да съдържа (основни данни за Е-електромерите, уникални Криптографски ключове за всеки Е-електромер) трябва да бъде подписан със собствения ключ на производителя на електромерите и да бъде криптиран. Получения пътен лист следва да бъде директно въведен в Централната система и след това трябва да започне процесът по декриптиране. Виж илюстрация(Фигура) 2.



Pic.2\_Фигура.2

9.29 Optionally the cryptographic service of central system

9.29. По желание криптографската услуга на

must support implementation of external Hardware Security Module (HSM) for storing cryptographic keys in a secured way.

10. General requirements for Concentrator:

10.1 The Concentrator must have only one maintenance interface. (port P3)

10.2 The Concentrator must not be able to be configured through port P2. If there is a compromised E-Meter, it must be not possible to edit the configuration in the Concentrator based upon the credentials from the E-Meter.

10.3 The Concentrator must be able to be configured through port P4 from the central system.

10.4 The configuration of data Concentrator via a local interface port P3 must be adequately protected against attacks.

10.5 If the Concentrator has to use the local maintenance interface for reconfiguration or other maintenance activities, a unique combination of username and password must be possible for authentication, which corresponds to the defined password policy.(see point 9.5). Record of the event must be logged in it.

10.6 From maintenance port P3 of Concentrator must be not possible to reach protected area of cryptographic keys, which are eventually stored in it.

10.7 The unauthorized attempt for access to a data concentrator must be reported (viewed) by security measures from monitoring service of central system. Record of the event must be logged in it.

10.8 Each concentrator must be able to communicate over PLC technology with at least 1000 pieces of E-meters which are directly assigned to it.

10.9 The credentials for the automatic registration in a mobile network must be unique for every Concentrator. It is not permitted the usage of general login information contained by several units together.

10.10 The credentials for the automatic registration in mobile network may be saved only in Concentrator. The login Information must be not stored in the SIM card itself.

10.11 The mobile service provider will allow traffic only between central system and concentrator. Data traffic between concentrators will be prevented by appropriate routing rules.

10.12 If one data concentrator will be compromised by an attacker, the attacker should not be able to reach other data concentrators from the compromised data concentrator.

11. Performance requirements:

11.1 All installed E-Meters must be read out once per day.

централната система трябва да поддържа въвеждането на външен Модул за Хардуерна Безопасност (HSM) за съхраняване на криптографски ключове по безопасен начин.

10. Общи изисквания за Концентратора:

10.1 Концентраторът трябва да разполага само с един интерфейс за поддръжка. (порт 3)

10.2 Концентраторът не трябва да може да бъде конфигуриран през порт P2. При Е-електромер с нарушена сигурност, трябва да не е възможно да се редактира конфигурацията на Концентратора, въз основа на правата и данните за достъп, получени от Е-електромера.

10.3 Концентраторът трябва да може да бъде конфигуриран чрез P4 от централната система.

10.4 Конфигурирането на Концентратора на данни чрез местния интерфейс порт P3 трябва да бъде достатъчно надеждно защитено от атаки.

10.5 Ако се налага Концентраторът да използва местен интерфейс за поддръжка за преконфигуриране или други дейности по поддръжка, уникална комбинация от потребителско име и парола трябва да бъдат използвани за валидиране, като те трябва да съответстват на определената политика за паролите. (виж т. 9.5). Трябва да бъде извършен запис за съответното събитие.

10.6 От порт за поддръжка P3 на Концентратора не трябва да е възможен достъп до защитените зони на Криптографските ключове, които евентуално се съхраняват в него.

10.7 Неоторизирани опити за достъп до Концентратора на данни трябва да бъдат докладвани (разглеждани) чрез мерките за сигурност от направлението за контрол на централната система. Задължително се прави запис в архива за съответното събитие.

10.8 Всеки концентратор трябва да може да комуникира чрез технологията PLC с не по-малко от 1024 бр. Е-електромери, за които отговаря.

10.9 Данните за достъп при автоматична регистрация в мобилна мрежа трябва да бъдат уникални за всеки Концентратор. Не се допуска използване на обща информация за влизане в системата, едновременно от няколко единици.

10.10 Данните за достъп при автоматична регистрация в мобилна мрежа, могат да бъдат запазвани единствено в Концентратора. При използване на SIM карта, информацията за влизане в системата не трябва да бъде съхранявана на самата SIM карта.

10.11 Доставчикът на мобилни услуги следва да допуска трафик единствено между централна система и концентратора. Трафикът на данни между концентраторите се предотвратява чрез подходящи правила за маршрутизация.

10.12 Ако даден концентратор на данни е компроментиран от хакер, не би следвало хакерът да може да стига до други концентратори на данни от компроментирания концентратор на данни.

11. Изисквания относно работните характеристики:

11.1 Показанията от всички монтирани Е-електромери

In case of E-Meters with load profile, 15 minutes load profile must be read with all 96 values for it. In the final stage of implementation about 500 000 E-Meters must be able to be read out from the central system. The reading activity has to start at 00:00h and finish till 12:00h at the same day and all read data to be transported in the central system. In addition event information must be transported from E-Meters and Concentrators also within that period to central system.

11.2 The architecture of the Central system must be able to be extended till 1500000 E-Meters with the same KPIs (key performance indicators) defined in point 11.1.

11.3 Success rate must be minimum 98% of all installed E-Meters to be readout within defined time frame in point 11.1.

11.4 The cryptographic service is a highly critical component in the future of entire Central system infrastructure. The high availability requirements for the cryptographic service must be like all components of the E-Meter infrastructure. The availability of the central system environment needs to be 99.99% under a 24/7/365 window per year base. (Unplanned downtime max. 53 minutes per year)

11.5 A (geographical) redundant design and architecture as well as providing the relevant Fail Over functionality must be available of the central system.

11.6 Cryptographic service must be so designed in a way that not only the productive instance of the central system, but also a test system (environment) can use its functionalities.

11.7 The Bidder must propose adequate IT architecture which refers to requirement in point 11.1 for productive environment of central system.

12. E-Meter:

12.1 Only physical interface P0 can be accessible without removing the cover of E-Meter.

12.2 The E-Meters must be able automatically to record the events related to the process of opening the meter housing or terminal cover is detected and to send notification to the corresponding central system and store it in the registry(memory) of E-Meter.

12.3 The counter values and terminal cover must be suitable protected from unauthorized physical intrusion. Manipulation attempts upon the E-Meter itself or at the interfaces must be optically visible (for example, broken seals).

12.4 The built-into E-Meter - microcontrollers, processors are usually with appropriate interfaces (like JTAG - IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture) provided which are allowing programming

трябва да бъдат снемани веднъж дневно. В случай че Е-електромерите имат профил на товара, трябва да бъде отчетен профила на товара за 15 минути, заедно с всички 96 стойности. В окончателните етапи на въвеждане трябва да могат да бъдат отчетени около 500 000 Е-електромера. Дейностите по отчитането трябва да започват в 00:00 ч и да приключват в 12:00 ч. в същия ден, като всички отчетени данни се прехвърлят в Централната система. Освен това трябва да бъде генерирана информация за събитията през този период.

11.2 Архитектурата на Централната система трябва да може да бъде разширявана до достигане на 1 500 000 Е-електромера с едни и същи основни показатели за дейността (KPI), както е посочено в т. 11.1.

11.3 Процентът на успеваемост трябва да бъде минимум 98% от всички монтирани Е-Електромери.

11.4 Криптографската услуга представлява жизненоважен компонент за бъдещето на инфраструктурата на цялата Централна система. Високите изисквания за достъпност, по отношение на криптографската услуга трябва да са като всички компоненти на инфраструктурата на Е-електромерите. Достъпността на средата на централната система трябва да достига 99.99% 24 часа в денонощието, 7 дни в седмицата, 365 дни в годината. (непланирано спиране на работата се допуска за не повече от 53 минути годишно).

11.5 (Географски) съкратената структура и архитектура, както и осигуряването на съответната функционалност Възстановяване след Срив трябва да са налични на централната система.

11.6 Криптографската система трябва да е разработена така, че не само продуктивната част на Централната система, а и тестовата система (среда) да могат да се възползват от нейната функционалност.

11.7 Участникът трябва да предложи съответната IT архитектура, която се отнася за изискването в т. 11.1 за продуктивна среда на централната система.

12. Е-електромер:

12.1 Единствено физически интерфейс P0 може да се ползва да достъп без отстраняване на капака на Е-електромера.

12.2 Е-електромерите трябва да могат автоматично да записват събитията, свързани с процесите по отваряне на корпуса на електромера или капака на клемния блок, и да изпращат известия до съответната централна система и да ги съхраняват в регистъра (паметта) на Е-електромера.

12.3 Насрещните стойности и капака на клемния блок трябва да бъдат надлежно защитени от неоторизирано физическо проникване. Опити за манипулации върху самия Е-електромер или върху интерфейсите трябва да се виждат оптически (напр. нарушени пломби).

12.4 Вградените в Е-електромера елементи - микроконтролери, процесори обикновено разполагат с подходящи интерфейси (като JTAG - IEEE 1149.1 Стандартен порт за достъп при изпитване и и

or debugging of the respective components. These interfaces are required, for example in the process of production of E-Meter. All hardware interfaces, which can be used immediately for programming or debugging after the production of E-Meter must be disabled.

12.5 E-Meter must also preserve a secure state when errors and unwanted or unintended operating states (random or willfully) are caused.

Examples of such errors are:

- voltage loss
- integrity error
- self-test error of E-meter
- error in the process of executing cryptographic functions
- error in process of validating access permissions
- error in data entry (wrong data formats, incorrect data field length,
- invalid commands, etc.)
- error in the operation of the local cryptographic keys

12.6 The memory for the system log must be with adequate size, which ensures that no system log messages can be overwritten before they are read out by a central system. A minimum storage for minimum 100 events must be available in it.

12.7 The cryptographic key(s) must be itself safely stored in the E-meter. It must be not possible to be read in plain text or exported.

12.8 The E-meter must have internal clock and at periodic intervals must be synchronized with the central system

12.9 The E-meter manufacturer must disclose (declare) before the first delivery, which components and types (like communication module or unit of measurement) are installed in E-meter as well as from which suppliers these components are coming. The configuration of the E-meter must be provided to EVN EP. Subsequent changes of the configuration (for example change of supplier of built-in chips and etc.) are only permitted if EVN EP previously was notified in written form and if EVN EP agrees.

12.10 The communication on all interfaces of the E-Meter must be done in a way to guarantee and protect the confidentiality and integrity. The availability of the information from E-Meter must be guaranteed at all the time.

12.11 At all bidirectional interfaces of E-Meter only messages must be accepted which are previously defined for each port from the vendor. Before a message is accepted, it must be validated and accuracy to be checked. Messages that do not pass this test must be

Архитектура за сканиране на граничните повърхности), които позволяват програмиране или проверка за неизправности и ремонт на съответните компоненти. Тези интерфейси са необходими, например в процеса на производство на Е-електромера. Всички хардуерни интерфейси, които могат да се използват непосредствено за програмиране или разрешаване на проблеми, след производството на Е-електромера трябва да бъдат изключени.

12.5 Е-електромерът трябва да запазва сигурността си и при наличие на грешки или възникване на нежелани или неволно предизвикани работни състояния (случайно или злоумишлено причинени).

Примери за подобни грешки са:

- загуба на захранване
- грешка, свързана с целостта електромера
- грешка при самотестуване на Е-електромер
- грешка в процеса на изпълнение на криптографски функции
- грешка в процеса на валидиране на достъпа
- грешка във въведените данни (грешен формат на данни, неправилна дължина на полето с данни, невалидни команди и т.н.) - грешка в ориентацията на локалните Криптографски ключове

12.6 Паметта за регистъра на системата трябва да бъде с достатъчна големина, което гарантира невъзможността за записване на нови съобщения за системния регистър, върху съществуващи такива, преди да бъдат прочетени от централната система. Минималната памет, която трябва да е налична е за 100 събития.

12.7 Криптографските ключове трябва да бъдат съхранявани по сигурен начин в Е-електромера. Не трябва да е възможно да бъдат прочитани или записвани на друг носител.

12.8 Е-електромерите трябва да разполагат с вграден часовник и периодично трябва да бъдат синхронизирани с Централната система

12.9 Производителят на Е-електромерите трябва да разкрие (декларира) преди първата доставка, които компоненти и типове (като комуникационния модул или измерващия блок) са инсталирани в Е-електромер, както и от кои доставчици са набавени тези компоненти. Конфигурацията на Е-електромера трябва да бъде представена на EVN EP. Последващи промени в конфигурацията (напр. промяна на доставчика на вградените чипове и т.н.) се допускат единствено, ако EVN EP е било предварително уведомено в писмен вид и е приело промяната.

12.10 Комуникацията по всички интерфейси на Е-електромера трябва да се осъществява по начин, който гарантира и защитава конфиденциалността и почтеността. Достъпът до информацията в Е-електромера трябва да бъде гарантиран по всяко време.

12.11 При всички двупосочни интерфейси на Е-електромера трябва да бъдат приемани единствено съобщения, които са предварително дефинирани за всеки порт, от страна на доставчика. Преди приемане на съобщение, то трябва да бъде валидирано и

discarded.

12.12 If E-Meter is installed, but no communication link with the central system is established, the E-meter must operate as a standard electronic meter. Basic functions must be possible such as:

12.12.1 Unencrypted reading out of data stored in the counter register values and the load profiles. (port P0 can be used by HHU)

12.12.2 Unencrypted reading out of data stored in the counter event log entries (port P0 can be used by HHU)

12.12.3 Set the Date and Time. (port P0 can be used by HHU)

12.13 The E-Meter must be initially loaded with a firmware image in the process of its production from the vendor.

12.14 Manipulation of a custom portion of the firmware or of the contained firmware settings must not be possible.

12.15 Firmware update must be possible from the central system and must not influence the metrological part of E-Meter. The integrity of the firmware updates must be protected at least by hash code of the downloadable file which is sent through a unicast (one to one) authenticated and encrypted message and the E-Meter must not activate downloading process without having received the authenticated hash code.

12.16 In case of corruption of the update firmware operation, the operation must not affect the respective component and E-Meter must continue to operate with old firmware.

12.17 The metered data (stored data – counter values, events and configuration) are not allowed to be changed or deleted during the process of update of the firmware.

12.18 Unnecessary functions of the firmware of E-Meters must be explicitly disabled.

12.19 The vendor of E-meter must ensure that only a firmware image which is derived from the associated E-meter manufacturers has been released by a defined approval process.

12.20 The vendor during the research and development of components which are installed in E-Meter must have a detailed documentation. In case of discovery of vulnerabilities in firmware and software in context of internal quality checks they must be recorded. All measures taken into account for filling the gaps must be documented. That documentation must be provided to EVN EP in written form, if it is requested.

истинността му да бъде проверена. Съобщения, които не преминат тази проверка, не трябва да бъдат отваряни.

12.12 Ако Е-електромерът е монтиран, но няма комуникационна връзка с Централната система, Е-електромерът трябва да работи като стандартен електронен електромер. Трябва да са възможно основни функции, като:

12.12.1 Некриптирано отчитане на данните, съхранявани в насрещните регистрирани стойности и профилите на товарите. (порт P0 може да бъде използван с Преносим терминал)

12.12.2 Некриптирано отчитане на данните, съхранявани в записите в регистъра на събитията (порт P0 може да бъде използван с Преносим терминал)

12.12.3 Настройване на датата и часа. (порт P0 може да бъде използван с Преносим терминал)

12.13 Е-електромерът трябва първоначално да бъде зареден с дигитално подписан фърмуер в процеса на своето производство от продавача.

12.14 манипулирането на определена част от фърмуера или на настройките на фърмуер трябва да е невъзможно.

12.15 Трябва да е възможно и актуализиране на фърмуера чрез Централната система. Коректността на актуализациите на фърмуера и самоличността на подписаните актуализациите трябва да бъдат проверени чрез цифровия подпис. Ако новия фърмуер не е дигитално подписан, той не трябва да бъде ползван.

12.16 В случай на повреда при инсталирането на актуализацията на фърмуера, започналата операция не трябва да влияе съответните компоненти и Е-електромера трябва да продължи да работи със стария фърмуер.

12.17 Измерените данни (съхранени данни – стойности от брояча, събития и конфигурация) не могат да бъдат променяни или трети в процеса на актуализация на фърмуера.

12.18 ненужните функции на фърмуера на Е-електромерите трябва изрично да бъдат деактивирани.

12.19 Фърмуерът на Е-електромера трябва да бъде цифрово подписан, така че автентичността и неприкосновеността на фърмуера гарантират, че той действително е разработка на производителите на Е-електромера и се предоставя след преминаване на обстоен процес по одобрение и след полагане на електронен подпис.

12.20 При научно-изследователската си дейност, свързана с компонентите, монтирани в Е-електромера, продавачът трябва да разполага с подробна документация. При разкриване на слабости във фърмуера и софтуера, в контекста на вътрешните проверки на качеството, същите трябва да бъдат регистрирани. Всички мерки, предвидени за запълване на непълноти, трябва да бъдат документираны. Тази документация трябва да се



- 12.21 The manufacturer or supplier of the software or firmware has to confirm by a written agreement that measures have been taken that availability of backdoors in the firmware are strictly prohibited. Through these backdoors might unauthorized access to the components of the E-meter and Concentrator infrastructure to be possible. As a backdoor applies in that case, a remote maintenance function, which without knowledge of EVN EP could be put into operation from the vendor (manufacturer).
- 12.22 Manufacturer or supplier must cooperate in case of IT Security Audits.
13. Central system
- 13.1 The software of Central system must be compatible with x86 server architecture.
- 13.2. Productive and test environments must be deployed.
- 13.3 The Central system must be compatible with operating system Microsoft Windows 2008 server 64 bit or higher or Red Hat v. 6.3 / 64 bit or higher.
- 13.4 Graphical user interface of software of central system must be ergonomic and refer to EN ISO 9241 standardization.
- 13.5 The Central system must allow implementation of role-based authorization concept. User rights must be defined for each role with appropriate necessary permissions. The various users depending on their function must have assigned role corresponding to their duties. The implementation of a role-based authorization concept must allow maximum separation of functions.
- 13.6 Passwords corresponding to user rights must be kept in a way which correlates to the deployed secure encryption mechanism and must be not reproducible. Passwords must be managed centrally.
- 13.7 Software must assist 4-eyes principle for a critical central system functions. Critical system functions that need confirmation before execution must be configured in a way that requires at least 2 employees approve before the start of execution (example: process for switch off / switch on of electricity).
- 13.8 Commands for critical system functions for each E-Meters must be unique and their distribution must be not performed as a broadcast to all E-Meters.
- 13.9 Tamper-proof (secure) logging of all activities must be undertaken during the execution of critical commands towards the E-Meters.
- 13.10 Assignment of log entries must easily and uniquely identify employees' activities.
- предоставя на EVN EP в писмен вид, при поискване.
- 12.21 Производителят или доставчика на софтуера или фърмуера трябва да потвърди с писмено известие, че са взети всички мерки да се предотврати наличието на всякакви „задни вратички“ (средства за неоторизиран достъп) до фърмуера. Подобни „задни вратички“ биха могли да осигурят неоторизиран достъп до компонентите на Е-електромера. Под „задна вратичка“ в случая се разбира и функция за дистанционна поддръжка, която, без знанието на EVN EP, би могла да бъде активирана от доставчика (производителя).
- 12.22 Производителят или доставчика трябва да осигурят съдействие при Одити за ИТ сигурност.
13. Централна система
- 13.1 Софтуерът на Централна система трябва да е съвместим със сървърна архитектура x86.
- 13.2. Трябва да бъдат създадени продуктивна и тестова среда.
- 13.3 Централната система трябва да е съвместима с операционна система Microsoft Windows 2008 сървър 64 bit или следващи варианти или Red Hat v 6.3 64 битова и следващи версии.
- 13.4 Графичният потребителски интерфейс на софтуера на централната система трябва да бъде ергономичен и да съответства на стандарт EN ISO 9241.
- 13.5 Централната система трябва да дава възможност за реализация на концепцията за оторизация по роли. Правата на потребителите трябва да бъдат дефинирани за всяка отделна роля, заедно със съответните разрешителни. Различните потребители, в зависимост от своите функции, трябва да имат роли, съответстващи на задълженията им. Прилагането на ролева оторизация би трябвало да позволи максимално разделение на функциите.
- 13.6 Паролите, съответстващи на правата на потребителите, трябва да се съхраняват по начин отговарящ на въведения механизъм за сигурно криптиране и трябва да не подлежат на възпроизвеждане. Паролите трябва да бъдат управлявани на централно ниво.
- 13.7 При софтуера следва да се прилага принципа на 4-те очи за особено важните функции на централната система. Най-съществените функции на системата, които се нуждаят от потвърждение преди изпълнението си, трябва да бъдат конфигурирани по начин, който налага присъствието на поне 2 служители, които да одобряват съответните дейности, преди започване на тяхното изпълнение (пример: процес за прекъсване на електричеството).
- 13.8 Командите за функциите на критични системи функции за всеки от Е-електромерите трябва да бъдат уникални и разпространението им не трябва да се изпълнява като излъчване до всички Е-електромери.
- 13.9 Сигурно регистриране на всички дейности, защитено от посегателства трябва да се осъществява по време на изпълнението на особено важни команди по отношение на Е-електромерите.
- 13.10 Записите в регистъра трябва лесно и по уникален начин да идентифицират дейностите на служителите.

- 13.11 The Central system must provide the possibility of maximum number of daily activities towards the E-Meter. If the configurable limit is reached, the system must send an alert. The change of the daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle).
- 13.12 Due to the uniqueness of "switch off" command towards the circuit breaker for each E-Meter, a logical algorithm must be applied which regulates how many E-Meters can be switched off maximum per day. If the configurable limit is reached, the central system must stop the process of execution and generate an alert. The change of daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle and approving procedure).
- 13.13 The central system must provide for all E-Meters and Concentrators time synchronization based upon international standard, like NTP protocol with an external timer or an already implemented in the internal network timers.
- 13.14 The time of central system can have difference of maximum of one second from the time of the external or internal timer.
- 13.15 The time from all installed E-Meters must be periodically checked and, if necessary, synchronized with the central system. Deviations of the time of installed E-Meters and Central system must be reported as an alarm message. (Excessive deviations could be a sign of a malfunctioning or manipulation of the E-Meter)
- 13.16 The central system must make an appropriate monitoring and reporting of all its functionalities. In case of malfunctions automatically a corresponding notification to the responsible personnel to be generated.
- 13.17 The assigned permissions and user rights of all employees which have an access in the Central system and to the respective components of E-Meter infrastructure should be checked periodically. For this review the provision of certain reports is necessary and they must contain:
- 13.17.1 List of all users with the date of definition, date of first registration, date of last successful login, role membership of the user.
- 13.17.2 List of all permissions associated with a role in the central system.
- 13.17.3 List of evaluation according to various dimensions (for example- all users who are allowed to perform a certain action)
- 13.17.4 Identification of critical authorization combinations (for example, a user could run without the confirmation of
- 13.11 Централната система трябва да осигури възможност за максимален брой дневни дейности по отношение на Е-електромера. При достигане на подлежащия на конфигуриране максимален брой, системата трябва да изпрати предупреждение. Промяната в дневните лимити трябва да може да е извършва от поне двама служители на EVN EP (съответствие с принципа на 4те очи).
- 13.12 Поради уникалността на командата за прекъсване на захранването чрез главния прекъсвач за всеки Е-електромер, трябва да бъде приложен логически алгоритъм, който регулира колко Е-електромера максимално могат да бъдат изключени в рамките на един ден. При достигане на конфигурираната максимална стойност, Централната система трябва да спре процесът по изпълнение и генериране на предупреждение. Промяната на дневните максимални стойности трябва да е възможна единствено при участие на двама или повече служителя на EVN EP (спазване на принципа за 4-те очи и процедурата за одобряване).
- 13.13 Централната система трябва да осигурява за всички Е-електромери и Концентратори синхронизация на часа, въз основа на вътрешен стандарт, като NTP с външен таймер или вече приложен такъв във вътрешните мрежови таймери.
- 13.14 Часът според централна система може да се различава с максимум една секунда от часа на външния или вътрешния таймер.
- 13.15 Часът на монтираните Е-електромери трябва да бъде периодично проверяван и, ако е необходимо, синхронизиран с Централната система. Отклоненията в часа на инсталираните Е-Електромери и Централната система трябва да се съобщават под формата на алармено съобщение. (Прекомерните отклонения могат да са знак за неизправност или манипулация на Е-електромера)
- 13.16 Централната система трябва да осъществява надлежен контрол и отчетност на всичките си функции. При неизправност следва незабавно да се генерира и изпраща известие до отговорния персонал.
- 13.17 Дадените разрешения и потребителски права на всички служители, които имат достъп до Централната система и до съответните компоненти на Е-електромера, трябва да бъдат проверявани периодично. За тази проверка е необходимо изготвянето на определени доклади, които следва да съдържат следната информация:
- 13.17.1 Списък с всички потребители с дата на определяне на пълномощията, дата на първа регистрация, дата на последен успешен вход в системата, роля на потребителя.
- 13.17.2 Списък с всички разрешения, свързани с дадена роля в Централната система.
- 13.17.3 Списък с оценка, според различни показатели (напр. всички потребители, които имат право да осъществяват дадено действие)
- 13.17.4 Идентифициране на критични валидиращи комбинации (напр. даден потребител може да

- another employee critical commands for a plurality of measurement points)
- 13.17.5 Historization of permissions of users (it should be comprehensible, about what permissions a user had at a particular time)
- 13.18 Any changes to the configuration of the central system have to be recorded. The stored log entries against subsequent change have to be protected. The log information must be clearly reported.
- 13.19 All changes in the central system (for example - manual manipulation of readings, replacement of values) must be logged, unique and assigned to a particular user. Historization of all user activities must be available.
- 13.20 If in the installed (deployed) E-Meters a critical system event is recognized then an appropriate alarm must be within 5 minutes sent to the central system.
- 13.21 During the periodic reading of the corresponding measured values from E-Meter, all stored in it event information must be able to be transported to central system.
- 13.22 For avoiding a re-recording possibility of encrypted commands towards the E-Meter from the central system or concentrator the Vendor has to implement an adequate mechanism to resist on it. (like framecounter of commands)
- 13.23 The application for maintenance tasks must be compatible with HHU operating system - Microsoft Windows mobile professional v.6.5 or libraries (SDK) for integration with existing legacy application.
- 13.24 The client part of the central system application must be able to run on terminal server environment with Microsoft Windows 2008 server 64bit.
- 13.25 The central system must be able to be customized with modern technologies (interfaces) to exchange information with Contractor legacy systems in both directions. For example - billing and ERP system (kVAsy) and meter data management environment.
- 13.26 In case of not successful execution of „switch on“ or „switch off“ function from central system towards the E-Meter in the timeframe within 4 hours, an automatic workorder must be created for maintenance task towards the HHU in order manually to perform the „switch on“ or „switch off“ function for the E-Meter.
- 13.27 After manual execution of „switch on“ or „switch off“ function by HHU from employee, the central system must give possibility (interface) that HHU can report statuses of already executed workorders towards E-Meters.
- 13.28 Central system must support reporting mechanism with which the Contractor can create by itself adequate reports from the system.
- осъществява без потвърждение от друг служител критични команди за редица елементи от системата)
- 13.17.5 Исторически данни за разрешенията на потребителите (трябва да се съдържа подробна информация относно това кои потребители, какви права са имали в даден момент)
- 13.18 Всички промени в конфигурацията на Централната система трябва да бъдат регистрирани. Съхранените записи за съответните промени следва да бъдат защитени. Информацията в регистъра трябва да бъде ясна и точна.
- 13.19 Всички промени в Централната система (напр. – ръчно манипулиране на показания, замяна на стойности) трябва да бъдат регистрирани, уникални и обвързани със съответния потребител. Трябва да има налични хронологични данни за дейностите на всички потребители.
- 13.20 Ако в монтирани Е-електромери възникне критично системно събитие, съответната аларма трябва да бъде изпратена до Централната система.
- 13.21 По време на периодичното отчитане на съответните измерени стойности от Е-електромерите, цялата съхранена в тях информация за събития трябва да може да бъде прехвърлена в централната система.
- 13.22 За да се избегне повторен запис на криптирани команди към Е-електромерите от Централната система или концентратора, Доставчикът трябва да въведе подходящ механизъм за предпазване от подобно повторение. (брояч на команди)
- 13.23 Приложението за дейности по поддръжката трябва да е съвместимо с операционната система на Преносимия терминал - Microsoft Windows mobile professional v.6.5 или библиотеките (SDK) за интегриране в съществуващи приложения.
- 13.24 Клиентската част от приложението на Централната система трябва да може да работи на терминален сървър с Microsoft Windows 2008 server 64bit.
- 13.25 Централната система трябва да подлежи на адаптация съобразно със съвременните технологии (интерфейси) за обмен на информация с предишните системи на Изпълнителя.
- 13.26 При неуспешно изпълнение на функцията по „включване“ от Централната система по отношение на даден Е-електромер в рамките на 12 часа, трябва да се генерира автоматична команда за задача по поддръжка към Преносимия терминал за да се осъществи ръчно „включването“ на Е-електромера.
- 13.27 След ръчното изпълнение на функцията „вкл.“ или „изкл.“ от HHU от страна на служител, централната система трябва да дава възможност (интерфейс) HHU да може да отчита състоянията на вече изпълнените заявки за работа към Е-електромерите.
- 13.28 Централната система трябва да поддържа отчитащ механизъм, с който Изпълнителят да може сам да създава съответните доклади от системата.

central system.

14.1 Maintenance of an up-to-date program-license catalogue.

14.2 Agreed maintenance percentage for the entire period of the contract.

14.3 Provision of software maintenance, covering the provision of ticket system and maintenance work.

14.4 Provision of communication service (ticket system) in the period from Monday to Friday and on the specified in Bulgaria working days in the period from 08:00-18:00 BG without the Bulgarian public holidays.

14.5 Provision of communication service also on weekend (Saturday/Sunday) and the Bulgarian holidays after the prior order by EVN within 7 working days.

14.6. The contractor shall provide the software maintenance, which consists of the following tasks:

14.6.1. Improvements: The Contractor shall remove all errors, ensuring its own quality of its product shall create new versions of the software and shall provide them to the Employer in the form of software packages for maintenance. The Employer is interested in any type of updates/upgrades, to be sure that he works with the latest version, although he is not bound.

All software updates and re-works shall be made available to the Employer in a current version with all the documentation for bringing the software into a working service and execution of operations with the software.

14.6.2 Error Management: The responsibility for debugging and troubleshooting is fundamental for the Contractor for the purpose of providing correctly running software to the Employer. The Contractor shall meet all the requirements after receiving error information from the Employer, by providing information how to avoid errors, self-removal of errors, errors specific for EVN, software re-works, future versions, packages, etc.

The type of delivery (information on the avoidance of errors, debugging of errors specific to EVN EP, software re-works, future versions, packages, etc.) depends on the class of the error. The delivery and implementation of an alternative solution for the management of the errors in an environment of the Employer (EVN EP) must be discussed in advance. These alternative solutions must be included in the next package of services or in correctly and fully integrated system within half a year with the latest changes and amendments. All required tasks for solving problems and alternative solutions are without additional and separate prices. EVN EP shall give permission in case of troubleshooting or an alternative solution to be implemented, because the Employer undertakes additional installations, implementations or other changes of the software or its functionalities.

14.6.3. Exchange of information on current re-works and status: The Contractor shall provide estimated information at a neutral price at least once a year on current technical and commercial affairs, planned and ordered

централната система.

14.1 Поддръжка на актуален програмно-лицензен каталог.

14.2 Договорен процент на поддръжка за целия период на договора.

14.3 Осигуряване на софтуерна поддръжка, обхващаща предоставяне на служба за съобщения и поддръжка.

14.4 Предоставяне на служба за съобщения в периода понеделник-петък и на определените в България работни дни в периода от 08:00-18:00 BG без българските официални празници.

14.5. Предоставяне на служба за съобщения и в събота и неделя, както и българските празници след предварително заявяване от EVN в периода от 7 работни дни.

14.6 Изпълнителят осигурява софтуерната поддръжка ,която се състои от следните задачи:

14.6.1 Подобрения: Изпълнителят премахва всички грешки, осигурявайки собственото качество на продукта си, създава нови версии на софтуера и ги предоставя на Възложителя под формата на софтуерни пакети за поддръжка. Възложителят е заинтересован за всякакъв тип актуализации/надстройки, за да е сигурен, че работи с последната версия, въпреки че не е задължен.

Всички софтуерни актуализации и доработки се предоставят на Възложителя в съвременен вариант с цялата документация за привеждане на софтуера в работеща услуга и изпълняване на операции със софтуера.

14.6.2 Управление на грешките: Отговорността за отстраняване на грешки и проблеми е основна за Изпълнителя с цел предоставяне на коректно работещ софтуер на Възложителя. Изпълнителят изпълнява всички изисквания след информация за грешка от Възложителя, като предоставя информация за избягване на грешки, самостоятелно отстраняване на грешки, грешки специфични за EVN, софтуерни доработки, бъдещи версии, пакети и др. Видът на доставката (информация за избягване на грешки, отстраняване на грешки специфични за EVN, софтуерни доработки, бъдещи версии, пакети и др.) зависи от класа на грешката. Доставката и имплементацията на алтернативно решение за управление на грешките в среда на Възложителя (EVN) трябва да бъде предварително обсъдено. Тези алтернативни решения трябва да бъдат включени в следващия пакет услуги или в коректно и напълно интегрирана система в рамките на половин година с последните промени и изменения. Всички задължителни задачи за разрешаване на проблеми и алтернативни решения са без допълнителни и отделни цени. Разрешението при отстранен проблем или алтернативно решение да се имплементира е на EVN, защото Възложителят поема допълнителни инсталации, имплементации или други промени на софтуера или функционалностите му.

14.6.3 Обмяна на информация за текущи разработки и статус: Изпълнителят предоставя прогнозна информация на неутрална цена поне веднъж годишно за текущи технически и търговски въпроси, планирани



functionalities of the software (such as changes in technical matters, licenses, contact persons, owner, etc.)

#### 14.7. Removal of failures

##### 14.7.1 Classification of the failures:

14.7.1.1. Damage of category 1 - the central system is not functioning and/or false data arise. The meter reading system does not function. Work in at least one module is not possible. Separate functions of the mass processing, which must be implemented without time delay (meter reading of individual electric meters, etc.), may not be carried out.

14.7.1.2. Damage of category 2 - individual functions of the Central system do not work or work incorrectly. The functionalities necessary for the daily work are not, or are partially available. There are alternative options. The operation of individual functions of one module is not possible and it can be resumed only with extraordinary spending of time and funds, wherein is concerned an essential function of the module, which must constantly be used. It is not possible to carry out a service, which must be immediately carried out for individual electric meter or it is not possible the immediate required preparation of meter reading. The work in a module or of one major feature of the module is seriously obstructed, as far as this affects the entire availability of the data base.

14.7.1.3 Damage of category 3 - one or more functions do not work optimally, but there is no severe obstruction of the daily work.

14.8. Response times is 4 hours after registering the problem into the ticketing system of contractor. Repair time is defined as follow based upon the categories of failures.

14.8.1 For category 1 - after registration should be started with identification of the cause of damage and the troubleshooting must be done latest the next working day.

14.8.2 For category 2 - after registration should be started with identification of the cause of damage, and the troubleshooting must be done within the next three working days.

14.8.3 For category 3 - one day after registration should be started with identification of the cause of damage, and the troubleshooting must be done within the deadline agreed between the two parties.

14.9 Transmitting the status of troubleshooting must be assured.

14.10 The damage/incident is considered resolved after making tests and after the approval of EVN EP.

14.11 The Contractor must provide the following process for debugging the software:

14.11.1 The Employer shall send a message to the support team (Helpdesk/ticket system) for available errors through a system for issues registration / e-mail with the required information. Such message shall contain also the error class.

14.11.2 The error is logged in the issues registration system

и заявени функционалности на софтуера (като промени по технически въпроси, лицензи, лица за контакт, собственик и т.н.)

#### 14.7 Отстраняване на повреди

##### 14.7.1 Класифициране на повредите

14.7.1.1 Повреда от категория 1 – Централната система не функционира и/или възникват грешни данни. Системата за отчет не функционира. Работата най-малко в един модул е невъзможна. Отделни функции от масовата обработка на данни, които трябва да бъдат реализирани без времево закъснение (отчет на отделни електромери и др.), не могат да бъдат извършени.

14.7.1.2 Повреда от категория 2 - отделни функции на Централната система не работят или работят грешно. Необходимите за ежедневната работа функционалности не са или отчасти са на разположение. Съществуват алтернативни възможности. Работата на отделни функции на един модул не е възможна и тя може да бъде възстановена само с извънреден разход на време и средства, при което се касае за съществена функция от модула, която трябва постоянно да бъде използвана. Не е възможно да се извърши услуга, която трябва незабавно да се извърши за отделен електромер или не е възможно незабавно необходимото изготвяне на отчет. Работата в един модул или на една основна функция от модула е сериозно възпрепятствана, доколкото от това е засегната цялата наличност на базата от данни.

14.7.1.3 Повреда от категория 3 - не работят оптимално една или повече функции, но няма сериозно възпрепятстване на дневната работа.

14.8. Времена на реакция 4 часа след регистриране на проблема и време за отстраняване на проблема както следва по категории:

14.8.1 За категория 1 - след регистриране се започва с идентифициране на причината за повредата, а отстраняването трябва да стане в рамките най-късно на следващия работен ден.

14.8.2 За категория 2 - след регистриране се започва с идентифициране на причината за повредата, а отстраняването трябва да стане в рамките на следващите три работни дни.

14.8.3 За категория 3 - един ден след регистриране се започва с идентифициране на причината за повредата, а отстраняването да стане в срок договорен между двете страни.

14.9. Да се осигури предаване на статуса на отстраняване на повредата.

14.10 Повредата се счита за отстранена след тестове и съгласие от страна на EVN.

14.11 Изпълнителят да осигури следния процес за отстраняване на грешки в софтуера

14.11.1 Възложителят изпраща съобщение към екипа за поддръжка (Helpdesk) за наличие на грешка чрез система за регистриране на проблеми / имейл с необходимата информация. Съобщението съдържа и класа грешка.

14.11.2 Грешката се въвежда в системата за



(ticket system) and response shall be returned within the specified response time.

14.11.3 After finding a solution the Employer shall be notified and asked to carry out a test in the test system, and the required documentation shall be sent.

14.11.4 After approval shall be made an installation in the test system.

14.11.5 Test and confirmation of the decision.

14.11.6 Approval for installation in a productive system.

14.11.7 Installation make in a productive system and official confirmation. The procedure is carried out in accordance with the agreed hours for each error class.

14.12. There must be guaranteed assistance in the case of installations, making a connection to databases, interfaces, reports, additions, technical problems or errors that have occurred during the use of the software, etc

14.13. There must be provided documentation for standard and configured / specific to the software functionalities according to the current version, which is in use. For each implementation the Contractor shall provide documentation about the changes performed in the programming code.

14.14 The Contractor must notify the Employer at least once a year for all committed changes and additions on components of the desktop publishing software, which the Employer uses. The information should contain at least the date of issue, description of the functionality, the change request number to the software and any other changes made, if any.

In particular the Contractor must provide this information upon EVN's request within one week.

14.15. The option remote control must be possible through desktop sharing and VPN connection through EVN EP network whenever debugging is needed and/or software updates and upgrades. The decision of how the remote assistance will be done will be taken by EVN EP.

14.16 Supply of new program versions

14.16.1 EVN EP must receive information for the availability of new software versions.

14.16.2 EVN EP must approve the methods and the time window for installation.

14.16.3 New versions must be controlled with antivirus programs

14.17. Process for purchase of a new / additional licenses

14.17.1 Submission of a quotation/offer by the Contractor.

14.17.2 EVN EP makes an order.

## **VI. Standards**

References to relevant standards and other technical regulations and recommendations to be followed.

Es gelten die jeweils aktuellsten Fassungen zum Zeitpunkt der Erstellung dieses Dokuments.

регистриране на проблеми и се връща отговор в определеното време за реакция.

14.11.3 След намиране на решение Възложителят бива уведомен и запитан за извършване на тест в тестовата система, а нужната документация бива изпратена.

14.11.4 След одобрение се извършва инсталация в тестовата система.

14.11.5 Тест и потвърждение за решението.

14.11.6 Съгласуване за инсталация в продуктивна система.

14.11.7 Извършване на инсталация в продуктивна система и официално потвърждение. Процедурата се осъществява съгласно договорените часове за всеки клас грешка.

14.12. Трябва да бъде гарантирана помощ в случай на инсталации, осъществяване на връзка с бази данни, интерфейси, доклади, допълнения, технически проблеми или грешки, появили се по време на употреба на софтуера и т.н.

14.13 Трябва да бъде предоставена документация за стандартни и конфигурирани / специфични за софтуера функционалности според текущата версия, която е в употреба. За всяка една имплементация Изпълнителят предоставя документация за извършените в програмния код промени.

14.14. Изпълнителят трябва да уведомява Възложителя поне веднъж годишно за всички извършени промени и допълнения върху компоненти на софтуера за предпочатна подготовка, които Възложителя употребява. Информацията трябва да съдържа поне дата на издаване, описание на функционалността, номера изискване към софтуера и извършени други промени в случай на наличие на такива.

В частност Изпълнителя трябва да предостави тази информация при заявка от страна на EVN EP в срок от една седмица.

14.15. Трябва да има възможност за отдалечен контрол, чрез използване на споделен екран (desktop sharing) и VPN връзка през EVN мрежа, при нужда от отстраняване на грешки и/или софтуерни актуализации и надстройки. Методът ще бъде избран от EVN EP.

14.16. Доставка на нови програмни версии.

14.16.1 EVN EP да получава информация за наличие на нови програмни версии.

14.16.2 EVN EP да съгласува начините и времената за инсталация.

14.16.3 Новите версии трябва да са контролирани с антивирусни програми

14.17 Процес за закупуване на нови лицензи

14.17.1 Представяне на оферта от изпълнителя

14.17.2 Поръчка от EVN EP.

## **VI. Стандарти**

Изискванията на съответните технически стандарти и препоръки трябва да бъде спазено.

Es gelten die jeweils aktuellsten Fassungen zum Zeitpunkt der Erstellung dieses Dokuments.

IEC/ISO	Designation
IEC Publ. 60529	Degree of protection provided by

IEC/ISO	Предназначение
IEC Publ. 60529	Степени на защита, осигурени от

	enclosures (IP-CODE)		обвивката (IP код)
ISO Publ. 75	Plastics and ebonite, determination of temperature of deflection under load.	ISO Publ. 75	Пластмаси и ебонит, определяне на температурата на деформация при натоварване.
Europe Standards	Designation	Европ. стандарти	Предназначение
EN 62052-11	Electricity metering equipment (AC) – Gen Part 11: Metering equipment	EN 62052-11	Променливотокови уреди за измерване на електрическа енергия. Общи изисквания, изпитвания и условия на изпитване. Част 11: Уреди за измерване (електромери)
EN 62053-21	Electricity metering equipment (a.c.) – Particular requirements – Part 21: Static meters for active energy (classes 1 and 2)	EN 62053-21	Променливотокови уреди за измерване на електрическа енергия. Специфични изисквания. Част 21: Статични електромери за активна енергия (класове 1 и 2)
EN 62056-21	Electricity metering – Data exchange for meter reading, tariff and load control – Part 21: Direct local data exchange	EN 62056-21	Измерване на електрическа енергия. Обмен на данни за измервателни уреди за отчитане, управление на тарифи и товар. Част 21: Директен локален обмен на данни
EN 62056-61	Electricity metering. Data exchange for meter reading, tariff and load control Part 61: Object identification system (OBIS)	EN 62056-61	Измерване на електрическа енергия. Обмен на данните за показанията на електромера, управление на тарифите и товарите. Част 61: Система за идентификация на обекти
EN 55011	Industrial, scientific and medical equipment. Radio-frequency disturbance characteristics. Limits and methods of measurement ( Basisdocument CISPR 11)	EN 55011	Промислени, научни и медицински (ПНМ) радиочестотни устройства. Характеристики на радиочестотните смущаващи въздействия. Гранични стойности и методи за измерване (CISPR 11)
EN 55014	Electromagnetic compatibility. Requirements for household appliances, electric tools and similar apparatus Emission (Basisdokument CISPR 14)	EN 55014	Електромагнитна съвместимост. Изисквания за електрически уреди, електрически инструменти и подобни на тях уреди. (CISPR 14)
EN 62053-52	Electricity metering equipment (AC) – Particular requirements – Part 52: Symbols	EN 62053-52	Променливотокови уреди за измерване на електрическа енергия. Специфични изисквания. Част 52: Символи за променливотокови електромери
EN 61000-3-2 + A2	Electromagnetic compatibility (EMC). Limits. Part 3-2 Limits for harmonic current emissions	EN 61000-3-2 + A2	Електромагнитна съвместимост (EMC). Част 3: Норми. Раздел 2: Норми за излъчвания на хармонични съставлящи на тока
EN 61000-4-4	Electromagnetic compatibility (EMC) - Part 4-4: Testing and measurement techniques - Electrical fast transient/burst immunity test (Burst) (Basisdokument IEC 801-4)	EN 61000-4-4	Електромагнитна съвместимост (EMC). Част 4-4: Методи за изпитване и измерване. Изпитване на устойчивост на електрически бърз преходен процес/пакет импулси (Burst) (Basisdokument IEC 801-4)
EN 61000-4-5	Electromagnetic compatibility (EMC) -	EN 61000-4-5	Електромагнитна съвместимост

	- Part 4-5: Testing and measurement techniques - Surge immunity test (Surge)
EN 62052-11 of 2003-02-12	Alternating current electricity metering equipment. General requirements, tests and testing conditions. Part 11: Metering equipment (electricity meters)
EN 62053-21 of 2003-01-28	Alternating current electricity metering equipment. Specific requirements. Part 21: Static active energy electricity meters (classes 1 and 2)
EN 62054-21 edition 2005-08-01	Alternating current electricity metering devices. Tariff and load control Part 21: Specific requirements applicable to switching timers
DIN/DIN-VDE Standards	Designation
DIN 43859 6.77	Watt-hour meters for instrument-transformer connection; main dimensions for three-phase meters
DIN VDE 0160 05.88	Electronic equipment for use in power installations (with change A1/04.89 and A2/10.88)
Common	Designation
IEC 13 (SEC) 1022	Reliability requirements for static meters
OIML 11	General requirements for measuring instruments
OIML 12	Fields of use of measuring instruments subject to verification

TABLE - STANDARDS

	(EMC). Част 4-5: Методи за изпитване и измерване. Изпитване на устойчивост на отскок
EN 62052-11 издание: 2003-02-12	Променливотокови уреди за измерване на електрическа енергия. Общи изисквания, изпитвания и условия на изпитване. Част 11: Уреди за измерване (електромери)
EN 62053-21 издание 2003-01-28	Променливотокови уреди за измерване на електрическа енергия. Специфични изисквания. Част 21: Статични електромери за активна енергия (класове 1 и 2)
EN 62054-21 издание 2005-08-01	Променливотокови уреди за измерване на електрическа енергия. Управление на тарифите и товара Част 21: Специфични изисквания към превключващи часовници
DIN/DIN-VDE Стандарти	Предназначение
DIN 43859 6.77	Електромери за индиректно свързване; основни размери за трифазни електромери
DIN VDE 0160 05.88	Електронно оборудване за използване в електрически инсталации (с промяна A1/04.89 и A2/10.88)
Общи	Предназначение
IEC 13 (SEC) 1022	Изисквания за надеждност за статични електромери
OIML 11	Общи изисквания за измервателните уреди
OIML 12	Области на употреба на измервателни уреди, подлежащи на проверка

ТАБЛИЦА - СТАНДАРТИ

## VII. Documentation and samples

1. In order to ensure the proper operation of the equipment, the following documents must be provided at applicant's disposal.

- 1.1. System description
- 1.2. Description of the components
- 1.3. Description of the requirements towards the hardware of each element (communication servers, applications, database), as well as the required architecture, where the elements will be installed, to be agreed with the Employer
- 1.4. User manual
- 1.5. Maintenance manual
- 1.6. Certificates of the separate components of the system (electricity meters, Data Concentrator)

2. Test samples of the system: Samples must be provided

## VII. Документация и мостри

9.12.5.1.1. За да се осигури правилна работа на оборудването, следните документи трябва да бъдат предоставени на разположение на заявителя.

- 1.1. Описание на системата
- 1.2. Описание на компонентите
- 1.3. Описание на изискванията към хардуера за всеки елемент (комуникационни сървъри, приложения, база данни), като е необходимо архитектурата, върху която ще бъдат инсталирани елементите, да бъде съгласувана с Възложителя
- 1.4. Ръководство за потребителя
- 1.5. Ръководство поддръжка
- 1.6. Сертификати на отделните компоненти от системата (електромери, Концентратор на данни..)
2. Тестова мостра на ситемата: Трябва да бъдат предоставени

marked accordingly the corresponding name of the Technical Specification:

3. Place of delivery of the samples:

3.1. **Bulgaria.**

3.1.1. Meters: 2nr. Per Position

3.1.2. Data concentrator: 1nr.

3.1.3. Softwar of the test variant of the System installed on the hardware of the Applicant.

Contact person: Dipl.eng. Svetoslav Peykov. EVN Bulgaria ER, 4000 Plovdiv, Hr. G Danov str. № 37

3.2. **Austria.**

3.2.1. Meters: 2nr. Per Position

3.2.2. Data concentrator: 1nr.

Contact person: Dipl.eng. Mehdi Safaei, Netz Niederosterreich GmbH Zählerwesen, A- 3100 St. Pölten, Jahnstraße 29

следните мостри уреди и да са със съответното име на Техническата спецификация:

3. Място на доставка на мостри:

3.1. **България.**

3.1.1. Електромери: 2бр. За всяка Позиция

3.1.2. Концентратори за данни: 1бр.

3.1.3. Софтуерът на тестовия вариант на Системата инсталиран на хардуер на Кандидата

Лице за контакти: инж. Светослав Пейков. EVN Bulgaria ER, Пловдив 4000, ул. „Хр. Г. Данов“ № 37

3.2. **Австрия.**

3.2.1. Електромери: 2бр. За всяка Позиция

3.2.2. Концентратори за данни: 1бр.

Лице за контакти: инж. Mehdi Safaei, Netz Niederosterreich GmbH Zählerwesen, A- 3100 St. Pölten, Jahnstraße 29 Електромерни мостри

**С подписването на настоящите Технически изисквания, Изпълнителят гарантира за тяхното приемане, спазване и точно изпълнение.**

Фирмен печат:.....

Подпис с правна сила: .....

Дата .....

Гр. ....

## Приложение 1:

Към Технически изисквания (Издание Юни.2014 г.), към система за предварителен подбор на изпълнители № С-14-НМ-Д-XXX, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

### ТЕСТОВ ПРОТОКОЛ

#### I. Електромагнитна съвместимост

3.2.2.1.1. Участник	
Фирма:	
Адрес:	
Град:	
Телефон:	
Факс:	
Електронна поща:	

3.2.2.1.2. Изпитвана апаратура	
Описание:	
Сериен номер:	
FW/SW Версия:	

3.2.2.1.3. Описание на тестовете:			
Стандарт:	Резултат	Критерии	Бележка
IEC/EN61000-4-4 (Burst)	Да <input type="checkbox"/> / Не <input type="checkbox"/>		
IEC/EN61000-4-5 (Combination Wave)	Да <input type="checkbox"/> / Не <input type="checkbox"/>		
IEC/EN61000-4-2 (ESD)	Да <input type="checkbox"/> / Не <input type="checkbox"/>		
Alternating Voltage Test	Да <input type="checkbox"/> / Не <input type="checkbox"/>		
IEC/EN61000-4-3 (Handfunk)	Да <input type="checkbox"/> / Не <input type="checkbox"/>		
Electro Magnetic Pulse(EMP)	Да <input type="checkbox"/> / Не <input type="checkbox"/>		

3.2.2.1.4. Описание на критериите:	
Критерии	Описание
A	нормално поведение; пълна функционалност;
B	временна загуба на функционалност или временно нарушаване на нормалното поведение, без нужда от външна намеса
C	временна загуба на функционалност или временно нарушаване на нормалното поведение, с нужда от външна намеса
D	загуба на функционалност с трайна повреда в изпитваната апаратура

Извършил теста: .....  
[име и фамилия]

Дата: .....

Подпис:.....



## II. Описание на използваната апаратура

2. Основна апаратура:		
Производител	Тип	Сериен номер

3. Модули:					
Производител	Тип	Сериен номер	Версия / FW	Дата на калибриране	№ Сертификат

4. Ръчна/допълнителна апаратура :					
Производител	Тип	Сериен номер	Версия / FW	Дата на калибриране	№ Сертификат

### 5. Настройки:

Захранващо напрежение за сравнителна стойност  $U_{in}$ :

Измерено захранващо напрежение:

Измерена захранваща честота:

Захранване при повреда в изпитваната апаратура:

Изкл.

Действие при повреда в изпитваната апаратура:

Стоп

### 6. Описания и забележки:

.....

.....

.....

.....

.....

.....

7. Околна среда:		
Температура	Влажност	Налягане
23°C	40%	1025

## III. Резултати

### 1. Sequence:

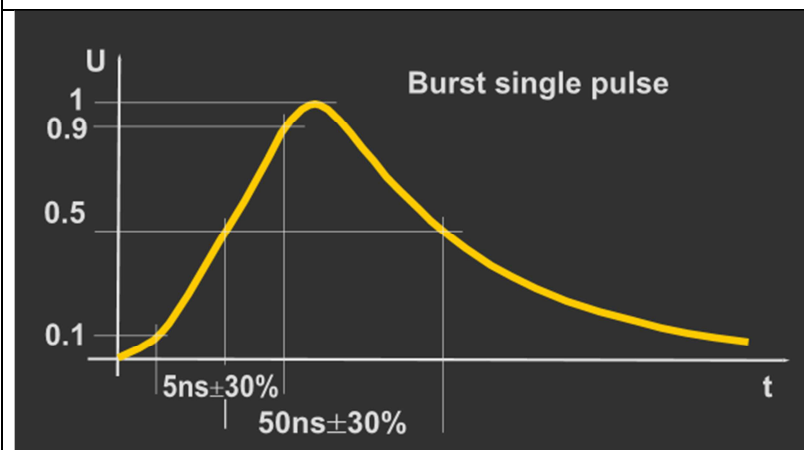
C:\Programme\Teseq AG\WIN 3000\UserTests\3~EMV\_Test\_Burst\_Combinationwave\_4kV.seq

### Burst / Electrical Fast Transient:

C:\Programme\Teseq AG\WIN 3000\UserTests\Burst - IEC 61000-4-4\3~ Level

4\Test\_Level4\_500;1000;2000;4000V\_5kHz;2500kHz\_IEC\_L3,L2,L1,N,PE.eft

EFT Test for 3-phase power line up to 4000V, alternate polarity, burst frequency 5 kHz (2.5 kHz), coupling to all lines.



Time	Volt	Polarity	Frequency	Phase	Burst Time	Repetition Time	Step Duration	Coupling	Status
2/27/2014 8:56:26 AM	500 V	Alt	5 kHz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed
2/27/2014 8:58:29 AM	1000 V	Alt	5 kHz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed
2/27/2014 9:00:35 AM	2000 V	Alt	5 kHz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed
2/27/2014 9:02:42 AM	4000 V	Alt	2500 Hz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed

### Dialog:

C:\Programme\Teseq AG\WIN 3000\UserTests\Break between Sequences.dlg

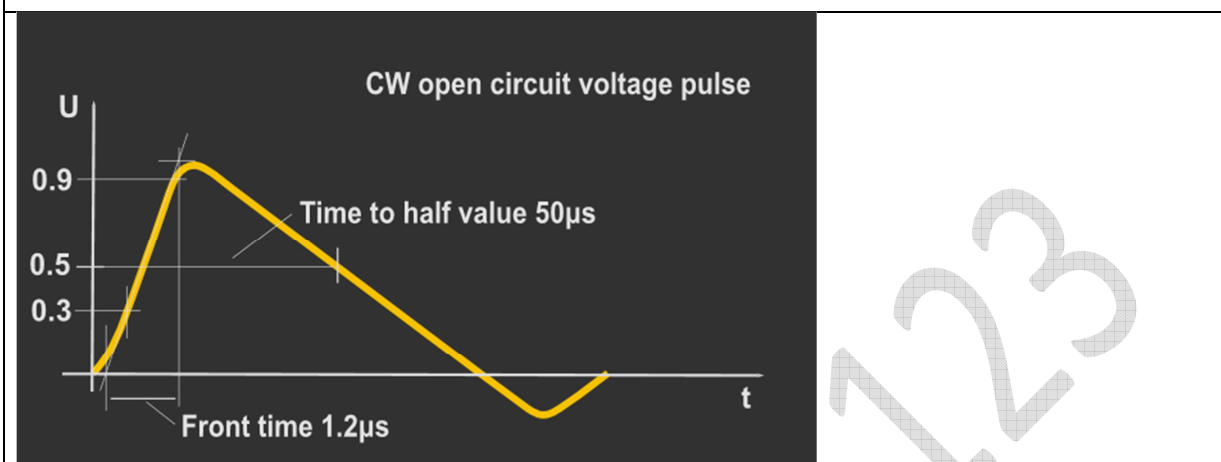
### Testbreak

Change Test Equipment and press Continue Button

Time	User Action
2/27/2014 9:08:51 AM	Continue

Combination Wave:								
C:\Programme\Teseq AG\WIN 3000\UserTests\Combination Wave - ICE 61000-4-5\3~\3~ 4000V 20hm\Test_Level_EVN_4000V_20hm_Lx-Lx.cw								
Combination wave test for 3-phase power lines up to 4000V, alternate polarity, synch. coupling from 0° to 270° in 90° step, line to line coupling.								
<p>CW open circuit voltage pulse</p> <p>U</p> <p>0.9</p> <p>0.5</p> <p>0.3</p> <p>Time to half value 50µs</p> <p>Front time 1.2µs</p> <p>t</p>								
Time	Volt	Polarity	Impedance	Phase	Repetition Time	Step Duration	Coupling	Status
2/27/2014 9:19:02 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> N	Passed
2/27/2014 9:29:10 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L2 -> N	Passed
2/27/2014 9:39:19 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L3 -> N	Passed
2/27/2014 9:49:29 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> L2	Passed
2/27/2014 9:59:38 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> L3	Passed
2/27/2014 10:09:18 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L2 -> L3	Passed

Combination Wave:
C:\Programme\Teseq AG\WIN 3000\UserTests\Combination Wave - ICE 61000-4-5\3~\3~ 4000V 20hm\Test_Level_EVN_4000V_20hm_Lx-PE.cw
Combination wave test for 3-phase power lines up to 4000V, alternate polarity, synch. coupling from 0° to 270° in 90° step, line to ground coupling.



Time	Volt	Polarity	Impedance	Phase	Repetition Time	Step Duration	Coupling	Status
2/27/2014 10:19:29 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> PE	Passed
2/27/2014 10:29:38 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L2 -> PE	Passed
2/27/2014 10:39:48 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L3 -> PE	Passed
2/27/2014 10:49:27 AM	4000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC N -> PE	Passed

Dialog:	
C:\Programme\Teseq AG\WIN 3000\UserTests\End of the test.dlg	
Test Ends	
Check the Results and click Exit Button.	
Time	User Action
2/27/2014 10:49:59 AM	STOP

## 2.Sequence:

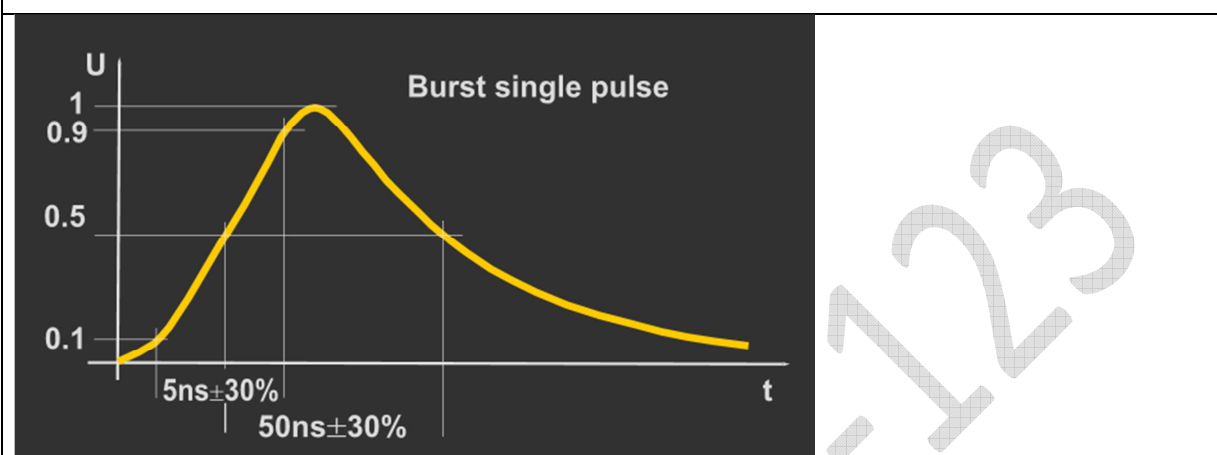
C:\Programme\Teseq AG\WIN 3000\UserTests\3~EMV\_Test\_Burst\_Combinationwave\_6kV.seq

## Burst / Electrical Fast Transient:

C:\Programme\Teseq AG\WIN 3000\UserTests\Burst - IEC 61000-4-4\3~ Level

4\Test\_Level4\_500;1000;2000;4000V\_5kHz;2500kHz\_IEC\_L3,L2,L1,N,PE.eft

EFT Test for 3-phase power line up to 4000V, alternate polarity, burst frequency 5 kHz (2.5 kHz), coupling to all lines.



Time	Volt	Polarity	Frequency	Phase	Burst Time	Repetition Time	Step Duration	Coupling	Status
2/27/2014 10:50:21 AM	500 V	Alt	5 kHz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	PAUSE ON
2/27/2014 10:50:52 AM									PAUSE OFF
2/27/2014 10:52:44 AM	500 V	Alt	5 kHz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed
2/27/2014 10:54:49 AM	1000 V	Alt	5 kHz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed
2/27/2014 10:56:55 AM	2000 V	Alt	5 kHz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed
2/27/2014 10:59:03 AM	4000 V	Alt	2500 Hz	---	15 ms	300 ms	120 s	IEC L3, L2, L1, N, PE	Passed

## Dialog:

C:\Programme\Teseq AG\WIN 3000\UserTests\Break between Sequences.dlg

Testbreak

Change Test Equipment and press Continue Button

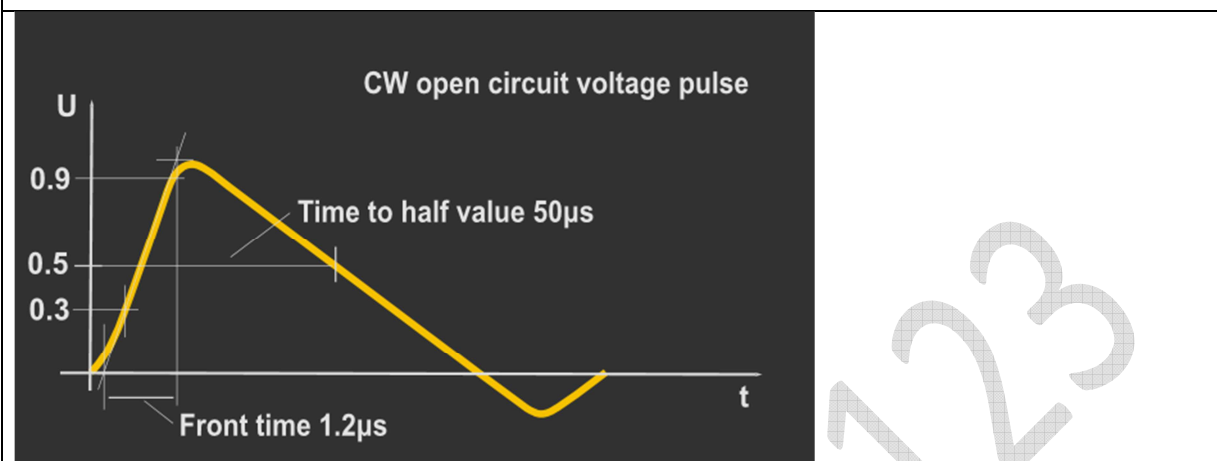
Time	User Action
2/27/2014 10:59:32 AM	Continue



### 3. Combination Wave:

C:\Programme\Teseq AG\WIN 3000\UserTests\Combination Wave - ICE 61000-4-5\3~\3~ 6000V  
20hm\Test\_Level\_EVN\_6000V\_20hm\_Lx-Lx.cw

Combination wave test for 3-phase power lines up to 4000V, alternate polarity, synch. coupling from 0° to 270° in 90° step, line to line coupling.



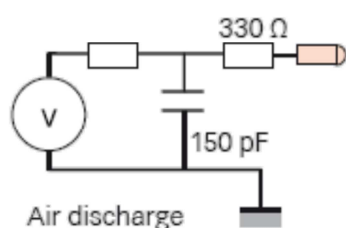
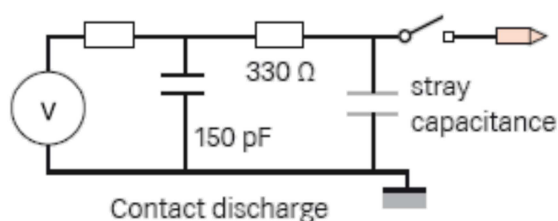
Time	Volt	Polarity	Impedance	Phase	Repetition Time	Step Duration	Coupling	Status
2/27/2014 11:09:51 AM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> N	Passed
2/27/2014 11:20:07 AM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L2 -> N	Passed
2/27/2014 11:30:25 AM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L3 -> N	Passed
2/27/2014 11:40:42 AM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> L2	Passed
2/27/2014 11:50:59 AM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> L3	Passed
2/27/2014 12:00:47 PM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L2 -> L3	Passed

4. Combination Wave:								
C:\Programme\Teseq AG\WIN 3000\UserTests\Combination Wave - ICE 61000-4-5\3~\3~ 6000V 20hm\Test_Level_EVN_6000V_20hm_Lx-PE.cw								
Combination wave test for 3-phase power lines up to 4000V, alternate polarity, synch. coupling from 0° to 270° in 90° step, line to ground coupling.								
Time	Volt	Polarity	Impedance	Phase	Repetition Time	Step Duration	Coupling	Status
2/27/2014 12:08:12 PM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin @ 60 °	30 s	10 Pulses	IEC L1 -> PE	PAUSE ON
2/27/2014 1:07:15 PM								PAUSE OFF
2/27/2014 1:07:19 PM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin @ 60 °	30 s	10 Pulses	IEC L1 -> PE	PAUSE ON
2/27/2014 1:07:40 PM								PAUSE OFF
2/27/2014 1:17:54 PM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L1 -> PE	Passed
2/27/2014 1:28:11 PM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L2 -> PE	Passed
2/27/2014 1:38:29 PM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC L3 -> PE	Passed
2/27/2014 1:48:16 PM	6000 V	Alt	2 Ω	60/240 ° 180 ° Lin	30 s	10 Pulses	IEC N -> PE	Passed

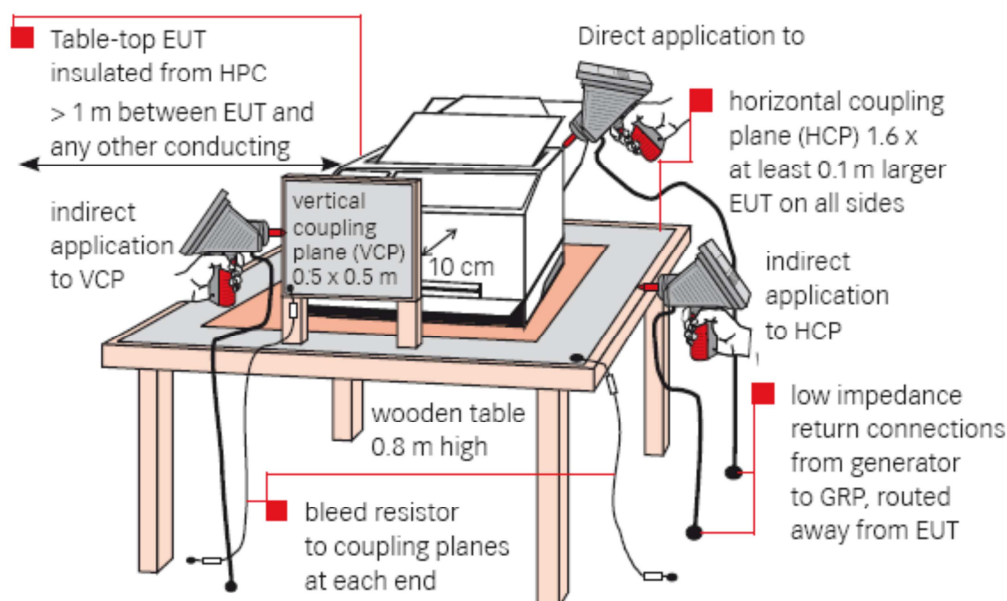
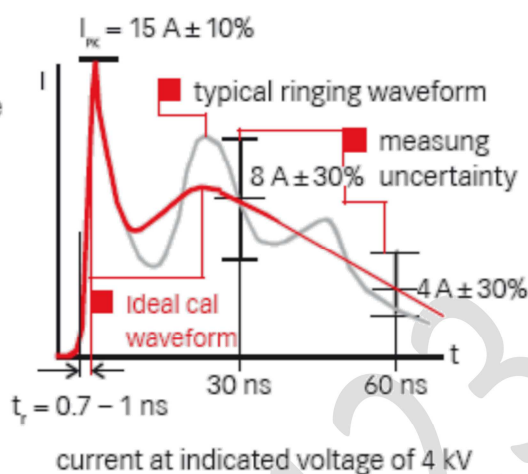
Dialog:	
C:\Programme\Teseq AG\WIN 3000\UserTests\End of the test.dlg	
Test Ends	
Check the Results and click Exit Button.	

## 3.2.2.1.4.1. Ръчни тестове

### 1. ESD / Електростатичен разряд



ESD generator equivalent circuit



Метод	Напрежение	Поляритет	Честота	Брой	Статус
Въздушен разряд	15kV	Положителен	5 kHz	3x10	
Въздушен разряд	15kV	Отрицателен	5 kHz	3x10	
Контактен разряд	8kV	Положителен	5 kHz	10x	
Контактен разряд	8kV	Отрицателен	5 kHz	10x	

Забележка:

.....

.....

.....

.....

.....

## 2. Поносимост на електромагнитни влияния



Радиостанция	Честотен обхват	Сила на сигнала	Честота	Статус
	26MHz-1000MHz	10V/m	144,5MHz	
	26MHz-1000MHz	10V/m	435 MHz	

Мобилен телефон	Статус

Забележка:

.....

.....

.....

.....

## 3. Променливотоково изпитание



Напрежение	Времетраене	Статус
4 000 V	00:00:60 Часа	

Забележка:

.....

.....

.....

.....

9.12.5.1.1.1. **Тестов каталог за сигурността на системата за дистанционно отчитане на електромери и управление за EVN БГ ЕР. Test catalogue for security requirements for distant meter reading of electrometers and control system for EVN BG EP**

Описани_Description	Резултат_Result ДА_YES or НЕ_No
<p><b>1.</b> Средата за пренос на данните от измерването, получени от Е-електромерите, трябва да се реализира посредством GPRS или PLC (комуникация по силов кабел). Техническият модул, който отговаря за комуникацията с Е-електромера, трябва да бъде монтиран в корпуса на Е-електромера. При използване на PLC комуникация, Концентраторът трябва да бъде част от комуникационната верига с Е-електромера, който трябва да може да пренася /събира данни и да комуникира с множество Е-електромери и след това да прехвърли данните до Централната система. Концентраторът трябва да може да използва комуникационната среда GPRS за установяване на канал за пренос на данни с Централната система. Централната система трябва да осигури криптографските услуги, чрез които преносът на данни до/от Концентратора и Е-електромера ще бъде криптиран. Централната система трябва да управлява криптираното съхранение на уникалните ключове на Е-електромера. The transfer environment of metering data from E-Meter must be realized with GPRS or PLC (power line communication). The technical module which is responsible for communication with E-Meter must be installed in the same corpus of E-Meter. In case of usage of PLC communication, a Concentrator must be a part of communication chain with the E-Meter which must be capable to transfer/collect data and communicate with many E-Meters and after that to transfer the data to the Central system. The Concentrator must be able to use GPRS communication environment or Ethernet connection for establishing transfer channel with the Central system. The Central system must provide a cryptographic service with which the data transfer to/from Concentrator and E-Meter to be encrypted. The central system must support the encrypted storage of the unique E-meter cryptographic keys</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>2.</b> При обработване на потокът от лични данни в системата, тези от тях които не са необходими, не трябва да бъдат запазвани или записвани. During the processing of sensitive / personal data in the system, those which are not needed must be not saved or recorded.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>3.</b> Запазената информация, която вече не е важна/необходима трябва да бъде изтривана. Saved information which is not anymore important / needed must be deleted</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>4.</b> Деликатни/лични данни от Е-електромер трябва да може в срок от не повече от 12 часа да се прехвърлят и запазват в Централната система. Sensitive/personal data from E-Meter must be able maximum within 12 hours to be transferred and saved in Central system</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>5.</b> Без разрешение, неототоризирания достъп до потока от данни трябва да бъде строго забранен. Without permission, the unauthorized access to the data flow must be strictly prohibited.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>6.</b> Всякакъв неототоризиран достъп до защитените канали (комуникационни интерфейси) трябва да е невъзможен. Unauthorized access to the protected channels (communication interfaces) must be not possible.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>7.</b> Трябва да е невъзможно получаването на непоискана информация отчетена от Е-електромерите, освен ако не става въпрос за аларми и предварително определени критични събития. The E-Meter must deliver reading out information from its registers if it is requested, with exception of alarms and defined critical events.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>8.</b> Паролите и криптографския механизъм (ключове) трябва да бъдат уникални за всеки Е-електромер в процеса на експлоатация на Централната система. Passwords and cryptographic keys must be unique for each E-Meter in the process of exploitation from Central system</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>9.</b> Командите за изключване и включване на всеки Е-електромер трябва да бъдат уникални, криптирани и кодирани с надлежните ключове, свързани с въведените криптографски услуги. Commands for switch-off and switch-on for each E-Meter must be unique, encrypted and coded with the proper keys related to deployed cryptographic service</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No
<p><b>10.</b> IT сигурността на предложеното решение трябва да може да бъде управлявана от оператора на електроразпределителната мрежа. IT security of proposed solution must be able to be managed from distribution system operator.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_No



<p><b>11.</b> Потокът от данни свързан с лична информация, като данни от измервания, актуализация на фърмуер, контролни команди (Включване/изключване на електромера, настройки и конфигурации на устройствата (Е-електромери и концентратори) трябва да се изпраща единствено по сигурна криптирана връзка. The data flow related with personal data like metered data values, firmware updates, Control commands (Switch on/off of E-Meter), device settings and configurations of E-meters and Concentrators must be solely transmitted with secured encrypted connection.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>12.</b> Всички Криптографски ключове трябва да бъдат съхранявани в Централната система, но само в рамките на защитената зона и да бъдат криптирани или неподлежащи на извличане. All cryptographic keys must be located (stored) into the Central system, but only within a protected encrypted area or unexportable</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>13.</b> Концентраторът може да се използва за съхраняване на Криптографските ключове, единствено за осъществяване на комуникационна верига с Централната система и съответните Е-електромери към нея. Криптографските ключове трябва да се съхраняват в рамките на защитена зона, криптирани или неподлежащи на извличане. The Concentrator can store in it the cryptographic keys only for communication chain with the Central system and assigned E-Meters behind it. The cryptographic keys must be stored within a protected encrypted area or unexportable</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>14.</b> Всяка команда от Централната система към Е-електромера трябва да бъде криптирана и да се изпълнява само веднъж в посока Е-електромера (Защита от атаки чрез повторение). Съобщенията се приемат единствено от удостоверени страни. Each command from Central system to the E-Meter must be encrypted and must be executed only once towards the E-meter (Protection from Reply Attacks). Messages are accepted only from authenticated parties.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>15.</b> Всички използвани криптографски алгоритми трябва да имат най-малко криптографската сила, сравнима с AES 128 (криптографската сила на алгоритъм, напр. може да бъде подобрен чрез увеличаване на дължината на ключа). All used cryptographic algorithms need minimum to have cryptographic strength comparable to AES 128 (the cryptographic strength of an algorithm, for example, can be improved by increasing key length).</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>16.</b> Уникалните криптографски ключове трябва да бъдат инсталирани от доставчика във всеки Е-електромер. Unique cryptographic keys must be deployed in each E-Meter from the vendor.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>17.</b> За вече монтираните Е-електромери, актуализацията на фърмуера трябва да се извършва чрез криптирани и сигурни комуникационни канали. Трябва да бъде дадена гаранция, че файлът с фърмуера не е манипулиран и е действително издаден от производителя. For already installed E-meters the firmware update must be done in encrypted and secured communication channel. Guarantee must be available that firmware image was not manipulated and was issued by the vendor.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>18.</b> Всички пароли, използвани в Е-електромер и Концентратора на данни, трябва да съответстват на следните минимални изисквания: Минимална дължина - 10 символа, съставени от малки, главни букви и числа, генерирани произволно и не подлежащи на възпроизвеждане. All passwords, which are implemented for E-Meter and data Concentrator, must meet the following minimum requirements: Minimum length of 10 characters, Composed of lowercase letters, uppercase letters and digits, Randomly generated and not reproducible.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>19.</b> Паролите и Криптографските ключове трябва да бъдат уникални за всяко устройство (Е-електромер или Концентратор), което взема участие в криптирането и декриптирането или в съобщенията за валидиране. Passwords and cryptographic keys must be unique for each device (E-Meter or Concentrator), which are participating the process of encryption and decryption or messages for authentication.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

<p><b>20.</b> Пароли и Криптографските ключове, които могат да бъдат използвани за съобщения за криптиране и декриптиране или за валидиране на комуникационните данни, трябва да бъдат генерирани произволно и да не подлежат на възпроизвеждане. Като пример за възможното използване, насочваме вниманието ви към следните документи: NIST Специална публикация 800-90A – Препоръки за генериране на произволни числа, чрез използване на детерминистични генератори на произволни битове. BSI TR-02102 - Криптографски модул: препоръки и дължина на ключовете. Passwords and cryptographic keys, which can be used for encryption and decryption messages or for authentication of the communication data flow, must be generated with a cryptographically secure (pseudo) random number generator and not to be able to be reproduced. As an example of a possible implementation is made at this point to the following documents NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators and BSI TR-02102 - Cryptographic module: recommendations and key lengths</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>21.</b> Всички пароли, които участват в кореспонденцията в рамките на Централната система, Концентратора и Е-електромера трябва да може да бъдат променяни дистанционно от централната система. All passwords which are participating the communication chain from Central system, Concentrator to E-Meter must be possible to be remotely changed from central system</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>22.</b> След монтаж на съответния елемент (Е-електромер или Концентратор), първоначално използваните пароли трябва да може да бъдат сменени. After installing the appropriate component (E-Meter or Concentrator), the initial used passwords must be possible to be changed</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>23.</b> Трябва да е възможно сигурно съхранение на резервни копия и съответното възстановяване на данни, съхранявани в криптографската услуга на централната система. Secure backup and restore of data stored in the cryptographic service in central system must be possible.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>24.</b> Трябва да има функции за докладване и контрол и представяне на текущото оперативно състояние на криптографските дейности. Reporting and monitoring functions and representation of the current operating state of the cryptographic service must be available.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>25.</b> Криптографската услуга трябва да осигурява въвеждане на първоначалните ключове, които се изискват за криптографските дейности. The cryptographic service should provide import of the initial cryptographic keys from vendor, which for the operation of the cryptographic service are required</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>26.</b> Криптографската услуга трябва да осигурява първоначално зареждане на криптографските ключове за криптиране на комуникацията на всеки Е-електромер в базата данни на Централната система. Всички ключове трябва да се съхраняват в криптирана форма по защитен начин в базата данни на централната система. The cryptographic service should provide initial loading of cryptographic keys for encryption of communication for each E-meter in the central system database. All keys must be stored in encrypted and protected way into the environment of Central system.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>27.</b> Криптографската услуга трябва да осигурява взаимно валидиране на Е-електромера и централната система, както и криптиране и декриптиране на съобщения между тях. The cryptographic service should provide mutual authentication of E-Meter and Central System and also Encryption and decryption of messages.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>28.</b> Криптографската услуга трябва да осигурява съдействие за подробно разследване на дефектни Е-електромери. The cryptographic service should provide support for a detailed investigation in case of defective E-Meters.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>29.</b> Криптографската услуга трябва да осигурява отчитане и контрол на статуса на системата. The cryptographic service should provide reporting and monitoring of system status</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>30.</b> Прехвърлянето на Криптографските ключове в Концентратора и Е-електромера трябва да се осъществява по начин, който съответства на процеса по сигурното доставяне (например SSH, SCP, SFTP, HTTPS или други методи с минимално равнище на криптиране AES 128). По време на мрежовата комуникация между Централната система, концентраторите и Е-електромерите може да се използва метод на валидиране – парола, сертификат, публичен ключ или симетричен ключ. Transfer of cryptographic keys to the Concentrator and E-Meter must be done in a way that corresponds to the process of secured shipping (for example SSH,SCP,SFTP,HTTPS or other methods with</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

minimum level of encryption AES 128). During the network communication between the Central system, concentrators and E-meters must be established under method of authentication – password or certificate or public key or symmetric key can be used.	
<b>31.</b> Криптографските ключове трябва да бъдат вградени в криптографската система, чрез предварително определен процес, за да може да се гарантира сигурното управление на ключовете. The cryptographic keys must be incorporated (imported) into the cryptographic service in advance defined process in order to be guaranteed the secure management of the keys.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>32.</b> Всеки Е-електромер трябва да бъде произведен с вградени уникални Криптографски ключове и в процеса на доставка на EVN EP следва да се представи пътен лист. В пътния лист се съдържа информация за производството на Е-електромерите (сериен номер и т.н.) и съответните Криптографски ключове за всеки Е-електромер. Електронната доставка следва да се осъществи в предварително определен формат и трябва да бъде изпратена на EVN EP по сигурен канал. Тази доставка след това се обработва безопасно от криптографската система на Централната система. Този пътен лист трябва да бъде криптиран и може да бъде декриптиран единствено от криптографската система към Централната система. В рамките на целия процес по доставка трябва да се гарантира, че неоторизирани трети страни няма да имат достъп до Криптографските ключове. Each E-Meter must be produced with embedded unique cryptographic keys and in the process of delivery a shipment file (list) must be delivered to EVN EP. The shipment file must contain the list of production information of E-Meters (serial number and etc.) and appropriate cryptographic keys for each E-Meter. The electronic delivery must occur in a defined format and must be transmitted to EVN EP via a secured channel. This delivery will be securely processed subsequently by the cryptographic service of the central system. That shipment file must be encrypted and can be decrypted only from the cryptographic service of Central system. Throughout the delivery process, it must be ensured that no unauthorized third party has an access to the cryptographic keys	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>33.</b> Криптографската система трябва да има възможност за изготвяне на отчети и доклади за това, кои пароли или ключове са променени, поради определени критерии. Reporting functions must be available from the cryptographic service for which keys or passwords have been changed due to certain criteria	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>34</b> Криптографската услуга би следвало да работи самостоятелно, без намесата на потребителя. Всякаква работа, по отношение на чувствителна информация или работа на криптографската услуга, трябва да се извършва съвместно от двама различни служителя. Задължително трябва да се спазва споделянето на задълженията. При опити за влизане в системата и работа с нея трябва да се реализират записи и да се генерират протоколи, които следва да бъдат защитени от неоторизирано манипулиране. Направените записи трябва да бъдат проследяеми до уникален потребител. Криптографската система трябва да позволява и прилагането на различни роли на потребителите. Cryptographic service should autonomously work without user interaction. Any operation upon sensitive information or operation of cryptographic service must be done in cooperation of two different employees. Separation of duties must be obeyed. All login attempts and user interactions have to be logged and generated protocol information must be protected against unauthorized manipulation. The log entries must be traceable to a unique user. The cryptographic service must further enable the implementation of different user roles.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>35.</b> Криптографската услуга трябва да генерира аларма в случай на неоторизирано използване. Тя трябва да предлага подходяща функционалност за отчетност и контрол, която да позволява контрол на текущото работно състояние. Cryptographic service must generate an alarm in case of unauthorized use. It should provide appropriate reporting and monitoring functionality, which allows monitoring of current operating state	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>36.</b> Криптографската услуга трябва да осигурява информация за текущо състояние на криптографската услуга – например – състояние след първоначална доставка, оперативна информация, синхронизиране с допълнителни криптографски системи, откриване на критични и не-критични грешки, открити опити за манипулации в резултат на евентуален възникнал инцидент). The Cryptographic service must provide information about current state of cryptographic service – for example initial delivery state, operational information, synchronization with redundant cryptographic service, discovering critical and not critical errors, discovered manipulation attempts as a result of occurred	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

possible security incident, ... )	
<b>37.</b> Криптографската услуга трябва да осигурява информация за подробен опис на всички възникнали грешки при работа (напр. успешно извършено запазване на резервно копие – час и дата XYZ, неуспешен опит за влизане в системата с потребителско име ABC – час и дата XYZ). The Cryptographic service must provide information about detailed listing of all occurred during operation errors (like failed logon attempt with username ABC time XYZ)	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>38.</b> Криптографската услуга трябва да осигурява информация за всички активни криптографски ключове, заедно със съответното описание за идентификация описание и последващо сравнение, за това дали резервния крипто модул също съдържа всички ключове. The Cryptographic service must provide information about representation of all active cryptographic keys together with appropriate identification description and subsequently comparing mechanism whether redundant crypto module contains all keys too.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>39.</b> Криптографската услуга трябва да осигурява информация за всички оторизирани потребителски имена със съответните им разрешителни и права. The Cryptographic service must provide information about representation of all authorized usernames with the respective designated permissions.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>40.</b> Пътният лист от продавача, който трябва да съдържа (основни данни за Е-електромерите, уникални Криптографски ключове за всеки Е-електромер) трябва да бъде подписан със собствения ключ на производителя на електромерите и да бъде криптиран. Получения пътен лист следва да бъде директно въведен в Централната система и след това трябва да започне процесът по декриптиране. The Shipment file from the vendor, which must contain (master data of E-Meters, unique cryptographic keys for each E-Meter) must be signed with the private key of the meter manufacturer and encrypted. The received shipment file must be directly imported into the Central system and after that a decryption process to be started.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>41.</b> Концентраторът трябва да разполага само с един интерфейс за поддръжка. Конфигурирането на Концентратора на данни през този порт трябва да е достатъчно надеждно защитено от кибер атаки. The Concentrator must have only one maintenance interface. The configuration of data Concentrator via a local maintenance port must be adequately protected against attacks.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>42.</b> Концентраторът трябва да може да бъде конфигуриран чрез GPRS (WAN) комуникационен порт от централната система. The Concentrator must be able to be configured through GPRS (WAN) communication port from the central system.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>43.</b> Ако се налага Концентраторът да използва местен интерфейс за поддръжка за преконфигуриране или други дейности по поддръжка, уникална комбинация от потребителско име и парола трябва да бъдат използвани за валидиране, като те трябва да съответстват на определената политика за паролите. (виж техническите изисквания). Трябва да бъде извършен запис за съответното събитие. If the Concentrator has to use the local maintenance interface for reconfiguration or other maintenance activities, a unique combination of username and password must be possible for authentication, which corresponds to the defined password policy.(see technical requirements). Record of the event must be logged in it.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>44.</b> От локалния порт за поддръжка на Концентратора не трябва да е възможен достъп до защитените зони на Криптографските ключове, които евентуално се съхраняват в него. From local maintenance port of Concentrator must be not possible to reach protected area of cryptographic keys, which are eventually stored in it.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>45.</b> Неоторизирани опити за достъп до Концентратора на данни трябва да бъдат докладвани (разглеждани) чрез мерките за сигурност от направлението за мониторинг и контрол на централната система. Задължително се прави запис в архива за съответното събитие. The unauthorized attempt for access to a data concentrator must be reported (viewed) by security measures from monitoring service of central system. Record of the event must be logged in it.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>46.</b> Данните за достъп при автоматична регистрация в мобилна мрежа трябва да бъдат уникални за всеки Концентратор. Не се допуска използване на обща информация за влизане в системата, едновременно от няколко единици. The credentials for the automatic registration in mobile network must be unique for every Concentrator. It is not permitted the usage of general login information contained by several units together.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

<p><b>47.</b> Данните за достъп при автоматична регистрация в мобилна мрежа, могат да бъдат запазвани единствено в Концентратора. При използване на SIM карта, информацията за влизане в системата не трябва да бъде съхранявана на самата SIM карта. The credentials for the automatic registration in mobile network may be saved only in Concentrator. The login Information must be not stored in the SIM card itself.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>48.</b> Доставчикът на мобилни услуги ще допуска трафик единствено между централна система и концентратора. Трафикът на данни между концентраторите трябва да се предотврати. The mobile service provider will allow traffic only between central system and concentrator. Data traffic between concentrators must be prohibited.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>49.</b> Единствено физически интерфейс (инфрачервен порт) може да се ползва за достъп без отстраняване на капака на Е-електромера. Only physical interface Infrared (IR) port must be accessible without removing the cover of E-Meter.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>50.</b> Е-електромерите трябва да могат автоматично да записват събитията, свързани с процесите по отваряне на корпуса на електромера или капака на клемния блок, и да изпращат известия до съответната централна система и да ги съхраняват в регистъра (паметта) на Е-електромера. The E-Meters must be able automatically to record the events related to the process of opening the meter housing or terminal cover is detected and to send notification to the corresponding central system and store it in the registry(memory) of E-Meter.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>51.</b> Отчетните стойности и капака на клемния блок трябва да бъдат надлежно защитени от неоторизирано физическо проникване. Опити за манипулации върху самия Е-електромер или върху интерфейсите трябва да се виждат оптически (напр. нарушени пломби). The counter values and terminal cover must be suitable protected from unauthorized physical intrusion. Manipulation attempts upon the E-Meter itself or at the interfaces must be optically visible (for example, broken seals).</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>52.</b> Е-електромерът трябва да запазва сигурността си и при наличие на грешки или възникване на нежелани или неволно предизвикани работни състояния (случайно или злоумишлено причинени). Като такива грешки могат да бъдат: загуба на захранване, грешка в процеса на изпълнение на криптографски функции, грешка в процеса на валидиране на достъпа. E-Meter must also preserve a secure state when errors and unwanted or unintended operating states (random or willfully) are caused. Such errors can be: voltage loss, error in the process of executing cryptographic functions, error in process of validating access permissions.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>53.</b> Паметта за регистъра на Е-електромерът трябва да бъде с достатъчна големина, което гарантира невъзможността за записване на нови съобщения за системния регистър, върху съществуващи такива, преди да бъдат прочетени от централната система. Минималната памет, която трябва да е налична е за поне 100 събития. The memory for the E-Meter log must be with adequate size, which ensures that no system log messages can be overwritten before they are read out by a central system. A minimum storage for minimum 100 events must be available in it.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>54.</b> Криптографските ключове трябва да бъдат съхранявани по сигурен начин в Е-електромера. Не трябва да е възможно да бъдат прочитани или записвани на друг носител. The cryptographic key(s) must be itself safely stored in the E-meter. It must be not possible to be read in plain text or exported.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>55.</b> Е-електромерите трябва да разполагат с вграден часовник и периодично трябва да бъдат синхронизирани с Централната система. The E-meter must have internal clock and at periodic intervals must be synchronized with the central system</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>56</b> При всички двупосочни интерфейси на Е-електромера трябва да бъдат приемани единствено съобщения, които са предварително дефинирани за всеки порт, от страна на доставчика. Преди приемане на съобщение, то трябва да бъде валидирано и истинността му да бъде проверена. Съобщения, които не преминат тази проверка, не трябва да бъдат отваряни. At all bidirectional interfaces of E-Meter only messages must be accepted which are previously defined for each port from the vendor. Before a message is accepted, it must be validated and accuracy to be checked. Messages that do not pass this test must be discarded.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO



<p><b>57</b> Ако Е-електромерът е монтиран, но няма комуникационна връзка с Централната система, Е-електромерът трябва да работи като стандартен електронен електромер. Трябва да са възможно основни функции, като: Некриптирано отчитане на данните, съхранявани в отчетните регистрирани стойности и профилите на товарите. (IR port може да бъде използван с Преносим терминал), некриптирано отчитане на данните, съхранявани в записите в регистъра на събитията (IR port може да бъде използван с Преносим терминал), настройване на датата и часа. (IR port може да бъде използван с Преносим терминал) If E-Meter is installed, but no communication link with the central system is established, the E-meter must operate as a standard electronic meter. Basic functions must be possible such as: Unencrypted reading out of data stored in the counter register values and the load profiles (IR port can be used by HHU), unencrypted reading out of data stored in the counter event log entries (IR port can be used by HHU), set the Date and Time. (IR port can be used by HHU).</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>58.</b> Е-електромерът в процеса на производство трябва да бъде първоначално зареден с фърмуер от производителя. The E-Meter must be initially loaded with a firmware image in the process of its production from the vendor</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>59.</b> Манипулирането на определена част от фърмуера или на настройките на фърмуер трябва да е невъзможно. Manipulation of a custom portion of the firmware or of the contained firmware settings must not be possible.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>60.</b> Трябва да е възможно актуализиране на фърмуера чрез Централната система. Коректността на актуализациите на фърмуера трябва да бъдат проверени поне чрез hash код на файла за даунлоад, който е поискан чрез криптирано съобщение между централната система и Е-електромера. Е-електромерът не трябва да започва процес на зареждане на новия фърмуер ако липсва автентичиран hash код. Firmware update must be possible from the central system and must not influence the metrological part of E-Meter. The integrity of the firmware updates must be protected at least by hash code of the downloadable file which is sent through a unicast (one to one) authenticated and encrypted message and the E-Meter must not activate downloading process without having received the authenticated hash code.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>61.</b> В случай на повреда при инсталирането на актуализацията на фърмуера, започналата операция не трябва да влияе на съответните компоненти и Е-електромера трябва да продължи да работи със стария фърмуер. In case of corruption of the update firmware operation, the operation must not affect the respective component and E-Meter must continue to operate with old firmware.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>62</b> Измерените данни (съхранени данни – стойности от брояча, събития и конфигурация) не трябва да бъдат променени или трети в процеса на актуализация на фърмуера. The metered data (stored data – counter values, events and configuration) are not allowed to be changed or deleted during the process of update of the firmware.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>63.</b> Производителят на Е-електромерите трябва да гарантира, че фърмуера за тях е произведен по дефиниран и внедрен вътрешен процес. The vendor of E-meter must ensure that only a firmware image which is derived from the associated E-meter manufacturers has been released by a defined approval process.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>64.</b> Софтуерът на Централна система трябва да е съвместим със сървърна архитектура x86. The software of Central system must be compatible with x86 server architecture.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>65</b> Централната система трябва да е съвместима с операционна система Microsoft Windows 2008 сървър 64 bit или следващи варианти или Red Hat v 6.3 64 битова и следващи версии. The Central system must be compatible with operating system Microsoft Windows 2008 server 64 bit or higher or Red Hat v. 6.3 / 64 bit or higher.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>66</b> Графичният потребителски интерфейс на софтуера на централната система трябва да бъде ергономичен и да съответства на стандарт EN ISO 9241. Graphical user interface of software of central system must be ergonomic and refer to EN ISO 9241 standardization</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>67</b> Централната система трябва да дава възможност за реализация на концепцията за оторизация по роли. Правата на потребителите трябва да бъдат дефинирани за всяка отделна роля, заедно със съответните разрешителни. Различните потребители, в зависимост от своите функции, трябва да имат роли, съответстващи на задълженията им. Прилагането на ролева оторизация трябва да позволи максимално разделение на функциите. The Central system must allow implementation of role-based authorization concept. User rights must be defined for each role with appropriate necessary permissions. The various users depending on their function must have assigned role corresponding to their</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

duties. The implementation of a role-based authorization concept must allow maximum separation of functions.	
<b>68</b> Паролите, съответстващи на правата на потребителите, трябва да се съхраняват по начин отговарящ на въведения механизъм за сигурно криптиране и трябва да не подлежат на възпроизвеждане. Паролите трябва да бъдат управлявани на централно ниво. Passwords corresponding to user rights must be kept in a way which correlates to the deployed secure encryption mechanism and must be not reproducible. Passwords must be managed centrally.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>69</b> При софтуера следва да се прилага принципа на 4-те очи за особено важните функции на централната система. Най-съществените функции на системата, които се нуждаят от потвърждение преди изпълнението си, трябва да бъдат конфигурирани по начин, който налага присъствието на поне 2 служители, които да одобряват съответните дейности, преди започване на тяхното изпълнение (пример: процес за прекъсване на електричеството). Software must assist 4-eyes principle for a critical central system functions. Critical system functions that need confirmation before execution must be configured in a way that requires at least 2 employees approve before the start of execution (example: process for switch off / switch on of electricity).	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>70</b> Командите за функциите на критични системи функции за всеки от Е-електромерите трябва да бъдат уникални и разпространението им не трябва да се изпълнява като излъчване до всички Е-електромери. Commands for critical system functions for each E-Meters must be unique and their distribution must be not performed as a broadcast to all E-Meters	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>71</b> Сигурно регистриране на всички дейности и защита от посегателства трябва да се осъществява по време на изпълнението на особено важни команди по отношение на Е-електромерите. Tamper-proof (secure) logging of all activities must be undertaken during the execution of critical commands towards the E-Meters.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>72</b> Записите в регистъра трябва лесно и по уникален начин да идентифицират дейностите на служителите. Assignment of log entries must easily and uniquely identify employees' activities.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>73</b> Централната система трябва да осигури възможност за максимален брой дневни дейности по отношение на Е-електромера. При достигане на подлежащия на конфигуриране максимален брой, системата трябва да изпрати предупреждение. Промяната в дневните лимити трябва да може да е извършва от поне двама служители на EVN EP (съответствие с принципа на 4те очи). The Central system must provide the possibility of maximum number of daily activities towards the E-Meter. If the configurable limit is reached, the system must send an alert. The change of the daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle).	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>74</b> Поради уникалността на командата за прекъсване на захранването чрез главния прекъсвач за всеки Е-електромер, трябва да бъде приложен логически алгоритъм, който регулира колко Е-електромера максимално могат да бъдат изключени в рамките на един ден. При достигане на конфигурираната максимална стойност, Централната система трябва да спре процесът по изпълнение и генериране на предупреждение. Промяната на дневните максимални стойности трябва да е възможна единствено при участие на двама или повече служителя на EVN EP (спазване на принципа за 4-те очи и процедурата за одобряване). Due to the uniqueness of "switch off" command towards the circuit breaker for each E-Meter, a logical algorithm must be applied which regulates how many E-Meters can be switched off maximum per day. If the configurable limit is reached, the central system must stop the process of execution and generate an alert. The change of daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle and approving procedure).	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>75</b> Централната система трябва да осигурява за всички Е-електромери и Концентратори синхронизация на часа, въз основа на вътрешен стандарт, като NTP с външен таймер или вече приложен такъв във вътрешните мрежови таймери. The central system must provide for all E-Meters and Concentrators time synchronization based upon international standard, like NTP protocol with an external timer or an already implemented in the internal network timers.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

<p><b>76</b> Часът на монтираните Е-електромери трябва да бъде периодично проверяван и, ако е необходимо, синхронизиран с Централната система. Отклоненията в часа на инсталираните Е-Електромери и Централната система трябва да се съобщават под формата на алармено съобщение. (Прекомерните отклонения могат да са знак за неизправност или манипулация на Е-електромера) The time from all installed E-Meters must be periodically checked and, if necessary, synchronized with the central system. Deviations of the time of installed E-Meters and Central system must be reported as an alarm message. (Excessive deviations could be a sign of a malfunctioning or manipulation of the E-Meter)</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>77</b> Централната система трябва да осъществява надлежен контрол и отчетност на всичките си функции. При неизправност следва незабавно да се генерира и изпраща известие до отговорния персонал. The central system must make an appropriate monitoring and reporting of all its functionalities. In case of malfunctions automatically a corresponding notification to the responsible personnel to be generated.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>78</b> Дадените разрешения и потребителски права на всички служители, които имат достъп до Централната система и до съответните компоненти на Е-електромера, трябва да бъде възможно да се проверяват периодично. The assigned permissions and user rights of all employees which have an access in the Central system and to the respective components of E-Meter infrastructure should able to be checked periodically.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>79.</b> Централната система трябва да генерира справка, в която да има списък с всички потребители с дата на определяне на пълномощията им, дата на първа регистрация, дата на последен успешен вход в системата, роля на потребителя. The central system must generate a List of all users with the date of definition, date of first registration, date of last successful login, role membership of the user.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>80.</b> Централната система трябва да генерира справка, в която да има списък с всички разрешения, свързани с дадена роля в Централната система. The central system must generate a List of all permissions associated with a role in the central system.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>81.</b> Централната система трябва да генерира списък с оценка, според различни показатели (напр. всички потребители, които имат право да осъществяват дадено действие). The central system must generate a list of evaluation according to various dimensions (for example- all users who are allowed to perform a certain action)</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>82.</b> Централната система трябва да може да поддържа исторически данни за разрешенията на потребителите (трябва да се съдържа подробна информация относно това кои потребители, какви права са имали в даден момент). The central system must support historization of permissions of users (it should be comprehensible, about what permissions a user had at a particular time).</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>83</b> Всички промени в конфигурацията на Централната система трябва да бъдат регистрирани. Съхранените записи за съответните промени следва да бъдат защитени. Информацията в регистъра трябва да бъде ясна и точна. Any changes to the configuration of the central system have to be recorded. The stored log entries against subsequent change have to be protected. The log information must be clearly reported.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>84</b> Всички промени в Централната система (напр. – ръчно манипулиране на показания, замяна на стойности) трябва да бъдат регистрирани, уникални и обвързани със съответния потребител. Трябва да има налични хронологични данни за дейностите на всички потребители. All changes in the central system (for example - manual manipulation of readings, replacement of values) must be logged, unique and assigned to a particular user. Historization of all user activities must be available.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>85</b> Ако в монтирани Е-електромери възникне критично системно събитие, съответната аларма трябва да бъде изпратена до 5 минути до Централната система. If in the installed (deployed) E-Meters a critical system event is recognized then an appropriate alarm must be within 5 minutes sent to the central system.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>86</b> По време на периодичното отчитане на съответните измерени стойности от Е-електромерите, цялата съхранена в тях информация за събития трябва да може да бъде прехвърлена в централната система. During the periodic reading of the corresponding measured values from E-Meter, all stored in it event information must be able to be transported to central system.</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<p><b>87</b> Приложението за дейности по поддръжката трябва да е съвместимо с операционната система на Преносимия терминал - Microsoft Windows mobile professional v.6.5 или библиотеките (SDK) за интегриране в съществуващи приложения. The application for maintenance tasks must be compatible with HHU operating system -</p>	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

Microsoft Windows mobile professional v.6.5 or libraries (SDK) for integration with existing legacy application.	
<b>88</b> Клиентската част от приложението на Централната система трябва да може да работи на терминален сървър с Microsoft Windows 2008 server 64bit. The client part of the central system application must be able to run on terminal server environment with Microsoft Windows 2008 server 64bit.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>89</b> При неуспешно изпълнение на функцията по „включване“ от Централната система по отношение на даден Е-електромер в рамките на 4 часа, трябва да се генерира автоматична команда за задача по поддръжка към Преносимия терминал за да се осъществи ръчно „включването“ на Е-електромера. In case of not successful execution of „switch on“ or „switch off“ function from central system towards the E-Meter in the timeframe within 4 hours, an automatic workorder must be created for maintenance task towards the HHU in order manually to perform the „switch on“ or “switch off” function for the E-Meter.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>90</b> След ръчното изпълнение на функцията „вкл.“ или „изкл.“ на Е-електромера от HHU от страна на служител, централната система трябва да дава възможност (интерфейс) HHU да може да отчита състоянията на вече изпълнените заявки за работа към Е-електромерите. After manual execution of “switch on” or “switch off ” function towards the E-Meter by HHU from employee, the central system must give possibility (interface) that HHU can report statuses of already executed workorders towards E-Meters.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>91</b> Централната система трябва да поддържа справочен механизъм, с който Изпълнителят да може сам да създава съответните доклади от системата. The Central system must support reporting mechanism with which the Contractor can create by itself adequate reports from the system.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO
<b>92.</b> Доставчикът на Централната система трябва да поддържа централна служба за съобщения (24/7/365), която да се ползва от възложителя за проследяване и категоризиране на възникнали грешки при експлоатация на системата. The vendor must assure an availability of ticketing and reporting portal (24/7/365) which can be used from the Contractor for tracing and categorization of errors which are coming in the process of exploitation of the central system.	<input type="checkbox"/> ДА_YES / <input type="checkbox"/> НЕ_NO

Становище: Представената от кандидата тестова мостра на „Система за дистанционно отчитане на електромери“ ПРЕМИНА\* / НЕПРЕМИНА\* теста.

\* Невярното се зачертава.

За Възложителя (комисия, име и подпис):

За Кандидата (Име, подпис и дата) :

### Въпросник за подбор\*

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

\*Точки от 1 до 5 от въпросника се попълват от Възложителя, а само т.6 се попълва от Кандидата .

1	<b>ОБЩА ИНФОРМАЦИЯ</b>	
1.1	Кандидат	
1.2	Лице за контакт	
1.3	Телефон, факс, имейл	
1.4	Налична ли е промяна в обстоятелствата, декларируани с подаване на заявлението	
2	<b>ЗАЯВЛЕНИЕ</b>	
2.1	Дата на подаване на заявлението	
2.2	Производител	
2.3	Кратък профил на производителя (основна дейност, интернет страница, новини от последните 12 месеца)	
2.4	Списък на приложените към заявлението документи. Копие на документа за закупуване на документацията за участие	
2.5	Подписани и подпечатани от участника: проекто-договор, търговски условия, технически изисквания, общи условия на закупуване на дружествата от групата на EVN и клауза за социална отговорност на дружествата от групата на EVN,	
2.6	Детайлно техническо описание на предлаганите стоки и/или услуги	
3	<b>ЮРИДИЧЕСКО ЛИЦЕ</b>	
3.1	Име	
3.2	Форма на ЮЛ	
3.3	Представляващи	
3.4	Начин на представяване	
3.5	Актуално състояние (несъстоятелност, ликвидация)	
3.6	Документи, удостоверяващи правосубектността на кандидата, съгласно т.1.4. от „изискванията за юридическо състояние“	
3.7	Декларации № 1, 2, 3, 4, 5	
4	<b>ТЕХНИЧЕСКИ ВЪЗМОЖНОСТИ И КВАЛИФИКАЦИЯ</b>	
4.1	Въпросник за подбор - т.6	
4.2	Описание на системата	
4.3	Описание на компонентите	
4.4	Описание на изискванията към хардуера за всеки елемент	
4.5	Ръководство за потребителя	
4.6	Протокол за успешно преминал функционален тест съгласно т.1.12 от изискванията за „технически възможности и квалификация	
4.7	Внедрена система за контрол на качеството, сертифицирана по ISO 9001-2008 или еквивалентна	
4.8	Доказателства за инсталация на поне 100 000 Електромера с Power Line Communication (PLC) управлявани от една система на територията на Европейския съюз	
4.9	Доказателства за собственост на соурс кода на софтуера, който управлява системата или права от собственика на софтуера да прави корекции в него	
4.10	Доказателства, за сътрудници на трудов и граждански договор за осъществяване на поддръжката на софтуера и хардуера на системата	
4.11	Доказателства, за 24/7 часов онлайн служба за съобщения и телефон хелп деск (Help Desck) – предоставяне на информация за тестов достъп до система	
4.12	Оторизация за разпространение на оборудването на територията на България.	
4.13	Дата на валидност на оторизацията	
5	<b>ФИНАНСОВА ИНФОРМАЦИЯ</b>	
5.1	Възложителя няма изисквания към кандидатите.	



6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
I. Функционални изисквания към Система за дистанционно отчитане		
1. Автоматично отчитане		
Системата за дистанционно отчитане трябва да има налични функционалности за автоматично отчитане, които позволяват:	Всички данни, към 00:00 ч. на текущия календарен ден, да са предадени в Централната система при мрежовия оператор най-късно до 12:00 ч. на същия ден	
	Всички събирани данни към 00:00 ч. да се съхраняват в системата. При следващи заявки за отчитане трябва да се отчетат само липсващи стойности	
	Ежедневно отчитане на всеки 15 минути на товари профили за електромерни показания (активна енергия в двете посоки) на електромери	
	Отчитанията на данните за фактуриране и дневниците да не подлежат на изискването за ежедневно отчитане. Мрежовият оператор може да планира индивидуално отчитане, както и различни фиксирани заявки за отчитане	
	Да се конфигурира времеви график за отчитане поотделно за режимите PUSH /предаване на данни/ и PULL /приемане на данни/.	
	При режим PUSH времевият график за отчитане да се конфигурира в електромера	
	При режим PULL графикът за отчитане се управлява от централната система	
	В графика за отчитане да се определя кои електромери кога трябва да се отчетат	
1.2 Ниво на поддръжка:		
Минимални изисквания:	При стартиране на отчитането на стойностите към 00:05 ч. в рамките на най-много 12 часа трябва да са отчетени 99 % от всички електромери	
2. Ad hoc- отчитане		
2.1 Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за Ad hoc-отчитане, които позволяват:	Получаване на актуални електромерни данни при запитване от страна на оторизирани участници (при спазване на разпоредбите за защита на данните). Това запитване мрежовият оператор изпраща на съответния електромер под формата на команда за отчитане. Обхватът на данните може да се дефинира (напр. дневници, данни за фактуриране, данни за товаров профил).	
	В случай, че ad hoc-отчитането е завършило без успех, следва да има възможност за отчитане на място	
2.2. Ниво на поддръжка:		
Минимални изисквания за нивото на поддръжка	В 99 % от случаите, за време по-малко от 5 мин.	
3. Отчитане на място		
3.1. Описание на функцията:		

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Системата за дистанционно отчитане трябва да има налични функционалности за отчитане на място, които позволяват:	Отчитане на електромера на място посредством мобилен терминал, през интерфейса за поддръжка P0	
	Спазване на строгите разпоредби относно защитата на данните: Въведен в мобилния терминал индивидуален ключ/ парола, който дава право да се отчете съответния електромер	
	Предаване на получените данни на централната система	
	Отбелязване на всяко отчитане в протокола за достъп.	
	Спазване на изискванията в областта на сигурността.	
3.2. Ниво на поддръжка:		
Минимални изисквания за нивото на поддръжка:	100% отчитане на данните и изпращане до централната системата	
4. Изключване		
4.1. Дистанционно изключване		
Минимално изискване	За изключванията не трябва да се използва групова респ. масова команда (Broadcast).	
4.1.1. Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за дистанционно изключване, които позволяват:	Електрозахранването на даден обект да бъде изключено дистанционно , като централната система на мрежовия оператор изпраща до желанния електромер команда за изключване	
	Изключването да се извършва чрез отваряне на прекъсвача (Breaker), намиращ се в електромера	
	Изключване на група електромери, посредством интерфейс с друга система (напр.Билинг) или файл - списък в подходящ формат – CSV, TXT, XLS с електромери със съответната команда.	
	След изпълнение на командата за изключване, подадена от централната системата електромера да изпраща обратно към централната системата статус „Изключен“	
	Статуса „Изключен“ също така да бъде ясно изобразен на дисплея на електромера (напр. OFF).	
	След изключване да няма възможност за незабавно повторно включване на място от страна на клиента	
4.1.2. Ниво на поддръжка:		
Минимални изисквания за нивото на поддръжка	В 99 % от случаите за време по-малко от 5 мин	
4.2. Изключване на място през интерфейса за обслужване		
4.2.1 Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за прекъсване на място през интерфейс P0, които позволяват:	Електромерите да се изключват на място посредством мобилен терминал чрез интерфейса за обслужване	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	Да бъдат спазени строгите разпоредби относно защитата на данните - в мобилния терминал трябва да се въведе индивидуален ключ/ парола, който дава право да се изключи съответния електромер	
	Управлението на ключовете да съответства на концепцията за сигурност	
4.2.2 Ниво на поддръжка:		
Минимални изисквания за нивото на поддръжка	В 100% от случаите, при непосредствено подаване на командата от мобилния терминал	
5. Включване		
5.1 Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за включване на комутиращото реле в електромера, които позволяват:	Електромерът да получи от централната системата или чрез интерфейса за поддръжка, команда, активираща включването.	
	След изпълнение на команда „включване“ електромерът да визуализира това състояние на дисплея и да изпраща това състояние като съобщение (статус) в централната системата	
	Включване на група електромери, посредством интерфейс с друга система (напр.Билинг) или файл - списък в подходящ формат – CSV, TXT, XLS с електромери със съответната команда.	
5.2. Ниво на поддръжка		
Минимални изисквания за нивото на поддръжка	В 99 % от случаите за време, по-малко от 5 мин	
6. Синхронизиране на дата и час		
6.1 Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за синхронизиране на дата и час, които позволяват:	Да се проверява актуалното време	
	Да не се предприемат действия, ако констатираното отклонение е до 2 секунди.	
	Ако отклонението е между 2 и 9 секунди, времето да се синхронизира, без вписване в дневника на събитията	
	Ако отклонението е по-голямо от 9 секунди, времето да се синхронизира и да се предприеме вписване в дневника на събитията и в товаровия профил, ако е конфигуриран (показание с дата и час и вписване за статуса).	
	Да се запази хронологията ("номерацията") на измервателните стойности	
	Синхронизирането да се извършва от централната системата през WAN-интерфейса. Да е възможно да се извърши също и на място чрез интерфейса за сервизно обслужване. Цикълът на синхронизиране да може да се параметризира	
6.2 Ниво на поддръжка:		

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Минимални изисквания за нивото на поддръжка	99,9 % от крайните устройства да имат правилно системно време.	
7. Изпращане на АЛАРМИ		
7.1 Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за изпращане на аларми, които позволяват:	Алармените събития да се дефинират от мрежовия оператор	
	Да се изпращат автоматично и незабавно от електромера към централната система	
	Алармата задължително да изисква действие респ. намеса (индиректна или директна).	
	Алармите да бъдат пренесени до централната система в рамките на максимум 5 минути (при минимум 10% от всички крайни устройства месечно)	
	Събитията и съобщенията да бъдат автоматично или индивидуално отчетени	
	Режимите на работа да бъдат отчетени дистанционно	
	Еднозначна идентификация на произхода	
	Тип на събитието респективно информация в ясно формулиран текст	
	Дата/Час на събитието	
	Събитие/Категория на грешката напр.: - Информативна - Критична грешка: не премахната - Грешката не е окончателно валидирана -	
7.2 Ниво на поддръжка:		
Минимални изисквания за нивото на поддръжка	99% в рамките на 5 минути	
8. СЪБИТИЯ / events /		
8.1 Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за изпращане на събития, които позволяват:	Събитията да бъдат протоколирани в подходяща форма от съответните системни компоненти, но без да се предават незабавно към централната система Събитията служат за гарантиране на качеството и се специфицират от мрежовия оператор	
	Компонентите да създават еднозначни съобщения за събитие (вид на събитието; момент на поява и продължителност; момент на предаване, ...), да се записват в паметта, предназначена за събития, / в дневника на събитията и да се прехвърлят към централната система по време на периодичното отчитане на електромерите или при поискване	
8.2 Ниво на поддръжка:		
Минимални изисквания за нивото на поддръжка	99 % до 6 часа	
9. Регистриране и идентифициране на крайни устройства		
9.1 Описание на функцията:		

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Системата за дистанционно отчитане трябва да има налични функционалности за регистриране и идентифициране на крайни устройства, които позволяват:	При монтаж и подмяна на електромери, обхващаща голяма територия, трябва да е възможно автоматичното идентифициране и регистриране в системата на минимум 1 000 крайни устройства дневно	
	Най малко 80% от крайните устройства да се регистрират в централната система до 15 минути	
	Максималното време за регистрация е 24 часа за най-малко 99% от крайните устройства, при монтаж на 1000 крайни устройства дневно.	
	При превключване на изводи НН (напр. към друг трафопост/концентратор на данни) всички засегнати електромери трябва до 24 часа автоматично да се изключат от вече недостъпния концентратор на данни и да се регистрират в новия концентратор на данни (най-малко 99% от всички засегнати електромери)	
9.2 Ниво на поддръжка:		
Минимални изисквания за нивото на поддръжка	99 % до 24 часа	
10. Дистанционно конфигуриране на системни компоненти		
10.1 Описание на функцията:		
Системата за дистанционно отчитане трябва да има налични функционалности за дистанционно конфигуриране на системни компоненти на крайни устройства, които позволяват:	Успешно дистанционното конфигуриране, извършено в рамките на 5 минути и потвърдено в централната система	
	Месечно да могат да бъдат прекофигурирани 3% от всички крайни устройства	
11. Паралелни процеси и приоритети		
11.1 Изисквания към преноса на данни		
Системата за дистанционно отчитане трябва да поддържа паралелна работа на следните процеси:	Изпращане на данни за потреблението	
	Автоматизиране на клиентски процеси (напр. прекъсване и възстановяване на захранването)	
	Автоматично регистриране и идентифициране на крайни устройства	
	Online-команди за комутиране	
	Дистанционно конфигуриране на системни компоненти	
	Автоматичен пренос на аларми	
	Пренос на събития и оперативни данни при поискване	
11.2 За различните приложения в системата за дистанционно отчитане трябва да е възможно да се зададат следните приоритети:	Автоматичната информация трябва да е предадена към централната система в рамките на 5 минути	
	Конфигурациите на системните компоненти трябва да се извършат успешно в рамките на 5 минути	
	Най-късно 24 часа след инсталирането им крайните устройства трябва автоматично да се регистрират в централната система	
12. Допълнителна функционалност, която не е дефинирана в настоящите изисквания		



6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
II. Допълнителни изисквания към системата		
1. PLC комуникация:		
Системата за дистанционно отчитане трябва да отговаря на следните изисквания по отношение на PLC комуникацията:	PLC-комуникацията трябва да е защитена срещу съседните й системи, така че при експлоатация на съседните системи да бъде гарантирано, че горепосочените данни ще бъдат пренесени с изискваната разполагаемост	
	При PLC комуникация следва да се декларира възможността за промяна на носещата честота за комуникация или друга фиксирана честота съобразена с наличната честота за модулация на съществуваща система и отстояща от честота на наличната система така че комуникационните сесии на отделните системи да не влияят една на друга, за да се гарантира работа на две системи в една мрежа	
	Широчините на честотните ленти на системните компоненти трябва да са така оразмерени, че да гарантират изпълнението на изисквания съгласно концепцията за сигурност	
	PLC-системата трябва да е оразмерена така, че при 1000 крайни устройства за един концентратор на данни при едновременни, максимални трансфери на данни да бъдат спазени необходимата разполагаемост и определените времена за реакция	
	Да гарантирана комуникация при изводи на трафопостове с дължина до 1,5 км., както и линии с до 5 прехода от въздушна линия към друга въздушна линия, състояща се от няколко проводника с еднакъв потенциал.	
	Системата PLC трябва да е устойчива срещу погрешни сигнали, така че въпреки временни обратни въздействия върху мрежата от страна на клиентски съоръжения, да се спазят необходимата разполагаемост и определените времена за реакция	
	За случаи на смущения от електрически уреди в клиентски съоръжения е необходимо да бъдат предложени подходящи филтри за намаляване на тези смущения	
2. Обхват на Системата за дистанционно отчитане		
Оразмеряването на Системата за дистанционно отчитане като йерархичната система: Централна система - Концентратор на данни- крайни устройства (електромери), да бъде направено така, че да позволява нормална работа при следните количества/бройки:	Най-малко 10 000 електромерни портали към централната система	
	Най-малко 1 000 крайни устройства към един Концентратор на данни	
3. Изисквания към мониторинга на разполагаемостта и на времената за изпълнение на процесите		

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Системата за дистанционно отчитане трябва да разполага с възможности за мониторинг и изпълнение на процесите при следните изисквания:	Времето за изпълнение (времето между възлагането на поръчката от водещите системи и предаването на положителна обратна информация до водещата система, на всяка отделна команда трябва да се измери и запише в централната система	
	Трябва да се измерва и записва също и времето за изпълнение на масови команди (напр. ежедневните отчитания)	
	Резултатите от този мониторинг трябва да се извеждат на интерфейс за предоставяне на информация (Webservice).	
4. Специфични изисквания за регистриране и обработка на събития и аларми		
Системата за дистанционно отчитане трябва да има следните специфични възможности по отношение на възникнали събития и аларми в крайните устройства:	Всички отчитания на електромери и събития на всички системни нива трябва да се протоколират и да им се добавят времеви печати (възникване и продължителност на събитието)	
	Събитията/Алармите трябва да се запамятват във всички децентрализирани компоненти (електромери, прекъсвачи, гейтове) както и в централизираната система за период от време, променлив и настройван за дадена Група Аларми и Събития, като се запамят минимум 100 записа	
4.1 Анализ на грешки и оптимизация		
4.1.1 Конфигурация за обработването на събития и аларми		
Системата за дистанционно отчитане трябва да има следните възможности за конфигуриране и обработка на възникнали събития и аларми::	За обработването на критични ситуации е необходимо централизираната система да е в състояние да интерпретира събития и аларми както и да генерира филтри с цел изготвяне на справки	
	Съдържанието на справките трябва да е достъпно за потребителите или да се съхранява в желан файлов формат (например *.csv, .txt, .xls ...).	
	В централизираната система е необходимо всяко прието събитие/аларма да се документира, като за целта е възможно правилата за това свободно да се изберат (напр. само да се протоколират, създаване на тикети, и др. )	
	При това трябва да се създаде времева връзка между събития/аларми	
4.1.2 Справка за активните и проверените събития и аларми		
Системата за дистанционно отчитане трябва да има следните възможности и функционалности за извеждане на справки/:	Централната система трябва да предлага функционалност за извеждане на информация относно активни събития и аларми и историята на различни събития/аларми	
	Да е налице възможност събитията/алармите да се сортират по различни критерии, като времеви период, тип на събитие/аларма, електромер, група от електромери, и др	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	Централната система трябва да предлага функционалност за ръчно и автоматично изтриване на събития/аларми	
4.1.3 Конфигурация на филтри за различни събития/аларми		
Системата за дистанционно отчитане трябва да има следните възможности за конфигуриране на филтри.	Да се правят конфигурации за един електромер, за група електромери както и за всички електромери	
	Възможности за получаване на събития/аларми трябва да са налични и за Концентратора на данни	
	Автоматично, съгласно зададения календарен график, да се генерират справки за комуникационните устройства, от които липсват данни или с които няма връзка	
	Автоматично, съгласно зададения календарен график за отчитане, да се генерират справки за крайните устройства, за които липсват данни.	
	Автоматично, съгласно зададения календарен график	
	За анализ на енергийния баланс: Системата да има възможност за изчисляване на баланс по участъци от мрежата, дефинирани от оператор – сума от отчетената енергия от търговски електромери с еднакъв календарен график за отчитане и балансов електромер със същия график. Автоматично, съгласно зададения календарен график, да се генерират файлове с участъците от мрежата (изводи), където е измерен дебаланс на енергията – извън предварително зададени от оператора граници	
	Измервателни данни – за период, последни данни, автоматично и ръчно генериране на файлове, шаблони за форматиране на файловете (дата, час, сер.ном.на устройството, ТП, извод, адрес, данни1, данни2, данни3 и т.н.), стандартни формати CSV,XLS	
4.1.4 Справки за събития/аларми и причислени филтри		
Системата за дистанционно отчитане трябва да има следните възможности за извеждане на справки и информация:	В централната система трябва да е възможно да се извежда информация относно това към кои събития/аларми какви активни филтри са причислени. Възможностите за анализиране относно филтрите, които в даден период от време са били активни, трябва да бъдат описани	
	В централизираната система трябва да е възможно проследяването на това какви събития/аларми и какви филтри за били зададени	
	Трябва да е налице възможността да се изготвят справки за историята на активни филтри	
III. Напълно електронен електромер с разпознаване на манипулации, интегриран модем и реле за управление на		


6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
товара		
1. Технически данни		
Вид консумация	Електромерите трябва да измерват активна и реактивна енергия – A+, A-, Опция: QI, QII, QIII, QIV	
Сила на тока	Позиции 1 и 2: 5(60)A или 10(60)A	
	Позиция 3: 5(10)A	
Номинално напрежение	Позиция 1: 230V	
	Позиции 2 и 3: 3x230/400V	
Номинална честота	50 Hz	
Клас на точност	Позиции 1 и 2: 2 (MID A, съгласно IEC клас 2)	
	Позиция 3: 1 (MID B, съгласно IEC клас 1)	
Видове тарифи	Електромерите трябва да бъдат много-тарифни (най-малко 4 тарифи) параметризирани с 2 тарифи	
	Електромерите трябва да разполагат с циклично показване на данните на LCD-дисплея	
	Запамените самоотчети (билинг стойности) от минали периоди не трябва да се визуализират на дисплея	
Управление на тарифите	Управление на тарифите трябва да бъде посредством вътрешен часовник (с лятно/зимно превключване)	
Самоотчет (билинг)	Самоотчетът (билингът), предизвикан от вътрешния часовник, трябва да се извършва в 00.00 на дата, дефинирана от системата дата. Определяне на дата за край на билинг период следва да може да се задава дистанционно	
Канал за обмен на данни	Електромерът трябва да разполага с IR порт за обмен на данни	
	Електромерът трябва да разполага с Power Line интерфейс за обмен на данни, според блоковата схема от техническата спецификация	
Контролен изход	Позиции 1 и 2: Препоръчително 1000 Imp./kWh	
	Позиция 3: Препоръчително 10000 Imp./kWh	
2 Общи изисквания		
Одобрение за използване за търговско измерване на ел. енергия в Р. България или MID сертификат	Допускат се електромери, вписани в Държавния регистър на одобрените за използване в страната средства за измерване. Следва да се представи копие от вписването в държавния регистър – свидетелство за одобрен тип	
	Допускат се електромери, сертифицирани съгласно Директива за измервателните уреди (MID). Следва да се представи копие от MID сертификат, заедно с типовото изпитание	
	Необходимо е наличието на валиден сертификат на производителя по EN ISO 9001 или еквивалентен	

6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Изисквания за проектиране и експлоатация	Електромерите трябва да са структурно проектирани и произведени така че при фиксирани експлоатационни и нормални условия на работа, да не възникват опасности	
Трябва да бъдат осигурени следните изисквания за безопасност	Безопасността на хората срещу токов удар	
	Безопасността на хората срещу ефектите на повишена температура	
	Сигурност и устойчивост на топлина и огън	
	Защитата на корпуса на електромера срещу проникване на твърди предмети, прах и вода (най-малко IP51 или по-висока)	
	Защита на хората срещу събития, засягащи здравето (изпарения, остри ръбове, ...).	
	Електромерите (включително и интерфейсите) трябва да имат защита срещу механични и електрически опити за манипулиране	
	При нормална работа всички части на електромерите трябва да бъдат ефективно защитени от корозия. Защитните слоеве трябва да бъдат достатъчно здрави, така че да не могат да бъдат повредени от атмосферните влияния, при определените условия на работа	
2.1 Корпус		
Изискване за монтиране на електромера към таблата за монтаж:	Продукта съответства на DIN 43857 част 1 за Позиция 1	
	Продукта съответства на DIN 43857 част 2 за Позиции 2 и 3	
Минимални изисквания за защита на корпуса	Електромерът трябва така да е конструиран че отваряне на корпуса не трябва да е възможно без неговото разбиване (например да е залепен или заварен). Препоръчително е да е налице възможност за пломбиране.	
Минимални изисквания за защита на електромера от манипулации и осигуряване на надеждна работа	Ако електромерът може да се отваря без да се уврежда, то трябва да е налице контакт, регистриращ отварянията на корпуса на електромера и задължително да е налице възможност за пломбиране	
	Корпусът трябва така да се пломбира, че вътрешните части на електромера да станат достъпни едва след счупване на пломбата/пломбите. Отстраняването на капака на корпуса не бива да е възможно без използване на инструменти.	
	Корпусът трябва да е конструиран и разположен така, че при временна деформация да не се наруши надеждната работа на електромера.	
	*Препоръчително е корпусите да се изработват от годен за повторна употреба изолационен материал в съответствие с клас на защита II	



6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Изисквания за защита на винтовите съединения	Всички болтове трябва да са изработени от метал и да се комбинират с метална втулка с резба. Пластината за телта на пломбата трябва да е отливка с кутията или с клемния капак.	
<b>2.2 Клеми, клемен блок</b>		
Когато клемите са подредени в един или повече клемни блокове, те трябва да имат достатъчно добра изолация и механична здравина	Задължително изискване	
На клемния блок електромерът не трябва да има връзки за калибриране	Задължително изискване	
Материалът на клемния блок трябва да издържи изпитванията по ISO 75-2 при температура от 135°C и налягане от 1,8 MPa (метод A).	Задължително изискване	
Входящите отвори в изолационния материал, които водят до клемите, трябва да бъдат достатъчно големи, така че през тях да може да премине и изолацията на проводника	Задължително изискване	
Основните клеми трябва да бъдат изработени като втулкови клеми или рамкови клеми с по един или два клемови винта за използването на прави и кръстати отвертки	Типът на главата на винта трябва да бъде Pozidriv-Kombi 2 за Позиции 1 и 2	
	Типът на главата на винта трябва да бъде Pozidriv 1 за Позиция 3	
На всеки електромер или капак на клемния блок трябва със стандартни символи да е трайно обозначена електрическата схема за свързване.	Задължително изискване	
Възможността за корозирание в следствие използването на различни проводникови материали трябва да се снижи до минимум с подходящ подбор на тези заготовки	Задължително изискване	
Електрическите свързки трябва да са направени така, че контактното налягане да не се провежда през изолационния материал	Задължително изискване	
Клемните връзки трябва така да са изпълнени, че да се гарантира траен контакт за времето на експлоатационния срок на електромера	Задължително изискване	
Съединителните клеми с различен потенциал, които са подредени гъсто една до друга, трябва да са обезопасени срещу случайно късо съединение	Задължително изискване	
<b>2.3 Клемен капак</b>		
Клемите на електромера, ако те са в клемен блок и не са защитени по друг начин, трябва да имат отделен клемен капак, който да може да бъде пломбиран независимо от основния капак.	Задължително изискване	
Клемният капак трябва да обхваща клемите, винтовете и присъединителните проводници, както и тяхната изолация на подходяща дължина.	Задължително изискване	
Не трябва да има достъп до клемите без да бъде разпломбиран клемния капак	Задължително изискване	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Винтовете на клемния капак трябва да бъдат изпълнени за същите инструменти като клемните винтове.	Задължително изискване	
Възможността за пломбиране трябва да бъде проектирана така, че да е възможно пломбиране с една или повече пломби, според изискванията на Българския Институт по Метрология	Задължително изискване	
Изисквания за съответствие на клемният капак	Изделието е в съответствие с DIN 43857	
2.4 Клас на защита		
Трябва да се доставят изключително и само електромери с изолиран корпус (вкл. капака на клемния блок) от клас на защита II.	Задължително изискване	
Материалите трябва да имат механична устойчивост и устойчивост на оцветяването срещу ултравиолетови лъчи	Задължително изискване	
Корпусът трябва да покрива всички метални части на електромера, с изключение на малки части като табелка, болтове, нитове и др. крепежни елементи	Задължително изискване	
За клемния блок и клемния капак се изисква подсилена изолация.	Задължително изискване	
При пломбиране пломбажната тел не трябва да докосва части под напрежение.	Задължително изискване	
2.5 Защита срещу проникване на прах и вода		
Минимални изисквания за защита от проникване на прах и вода	Електромерите трябва да разполагат със защита съгласно EN 60529 +A1 издание 2000-10-01	
2.6 Табелка с технически данни		
Изисквания за съдържанието на табелката на електромера	В случай че електромерите, са сертифицирани съгласно изискванията на Наредба за средствата за измерване подлежащи на метрологичен контрол, табелката с техническите данни трябва да отговаря на съответните предписания на Наредбата	
	В случай че електромерите, са сертифицирани съгласно MID табелката с техническите данни трябва да отговаря на съответните предписания на MID	
Всеки електромер трябва да разполага със следните означения:	всички маркировки, изисквани от MID или всички необходими предупредителни знаци съгласно Наредба за средствата за измерване подлежащи на метрологичен контрол	
	всички маркировки, необходими одобрения и сертификати	
	Име на производителя или фирмен знак	
	Означение на типа и знак за допускане за експлоатация. При MID електромери, се изобразява съответния номер на нотифицираният орган	
	Брой на фазите и брой на проводниците, за които е предвиден електромерът (едно- или трифазен). Тези данни могат да са означени с помощта на графични символи съгласно EN 62053-52 издание 2006-10-01	

6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	Заводски номер и година на производство. Заводският номер, както се вижда на табелката трябва да е програмиран и софтуерно в електромера. Когато табелката с техническите данни е част от капака на корпуса, отбелязаният върху табелката заводски номер трябва да е нанесен трайно и във вътрешната част на електромера.	
	Поставянето на табелка върху клемния капак не е разрешено	
	Изобразяване на номинално напрежение: брой на измервателните системи и на напрежение на клемите	
	Изобразяване на номинален ток и максимално допустим ток (например: 0,5-10(60)A	
	Изобразяване на номинална честота: в Hz	
	Изобразяване на константа на електромера, напр. в Imp/kWh	
	Изобразяване на класа на измервателна точност 2 (MID A) за активни и 2 за реактивни величини за Позиции 1 и 2, клас на измервателна точност 1 (MID B) за активни и 2 за реактивни величини при Позиция 3	
	Изобразяване на температурния обхват съгласно MID (-25°C до +55°C)	
	Изобразяване на знак за двойна защитна изолация	
	Изобразяване на Баркод	
	Изобразяване на маркировка за собственост: 	
	Изобразяване на CE – Маркировка с година на MID калибриране (напр. M14 ) и нотифициран орган	
	Изобразяване на броячите, които се визуализират на дисплея на електромера.	
2.7 Климатични условия – температурен диапазон		
Изискване за температурен диапазон при режим на работа	- 25°C до +55°C	
Изискване за температурен диапазон при съхранение и транспорт	- 25°C до +70°C	
3. Захранване		
3.1 Консумирана мощност в напреженовите и токовете вериги		
Изисквания за консумирана мощност	Мощността, консумирана от всяка напреженова и токова верига на електромера, както и от допълнителните модули при номинално напрежение, номинална температурата и номинална честота, включително консумацията на измервателните системи за активна и пълна мощност не трябва да надвишава стойностите, определени в EN 62053-21	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	Изискването за максималната консумация съгласно EN 62053-21 се отнася както за напълно интегрирана версия, така и за модулна версия като сбор от всички модули, включително електромера	
3.2 Захранващо напрежение		
3.2.1 Допусково поле на мрежовото напрежение		
Изисквания за захранването на електромера	номинално напрежение $U_n=230V$	
	нормален работен обхват: $0,9U_n$ до $1,10U_n$	
	граничен работен обхват: $0,8U_n$ до $1,15U_n$	
	В офертата да се посочват минималните напрежения, при която електромерът започва да измерва	
3.2.2 Нормирани номинални напрежения		
Номинално напрежение	Позиция 1: 230V	
	Позиции 2 и 3: 3x230/400V	
Честота	Уредите трябва да са предназначени за номинална честота от $50Hz \pm 2\%$	
3.3 Обратни въздействия върху мрежата		
Минимални изисквания за въздействие върху мрежата	Захранващият мрежови блок трябва да е конструиран така, че да не допуска обратни въздействия от високочестотни трептения по мрежата	
	Изделието съответства на EN 61000-3-2 +A2 издание 2005-11-01	
3.4. Защита срещу пренапрежение		
Минимални изисквания за защита от пренапрежение	Съгласно EN 62052-11, глава 7.3.2 тест импулсно напрежение -Форма на вълната на импулса 1,2/50 микросекунди, съгласно EN 60060-1 -Импеданс на източника: $500\Omega + 50\Omega$ -Пикова стойност на напрежението от 8kV.	
3.5 Устойчивост срещу импулсно напрежение		
Минимални изисквания за защита от импулсно напрежение	Съгласно EN 61000-4-5 тест при импулсно въздействие с вълна 1,2/50 микросекунди -Импеданс на източника: $2\Omega \pm 10\%$ -Пикова стойност на напрежението - 6 kV - Форма на вълната на импулса 1,2/50 микросекунди, съгласно EN 60060-1	
3.6 Електромагнитна съвместимост		
Минимални изисквания за електромагнитна съвместимост	Изделието съответства на CENELEC EN 55011	
	Изделието съответства на CENELEC EN 55014	
	Не трябва е възможно повлияване на захранванията от външни електрически и магнитни полета на предвидените места за монтаж на електромерите	
	Електромерът не трябва да се повлиява от GSM мобилни апарати с мощност на излъчване до 2Watt	
3.7 Устойчивост срещу преходни смущения (Burst)		
Минимални изисквания за устойчивост срещу преходни смущения	Изделието съответства на изискванията на EN 61000-4-4 (точност на изпитването 4)	
3.8 Магнитно повлияване от постоянни магнити		

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Минимални изисквания при въздействие от постоянни магнити	При поставянето на постоянен магнит с остатъчна намагнитеност 400mT електромерът не трябва да отчита нито измервателно-техническа, нито функционална грешка	
	При по-високи полета (>400mT) електромерът трябва да регистрира поява им. Задължително е вписването им в дневника на събитията (LogBook). Трябва да се изпрати алармен сигнал към системата	
3.9 Електромагнитни радиочестотни полета		
Минимални изисквания при въздействие на радиочестотни полета	Изделието съответства на изискванията на EN 61000-4-3. Съгласно глава 5 се изисква точност на изпитването 4 (сила на тестовото поле от 30V/m)	
3.10 Електростатично разреждане		
Минимални изисквания при въздействие на електростатичен разряд	Изделието съответства на изискванията на EN 61000-4-2, точност на изпитването 4 при контактен разряд: 8kV	
	Изделието съответства на изискванията на EN 61000-4-2, точност на изпитването 4 при въздушен разряд: 15kV	
3.12 Устойчивост на топлина и огън		
Минимални изисквания за устойчивост на клемния блок от топлина и огън	Клемният блок, клемният капак и корпусът на електромера трябва да са изработени от самогасящ се материал, осигуряващ защита срещу разпространението на огън	
	Продукта съответства на EN 62052-11	
	Продукта съответства на IEC 60695-2-11	
3.13 Поведение при отпадане и възстановяване на напрежението в мрежата		
Минимални изисквания към електромера при отпадане и възстановяване на напрежението в мрежата са:	Захранването на трифазния електромер трябва да е трифазно изпълнено така, че при отпадането на една респективно на две фази на мрежовото напрежение електромерът трябва да запази пълната си функционалността си, ако поне едното фазово напрежение възлиза на UN + 10%.	
	Функционалността на електромера трябва да позволява при прекъсване на нулевия проводник електромерът не бива да се увреди трайно и не бива настъпи генерална загуба на данни	
	Функционалността на електромера трябва да позволява при възстановяване на мрежовото напрежение, независимо дали ще е едно-, дву- или трифазно, електромерът трябва най-късно след 5 сек. да е изцяло годен за функциониране	
	Функционалността на електромера трябва да позволява при отпадане на напрежението за един период на измерване да не се запамятват данни в товаровия профил, но е необходимо да се идентифицира отпадането с подходящ статус	



6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	Функционалността на електромера трябва да позволява при по-дълги прекъсвания на захранващото напрежение, последните (непълни) данни за товарния профил следва да бъдат запазени с подходящ статус (Power down)	
	Функционалността на електромера трябва да позволява първите данни след възстановяване на напрежението да бъдат идентифицирани с подходящ статус (Power up).	
4 Технически изисквания		
4.1 Номинален и максимален ток		
I <sub>Ref</sub> Референтен ток	Позиция 1- 5 или 10А	
	Позиция 2- 5 или 10А	
	Позиция 3- 5А	
I <sub>max</sub> (макс. ток за класа на точност)	Позиция 1- 60А	
	Позиция 2- 60А	
	Позиция 3- 6А	
Минимални изисквания за максимален ток, който електромер може да понесе без да се повреди	Позиция 1- 80А	
	Позиция 2- 80А	
	Позиция 3- 10А	
Минималният комутиращ ток на релето за управление	най-малко I <sub>max</sub>	
4.2 Измервани величини		
Минимални изисквания за измерване и съхранение на активна енергия от електромера	Електромерът трябва да измерва обща активна енергия +А (кВтч)	
	Електромерът трябва да измерва обща активна енергия –А (кВтч)	
	Електромерът трябва да съхранява товарен профил 15 мин. +А: Формиране на измерените данни (кВтч) с дата/час и статус (например възстановяване на напрежението)	
	Електромерът трябва да съхранява товарен профил 15 мин. –А: Формиране на измерените данни (кВтч) с дата/час и статус (например възстановяване на напрежението)	
Възможност за измерване и съхранение на реактивна енергия	*Възможно ли е измерване на обща реактивна енергия Q <sub>I</sub> (кВАrh)?	
	*Възможно ли е измерване на обща реактивна енергия Q <sub>II</sub> (кВАrh)?	
	*Възможно ли е измерване на обща реактивна енергия Q <sub>III</sub> (кВАrh)?	
	*Възможно ли е измерване на обща реактивна енергия Q <sub>IV</sub> (кВАrh)?	
	*Възможно ли е съхраняване на товарен профил 15 мин. Q <sub>I</sub> : Формиране на измерените данни (кВАrh) с дата/час и статус (например възстановяване на напрежението)?	
	*Възможно ли е съхраняване на товарен профил 15 мин. Q <sub>II</sub> : Формиране на измерените данни (кВАrh) с дата/час и статус (например възстановяване на напрежението)?	

6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	*Възможно ли е съхраняване на товаров профил 15 мин. QIII: Формиране на измерените данни (kVAh) с дата/час и статус (например възстановяване на напрежението) ?	
	*Възможно ли е съхраняване на товаров профил 15 мин. QIV: Формиране на измерените данни (kVAh) с дата/час и статус (например възстановяване на напрежението) ?	
Минимални изисквания за конфигуриране на тарифни регистри	Електромерът трябва да притежава освен сумарните регистри (обща енергия) и най-малко четири тарифни регистри за: +A, -A	
	*Възможно ли е измерване на реактивна енергия в квадранти QI, QII, QIII, и QIV, и конфигуриране на тарифи?	
	Активирането на тарифните регистри трябва да бъде направено чрез вътрешна тарифна таблица с часови/дневни/седмични/месечни/годишни и празнични програми, които да могат да се конфигурират както от интерфейса за дистанционно отчитане, така и през сервисния порт на електромера	
	Всякакви промени в тарифната таблица, трябва да се регистрират с дата и час в дневника на събитията.	
4.3 Идентификация на измерваните величини		
Изискване към електромерите за недвусмислено идентифициране на измерените стойности може да се използва OBIS код	Продукта трябва съответства на EN 62056-01: система OBIS – Object Identification System	
Изисквания за регистрите на електромера	Регистрите на електромера трябва да са с водещи нули.	
	Изисква се определянето величините включени в списъка с данните да се конфигурира от мрежовия оператор	
4.4 Обем на паметта		
Минимални изисквания към обема на паметта на електромера	Електромерът трябва да разполага с възможност за съхраняване на товаров профил за всяка от параметризираните величини (включително информация за състоянието, дата и час) за последните минимум 40 дни	
	Електромерът трябва да разполага с памет на дневника на събитията с възможност за съхраняване на минимум 100 събития	
4.5 Софтуерна архитектура на електромера		
4.5.1 Общи изисквания		
Минимални изисквания за софтуерната структура на електромера съгласно на WELMEC Software Guide 7.2	Софтуерната структура на електромерите трябва да се съобразява с препоръките на WELMEC Software Guide 7.2 (Measuring Instruments Directive 2004 / 22 / EC).	
	Минимално изискване е фърмуера да се раздели на метрологичен (одобрен) и неметрологичен (неодобряем).	
4.5.2 Метрологичен фърмуер		

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Минимални изисквания за метрологичния firmware	Метрологичният фърмуер трябва да включва само тези функции, които са пряко необходими за измерване	
	Доставчикът трябва да уточни кои са метрологичните функции и под-функции на фърмуера	
4.6 Дисплей		
Минимални изисквания към функционалността дисплея	Визуализиране на данните на дисплея трябва да бъде възможно при температура на околната среда до -25°C със забавяне между две величини под 1 секунда	
	Поради съображения за поверителност показването на данни за товарния профил на дисплея чрез бутона за повикване трябва да бъде възможно само в специални случаи посредством активиране и деактивиране чрез WAN интерфейса за дистанционно отчитане P1 или посредством сервисния порт (интерфейс P0) за обслужване на електромера. Настройка по подразбиране е да няма данни за товарния профил на дисплея	
	Функционалността на дисплея трябва да позволява отварянето на клемния капак да се изобразява на дисплея	
	Електромерът трябва да разполага с фонов осветление	
Минимални изисквания за изобразяване на величини на дисплея на електромера	Електромерът трябва да разполага с възможност за изобразяване на енергийни регистри - 8 цифри с два знака след десетичната запетая (6/2). Минимален размер на символите 8x3mm за Позиции 1 и 2	
	Електромерът трябва да разполага с възможност за изобразяване на мощност с 8 цифри с 3 знака след десетичната запетая (5/3) за позиции 1 и 2	
	Електромерът трябва да разполага с възможност за изобразяване на енергийни регистри - 8 цифри с два знака след десетичната запетая (5/3). Минимален размер на символите 8x3mm за Позиция 3	
	Електромерът трябва да разполага с възможност за изобразяване на мощност с 8 цифри с 3 знака след десетичната запетая (5/3) за позиция 3	
	Електромерът трябва да разполага с възможност за изобразяване на мерни единици	
	Електромерът трябва да разполага с възможност за изобразяване на код на измерваната величина (OBIS или друг код)	
	Електромерът трябва да разполага с възможност за изобразяване на енергиен индикатор за +A, -A (Опция: * +R, -R), стрелка или квадрантна диаграма	
	Електромерът трябва да разполага с	

6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	възможност за изобразяване на фазови индикатори, които показват наличието на фазните напрежения и посоката на въртене на полето (например мигане при обратна посока)	
	Електромерът трябва да разполага с възможност за изобразяване на индикатор за липса на консумация	
	Електромерът трябва да разполага с възможност за изобразяване на код за грешка	
	Електромерът трябва да разполага с възможност за изобразяване на статус на релето за управление	
	Електромерът трябва да разполага с възможност за изобразяване на версията на фърмуера (одобрен и неodobряем)	
	Електромерът трябва да разполага с възможност за изобразяване на контролни суми на фърмуера	
	Електромерът трябва да разполага с възможност за изобразяване на дата и час	
	Електромерът трябва да разполага с възможност за изобразяване на моментни величини по желание (напр. ток, напрежение, фактор на мощността и др.)	
Кандидатът следва да предостави информация за възможност за изобразяване на следните величини	*Възможност за визуализиране на свързване на устройство към интерфейса за външни измервателни устройства	
	*Възможност за визуализиране на активен трансфер на данни	
	*Възможност за визуализиране на статус на комуникационния модул	
	*Възможност за визуализиране на статус на релето за управление (напр. ИЗКЛ., готов за включване...)	
	*Възможност за визуализиране на режима на работа (Нормален, Настройка, Параметризиране, Калибриране)	
	*Възможност за визуализиране на манипулационен статус	
Минимални изисквания за визуализиране на допълнителни функции	Визуализиране на активната тарифа	
	Визуализиране на номер на тарифната таблица	
4.7 Допълнителни функции		
Електромерът трябва да разполага със следните допълнителни функции	Активирането на тарифните регистри (и показанията им на дисплея) трябва да бъде възможно чрез конфигурационната таблица	
	Електромерът трябва да бъде калибриран за пълен набор от метрологични функции. Той винаги трябва да измерва и съхранява всички измервани величини.	
	За да се гарантира работоспособността и използваемостта само необходимите тарифни регистри трябва да бъдат активирани и показани на дисплея (напр. еднотарифен план с един регистър).	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ					
Техническа характеристика		Минимални изисквания на възложителя		Предложение на кандидата		
		Трябва да бъде възможно разрешаване на реактивните регистри (5.8.0/6.8.0/7.8.0/8.8.0), както и показването им на дисплея				
4.8 Вътрешен часовник и календар						
Минимални изисквания към вътрешния часовник и календар		Вътрешният часовник трябва да отговаря на изискванията на EN 62054-21 и EN 62052-21.				
		Управлението на вътрешния часовник трябва да е кварцово				
		Вътрешният часовников превключвател да разполага с пълен календар (дата и час) с превключване на лятно/зимно време и за почивните дни				
		Настройка/синхронизиране на датата и часа трябва да са възможни чрез интерфейс WAN интерфейса на централната системата, както и чрез сервисния интерфейс на място. Настройката на дата и час чрез бутони на електромера не е позволено поради съображения за сигурност				
		Смяната лятно/зимно време трябва да бъде параметризирана, съгласно европейския стандарт. Да се вземат предвид времената за превключване, валидни за България (UTC+2), както и всички високосни години до 2050				
Превключване на лятното часово време трябва да се извършва съгласно следващата таблица		DST time	DST:			
		Лято -> Зима	4:00 => 3:00 часа			
		Зима -> Лято	3:00 => 4:00 часа			
Превключването на тарифите трябва да се извършва съгл. Решение на Регулатора №Ц-002/29.03.2002.		Тарифна програма	Тарифна програма активна от:			
		Лято	00:00 на 01.04			
		Зима	00:00 на 01.11			
Минимални изисквания към часовниковия превключвател		Продължителността на живот на часовниковия превключвател трябва да бъде най-малко 20 години.				
		Точността трябва да е в рамките + 5ppm (максимално дневно отклонение 0,5 секунди на ден).				
		Часовниковият превключвател трябва да е с компенсиране на температурата				
Превключването на тарифите трябва да се извършва съгласно следната таблица		Измервателна величина	Тарифен брояч	Зимно часово време	Лятно часово време	
		P+	1.8.1	22:00 до 06:00	23:00 до 07:00	
			1.8.2	06:00 до 22:00	07:00 до 23:00	
4.9 Реле за управление на товара (Позиция 1 и 2)						
Минимални изисквани за релетата за управление на товара		Релето за управление на товара трябва да бъде интегрирано в електромера				



6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	Релето за изключване трябва да може да интерпретира следните команди – ВКЛЮЧВАНЕ/ ИЗКЛЮЧВАНЕ – както през локален интерфейс, така и дистанционно:	
	Форматираните команди за управление на релето трябва да бъдат предоставени в техническата документация	
4.9.1. Технически данни		
Устройството за изключване трябва да покрива следните минимални изисквания	Механичен полезен живот: 100 000 комутации	
	Механичен полезен живот съгл. EN 62055-31, анекс C: 10 000 комутации при 100 A, $\cos\phi=1$	
	Максимално напрежение на комутиране: 400 V (AC)	
	Максимален комутиран ток: 100 A	
	Късо съединение < 10 ms според EN 62053-21: 3 kA	
	Максимална мощност на комутиране: 25 kVA Изоляционна способност: 4 kV с продължителност от 1 минута	
5. Интерфейси. Изисквания към интерфейсите		
Минимални изисквания за комуникация посредством електромерните интерфейси	Електромерите трябва да се конструират така, че заявки до един интерфейс да не могат да се препредават чрез друг интерфейс (изолация на портовете). Неоправомощен достъп през сервисния интерфейс не може да бъде използван за взломен достъп във WAN-интерфейса и по този начин да може да се използва WAN-мрежата	
Минимум следните интерфейси трябва да са налични	P0-Инфрачервен (IR) интерфейс, чрез който външни дейности по поддръжка могат да бъдат извършвани с Е-електромера, с помощта на външно устройство (Преносим терминал)	
	P1-WAN интерфейс на електромера трябва да може да се справи с PLC комуникацията	
	P2-PLC интерфейсът между Концентратора на данни и Е-електромера	
5.1 Сервизен интерфейс (P0)		
Минимални изисквания към физическия слой на интерфейса	Сервизният интерфейс трябва да се изпълни като оптичен интерфейс. Скоростта на комуникация трябва да е минимум на 9600 бода.	
Минимални изисквания към протоколен слой на интерфейса	Сервизният достъп до електромера трябва да се осигури чрез DLMS/COSEM, IEC 62056-21 или друг стандартен протокол. Допустимият опция трябва да се определи от оператора на мрежата	
5.2 WAN Интерфейс (P1)		
Електромерът/модулът трябва да разполага с индикатори показващи комуникационния статус посредством LED	Наличие на комуникация при PLC	
	Статус (нормално работно състояние или състояние на грешка)	
5.2.1 Интегриран WAN Интерфейс PLC (C)		

6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Физически слой	Свързването на измервателните уреди и комуникационното оборудване към мрежата трябва да бъде съгласно техническите предписания на фирмата производител.	
	Фирмата-производител трябва да предложи техническо решение (напр. филтър за подтискане на смущенията), за да се отстранят евентуални влияния в съоръженията на клиента от електроуреди.	
Приложен слой	Допускат се собствени протоколи на електромерите	
Сигурност	Сигурността трябва да се осъществи в рамките на заданията в „Сигурност на електромера“.	
6 Допускане в експлоатация, първоначална и последваща проверка		
6.1 Одобрение на типа или MID сертифициране		
Изисквания при сертифициране на електромерите съгласно MID	При MID сертифициране на електромери е нужно да се посочат мястото на производство, акредитираният орган и нотифицираният орган за наблюдение на проверката.	
	Представено копие от сертификат към „Заявлението за участие“ от типово изпитание, включително температурната зависимост на метрологичните грешки и декларация за съответствие, както с всяка доставка така и при промяна на версията на продукта от производителя.	
Изисквания при сертифициране на електромерите с одобряване на типа	В случай че електромерът е одобрен за ползване в България посредством списване в регистъра на средствата за търговско измерване, да се предостави свидетелството за одобряване на типа	
6.2 Параметризиращ софтуер		
Минимални изисквания към лиценза на параметризиращия софтуер, който задължително се доставя с електромера.	Поддръжка на пълната функционалност на електромера.	
	Лицензът на параметризиращия софтуер трябва да включва всички софтуерни актуализации за времето на живот на електромера	
	Обучение относно работата със софтуера, задаване на параметрите и необходимата обработка на данните.	
	Възможност за криптиране на връзката с електромерите.	
6.3 Калибриране (и възможност за влизане в тестов режим)		
Минимални изисквания за статуса на тестовия режим	Статус на тестовия режим (вкл. или изкл.) за калибриране трябва да бъде видимо показан на електромера чрез сервисния интерфейс и дисплея	
Минимум следните команди, които да могат да бъдат подадени от тестовото устройство чрез сервисния интерфейс и изпълнени от	Тестов режим ВКЛЮЧЕН	
	Тестов режим ИЗКЛЮЧЕН	
	Настройка на час/дата	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
електромера трябва да бъдат налични	Увеличаване на константата на светодиода (за метрологична проверката)	
	Тест на дисплея (опционално)	
	Превключване на светодиода за активна/реактивна енергия в случай че електромера разполага само с един LED	
	Извършване на самоотчет	
	Превключване на тарифи за измерване на енергия и мощност	
	Реле за управление ВКЛЮЧЕНО (Без Позиция 3)	
	Реле за управление ИЗКЛЮЧЕНО (Без Позиция 3)	
6.3.1 Светодиод		
Минимални изисквания към метрологичния LED	Със стандартна оптична глава трябва да е възможно снемането на импулси по всяко време	
	За предпочитане е използването на червени и зелени светодиоди. LED-изпълнението трябва да гарантира безпроблемното снемане на импулси с оптични глави, които могат да бъдат задействани на разстояние от 30mm.	
	Ако налице е само един светодиод върху електромера трябва да е възможно превключването на импулсите между активна и реактивна енергия и обратно чрез IR команда	
6.3.2 Разположение на светодиодите и IR-интерфейса		
Минимални изисквания към LED при проверка на електромера	За да се създаде възможност за автоматична проверка на електромера, предвиденият за калибрирането светодиод от една страна и IR-интерфейса от друга страна трябва да бъдат така разположени, че да може да се извърши едновременна проверка, респективно калибриране на електромера чрез двата елемента	
6.3.3 Изисквания за чувствителност и допустими граници на грешката		
Минимални изисквания за чувствителност и допустими граници на грешката	Електромерите трябва да отговарят на допустими граници на грешките определени съгласно изискванията на БИМ за проверка на СИ	
	Допълнителните грешки при краткотрайно затопляне трябва да бъдат посочени в протокола от изпитанието	
	Електромерите трябва да бъдат изработени така, че да е възможна автоматична проверка на измервателни точки със стандартни средства за проверка	
6.3.4 Проверка на поведението в режим на работа		
Минимални изисквания за поведението в режим на работа	В режим на работа електромерът трябва да отговаря на изискванията на стандарт EN 62053-21 и съответно на утвърдените изисквания в българския Закон за Измерванията	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	Електромерите трябва да са така изработени, че да е възможна, както автоматична проверка на режима на работа (посредством LED) със съответна изпитвателна техника, така и проверка чрез визуален контрол (напр. на стрелката за посоката на енергията върху дисплея)	
	Константата на светодиода трябва да бъде такава, че при стартов тест да е възможно регистрирането на минимум 2 импулса за 10 минути	
6.3.5 Проверка на поведението на електромера в режим на самоход (празен ход)		
Минимални изисквания за поведение на електромера в режим на самоход	В режим на самоход електромерът трябва да отговаря на изискванията на стандарт EN 62053-21 и съответно на утвърдените в България изисквания на Закон за Измерванията	
	Електромерът трябва да бъде изработен така, че да е възможна, както автоматична проверка на самохода (посредством LED), така и проверка чрез визуален контрол на електромера. LED-диодът трябва да свети винаги когато електромерът няма товар	
6.3.7 Тестов режим		
Минимални изисквания за работа в тестов режим на електромера	Електромерът трябва да разполага с режим за проверка.	
	В режим на проверка, енергийните броячи трябва да имат 3 знака след запетаята (при индиректни електромери – 4 знака). Формата на данните на дисплей и при отчитане трябва да бъде идентичен	
	Електромерът трябва да разполага с възможност за увеличена резолюция на енергийните регистри в режим на тест с цел по ефективна проверка	
6.4. Измерване, свързване към мрежата		
6.4.1 Клас на точност		
Изискване за клас на точност при MID сертифициране	Директно свързване: най-малко MID Клас А	
	Индиректно свързване: най-малко MID Клас В	
	Реактивна енергия Клас 2	
6.4.2 Двупосочно измерване		
Изисквания за двупосочно измерване	Електромерите трябва да регистрират енергията в права и обратна посока в отделни енергийни регистри (сумарно и по тарифи). Това е валидно както за активната, така и за реактивната енергия	
6.4.3 Измерване, независимо от посоката на въртене на полето		
Минимални изисквания при различни посоки на въртене на полето	Измерването не трябва да се влияе от полета с различни посоки на въртене	
6.4.4 Мониторинг на функционалността (самодиагностика, watchdog)		
Минимални изисквания за самодиагностика на електромера	Чрез използването на watchdog функция трябва да се предотврати повреда на електромера чрез отказ на софтуера	
	По команда на watchdog функцията е	

6 МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ		
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	необходимо да се осъществи рестарт на софтуера на електромера	
	Електромерът трябва да разполага с функционалност при нарушаване на точността на енергийните регистри в резултат на рестарт на watchdog таймера да се върнат стойностите от последният 15 минутен период преди грешката	
	Всеки рестарт на watchdog таймера трябва да се запише в дневника на събитията	
	Рестартирането на watchdog таймера не трябва да трае повече от 10 секунди	
IV. Концентратор на данни		
1. Общи изисквания		
Изисквания за монтаж на концентратора	Концентратора трябва да разполага с възможност за монтаж посредством DIN-шина или триточково закрепване	
Изисквания за свързване на външна антена	Свързване на външна антена посредством SMA-конектор	
Изисквания за защита	Концентраторът трябва да разполага с минимум IP 40 клас на защита (съгласно EN 60529)	
Изисквания за влажност на въздуха	Концентраторът трябва да е конструиран за работа в диапазон от 5% до 90% относителна влажност (без конденз)	
Изисквания за захранване с напрежение	Номинален обхват по напрежение на концентратора 3 x 230/400 V (широк диапазон: 140 V до макс. 260 V)	
	Необходимо е обезопасяване с макс. 16 A-предпазител	
Изисквания за PLC - метод за комуникация	Необходимо е свързване с проводници със сечение на проводника макс. 2,5 mm <sup>2</sup>	
	Метод за комуникация трябва да бъде съвместим с CENELEC част A	
Изискване за температурен диапазон	Концентраторът трябва да разполага с възможност на управление на до 1.000 крайни устройства	
	Работен диапазон: - 25°C до 55°C	
Изисквания за наличните интерфейси на устройството	Граничен диапазон за съхранение и трансфер: - 25°C до 70°C	
	Концентраторът трябва да разполага с PLC интерфейс,	
	Концентраторът трябва да разполага със сервизен интерфейс P0: RS 232, Ethernet...	
	Концентраторът трябва да разполага с P3: RS 232, Ethernet,	
	Концентраторът трябва да разполага с P4: интерфейс към модул GSM/GPRS/UMTS-модем (SMA – конектор за свързване на външни антени)	
Изискване за съответствие със стандарти	Концентраторът трябва да разполага с CE-сертифициране	
	Концентраторът трябва да отговаря на изискванията на стандарт EN 61000-6-4	
	Концентраторът трябва да отговаря на изискванията на стандарт EN 50065-1	
Изискване за поддържане на мрежови протоколи	Минимум следните протоколи трябва да се	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
	поддържат TCP/IP, HTTP, FTP, SCP	
Изискване към вътрешния часовников модул / Часова база	Концентраторът трябва да разполага с възможност за синхронизация с NTP (Network Time Protocol) сървър	
	Концентраторът трябва да разполага с възможност за синхронизация с централната система	
1.2 Конструктивни изисквания		
Конструктивни изисквания относно безопасността при работа:	Концентраторът трябва така да бъде конструиран че да гарантира безопасност на лицата от попадане под напрежение (тоководещите части да са надежно изолирани)	
	Концентраторът трябва така да бъде конструиран че да гарантира безопасност на лицата при въздействия от повишена температура	
	Концентраторът трябва така да бъде конструиран че да гарантира безопасност и устойчивост на топлина и огън	
	Концентраторът трябва така да бъде конструиран че да гарантира защита срещу проникване на твърди тела, прах и вода	
Минимални изисквания за защита от корозия	Всички части, изложени на корозия при нормални условия на употреба, трябва да бъдат ефективно защитени. Защитните слоеве трябва да бъдат толкова устойчиви, че при определените условия на работа да не могат да бъдат повредени от атмосферните условия.	
1.2.2 Корпус		
Минимални изисквания към корпуса	*Корпусът, трябва да може да се пломбира, така че вътрешните части на уреда да са достъпни само след счупване на пломбата(ите). Отстраняване на капачката на корпуса не бива да бъде възможно без използването на инструмент.	
1.2.3 Клас на защита		
Минимални изисквания към устойчивост на UV лъчи	*За предпочитане е корпусите да бъдат изработени от рециклируем изолационен материал (устойчив на UV-светлина, устойчив на изпаренията от разтворителите), съответстващ на клас на защита II.	
Минимални изисквания за защита срещу проникване на прах и вода.	Концентраторът трябва да разполага с най-малко IP 40 клас на защита съгл. IEC 60529	
1.2.3.1 Климатични условия		
Минимални изисквания към температурните диапазони	Работната температура и температурата на околната среда трябва да бъдат между -20 °C до +60 °C.	
	Диапазонът на температурата при съхранение трябва да е между -25 °C до +65 °C.	
1.2.3.2 Захранване		
Изисквания за стандартизирано номинално напрежение:	Номинално захранващо напрежение 3x230/400 V; 50 Hz	



6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
Диапазони на допустимо отклонение на захранването	Концентраторът трябва да разполага със следния диапазон на захранващото напрежение - 230 +/- 20% Волта; 50 Hz	
Минимални изисквания към механичното закрепване на проводници към концентратора	Концентраторът трябва да разполага с възможност за 3-фазно захранване.	
	PLC-комуникация да се осъществява по всички 3 фази	
	Видът на закрепване на проводниците в клемите трябва да осигури достатъчен и постоянен контакт	
	Трябва да е предотвратено разхлабването на проводниците или прекомерното им загряване	
	Болтови връзки, които правят електрически контакт, и винтове, които могат да бъдат многократно затягвани и разхлабвани по време на полезния живот на Концентратор на данни трябва да имат втулка (букса) с резба от метал	
	Опасността от корозия поради различни контактни материали следва да бъде сведена до минимум чрез правилен подбор на тези материали	
	Електрическите връзки трябва да бъдат изпълнени така, че контактното налягане да не се определя от материала на изолацията	
1.2.4 Честота		
Минимални изисквания към номиналната честота	Концентраторът трябва да бъде конструиран за номинална честота 50 Hz. Трябва да могат да се експлоатират безупречно в диапазона на допустимо отклонение от $\pm 2\%$ от номиналната честота	
1.2.5 Мрежови обратни въздействия		
Минимални изисквания към обратните въздействия върху мрежата	Концентратор на данни (вкл. Мрежови уред и модем) трябва да бъде така проектиран, че в мрежата да не възникват недопустимо високи обратни въздействия под формата на висши хармоници. Следва да се гарантира спазването на EN 61000-3-2	
1.2.6 Защита от ударно напрежение		
Минимални изисквания към защитата от ударно напрежение	Концентраторът трябва да отговаря на изискванията на стандарт EN 61000-4-5 при проверка с вълна на ударно напрежение 1,2/50 $\mu$ s. Контролна степен на чувствителност 3 при максимална стойност от 2 kV (за предпочитане степен на чувствителност 4 при 6 kV).	
1.2.7 Електромагнитна съвместимост		
Минимални изисквания към електромагнитната съвместимост	Концентраторът трябва да отговаря на изискванията съгласно EN 61000-4-3.	
	Концентратор на данни трябва да може да поддържа радиосмущенията.	
	Концентратор на данни не трябва да оказва влияние върху мрежовите части чрез външни електрически и магнитни полета, които обикновено могат да се очакват в местата на експлоатация	

6	МИНИМАЛНИ ТЕХНИЧЕСКИ ИЗИСКВАНИЯ	
Техническа характеристика	Минимални изисквания на възложителя	Предложение на кандидата
1.2.8 Фирмена табелка за технически данни		
Върху уреда трябва да се нанесат минимум следните обозначения, които да бъдат добре четливи и в монтирано състояние на уреда - без използването на други помощни средства	Уникален номер на уреда	
	Баркод в съответствие със спецификациите на мрежовия оператор	
	Обозначаване от производителя и типа	
	Описание на LEDs със статуси	
	Година на производство	
	Схема на свързване	

V. Изисквания за сигурност за дистанционно отчитане на електромери и системи за управление за EVNBG БГ EP. Security requirements for distant meter reading of electrometers and control system for EVNBG ER		
<p><b>1.</b> Средата за пренос на данните от измерването, получени от Е-електромерите, трябва да се реализира посредством GPRS или PLC (комуникация по силов кабел). Техническият модул, който отговаря за комуникацията с Е-електромера, трябва да бъде монтиран в корпуса на Е-електромера. При използване на PLC комуникация, Концентраторът трябва да бъде част от комуникационната верига с Е-електромера, който трябва да може да пренася /събира данни и да комуникира с множество Е-електромери и след това да прехвърли данните до Централната система. Концентраторът трябва да може да използва комуникационната среда GPRS за установяване на канал за пренос на данни с Централната система. Централната система трябва да осигури криптографските услуги, чрез които преносът на данни до/от Концентратора и Е-електромера ще бъде криптиран. Централната система трябва да управлява криптираното съхранение на уникалните ключове на Е-електромера. The transfer environment of metering data from E-Meter must be realized with GPRS or PLC (power line communication). The technical module which is responsible for communication with E-Meter must be installed in the same corpus of E-Meter. In case of usage of PLC communication, a Concentrator must be a part of communication chain with the E-Meter which must be capable to transfer/collect data and communicate with many E-Meters and after that to transfer the data to the Central system. The Concentrator must be able to use GPRS communication environment or Ethernet connection for establishing transfer channel with the Central system. The Central system must provide a cryptographic service with which the data transfer to/from Concentrator and E-Meter to be encrypted. The central system must support the encrypted storage of the unique E-meter cryptographic keys</p>	Изисква се / Must be available	
<p><b>2.</b> При обработване на потокът от лични данни в системата, тези от тях които не са необходими, не трябва да бъдат запазвани или записвани. During the processing of sensitive / personal data in the system, those which are not needed must be not saved or recorded.</p>	Изисква се / Must be available	

3. Запазената информация, която вече не е важна/необходима трябва да бъде изтривана. Saved information which is not anymore important / needed must be deleted	Изисква се / Must be available	
4. Деликатни/лични данни от Е-електромер трябва да може в срок от не повече от 12 часа да се прехвърлят и запазват в Централната система. Sensitive/personal data from E-Meter must be able maximum within 12 hours to be transferred and saved in Central system	Изисква се / Must be available	
5. Без разрешение, неоторизирания достъп до потока от данни трябва да бъде строго забранен. Without permission, the unauthorized access to the data flow must be strictly prohibited.	Изисква се / Must be available	
6. Всякакъв неоторизиран достъп до защитените канали (комуникационни интерфейси) трябва да е невъзможен. Unauthorized access to the protected channels (communication interfaces) must be not possible.	Изисква се / Must be available	
7. Трябва да е невъзможно получаването на непоискана информация отчетена от Е-електромерите, освен ако не става въпрос за аларми и предварително определени критични събития. The E-Meter must deliver reading out information from its registers if it is requested, with exception of alarms and defined critical events.	Изисква се / Must be available	
8. В случай на неочаквана намеса в потока данни, както е показан на илюстрация 1 операторът на мрежата трябва да бъде предупреден чрез механизъм за мониторинг, вграден в Централната система. In case of unexpected intervention in the data flow shown in pic.1 the grid operator must be alerted from a monitoring mechanism implemented in the central system.	Изисква се / Must be available	
9. Паролите и криптографския механизъм (ключове) трябва да бъдат уникални за всеки Е-електромер в процеса на експлоатация на Централната система. Passwords and cryptographic keys must be unique for each E-Meter in the process of exploitation from Central system	Изисква се / Must be available	
10. Командите за изключване и включване на всеки Е-електромер трябва да бъдат уникални, криптирани и кодирани с надлежните ключове, свързани с въведените криптографски услуги. Commands for switch-off and switch-on for each E-Meter must be unique, encrypted and coded with the proper keys related to deployed cryptographic service	Изисква се / Must be available	
11. ИТ сигурността на предложеното решение трябва да може да бъде управлявана от оператора на електроразпределителната мрежа. IT security of proposed solution must be able to be managed from distribution system operator.	Изисква се / Must be available	

<p><b>12.</b> Конструкцията и архитектурата на приложеното решение за сигурност трябва да бъде предоставено от Участника на EVN EP, както и свързаните процеси, за да може да бъде подложен на одит от страна на Изпълнителя, или от трета страна. EVN EP третира всяка получена информация строго конфиденциално. The design and architecture of implemented IT security solution must be provided from bidder to EVN EP and also related processes in order to be able to be audited either from Contractor, or either from third party company. EVN EP will treat the received information with respected confidentiality</p>	<p>Изисква се / Must be available</p>	
<p><b>13.</b> Участникът (продавачът) трябва да съдейства за одита на IT сигурността на цялата система, осъществяван от EVN EP или от трета страна, в случай, че EVN EP го поиска. Участникът трябва да осигури човешки ресурси и информация в процеса на одитиране на цялата система от страна на Изпълнителя. The bidder (vendor) must support the audit of IT security of the whole system by EVN EP or by third party company in case of request from EVN EP. The bidder must provide human resources and information in the process of auditing the whole system from the contractor.</p>	<p>Изисква се / Must be available</p>	
<p><b>14.</b> Потокът от данни свързан с лична информация, като данни от измервания, актуализация на фърмуер, контролни команди (Включване/изключване на електромера, настройки и конфигурации на устройствата (Е-електромери и концентратори) трябва да се изпраща единствено по сигурна криптирана връзка. The data flow related with personal data like metered data values, firmware updates, Control commands (Switch on/off of E-Meter), device settings and configurations of E-meters and Concentrators must be solely transmitted with secured encrypted connection.</p>	<p>Изисква се / Must be available</p>	
<p><b>15.</b> Всички Криптографски ключове трябва да бъдат съхранявани в Централната система, но само в рамките на защитената зона и да бъдат криптирани или неподлежащи на извличане. All cryptographic keys must be located (stored) into the Central system, but only within a protected encrypted area or unexportable</p>	<p>Изисква се / Must be available</p>	
<p><b>16.</b> Концентраторът може да се използва за съхраняване на Криптографските ключове, единствено за осъществяване на комуникационна верига с Централната система и съответните Е-електромери към нея. Криптографските ключове трябва да се съхраняват в рамките на защитена зона, криптирани или неподлежащи на извличане. The Concentrator can store in it the cryptographic keys only for communication chain with the Central system and assigned E-Meters behind it. The cryptographic keys must be stored within a protected encrypted area or unexportable</p>	<p>Изисква се / Must be available</p>	
<p><b>17.</b> Всяка команда от Централната система към Е-електромера трябва да бъде критпирана и да се изпълнява само веднъж в посока Е-</p>	<p>Изисква се / Must be available</p>	

електромера (Защита от атаки чрез повторение). Съобщенията се приемат единствено от удостоверени страни. Each command from Central system to the E-Meter must be encrypted and must be executed only once towards the E-meter (Protection from Reply Attacks). Messages are accepted only from authenticated parties.		
<b>18.</b> Всички криптографски методи, използвани в рамките на системата за сигурност, трябва да се основават на открити и обществено достъпни стандарти и трябва да бъдат разгледани от международни организации (като Размерите на ключовете и параметрите на алгоритми при криптиране на документи към ENISA). All cryptographic methods used within the framework of the security solution (service) must be based on open and public available standards and must be considered by international organizations (like ENISA Document Algorithms Key Sizes and Parameters).	Изисква се / Must be available	
<b>19.</b> Всички използвани криптографски алгоритми трябва да имат най-малко криптографската сила, сравнима с AES 128 (криптографската сила на алгоритъм, напр. може да бъде подобрен чрез увеличаване на дължината на ключа). All used cryptographic algorithms need minimum to have cryptographic strength comparable to AES 128 (the cryptographic strength of an algorithm, for example, can be improved by increasing key length).	Изисква се / Must be available	
<b>20.</b> Уникалните криптографски ключове трябва да бъдат инсталирани от търговеца към всеки Е-електромер. Unique cryptographic keys must be deployed in each E-Meter from the vendor.	Изисква се / Must be available	
<b>21.</b> За вече монтираните Е-електромери, актуализацията на фърмуера трябва да се извършва чрез криптирани и сигурни комуникационни канали. Трябва да бъде дадена гаранция, че файлът с фърмуера не е манипулиран и е действително издаден от производителя. For already installed E-meters the firmware update must be done in encrypted and secured communication channel. Guarantee must be available that firmware image was not manipulated and was issued by the vendor	Изисква се / Must be available	
<b>22.</b> Всички пароли, използвани в Е-електромер и Концентратора на данни, трябва да съответстват на следните минимални изисквания: Минимална дължина - 10 символа, съставени от малки, главни букви и числа, генерирани произволно и не подлежащи на възпроизвеждане. All passwords, which are implemented for E-Meter and data Concentrator, must meet the following minimum requirements: Minimum length of 10 characters, Composed of lowercase letters, uppercase letters and digits, Randomly generated and not reproducible.	Изисква се / Must be available	
<b>23.</b> Паролите и Криптографските ключове трябва да бъдат уникални за всяко устройство (Е-електромер или Концентратор), което взема участие в криптирането и декриптирането или в съобщенията за валидиране. Passwords and	Изисква се / Must be available	

cryptographic keys must be unique for each device (E-Meter or Concentrator), which are participating the process of encryption and decryption or messages for authentication.		
<b>24.</b> Пароли и Криптографските ключове, които могат да бъдат използвани за съобщения за криптиране и декриптиране или за валидиране на комуникационните данни, трябва да бъдат генерирани произволно и да не подлежат на възпроизвеждане. Като пример за възможното използване, насочваме вниманието ви към следните документи: NIST Специална публикация 800-90A – Препоръки за генериране на произволни числа, чрез използване на детерминистични генератори на произволни битове. BSI TR-02102 - Криптографски модул: препоръки и дължина на ключовете. Passwords and cryptographic keys, which can be used for encryption and decryption messages or for authentication of the communication data flow, must be generated with a cryptographically secure (pseudo) random number generator and not to be able to be reproduced. As an example of a possible implementation is made at this point to the following documents NIST Special Publication 800-90A - Recommendation for Random Number Generation Using Deterministic Random Bit Generators and BSI TR-02102 - Cryptographic module: recommendations and key lengths	Изисква се / Must be available	
<b>25.</b> Всички пароли, които участват в кореспонденцията в рамките на Централната система, Концентратора и Е-електромера трябва да може да бъдат променени дистанционно от централната система. All passwords which are participating the communication chain from Central system, Concentrator to E-Meter must be possible to be remotely changed from central system	Изисква се / Must be available	
<b>26.</b> След монтаж на съответния елемент (Е-електромер или Концентратор), първоначално използваните пароли трябва да може да бъдат сменени. After installing the appropriate component (E-Meter or Concentrator), the initial used passwords must be possible to be changed	Изисква се / Must be available	
<b>27.</b> Трябва да е възможно сигурно съхранение на резервни копия и съответното възстановяване на данни, съхранявани в криптографската услуга на централната система. Secure backup and restore of data stored in the cryptographic service in central system must be possible.	Изисква се / Must be available	
<b>28.</b> Трябва да има функции за докладване и контрол и представяне на текущото оперативно състояние на криптографските дейности. Reporting and monitoring functions and representation of the current operating state of the cryptographic service must be available.	Изисква се / Must be available	
<b>29.</b> Криптографската услуга трябва да осигурява въвеждане на първоначалните ключове, които се изискват за криптографските дейности. The cryptographic service should provide import of the initial cryptographic keys from vendor, which for the operation of the cryptographic service are required	Изисква се / Must be available	



<b>30.</b> Криптографската услуга трябва да осигурява първоначално зареждане на основния и работните криптографски ключове за критпиране на комуникацията на всеки Е-електромер в базата данни на Централната система. Всички ключове трябва да се съхраняват в криптирана форма по защитен начин в базата данни на централната система. The cryptographic service should provide initial loading of cryptographic keys for encryption of communication for each E-meter in the central system database. All keys must be stored in encrypted and protected way into the environment of Central system.	Изисква се / Must be available	
<b>31.</b> Криптографската услуга трябва да осигурява взаимно валидиране на Е-електромера и централната система, както и критпиране и декритпиране на съобщения между тях. The cryptographic service should provide mutual authentication of E-Meter and Central System and also Encryption and decryption of messages.	Изисква се / Must be available	
<b>32.</b> Криптографската услуга трябва да осигурява съдействие за подробно разследване на дефектни Е-електромери. The cryptographic service should provide support for a detailed investigation in case of defective E-Meters.	Изисква се / Must be available	
<b>33.</b> Криптографската услуга трябва да осигурява отчитане и контрол на статуса на системата. The cryptographic service should provide reporting and monitoring of system status	Изисква се / Must be available	
<b>34.</b> Прехвърлянето на Криптографските ключове в Концентратора и Е-електромера трябва да се осъществява по начин, който съответства на процеса по сигурното доставяне (например SSH, SCP, SFTP, HTTPS или други методи с минимално равнище на критпиране AES 128). По време на мрежовата комуникация между Централната система, концентраторите и Е-електромерите може да се използва метод на валидиране – парола, сертификат, публичен ключ или симетричен ключ. Transfer of cryptographic keys to the Concentrator and E-Meter must be done in a way that corresponds to the process of secured shipping (for example SSH,SCP,SFTP,HTTPS or other methods with minimum level of encryption AES 128). During the network communication between the Central system, concentrators and E-meters must be established under method of authentication – password or certificate or public key or symmetric key can be used.	Изисква се / Must be available	
<b>35.</b> Криптографските ключове трябва да бъдат вградени в криптографската система, чрез предварително определен процес, за да може да се гарантира сигурното управление на ключовете. The cryptographic keys must be incorporated (imported) into the cryptographic service in advance defined process in order to be guaranteed the secure management of the keys.	Изисква се / Must be available	
<b>36.</b> Всеки Е-електромер трябва да бъде произведен с вградени уникални Криптографски ключове и в процеса на доставка на EVN EP следва да се представи пътен лист. В пътния лист	Изисква се / Must be available	

<p>се съдържа информация за производството на Е-електромерите (сериен номер и т.н.) и съответните Криптографски ключове за всеки Е-електромер. Електронната доставка следва да се осъществи в предварително определен формат и трябва да бъде изпратена на EVN EP по сигурен канал. Тази доставка след това се обработва безопасно от криптографската система на Централната система. Този пътен лист трябва да бъде криптиран и може да бъде декриптиран единствено от криптографската система към Централната система. В рамките на целия процес по доставка трябва да се гарантира, че неоторизирани трети страни няма да имат достъп до Криптографските ключове. Each E-Meter must be produced with embedded unique cryptographic keys and in the process of delivery a shipment file (list) must be delivered to EVN EP. The shipment file must contain the list of production information of E-Meters (serial number and etc.) and appropriate cryptographic keys for each E-Meter. The electronic delivery must occur in a defined format and must be transmitted to EVN EP via a secured channel. This delivery will be securely processed subsequently by the cryptographic service of the central system. That shipment file must be encrypted and can be decrypted only from the cryptographic service of Central system. Throughout the delivery process, it must be ensured that no unauthorized third party has an access to the cryptographic keys</p>		
<p><b>37.</b> Криптографската система трябва да има възможност за изготвяне на отчети и доклади за това, кои пароли или ключове са променени, поради определени критерии. Reporting functions must be available from the cryptographic service for which keys or passwords have been changed due to certain criteria</p>	<p>Изисква се / Must be available</p>	
<p><b>38.</b> Ако Е-електромерите бъдат демонтирани (изведени от експлоатация) и ако Е-електромерът и Криптографската система предлагат възможност за прилагане на процес по замяна на работните Криптографски ключове, всички запазени работни Криптографски ключове също трябва а бъдат унищожени. Единствено оторизирани служители имат право да инициират подобно унищожаване. Неизползваните Криптографски ключове не трябва да се съхраняват в Е-електромерите или Концентратора. If E-Meter is deinstalled (decommissioned) and if E-Meter and cryptographic service support a replacement process of operational cryptographic keys, all stored operational cryptographic keys must also be destroyed. Only authorized employees may be able to initiate such a deletion. Unused cryptographic keys must be no longer stored in E-Meter or Concentrator.</p>	<p>Изисква се / Must be available</p>	
<p><b>39.</b> Ако Криптографската система може да заменя работните Криптографски ключове в Е-електромера, трябва да съществуват мерки, свързани с техническия и организационен процес, чрез които да се намали риска от случайно анулиране на Криптографските</p>	<p>Изисква се / Must be available</p>	

<p>ключове в Е-електромера или Концентратора. If cryptographic service is allowing a replacement of operational cryptographic keys in the E-Meter, technical and organizational process measures must be possible to reduce the risk of accidental reset of cryptographic keys in E-Meter or Concentrator</p>		
<p><b>40</b> При наличие на функция за замяна на работните ключове, трябва да бъде приложен уникален процес, за прилагане на работни криптографски ключове спрямо действащите Е-електромери. In case of availability of function for replacing of operational keys a unique process must be executed for deploying operational cryptographic key into a current E-Meter</p>	<p>Изисква се / Must be available</p>	
<p><b>41.</b> Криптографската услуга е от жизненоважно значение за функционирането на цялата Централна система. Криптографската система трябва да бъде изградена с архитектура, позволяваща висока производителност и достъпност. Централната система трябва да осигури сигурни механизми за запазване и възстановяване на резервни копия за всички запазени Криптографски ключове. Cryptographic service is very critical for operation of whole Central system. Cryptographic service must be deployed with high availability architecture. The central system must provide a secure backup and restore capabilities for all stored cryptographic keys.</p>	<p>Изисква се / Must be available</p>	
<p><b>42</b> Криптографската услуга би следвало да работи самостоятелно, без намесата на потребителя. Всякаква работа, по отношение на чувствителна информация или работа на криптографската услуга, трябва да се извършва съвместно от двама различни служителя. Задължително трябва да се спазва споделянето на задълженията. При опити за влизане в системата и работа с нея трябва да се реализират записи и да се генерират протоколи, които следва да бъдат защитени от неоторизирано манипулиране. Направените записи трябва да бъдат проследяеми до уникален потребител. Криптографската система трябва да позволява и прилагането на различни роли на потребителите. Cryptographic service should autonomously work without user interaction. Any operation upon sensitive information or operation of cryptographic service must be done in cooperation of two different employees. Separation of duties must be obeyed. All login attempts and user interactions have to be logged and generated protocol information must be protected against unauthorized manipulation. The log entries must be traceable to a unique user. The cryptographic service must further enable the implementation of different user roles.</p>	<p>Изисква се / Must be available</p>	
<p><b>43.</b> Криптографската услуга трябва да генерира аларма в случай на неоторизирано използване. Тя трябва да предлага подходяща функционалност за отчетност и контрол, която да позволява контрол на текущото работно състояние. Cryptographic service must generate an alarm in case of unauthorized use. It should provide</p>	<p>Изисква се / Must be available</p>	

appropriate reporting and monitoring functionality, which allows monitoring of current operating state		
<b>44.</b> Криптографската услуга трябва да осигурява информация за текущо състояние на криптографската услуга – например – състояние след първоначална доставка, оперативна информация, синхронизиране с допълнителни криптографски системи, откриване на критични и не-критични грешки, открити опити за манипулации в резултат на евентуален възникнал инцидент). The Cryptographic service must provide information about current state of cryptographic service – for example initial delivery state, operational information, synchronization with redundant cryptographic service, discovering critical and not critical errors, discovered manipulation attempts as a result of occurred possible security incident, ... )	Изисква се / Must be available	
<b>45.</b> Криптографската услуга трябва да осигурява информация за подробен опис на всички възникнали грешки при работа (напр. успешно извършено запазване на резервно копие – час и дата XYZ, неуспешен опит за влизане в системата с потребителско име ABC – час и дата XYZ). The Cryptographic service must provide information about detailed listing of all occurred during operation errors (like failed logon attempt with username ABC time XYZ)	Изисква се / Must be available	
<b>46.</b> Криптографската услуга трябва да осигурява информация за всички активни криптографски ключове, заедно със съответното описание за идентификация описание и последващо сравнение, за това дали резервния крипто модул също съдържа всички ключове. The Cryptographic service must provide information about representation of all active cryptographic keys together with appropriate identification description and subsequently comparing mechanism whether redundant crypto module contains all keys too.	Изисква се / Must be available	
<b>47.</b> Криптографската услуга трябва да осигурява информация за всички оторизирани потребителски имена със съответните им разрешителни и права. The Cryptographic service must provide information about representation of all authorized usernames with the respective designated permissions.	Изисква се / Must be available	
<b>48.</b> В процеса на прилагане на нови версии на приложението, предоставяни от производителя, трябва да има поддръжка на всички вече използвани криптографски методи и в новата версия. In the process of provisioning of new releases of application by the manufacturer (vendor), the support for all already used cryptographic methods also in the new release must be available.	Изисква се / Must be available	
<b>49.</b> В процеса на прилагане на нови версии на приложението трябва да се осигури непрекъснатото функциониране на системата по време на процеса на актуализация. In the process of provisioning of new releases of application by the manufacturer (vendor) uninterrupted operation must be secured in the process of update.	Изисква се / Must be available	
<b>50.</b> Преди прилагане на нови версии на	Изисква се / Must be available	

приложението трябва да се осигури документация, в която са описани всички нови елементи, характеристики и промени, както и обучение за персонала за работа с новата версия. Before the process of provisioning of new releases by the manufacturer a delivery of documentation must be provided in which all new features and changes are documented as well as training for the staff for the new version.		
<b>51.</b> EBH EP да може да вземе решение дали и кога да приложи определена нова версия. EVN EP itself can decide whether and when a new release will be implemented or not.	Изисква се / Must be available	
<b>52</b> Пътният лист от продавача, който трябва да съдържа (основни данни за Е-електромерите, уникални Криптографски ключове за всеки Е-електромер) трябва да бъде подписан със собствения ключ на производителя на електромерите и да бъде криптиран. Получения пътен лист следва да бъде директно въведен в Централната система и след това трябва да започне процесът по декриптиране. The Shipment file from the vendor, which must contain (master data of E-Meters, unique cryptographic keys for each E-Meter) must be signed with the private key of the meter manufacturer and encrypted. The received shipment file must be directly imported into the Central system and after that a decryption process to be started.	Изисква се / Must be available	
<b>53.</b> Концентраторът трябва да разполага само с един интерфейс за поддръжка. Конфигурирането на Концентратора на данни през този порт трябва да е достатъчно надеждно защитено от кибер атаки. The Concentrator must have only one maintenance interface. The configuration of data Concentrator via a local maintenance port must be adequately protected against attacks.	Изисква се / Must be available	
<b>54.</b> Концентраторът не трябва да може да бъде конфигуриран през PLC комуникационен порт. При Е-електромер с нарушена сигурност, трябва да не е възможно да се редактира конфигурацията на Концентратора, въз основа на правата и данните за достъп, получени от Е-електромера. The Concentrator must not be able to be configured through PLC communication port. If there is a compromised E-Meter, it must be not possible to edit the configuration in the Concentrator based upon the credentials from the E-Meter.	Изисква се / Must be available	
<b>55.</b> Концентраторът трябва да може да бъде конфигуриран чрез GPRS (WAN) комуникационен порт от централната система. The Concentrator must be able to be configured through GPRS (WAN) communication port from the central system.	Изисква се / Must be available	

<p><b>56.</b> Ако се налага Концентраторът да използва местен интерфейс за поддръжка за преконфигуриране или други дейности по поддръжка, уникална комбинация от потребителско име и парола трябва да бъдат използвани за валидиране, като те трябва да съответстват на определената политика за паролите. (виж техническите изисквания). Трябва да бъде извършен запис за съответното събитие. If the Concentrator has to use the local maintenance interface for reconfiguration or other maintenance activities, a unique combination of username and password must be possible for authentication, which corresponds to the defined password policy.(see technical requirements). Record of the event must be logged in it.</p>	<p>Изисква се / Must be available</p>	
<p><b>57.</b> От локалния порт за поддръжка на Концентратора не трябва да е възможен достъп до защитените зони на Криптографските ключове, които евентуално се съхраняват в него. From local maintenance port of Concentrator must be not possible to reach protected area of cryptographic keys, which are eventually stored in it.</p>	<p>Изисква се / Must be available</p>	
<p><b>58.</b> Неоторизирани опити за достъп до Концентратора на данни трябва да бъдат докладвани (разглеждани) чрез мерките за сигурност от направлението за мониторинг и контрол на централната система. Задължително се прави запис в архива за съответното събитие. The unauthorized attempt for access to a data concentrator must be reported (viewed) by security measures from monitoring service of central system. Record of the event must be logged in it.</p>	<p>Изисква се / Must be available</p>	
<p><b>59.</b> Всеки концентратор трябва да може да комуникира чрез технологията PLC с не по-малко от 1000 бр. Е-електромери, за които отговаря. Each concentrator must be able to communicate over PLC technology with at least 1000 pieces of E-meters which are directly assigned to it.</p>	<p>Изисква се / Must be available</p>	
<p><b>60.</b> Данните за достъп при автоматична регистрация в мобилна мрежа трябва да бъдат уникални за всеки Концентратор. Не се допуска използване на обща информация за влизане в системата, едновременно от няколко единици. The credentials for the automatic registration in mobile network must be unique for every Concentrator. It is not permitted the usage of general login information contained by several units together.</p>	<p>Изисква се / Must be available</p>	
<p><b>61.</b> Данните за достъп при автоматична регистрация в мобилна мрежа, могат да бъдат запазвани единствено в Концентратора. При използване на SIM карта, информацията за влизане в системата не трябва да бъде съхранявана на самата SIM карта. The credentials for the automatic registration in mobile network may be saved only in Concentrator. The login Information must be not stored in the SIM card itself.</p>	<p>Изисква се / Must be available</p>	



<p><b>62.</b> Доставчикът на мобилни услуги ще допуска трафик единствено между централна система и концентратора. Трафикът на данни между концентраторите трябва да се предотврати. The mobile service provider will allow traffic only between central system and concentrator. Data traffic between concentrators must be prohibited.</p>	<p>Изисква се / Must be available</p>	
<p><b>63.</b> Ако даден концентратор на данни е компроментиран от хакер, не би следвало хакерът да може да стига до други концентратори на данни от компроментирания концентратор на данни. If one data concentrator will be compromised by an attacker, the attacker should not be able to reach other data concentrators from the compromised data concentrator.</p>	<p>Изисква се / Must be available</p>	
<p><b>64.</b> Показанията от всички монтирани Е-електромери трябва да бъдат снемани веднъж дневно. В случай че Е-електромерите имат профил на товара, трябва да бъде отчетен профила на товара за 15 минути, заедно с всички 96 стойности. В окончателните етапи на въвеждане трябва да могат да бъдат отчетени около 500 000 Е-електромера. Дейностите по отчитането трябва да започват в 00:00 ч и да приключват в 12:00 ч. в същия ден, като всички отчетени данни се прехвърлят в Централната система. Освен това трябва да бъде генерирана информация за събитията през този период. All installed E-Meters must be read out once per day. In case of E-Meters with load profile, 15 minutes load profile must be read with all 96 values for it. In the final stage of implementation about 500 000 E-Meters must be able to be read out from the central system. The reading activity has to start at 00:00h and finish till 12:00h at the same day and all read data to be transported in the central system. In addition event information must be transported from E-Meters and Concentrators also within that period to central system</p>	<p>Изисква се / Must be available</p>	
<p><b>65.</b> Архитектурата на Централната система трябва да може да бъде разширявана до достигане на 1 500 000 Е-електромера с едни и същи основни показатели за дейността (KPI). The architecture of the Central system must be able to be extended till 1500000 E-Meters with the same KPIs (key performance indicators) defined in point 64.</p>	<p>Изисква се / Must be available</p>	
<p><b>66.</b> Процентът на успеваемост на отчет трябва да бъде минимум 98% от всички монтирани Е-Електромери в дефинирания диапазон в т 64. Success rate must be minimum 98% of all installed E-Meters to be readout within defined time frame in point 64.</p>	<p>Изисква се / Must be available</p>	
<p><b>67.</b> Криптографската услуга представлява жизненоважен компонент в цялата Централна система. Високите изисквания за достъпност, по отношение на криптографската услуга трябва да са като всички компоненти на инфраструктурата на Е-електромерите. Достъпността на средата на централната система трябва да достига 99.99% 24 часа в денонощието, 7 дни в седмицата, 365 дни в годината. (непланирано спиране на</p>	<p>Изисква се / Must be available</p>	

работата се допуска за не повече от 53 минути годишно). The cryptographic service is a highly critical component in entire Central system infrastructure. The high availability requirements for the cryptographic service must be like all components of the E-Meter infrastructure. The availability of the central system environment needs to be 99.99% under a 24/7/365 window per year base. (Unplanned downtime max. 53 minutes per year).		
<b>68.</b> (Географски) разпределена инфраструктура и архитектура, както и осигуряването на съответната функционалност Възстановяване след Слив трябва да са налични за централната система. A (geographical) redundant design and architecture as well as providing the relevant Fail Over functionality must be available of the central system.	Изисква се / Must be available	
<b>69.</b> Криптографската услуга трябва да е разработена така, че не само продуктивната среда на Централната система, а и тестовата среда (среда) да могат да се възползват от нейната функционалност. Cryptographic service must be so designed in a way that not only the productive instance of the central system, but also a test system (environment) can use its functionalities.	Изисква се / Must be available	
<b>70.</b> Освен Продуктивна среда за Централната система трябва да има и наличието на тестова среда. Productive and test environment must be available for the central system.	Изисква се / Must be available	
<b>71.</b> Единствено физически интерфейс (инфрачервен порт) може да се ползва за достъп без отстраняване на капака на Е-електромера. Only physical interface Infrared (IR) port must be accessible without removing the cover of E-Meter.	Изисква се / Must be available	
<b>72.</b> Е-електромерите трябва да могат автоматично да записват събитията, свързани с процесите по отваряне на корпуса на електромера или капака на клемния блок, и да изпращат известия до съответната централна система и да ги съхраняват в регистъра (паметта) на Е-електромера. The E-Meters must be able automatically to record the events related to the process of opening the meter housing or terminal cover is detected and to send notification to the corresponding central system and store it in the registry(memory) of E-Meter.	Изисква се / Must be available	
<b>73.</b> Отчетните стойности и капака на клемния блок трябва да бъдат надлежно защитени от неоторизирано физическо проникване. Опити за манипулации върху самия Е-електромер или върху интерфейсите трябва да се виждат оптически (напр. нарушени пломби). The counter values and terminal cover must be suitable protected from unauthorized physical intrusion. Manipulation attempts upon the E-Meter itself or at the interfaces must be optically visible (for example, broken seals).	Изисква се / Must be available	
<b>74.</b> Вградените в Е-електромера елементи - микроконтролери, процесори обикновено разполагат с подходящи интерфейси (като JTAG - IEEE 1149.1 Standard Test Access Port and	Изисква се / Must be available	

<p>Boundary-Scan Architecture), които позволяват програмиране или проверка за неизправности и ремонт на съответните компоненти. Тези интерфейси са необходими, например в процеса на производство на Е-електромера. Всички хардуерни интерфейси, които могат да се използват непосредствено за програмиране или разрешаване на проблеми, след производството на Е-електромера трябва да бъдат изключени. The built-into E-Meter - microcontrollers, processors are usually with appropriate interfaces (like JTAG - IEEE 1149.1 Standard Test Access Port and Boundary-Scan Architecture) provided which are allowing programming or debugging of the respective components. These interfaces are required, for example in the process of production of E-Meter. All hardware interfaces, which can be used immediately for programming or debugging after the production of E-Meter must be disabled.</p>		
<p><b>75.</b> Е-електромерът трябва да запазва сигурността си и при наличие на грешки или възникване на нежелани или неволно предизвикани работни състояния (случайно или злоумишлено причинени). Като такива грешки могат да бъдат: загуба на захранване, грешка в процеса на изпълнение на криптографски функции, грешка в процеса на валидиране на достъпа E-Meter must also preserve a secure state when errors and unwanted or unintended operating states (random or willfully) are caused. Such errors can be: voltage loss, error in the process of executing cryptographic functions, error in process of validating access permissions.</p>	<p>Изисква се / Must be available</p>	
<p><b>76.</b> Паметта за регистъра на Е-електромерът трябва да бъде с достатъчна големина, което гарантира невъзможността за записване на нови съобщения за системния регистър, върху съществуващи такива, преди да бъдат прочетени от централната система. Минималната памет, която трябва да е налична е за поне 100 събития. The memory for the E-Meter log must be with adequate size, which ensures that no system log messages can be overwritten before they are read out by a central system. A minimum storage for minimum 100 events must be available in it.</p>	<p>Изисква се / Must be available</p>	
<p><b>77.</b> Криптографските ключове трябва да бъдат съхранявани по сигурен начин в Е-електромера. Не трябва да е възможно да бъдат прочетени или записвани на друг носител. The cryptographic key(s) must be itself safely stored in the E-meter. It must be not possible to be read in plain text or exported.</p>	<p>Изисква се / Must be available</p>	
<p><b>78.</b> Е-електромерите трябва да разполагат с вграден часовник и периодично трябва да бъдат синхронизирани с Централната система. The E-meter must have internal clock and at periodic intervals must be synchronized with the central system</p>	<p>Изисква се / Must be available</p>	

<p><b>79.</b> Производителят на Е-електромерите трябва да разкрие (декларира) преди първата доставка, които компоненти и типове (като комуникационния модул или измерващия блок) са инсталирани в Е-електромер, както и от кои доставчици са набавени тези компоненти. Конфигурацията на Е-електромера трябва да бъде представена на EVN EP. Последващи промени в конфигурацията (напр. промяна на доставчика на вградените чипове и т.н.) се допускат единствено, ако EVN EP е било предварително уведомено в писмен вид и е приело промяната. The E-meter manufacturer must disclose (declare) before the first delivery, which components and types (like communication module or unit of measurement) are installed in E-meter as well as from which suppliers these components are coming. The configuration of the E-meter must be provided to EVN. Subsequent changes of the configuration (for example change of supplier of built-in chips and etc.) are only permitted if EVN EP previously was notified in written form and if EVN EP agrees.</p>	<p>Изисква се / Must be available</p>	
<p><b>80.</b> Комуникацията по всички интерфейси на Е-електромера трябва да се осъществява по начин, който гарантира и защитава конфиденциалността и почтеността. Достъпът до информацията в Е-електромера трябва да бъде гарантиран по всяко време. The communication on all interfaces of the E-Meter must be done in a way to guarantee and protect the confidentiality and integrity. The availability of the information from E-Meter must be guaranteed at all the time.</p>	<p>Изисква се / Must be available</p>	
<p><b>81</b> При всички двупосочни интерфейси на Е-електромера трябва да бъдат приемани единствено съобщения, които са предварително дефинирани за всеки порт, от страна на доставчика. Преди приемане на съобщение, то трябва да бъде валидирано и истинността му да бъде проверена. Съобщения, които не преминат тази проверка, не трябва да бъдат отваряни. At all bidirectional interfaces of E-Meter only messages must be accepted which are previously defined for each port from the vendor. Before a message is accepted, it must be validated and accuracy to be checked. Messages that do not pass this test must be discarded.</p>	<p>Изисква се / Must be available</p>	

<p><b>82</b> Ако Е-електромерът е монтиран, но няма комуникационна връзка с Централната система, Е-електромерът трябва да работи като стандартен електронен електромер. Трябва да са възможно основни функции, като: Некриптирано отчитане на данните, съхранявани в отчетните регистрирани стойности и профилите на товарите. (IR port може да бъде използван с Преносим терминал), некриптирано отчитане на данните, съхранявани в записите в регистъра на събитията (IR port може да бъде използван с Преносим терминал), настройване на датата и часа. (IR port може да бъде използван с Преносим терминал) If E-Meter is installed, but no communication link with the central system is established, the E-meter must operate as a standard electronic meter. Basic functions must be possible such as: Unencrypted reading out of data stored in the counter register values and the load profiles (IR port can be used by HHU), unencrypted reading out of data stored in the counter event log entries (IR port can be used by HHU), set the Date and Time. (IR port can be used by HHU).</p>	<p>Изисква се / Must be available</p>	
<p><b>83.</b> Е-електромерът в процеса на производство трябва да бъде първоначално зареден с фърмуер от производителя. The E-Meter must be initially loaded with a firmware image in the process of its production from the vendor</p>	<p>Изисква се / Must be available</p>	
<p><b>84.</b> Манипулирането на определена част от фърмуера или на настройките на фърмуер трябва да е невъзможно. Manipulation of a custom portion of the firmware or of the contained firmware settings must not be possible.</p>	<p>Изисква се / Must be available</p>	
<p><b>85.</b> Трябва да е възможно актуализиране на фърмуера чрез Централната система. Коректността на актуализациите на фърмуера трябва да бъдат проверени поне чрез hash код на файла за даунлоад, който е поискан чрез криптирано съобщение между централната система и Е-електромера. Е-електромерът не трябва да започва процес на зареждане на новия фърмуер ако липсва автентичиран hash код. Firmware update must be possible from the central system and must not influence the metrological part of E-Meter. The integrity of the firmware updates must be protected at least by hash code of the downloadable file which is sent through a unicast (one to one) authenticated and encrypted message and the E-Meter must not activate downloading process without having received the authenticated hash code.</p>	<p>Изисква се / Must be available</p>	
<p><b>86.</b> В случай на повреда при инсталирането на актуализацията на фърмуера, започналата операция не трябва да влияе на съответните компоненти и Е-електромера трябва да продължи да работи със стария фърмуер. In case of corruption of the update firmware operation, the operation must not affect the respective component and E-Meter must continue to operate with old firmware.</p>	<p>Изисква се / Must be available</p>	

<p><b>87</b> Измерените данни (съхранени данни – стойности от брояча, събития и конфигурация) не трябва да бъдат променяни или трети в процеса на актуализация на фърмуера. The metered data (stored data – counter values, events and configuration) are not allowed to be changed or deleted during the process of update of the firmware.</p>	<p>Изисква се / Must be available</p>	
<p><b>88</b> Ненужните функции на фърмуера на Е-електромерите трябва изрично да бъдат деактивирани. Unnecessary functions of the firmware of E-Meters must be explicitly disabled.</p>	<p>Изисква се / Must be available</p>	
<p><b>89.</b> Производителят на Е-електромерите трябва да гарантира, че фърмуера за тях е произведен по дефиниран и внедрен вътрешен процес. The vendor of E-meter must ensure that only a firmware image which is derived from the associated E-meter manufacturers has been released by a defined approval process.</p>	<p>Изисква се / Must be available</p>	
<p><b>90</b> При научно-изследователската си дейност, свързана с компонентите, монтирани в Е-електромера, продавачът трябва да разполага с подробна документация. При разкриване на слабости във фърмуера и софтуера, в контекста на вътрешните проверки на качеството, същите трябва да бъдат регистрирани. Всички мерки, предвидени за запълване на непълноти, трябва да бъдат документирани. Тази документация трябва да се предоставя на EVN EP в писмен вид, при поискване. The vendor during the research and development of components which are installed in E-Meter must have a detailed documentation. In case of discovery of vulnerabilities in firmware and software in context of internal quality checks they must be recorded. All measures taken into account for filling the gaps must be documented. That documentation must be provided to EVN EP in written form, if it is requested.</p>	<p>Изисква се / Must be available</p>	
<p><b>91.</b> Производителят или доставчика на софтуера или фърмуера трябва да потвърди с писмено известие, че са взети всички мерки да се предотврати наличието на всякакви „задни вратички“ (средства за неоторизиран достъп) до фърмуера. Подобни „задни вратички“ биха могли да осигурят неоторизиран достъп до компонентите на Е-електромера. Под „задна вратичка“ в случая се разбира и функция за дистанционна поддръжка, която, без знанието на EVN EP, би могла да бъде активирана от доставчика (производителя). The manufacturer or supplier of the software or firmware has to confirm by a written agreement that measures have been taken that availability of backdoors in the firmware are strictly prohibited. Through these backdoors might unauthorized access to the components of the E-meter and Concentrator infrastructure to be possible. As a backdoor applies in that case, a remote maintenance function, which without knowledge of EVN EP could be put into operation from the vendor (manufacturer).</p>	<p>Изисква се / Must be available</p>	



<p><b>92</b> Производителят или доставчика трябва да осигурят съдействие при Одити за ИТ сигурност. Manufacturer or supplier must cooperate in case of IT Security Audits.</p>	<p>Изисква се / Must be available</p>	
<p><b>93.</b> Софтуерът на Централна система трябва да е съвместим със сървърна архитектура x86. The software of Central system must be compatible with x86 server architecture.</p>	<p>Изисква се / Must be available</p>	
<p><b>94.</b> Трябва да бъдат създадени продуктивна и тестова среда на Централната система. Productive and test environments must be deployed for the central system.</p>	<p>Изисква се / Must be available</p>	
<p><b>95</b> Централната система трябва да е съвместима с операционна система Microsoft Windows 2008 сървър 64 bit или следващи варианти или Red Hat v 6.3 64 битова и следващи версии. The Central system must be compatible with operating system Microsoft Windows 2008 server 64 bit or higher or Red Hat v. 6.3 / 64 bit or higher.</p>	<p>Изисква се / Must be available</p>	
<p><b>96</b> Графичният потребителски интерфейс на софтуера на централната система трябва да бъде ергономичен и да съответства на стандарт EN ISO 9241. Graphical user interface of software of central system must be ergonomic and refer to EN ISO 9241 standardization</p>	<p>Изисква се / Must be available</p>	
<p><b>97</b> Централната система трябва да дава възможност за реализация на концепцията за оторизация по роли. Правата на потребителите трябва да бъдат дефинирани за всяка отделна роля, заедно със съответните разрешителни. Различните потребители, в зависимост от своите функции, трябва да имат роли, съответстващи на задълженията им. Прилагането на ролева оторизация трябва да позволи максимално разделение на функциите. The Central system must allow implementation of role-based authorization concept. User rights must be defined for each role with appropriate necessary permissions. The various users depending on their function must have assigned role corresponding to their duties. The implementation of a role-based authorization concept must allow maximum separation of functions.</p>	<p>Изисква се / Must be available</p>	
<p><b>98</b> Паролите, съответстващи на правата на потребителите, трябва да се съхраняват по начин отговарящ на въведения механизъм за сигурно криптиране и трябва да не подлежат на възпроизвеждане. Паролите трябва да бъдат управлявани на централно ниво. Passwords corresponding to user rights must be kept in a way which correlates to the deployed secure encryption mechanism and must be not reproducible. Passwords must be managed centrally.</p>	<p>Изисква се / Must be available</p>	
<p><b>99</b> При софтуера следва да се прилага принципа на 4-те очи за особено важните функции на централната система. Най-съществените функции на системата, които се нуждаят от потвърждение преди изпълнението си, трябва да бъдат конфигурирани по начин, който налага присъствието на поне 2 служители, които да одобряват съответните дейности, преди започване</p>	<p>Изисква се / Must be available</p>	

на тяхното изпълнение (пример: процес за прекъсване на електричеството). Software must assist 4-eyes principle for a critical central system functions. Critical system functions that need confirmation before execution must be configured in a way that requires at least 2 employees approve before the start of execution (example: process for switch off / switch on of electricity).		
<b>100</b> Командите за функциите на критични системи функции за всеки от Е-електромерите трябва да бъдат уникални и разпространението им не трябва да се изпълнява като излъчване до всички Е-електромери. Commands for critical system functions for each E-Meters must be unique and their distribution must be not performed as a broadcast to all E-Meters	Изисква се / Must be available	
<b>101</b> Сигурно регистриране на всички дейности и защита от посегателства трябва да се осъществява по време на изпълнението на особено важни команди по отношение на Е-електромерите. Tamper-proof (secure) logging of all activities must be undertaken during the execution of critical commands towards the E-Meters.	Изисква се / Must be available	
<b>102</b> Записите в регистъра трябва лесно и по уникален начин да идентифицират дейностите на служителите. Assignment of log entries must easily and uniquely identify employees' activities.	Изисква се / Must be available	
<b>103</b> Централната система трябва да осигури възможност за максимален брой дневни дейности по отношение на Е-електромера. При достигане на подлежащия на конфигуриране максимален брой, системата трябва да изпрати предупреждение. Промяната в дневните лимити трябва да може да е извършва от поне двама служители на EVN EP (съответствие с принципа на 4те очи). The Central system must provide the possibility of maximum number of daily activities towards the E-Meter. If the configurable limit is reached, the system must send an alert. The change of the daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle).	Изисква се / Must be available	
<b>104</b> Поради уникалността на командата за прекъсване на захранването чрез главния прекъсвач за всеки Е-електромер, трябва да бъде приложен логически алгоритъм, който регулира колко Е-електромера максимално могат да бъдат изключени в рамките на един ден. При достигане на конфигурираната максимална стойност, Централната система трябва да спре процесът по изпълнение и генериране на предупреждение. Промяната на дневните максимални стойности трябва да е възможна единствено при участие на двама или повече служителя на EVN EP (спазване на принципа за 4-те очи и процедурата за одобряване). Due to the uniqueness of "switch off" command towards the circuit breaker for each E-Meter, a logical algorithm must be applied which regulates how many E-Meters can be switched off maximum per day. If the configurable limit is reached, the central system must stop the process of	Изисква се / Must be available	

execution and generate an alert. The change of daily limits must be possible from at least two employees of EVN EP (compliance with 4-eyes principle and approving procedure).		
<b>105</b> Централната система трябва да осигурява за всички Е-електромери и Концентратори синхронизация на часа, въз основа на вътрешен стандарт, като NTP с външен таймер или вече приложен такъв във вътрешните мрежови таймери. The central system must provide for all E-Meters and Concentrators time synchronization based upon international standard, like NTP protocol with an external timer or an already implemented in the internal network timers.	Изисква се / Must be available	
<b>106</b> Часът според централна система може да се различава с максимум една секунда от часа на външния или вътрешния таймер. The time of central system can have difference of maximum of one second from the time of the external or internal timer.	Изисква се / Must be available	
<b>107</b> Часът на монтираните Е-електромери трябва да бъде периодично проверяван и, ако е необходимо, синхронизиран с Централната система. Отклоненията в часа на инсталираните Е-Електромери и Централната система трябва да се съобщават под формата на алармено съобщение. (Прекомерните отклонения могат да са знак за неизправност или манипулация на Е-електромера) The time from all installed E-Meters must be periodically checked and, if necessary, synchronized with the central system. Deviations of the time of installed E- Meters and Central system must be reported as an alarm message. (Excessive deviations could be a sign of a malfunctioning or manipulation of the E-Meter)	Изисква се / Must be available	
<b>108</b> Централната система трябва да осъществява надлежен контрол и отчетност на всичките си функции. При неизправност следва незабавно да се генерира и изпраща известие до отговорния персонал. The central system must make an appropriate monitoring and reporting of all its functionalities. In case of malfunctions automatically a corresponding notification to the responsible personnel to be generated.	Изисква се / Must be available	
<b>109</b> Дадените разрешения и потребителски права на всички служители, които имат достъп до Централната система и до съответните компоненти на Е-електромера, трябва да бъде възможно да се проверяват периодично. The assigned permissions and user rights of all employees which have an access in the Central system and to the respective components of E-Meter infrastructure should able to be checked periodically.	Изисква се / Must be available	

<p><b>110.</b> Централната система трябва да генерира справка, в която да има списък с всички потребители с дата на определяне на пълномощията им, дата на първа регистрация, дата на последен успешен вход в системата, роля на потребителя. The central system must generate a List of all users with the date of definition, date of first registration, date of last successful login, role membership of the user.</p>	<p>Изисква се / Must be available</p>	
<p><b>111.</b> Централната система трябва да генерира справка, в която да има списък с всички разрешения, свързани с дадена роля в Централната система. The central system must generate a List of all permissions associated with a role in the central system.</p>	<p>Изисква се / Must be available</p>	
<p><b>112</b> Централната система трябва да генерира списък с оценка, според различни показатели (напр. всички потребители, които имат право да осъществяват дадено действие). The central system must generate a list of evaluation according to various dimensions (for example- all users who are allowed to perform a certain action)</p>	<p>Изисква се / Must be available</p>	
<p><b>113</b> Централната система трябва да може да идентифицира критични валидиращи комбинации (напр. даден потребител може да осъществява без потвърждение от друг служител критични команди за редица елементи от системата). The central system must be able to identify critical authorization combinations (for example, a user could run without the confirmation of another employee critical commands for a plurality of measurement points)</p>	<p>Изисква се / Must be available</p>	
<p><b>114.</b> Централната система трябва да може да поддържа исторически данни за разрешенията на потребителите (трябва да се съдържа подробна информация относно това кои потребители, какви права са имали в даден момент). The central system must support historization of permissions of users (it should be comprehensible, about what permissions a user had at a particular time).</p>	<p>Изисква се / Must be available</p>	
<p><b>105</b> Всички промени в конфигурацията на Централната система трябва да бъдат регистрирани. Съхранените записи за съответните промени следва да бъдат защитени. Информацията в регистъра трябва да бъде ясна и точна. Any changes to the configuration of the central system have to be recorded. The stored log entries against subsequent change have to be protected. The log information must be clearly reported.</p>	<p>Изисква се / Must be available</p>	
<p><b>106</b> Всички промени в Централната система (напр. – ръчно манипулиране на показания, замяна на стойности) трябва да бъдат регистрирани, уникални и обвързани със съответния потребител. Трябва да има налични хронологични данни за дейностите на всички потребители. All changes in the central system (for example - manual manipulation of readings, replacement of values) must be logged, unique and assigned to a particular user. Historization of all user</p>	<p>Изисква се / Must be available</p>	

activities must be available.		
<b>107</b> Ако в монтирани Е-електромери възникне критично системно събитие, съответната аларма трябва да бъде изпратена до 5 минути до Централната система. If in the installed (deployed) E-Meters a critical system event is recognized then an appropriate alarm must be within 5 minutes sent to the central system.	Изисква се / Must be available	
<b>108</b> По време на периодичното отчитане на съответните измерени стойности от Е-електромерите, цялата съхранена в тях информация за събития трябва да може да бъде прехвърлена в централната система. During the periodic reading of the corresponding measured values from E-Meter, all stored in it event information must be able to be transported to central system.	Изисква се / Must be available	
<b>109</b> За да се избегне повторен запис на криптирани команди към Е-електромерите от Централната система или концентратора, Доставчикът трябва да въведе подходящ механизъм за предпазване от подобно повтаряне. (брояч на команди) For avoiding a re-recording possibility of encrypted commands towards the E-Meter from the central system or concentrator the Vendor has to implement an adequate mechanism to resist on it. (like framecounter of commands)	Изисква се / Must be available	
<b>110</b> Приложението за дейности по поддръжката трябва да е съвместимо с операционната система на Преносимия терминал - Microsoft Windows mobile professional v.6.5 или библиотеките (SDK) за интегриране в съществуващи приложения. The application for maintenance tasks must be compatible with HNU operating system - Microsoft Windows mobile professional v.6.5 or libraries (SDK) for integration with existing legacy application.	Изисква се / Must be available	
<b>111</b> Клиентската част от приложението на Централната система трябва да може да работи на терминален сървър с Microsoft Windows 2008 server 64bit. The client part of the central system application must be able to run on terminal server environment with Microsoft Windows 2008 server 64bit.	Изисква се / Must be available	
<b>112</b> Централната система трябва да подлежи на адаптация съобразно със съвременните технологии (интерфейси) за обмен на информация в двете посоки със съществуващите системи на Възложителя. Например с билинг системата(kVASy) и системата за управление на измервателни данни.The central system must be able to be customized with modern technologies (interfaces) to exchange information with Contractor legacy systems in both directions. For example - billing and ERP system (kVASy) and meter data management environment.	Изисква се / Must be available	

<p><b>113</b> При неуспешно изпълнение на функцията по „включване“ от Централната система по отношение на даден Е-електромер в рамките на 4 часа, трябва да се генерира автоматична команда за задача по поддръжка към Преносимия терминал за да се осъществи ръчно „включването“ на Е-електромера. In case of not successful execution of „switch on“ or „switch off“ function from central system towards the E-Meter in the timeframe within 4 hours, an automatic workorder must be created for maintenance task towards the HHU in order manually to perform the „switch on“ or „switch off“ function for the E-Meter.</p>	<p>Изисква се / Must be available</p>	
<p><b>114</b> След ръчното изпълнение на функцията „вкл.“ или „изкл.“ на Е-електромера от HHU от страна на служител, централната система трябва да дава възможност (интерфейс) HHU да може да отчети състоянията на вече изпълнените заявки за работа към Е-електромерите. After manual execution of “switch on” or “switch off “ function towards the E-Meter by HHU from employee, the central system must give possibility (interface) that HHU can report statuses of already executed workorders towards E-Meters.</p>	<p>Изисква се / Must be available</p>	
<p><b>115</b> Централната система трябва да поддържа справочен механизъм, с който Изпълнителят да може сам да създава съответните доклади от системата. The Central system must support reporting mechanism with which the Contractor can create by itself adequate reports from the system.</p>	<p>Изисква се / Must be available</p>	
<p><b>116.</b> Доставчикът на Централната система трябва да поддържа централна служба за съобщения (24/7/365), която да се ползва от възложителя за проследяване и категоризиране на възникнали грешки при експлоатация на системата. The vendor must assure an availability of ticketing and reporting portal (24/7/365) which can be used from the Contractor for tracing and categorization of errors which are coming in the process of exploitation of the central system.</p>		

VI. Стандарти		
<p>Изискванията на съответните технически стандарти и препоръки трябва да бъде спазено</p>	<p>Продукта съответства на IEC Publ. 60529</p>	
	<p>Продукта съответства на ISO Publ. 75</p>	
	<p>Продукта съответства на EN 62052-11</p>	
	<p>Продукта съответства на EN 62053-21</p>	
	<p>Продукта съответства на EN 62056-21</p>	
	<p>Продукта съответства на EN 62056-61</p>	
	<p>Продукта съответства на EN 55011</p>	
	<p>Продукта съответства на EN 55014</p>	
	<p>Продукта съответства на EN 62053-52</p>	
	<p>Продукта съответства на EN 61000-3-2 + A2</p>	



	Продукта съответства на EN 61000-4-4	
	Продукта съответства на EN 61000-4-5	
	Продукта съответства на EN 62052-11 издание: 2003-02-12	
	Продукта съответства на EN 62053-21 издание 2003-01-28	
	Продукта съответства на EN 62054-21 издание 2005-08-01	
	Продукта съответства на DIN 43859 6.77	
	Продукта съответства на DIN VDE 0160 05.88	
	Продукта съответства на IEC 13 (SEC) 1022	
	Продукта съответства на OIML 11	
	Продукта съответства на OIML 12	

**\*Посочените изисквания са пожелателни / незадължителни!**

**Кандидат който не покрие задължителните минимални технически изисквания на Възложителя няма да бъде допуснат до участие в системата.**

## Декларация № 1

за липса на обстоятелствата по чл.47, ал. 1, т.2, т.3; ал.2, т. 2а, т.3, т.4 и ал.5,т.2 от ЗОП към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

Долуподписаният/а1:

....., роден/а на  
....., с лична карта/паспорт № ..... издаден/а от  
....., на ..... валиден/а до ..... действащ  
като ..... на  
....., със седалище и адрес на  
управление ..... вписано в  
търговския регистър на ..... с ЕИК №  
....., ИН по ДДС .....

Д Е К Л А Р И Р А М, че:

1. Представляваният от мен кандидат:

- а) не е обявен в несъстоятелност;
- б) не е в производство по ликвидация и не се намира в подобна процедура съгласно националните закони и подзаконови актове.
- в) не е виновен за неизпълнение на задължения по договор за обществена поръчка
- г) няма задължения по смисъла на чл. 162, ал. 2, т. 1 от Данъчно-осигурителния процесуален кодекс към държавата и към община, установени с влязъл в сила акт на компетентен орган, освен ако е допуснато разсрочване или отсрочване на задълженията, или има задължения за данъци или вноски за социалното осигуряване съгласно законодателството на държавата, в която кандидатът или участникът е установен.
- д) няма наложено административно наказание за наемане на работа на незаконно пребиваващи чужденци през последните 5 години.
- е) не е в договорни отношения с лице по чл. 21 или чл. 22 от Закона за предотвратяване и установяване на конфликт на интереси.

2. Се задължавам при промяна на горепосочените обстоятелства писмено да уведомя Възложителя за всички настъпили промени в процеса на провеждане на обявената процедура за възлагане на обществена поръчка.

Известно ми е, че при деклариране на неверни данни нося наказателна отговорност по чл. 313 от НК.

.....  
(дата на подписване)

.....  
Декларатор: (подпис и печат)

<sup>1</sup> Декларацията се подава от лицата по Чл.47, ал.6, а именно едно от лицата, които могат самостоятелно да представляват лицето.

## Декларация № 2

за липса на обстоятелствата по чл.47, ал.1, т.1, ал. 2, т.5 и ал.5, т.1 от ЗОП

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

Долуподписаният/а1:

....., роден/а на  
....., с лична карта/паспорт № ....., издаден/а от  
....., на ....., валиден/а до..... действащ  
като ..... на  
....., със седалище и адрес на  
управление ..... вписано в  
търговския регистър на ..... с ЕИК №  
....., ИН по ДДС ....., в качеството си  
на кандидат / подизпълнител (невярното се зачертава).

Д Е К Л А Р И Р А М, че:

1. Не съм осъждан(а) с влязла в сила присъда за:

а) престъпление против финансовата, данъчната или осигурителната система, включително изпиране на пари, по чл. 253 - 260 от Наказателния кодекс;

б) подкуп по чл. 301 - 307 от Наказателния кодекс;

в) участие в организирана престъпна група по чл. 321 и 321а от Наказателния кодекс;

г) престъпление против собствеността по чл. 194 - 217 от Наказателния кодекс;

д) престъпление против стопанството по чл. 219 - 252 от Наказателния кодекс.

е) престъпление по чл. 313 от Наказателния кодекс във връзка с провеждане на процедура за възлагане на обществена поръчка

2. Не съм свързано лице по смисъла на § 1, т.23а от допълнителните разпоредби на Закона за обществените поръчки с възложителя или със служители на ръководна длъжност в неговата организация.

3. Се задължавам при промяна на горепосочените обстоятелства писмено да уведомя Възложителя за всички промени в процеса на провеждане на обявената процедура за възлагане на обществена поръчка.

Известно ми е, че при деклариране на неверни данни нося наказателна отговорност по чл. 313 от НК.

.....  
(дата на подписване)

.....  
Декларатор: (подпис и печат)

<sup>1</sup> Декларацията се подава от всяко от лицата по Чл.47, ал.4.

### Декларация № 3

за обстоятелствата по чл. 56, ал. 1, т. 11 и т.12 от ЗОП  
към система за предварителен подбор на изпълнители  
№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени,  
обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

Долуподписаният/а1

....., роден/а на  
....., с лична карта/паспорт № ..... издаден/а от  
....., на ..... валиден/а до ..... действащ  
като ..... на  
....., със седалище и адрес на  
управление ..... вписано в  
търговския регистър на ..... с ЕИК №  
....., ИН по ДДС .....

Д Е К Л А Р И Р А М, че:

В случай на допускане до участие в договаряне, при изготвяне на първоначална оферта ще са спазени изискванията за закрила на заетостта, включително минимална цена на труда и условията на труд.

Запознат съм със съдържанието на проекта на договор, ведно с всички приложения към него, от документацията за участие в процедурата по възлагане на обществена поръчка и приемам изцяло клаузите в него.

Известно ми е, че при деклариране на неверни данни нося наказателна отговорност по чл. 313 от НК.

.....  
(дата на подписване)

.....  
Декларатор: (подпис и печат)

<sup>1</sup> Декларацията се подава от лицата по Чл.47, ал.6, а именно едно от лицата, които могат самостоятелно да представляват кандидата.

#### Декларация № 4

за обстоятелствата по чл. 56, ал.1, т.8 от ЗОП

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

Долуподписаният/а<sup>1</sup>

1. ...., роден/а на  
....., с лична карта/паспорт № ..... издаден/а от  
....., на ..... валиден/а до ..... действащ  
като ..... на  
....., със седалище и адрес на  
управление ..... вписано в  
търговския регистър на ..... с ЕИК №  
....., ИН по ДДС .....

Д Е К Л А Р И Р А М, че:

Представявания от мен кандидат при изпълнението на горепосочената обществена поръчка няма да използва / ще използва подизпълнители (невярното се зачертава);

Подизпълнител/и ще бъде/бъдат ..... (изписват се наименованията на фирмите/лицата подизпълнители), които са запознати с предмета на поръчката и са дали съгласието си за участие в процедурата;

Делът на участие на подизпълнителите при изпълнение на поръчката ще бъде общо .....% от общата стойност на поръчката, в т.ч. участието на

Подизпълнител 1 ..... (изписва се името на първия подизпълнител) ..... ще бъде .....% от общата стойност на поръчката

Подизпълнител 2 ..... (изписва се името на първия подизпълнител) ..... ще бъде .....% от общата стойност на поръчката и т.н.

Видът на работите, които ще извършва ще бъдат:

Подизпълнител 1 .....

Подизпълнител 2 .....

Известно ми е, че при деклариране на неверни данни нося наказателна отговорност по чл. 313 от НК.

.....  
(дата на подписване)

.....  
Декларатор: (подпис и печат)

<sup>1</sup> Декларацията се подава от лицата по Чл.47, ал.6, а именно едно от лицата, които могат самостоятелно да представляват кандидата.

## Декларация № 5

от подизпълнител

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

Долуподписаният/а1

1. ...., роден/а на  
....., с лична карта/паспорт № ..... издаден/а от  
....., на ..... валиден/а до ..... действащ  
като ..... на  
....., със седалище и адрес на  
управление ..... вписано в  
търговския регистър на ..... с ЕИК №  
....., ИН по ДДС .....

Д Е К Л А Р И Р А М, че:

съм запознат/а и напълно съгласен/а с условията и цялата документация за участие в процедурата по възлагане на обществената поръчка;

съм съгласен/а представляваното от мен лице да вземе участие в процедурата като подизпълнител на дела на участие и вида на работите, които представляваното от мен лице ще извърши са:

.....  
.....  
.....  
.....

представляваното от мен лице е готово да извърша работата, за която е предвидено;

представляваното от мен лице не е част от обединение, което е кандидат по настоящата процедура;

представляваното от мен лице не участва самостоятелно като кандидат по настоящата процедура;

Известно ми е, че при деклариране на неверни данни нося наказателна отговорност по чл. 313 от НК.

.....  
(дата на подписване)

.....  
Декларатор: (подпис и печат)

<sup>1</sup> Декларацията се подава от лицата по Чл.47, ал.6, а именно едно от лицата, които могат самостоятелно да представляват подизпълнителя.



## Проект на договор

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

Проект на договор

Днес, ....., се сключи настоящият договор между:

ЕВН България Електроразпределение ЕАД, със седалище и адрес на управление гр.Пловдив, ул."Христо Г.Данов"№37, вписан в търговския регистър на Агенцията по вписванията ЕИК 115552190 , ИН по ДДС: BG 115552190, представлявано чрез всеки двама членове от съвета на директорите, в състав: Костадин Величков, Роналд Брехелмахер, Гочо Чемширов, наричано по-нататък ВЪЗЛОЖИТЕЛ

и  
##### със седалище и адрес на управление гр. #####, ул. "##### " № ##, ,вписан в търговския регистър на Агенцията по вписванията с ЕИК XXXXXXXXXX, ИН по ДДС: #####, представлявано от ##### - #####, наричано по-нататък Изпълнител.

## ПРЕДМЕТ

Чл.1(1). Възложителят възлага, а Изпълнителят приема да извърши, след Заявка за доставка от страна на Възложителя, доставка , инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери", накратко наричана „Системата“, съгласно условията на настоящия договор.

## СТОЙНОСТ

Чл.2(1). Прогнозната стойност на договора, възлиза на ####.###,## лева без ДДС.

## ЦЕНОВИ УСЛОВИЯ

Чл.3(1). Всички единични цени са посочени в протокола от договарянето, проведено между страните, представляващ неразделна част от настоящия договор и включват всички транспортно-командировъчни разходи, разходи за нощувки, дневни и други разходи на Изпълнителя във връзка с изпълнението на договора.

(2). Всички цени са окончателни, фиксирани за срока на договора, без ДДС и съгласно позиции от 00010 до #####, посочени по-горе.

(3). Всички цени за цялостна доставка и пускане в експлоатация на „Системата“ или за частична доставка на една или няколко от съставните и части, са по условията DDP Incoterms 2010, до адрес указан от Възложителя, опаковани, застраховани, обмитени, включително всички такси и стойност на разтоварването им.

(4). Цената на годишна поддръжка на софтуера на „Системата“ се определя, като % от стойността на актуалния лицензен каталог равен на ## %, който остава фиксиран за целия срок на договора включително и опциите за удължаването му, като плащанията се извършват на месечна база.

(5). Стойността на актуалния лицензен каталог се формира като сума от стойностите на лицензиите на инсталираните и пуснати в експлоатация функционалности на софтуера на „Системата“към датата на изчисляване на стойността..

## МЯСТО НА ИЗПЪЛНЕНИЕ

Чл.4(1). Мястото на изпълнение на договора е лицензионната територия на „ЕВН България Електроразпределение“ ЕАД.

(2). Доставката на „Системата“ или нейни съставни части, задължително се придружават минимум от следните документи: сертификат за качество, гаранционна карта, декларация за съответствие.

## СРОКОВЕ

Чл.5. (1). Първоначалния срок на действие на договора е за 4 години с едностранни опции с допълнително една календарна година от страна Възложителя за продължаване срока на действие считано от датата на подписването му.

(2). Едностранна опция от страна на Възложителя за продължаване на срока на действие на договора с допълнително 1+1+1 календарни година или до изчерпване на стойността съгл. чл.2, при запазване на всички цени и условия от настоящия договор. Максималният срок на действие на договора не може да надвишава 7 години. Активирането на опцията става с писмено предизвестие до Изпълнителя, подадено не по-късно от 30 календарни дни преди датата на изтичане на срока на договора. Опцията може да бъде активирана от Възложителя единствено ако не е изчерпана стойността съгласно чл. 2.

(3). Срокът за изпълнение на доставката, инсталацията и пускането в експлоатация на „Системата“ е до ## календарни дни считано от датата на подписване на договора.

(4). Сроковете за изпълнение на доставки свързани със функциониране и разширяване на „Системата“ са както следва:

1. На ##### до ## календарни дни
2. На ##### до ## календарни дни
3. На ##### до ## календарни дни
4. На нов лиценз до ## календарни дни

, след получаване на писмена „Заявка за доставка“ от Възложителя, съдържаща точна спецификация на доставката. Като отделните заявки за доставка се изпращат до Изпълнителя. Към изпълнение се пристъпва след изпращане от страна на Възложителя на „Заявка за доставка“ с посочени конкретни количества, по факс или имейл до лицето за контакт на Изпълнителя, посочено в чл. 12.(2).

(5). В случай че Изпълнителят не изпълни доставката в определените срокове(чл.5.(3) и(4)) и закъснението продължава 10 или повече календарни дни, Възложителят има право да откаже доставката. В този случай Възложителят (i) не носи отговорност за разходи и/или вреди, претърпени от Изпълнителя във връзка с отказа; и (ii) не дължи възнаграждение на Изпълнителя за отказаната доставка. Отказът на доставката се прави с писмено уведомление от Възложителя, изпратено до лицата за контакт на Изпълнителя, посочено в чл. 12.(2)..

(6). Сроктът за реакция е до 4 часа, след подаване на информация за проблем и нефункциониране на „Системата“ до посочените от Изпълнителя лица за контакт-чл. 12.(2)

(7). Сроковете за отстраняване на категоризирани проблеми, съгласно т. V. 14 от документа Технически изисквания са:

1. За Категория 1 до следващия работен ден след подаване на информация до посочените от Изпълнителя лица за контакт-чл. 12.(2)

2. За Категория 2, съгласно т. V. 14 от документа Технически изисквания е до 3 работни дни след подаване на информация до посочените от Изпълнителя лица за контакт-чл. 12.(2)

3. За Категория 3, съгласно т. V. 14 от документа Технически изисквания се договаря между страните, след подаване на информация до посочените от Изпълнителя лица за контакт-чл. 12.(2)

(10). Сроктът за тестване на нов лиценз е до 3 месеца след инсталация, като за този период не се дължи поддръжка.

(11) Сроктът за разработки на допълнителни функционалности, разработки, подобрения и други се договаря между страните за всеки един конкретен случай

(12). Сроктът на изпълнение на всяка „Заявка за доставка“ изпратена от Възложителя до Изпълнителя, започва да тече от датата на изпращане и се счита за потвърдена от Изпълнителя ако е изпратена на посочените по долу в чл. чл. 12.(2) факс или e-mail на Изпълнителя.

#### ПЛАЩАНЕ

Чл.6(1). Плащанията между страните се извършват при спазване на условията, уговорени в съответния раздел от Търговските условия.

(2). Плащанията от страна на Възложителя се извършват в срок до 45 календарни дни след изпълнение на условията за реализиране на плащане от съответния раздел на търговските условия.

(3). За доставка на хардуерни елементи на „Системата“ до 45 календарни дни след приемо-предавателен протокол и фактура.

(4). За поддръжка на „Системата“, на месечни вноски. Фактуририте се издават в месеца след месеца за изпълнение обхваща дейности извършени през предходния месец до 45 календарни дни от датата на фактурата.

(5). За допълнителни лицензи, разработка на нови функционалности на софтуера на „Системата“, както и предоставяне на свързани с това услуги за консултации, обучения и др. до 45 календарни дни след приемо-предавателен протокол и фактура.

(6). В случай че е дължим данък при източника: Приспадат се 10% от общото плащане, в случай, че се изисква от общата сума на услугата, или ако съответните документи, необходими за изключване на данъка не са представени най-късно до момента на изпращане на фактура.

(7). Плащанията по настоящия договор не могат да надхвърлят стойността на договора, определена в Чл. 2(1). от настоящия договор.

(8). В случай че се дължи данък при източника Изпълнителят трябва да изпрати фактурата най-късно един ден след издаването ѝ на факс + 359 32 278 503 или имейл до [rositza.yancheva@evn.bg](mailto:rositza.yancheva@evn.bg) и [todorka.dublekova@evn.bg](mailto:todorka.dublekova@evn.bg)

#### ПРАВА И ЗАДЪЛЖЕНИЯ НА СТРАНИТЕ

Чл.7(1). В допълнение на правата и задълженията, уговорени в настоящия договор, страните притежават правата и имат задълженията, посочени в Търговските условия.

#### ГАРАНЦИОНЕН И СЛЕД ГАРАНЦИОНЕН ПЕРИОД.

Чл.8(1). Страните се съгласяват, че по отношение на гаранционния период приложение намира съответния раздел от Търговските условия.

(2). Гаранционният период на хардуерните елементи на „Системата“ е 36+1+1 месеца, считано от датата на приемо-предавателния протокол.

(3). Гаранционният период на софтуера на „Системата“ е ##### месеца, считано от датата на приемо-предавателния протокол.

(4). За времето на гаранционните срокове на „Системата“ всичките разходи за поддържането и са за сметка на Изпълнителя.

(5). Поддръжката на софтуера на „Системата“ за гаранционния и след гаранционния период се извършва съгласно т.V. 14. от документа Технически изисквания.

#### ГАРАНЦИЯ ЗА ИЗПЪЛНЕНИЕ

Чл.9(1). Страните се съгласяват, че по отношение на гаранцията за изпълнение приложение намира съответния раздел от Търговските условия

(2). При подписване на договора Изпълнителят предоставя гаранция за изпълнение на договора в размер на 3,0 % от стойността на договора посочена в чл. 2.1.

(3). Срокът на валидност на предоставената гаранция за изпълнение е 84 месеца, считано от датата на подписване на договора. Срокът на гаранцията = срока на договора + гаранционния срок на „Системата“.

#### НЕИЗПЪЛНЕНИЕ И НЕУСТОЙКИ

Чл.10(1).В случай че някоя от страните не изпълни свое задължение съгласно договора, изправната страна има право на неустойка съгласно условията, предвидени в съответния раздел на Търговските условия.

(2).При неспазване на определените срокове за изпълнение на доставката, Изпълнителят дължи неустойка за забава в размер на 0,5 % от стойността на договора/заявката за доставка за всеки календарен ден от забавата, но не повече от 8,0 % от стойността на договора/заявката за доставка, без включен ДДС. ( Предвиди неустойка за всеки срок).

Само ако предмета го позволява

(3). При забавяне отстраняването на дефекти/проблеми от договорените срокове съгласно Чл. 5. (7) се начисляват следните неустойки:

За Категория 1, неустойка за забава в размер на 10% от месечна такса за поддръжка на ден, но не повече от 50% от месечна такса за поддръжка за всеки календарен ден забава.

За Категория 2, неустойка за забава в размер на 15% от месечна такса поддръжка но не повече от 60% за всеки календарен ден забава.

(4). В случай, че Изпълнителят предоставя услуги по договора посредством специалисти, които не притежават изискваните от Възложителя компетенции (съгласно задължителните изисквания към кандидатите за допускане), Изпълнителят дължи неустойка в размер на 0,5 % от стойността на договора за всеки случай, който Възложителя констатира.

#### ТЕХНИЧЕСКИ ИЗИСКВАНИЯ

Чл.11(1).Приложимите технически изисквания към доставката са посочени в документа Технически изисквания към системата за предварителен подбор № С-14-НМ-Д-123, с предмет „Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери", представляващ неразделна част от настоящия договор.

#### РАЗНИ

Чл.12(1). Адрес за кореспонденция и лица за контакт на ВЪЗЛОЖИТЕЛЯ: п.к: 4023 гр. Пловдив, ул.Христо Г.Данов № 37, отдел „Управление на измервателни данни“, лице за контакт: Атанас Попов, тел.:+359 (0) 700-1-7777 в. 34535, мобилен 0882834535, имейл: atanas.porov@evn.bg.

(2). Адрес за кореспонденция и лица за контакт на ИЗПЪЛНИТЕЛЯ: Адрес за кореспонденция: п.к: ##### гр. #####, ул. "##### " № #####. Лице за контакт #####, тел.:+359/#####факс:+359/#####, мобилен #####, имейл: #####.

(3). При промяна на данните, посочени по-горе, ИЗПЪЛНИТЕЛЯТ се задължава своевременно да информира ВЪЗЛОЖИТЕЛЯ в писмена форма. В случай че Възложителят не бъде уведомен за настъпилата промяна, всяко съобщение, изпратено до ИЗПЪЛНИТЕЛЯ на посочения по-горе адрес, се счита за надлежно изпратено.

(4). Дефиниции-термините, използвани в договора, имат значението, посочено в дефинициите на Търговските условия, освен ако контекстът налага друго значение.

(5).Всички спорове, възникнали във връзка с тълкуването и изпълнението на настоящия договор, ще бъдат решавани от страните в добронамерен тон чрез преговори, консултации и взаимноизгодни споразумения. Ако такива не бъдат постигнати, спорът ще бъде отнесен за разрешение от компетентния Районен, съответно Окръжен съд по седалището на ВЪЗЛОЖИТЕЛЯ.

(6).Настоящият договор се сключи в два еднообразни екземпляра, по един за всяка от страните.

#### ПРИЛОЖЕНИЯ

Чл.13(1). Всички приложения, посочени по-долу се включват в този договор по подразбиране и представляват неделима част от него.

(2). Страните се споразумяват за следния приоритет на документи, които имат обвързваща сила в отношенията им по настоящия договор, като при противоречие между разпоредби на отделните документи се прилага разпоредбата на документа от по-горен ред:

Настоящия договор

Протокол от договаряне от дата #####, Приложение ##### – Договорени единични цени

Технически изисквания (Издание ) към процедура на договаряне с обявление № С-14-НМ-Д-123 с предмет „Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"“

Търговски условия (Издание ) към процедура на договаряне с обявление № С-14-НМ-Д-123, с предмет „Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"“

Общи условия на закупуване на дружествата от групата EVN - Януари 2011;

Клауза за социална отговорност на дружествата от групата EVN - Януари 2011

Гаранция за добро изпълнение: тих #####, стойност #####, номер ##### дата #####, издадена от #####, валидна до #####.

Релевантни документи, доказващи (i) декларираните по процедурата обстоятелства, съгласно Чл. 47 ал.10 от ЗОП и (ii) задължителните изисквания към процедурата

Начална оферта с Вх.№ #####

Мерки за безопасност при работа на външни фирми на територията на Възложителя.

Критерии за изключване от система за предварителен подбор на изпълнители и условия за прекратяване на сключен договор - Май 2014

ВЪЗЛОЖИТЕЛ :

.....  
#####

.....  
#####

ИЗПЪЛНИТЕЛ :

.....  
#####

.....  
#####

Банкова гаранция за изпълнение-мостра

към система за предварителен подбор на изпълнители

№ С-14-НМ-Д-123, с предмет: "Доставка, инсталация, пускане в експлоатация, поддръжка, желани промени, обучения и разработки от Възложителя на "Система за дистанционно отчитане на електромери"

**Банкова гаранция за изпълнение – мострена бланка с одобрен от Възложителя текст.**

<БАНКА >

До <ЕВН България Електроразпределение ЕАД >

<Пловдив, ул."Христо Г.Данов"№37>

**БАНКОВА ГАРАНЦИЯ № XXXXXXXX ЗА ИЗПЪЛНЕНИЕ НА ДОГОВОР ЗА ОБЩЕСТВЕНА ПОРЪЧКА**

До нашето внимание беше сведено, че между нашия клиент XXXXXXXXXXXX и ЕВН България Електроразпределение ЕАД предстои да сключи договор N XXXXXXXX с предмет XXXXXXXXXXXX. В съответствие с точка XXX на Търговските Условия, които са неразделна част от горепосочения договор, Изпълнителят се задължава преди подписването на договора да представи безусловна и неотменяема банкова гаранция за изпълнение.

Предвид гореизложеното ние <БАНКА> се задължаваме безусловно и неотменяемо, независимо от валидността и действието на горепосочения договор, отказвайки се от правото на всякакви възражения, без проучване на съответните законови отношения да Ви заплатим всяка сума, чийто максимален размер не надвишава

..... лева (с думи ..... лева)

Заплащането на всяка сума по тази гаранция до максималния размер .....лева

(с думи ..... лева) се извършва в срок от 3 работни дни след получаване на искане в писмена форма за плащане от името на ЕВН България Електроразпределение ЕАД

по посочена от Вас банкова сметка.

Нашият ангажимент по настоящата банкова гаранция автоматично се намалява с размера на всяко плащане, извършено по нея.

Настоящата банкова гаранция е валидна до ..... и изтича изцяло и автоматично в случай, че до 17:00 часа на ....., искането Ви, предявено при горепосочените условия, не е постъпило в ..... След тази дата ангажиментът на банката се обезсилва и се счита за окончателно приключен, независимо дали оригиналът на банковата гаранция е върнат в банката или не.

За всички спорове, произтичащи от тази гаранция ще бъде приложимо българското законодателство

## **Общи условия на закупуване на дружествата от групата EVN**

Доколкото в договора не е посочено нещо друго, то валидни са следните общи условия на закупуване. Търговските условия или общите условия на Изпълнителя, освен в случай, че не са изрично одобрени от Възложителя, няма да се прилагат, дори и те да не са изрично отхвърлени от Възложителя.

1. Всички договори както и изменения и допълнения към тях се сключват само в писмена форма. Всички устни споразумения между страните са недопустими, освен ако не са писмено потвърдени от Възложителя
2. В случай, че договорът се базира на предварителен разчет на разходите (предварителна оферта), изготвено от Изпълнителя и предоставен на Възложителя, то Изпълнителят ще се придържа към него, освен ако в предварителния разчет на разходите изрично не е посочено, че подлежи на промяна и е необвързващ.
3. Посочените в договора цени са твърди цени, не подлежат на промени, като доставките се извършват франко мястото на изпълнение, стоките са опаковани, застраховани, разтоварени. Всички рискове преминават върху Възложителя едва след като стоката е доставена и приета от Възложителя. До този момент всички рискове са за сметка на Изпълнителя. За място на изпълнение се счита посоченият в договора адрес за доставка/изпълнение на услугата.
4. Приемането на дадена доставка/услуга се счита за извършено единствено в случай, че е потвърдено от Възложителя в писмена форма чрез подписване на двустранен приемо-предавателен протокол (ППП).
5. Изпълнителят се задължава да гарантира и отговаря за това, че неговият персонал и подизпълнителите, които той наема, ще спазват законовите разпоредби относно опазване живота и здравето на работниците както и опазването на околната среда. Работещите имат правото на достъп единствено до посочените им от Възложителя участъци. Разпорежданията на строителния и монтажния надзор на Възложителя са задължителни и трябва да бъдат спазвани. Изпълнителят изрично се задължава че ще спазва всички закони и подзаконови нормативни актове и ще упражнява контрол върху наетите от него или от неговите подизпълнители граждани на Република България и чуждестранни граждани съгласно съответното българско и европейско трудово законодателство. Преди започване на работата Изпълнителят трябва да докаже спазването на задълженията относно контрол чрез представянето на пълен комплект от съответните документи (разрешително за пребиваване, разрешително за работа, и др.) без изрична покана от страна на Възложителя, а също и да гарантира, че Възложителят и/или негови служби и сътрудници няма да носят отговорност за неспазване на тези задължения, както и породени от това щети и искове.
6. Изпълнителят се ангажира със задължението за всеобхватно координиране и сътрудничество с всички работещи на обекта. Изпълнителят се задължава да спазва всички нормативни актове регулиращи правата и задълженията на служителите, които включват, но не се ограничават само до Кодекс на труда, Закон за здравословни и безопасни условия на труд, Закон за устройство на територията, и по възможно най- добросъвестен начин да подкрепя дружествата от групата EVN като Възложители на строителните работи както и отговорните лица (координатори, ръководители-проект) при изпълнението на задълженията им. Целта е да бъде гарантирано реализирането на принципите за предотвратяване на опасности като се спазват всички указания на съответните служби за трудова медицина. Изпълнителят е длъжен да гарантира, че Възложителят и/или негови служби и сътрудници няма да носят отговорност за възникналите вследствие на неспазване на тези задължения щети и искове.
7. Изпълнителят гарантира за безупречното, съгласно договореностите, изпълнение на съответната доставка/услуга. Относно гаранция на стоката/услугата важат валидните закони разпоредби, освен в случай че в договора не е договорено нещо друго. Правото на претенция за гаранционен случай важи и за всички дефекти, настъпили в рамките на договорения гаранционен срок. Доказването на безупречното, съгласно договора, изпълнение е задължение на Изпълнителя. В случай, че във връзка с отстраняването на дефекти възникнат разходи по демонтаж и монтаж, както и други допълнителни разходи, то те са за сметка на Изпълнителя.
8. Изпълнителят отговаря за всички вреди в резултат на действията или бездействието на Изпълнителя, неговия персонал, неговите подизпълнители или други помощни единици, в процеса на или по повод на изпълнение на доставката/услугата, както и за вреди, които са предизвикани от използването от него материали или части от тези материали. Изпълнителят отговаря също за всички предадени му за монтаж или съхраняване от Възложителя или от други предприятия материали, строителни елементи или други предмети. При всички случаи Изпълнителят трябва да докаже, че той, неговият персонал, неговите подизпълнители или други помощни единици нямат вина. Това важи и за вреди възникнали вследствие на непредпазливост или неполагане на грижа на добър търговец. Изпълнителят се задължава, че всички искове или претенции от страна на работници или трети лица, касаещи вреди, възникнали във връзка с изпълнение на договора да бъдат отправяни към Изпълнителя и гарантира, че Възложителят няма да носи отговорност. Изпълнителят се задължава за своя сметка да сключи съответната застраховка обща гражданска отговорност, която да покрива всички произтичащи от законовите разпоредби и от договора рискове при поемане на отговорност. Застрахователната защита трябва да покрива и отговорността за щети към трети лица на всички подизпълнители и наети от изпълнителя лица при изпълнението на договора.



9. Фактурите трябва да се изпращат на посочения в договора/заявката за тази цел адрес в един оригинален екземпляр и със задължително вписан номер на договора и/или заявката. Фактурите трябва да отговарят на актуалните данъчни изисквания, като особено важно е задължителното посочване на идентификационен номер по ДДС, както на Възложителя, така и на Изпълнителя, а така също отделно изписване на стойността на ДДС. Фактури, които не отговарят на тези условия, не са основание за дължимо плащане и Възложителят си запазва правото да ги върне обратно до Изпълнителя за корекция. Сроктът на плащане започва да тече от постъпването на фактурите и на всички прилежащи към доставката/услугата документи при посочения в договора получател на стоката/услугата, при условие, че е налице регламентираното, съгласно договора, приемане на доставката/услугата посредством двустранно подписан ППП.

10. В случай, че изрично не е договорено нещо друго, то при частични доставки, или при частично изпълнение на услугите, е допустимо издаването на една обща фактура след цялостното изпълнение на договора. Плащанията се извършват не по-късно от посочения в договора/заявката срок. Плащания, които са извършени в рамките на този срок, се считат като навреме извършени, относно договорени отстъпки, и не предизвикват последици от забава заради неспазване на срока за плащане. При просрочване на плащането от страна на Възложителя се прилага законовата лихва за забава при плащането съгласно чл. 86 от ЗЗД. Освен законовата лихва за забава Възложителят не дължи заплащане на други обезщетения и неустойки, освен в случаи на доказано умишлено виновно поведение.

11. В случай на цесия, Изпълнителят е длъжен да уведоми писмено (не по факс или e-mail) Възложителя за сключени договори за цесия. В случай на цесия Възложителят има право да начисли и задържи такса за обработка и поддържане в размер на 1% от прехвърленото вземане.

12. Право на задържане в полза на Изпълнителя не се допуска освен ако не е изрично законово уредено. Възложителят има право да прихваща собствени вземания, както и вземания, които Изпълнителят дължи на предприятия от концерна на Възложителя, от вземания, които се дължат към Изпълнителя.

13. Изпълнителят се задължава да пази като поверителна цялата информация и предоставената му документация (образци, чертежи, скици, данни в електронен вид, изчисления и др. подобни), станала му известна във връзка с процедурата, да я съхранява по надлежен начин, да я използва единствено във връзка с изпълнението на договора и да не я прави достъпни за трети лица, дотогава докато тя не стане публично известна или достъпна. При приемане на доставката/услугата предоставените му от Възложителя документи следва да бъдат върнати обратно в оригинал без да се правят копия от тях. На Изпълнителя може да се разреши само след изрично писмено съгласие от страна на Възложителя да публикува данни, свързани с проекта, или да назове името на Възложителя като негов клиент. В случай на неспазване на горе посочените задължения изпълнителят се задължава да заплати глоба в размер на 25 000 лева. Възложителят има право при неспазване на тези задължения да претендира и други обезщетения за вреди.

14. Изпълнителят гарантира, че доставките/услугите отговарят на най-новите технически постижения. Изпълнителят носи отговорност за всички възникнали щети, най-вече, но не единствено, свързани с IT-системи и/или данни на Възложителя, когато те не са на разположение, не са опазени в тайна или са изгубили целостта си.

15. Изпълнителят отговаря и гарантира, че чрез доставката/услугата няма да се нарушат правата на трети лица върху обекти на интелектуалната или индустриалната собственост. Възложителят не носи отговорност при възникнали евентуални претенции на трети лица в тази връзка и всички искове ще бъдат насочени към Изпълнителя.

16. Изпълнителят категорично се съгласява, че при изпълнение на този договор ще спазва Закона за защита на личните данни и подзаконовите нормативни актове и че всички данни, станали му известни във връзка с този договор, при необходимост могат да се предоставят на трети лица (като проектантски фирми, собственици на съоръжения, застрахователи и др. но не и на конкуренти) само при спазване на тези изисквания. Изпълнителят носи отговорност за това, че както неговите работници така и всички онези, които предоставят услуги във връзка с изпълнението на договора, ще спазват разпоредбите на настоящите Общи условия на закупуване и законовите изисквания. Те трябва изрично да са информирани, че нарушаването на изискването за полагане на необходимата грижа и за пазене в тайна може да доведе до претенции за обезщетение както и подвеждане под административно-наказателна отговорност.

17. Възложителят, има право едностранно да прекрати договора без предизвестие в случай, че срещу Изпълнителя е открито производство по обявяване в несъстоятелност, или е обявен в несъстоятелност, както и когато върху имуществото му е наложен заповед или възбрана за погасяване на дълг. При оттеглянето си от договора Възложителят трябва да покрие разходите за извършените до момента доставки/услуги от Изпълнителя в случай, че Възложителят ще може да ги използва по предназначението им отбелязано в договора. В никакъв случай той не дължи като заплащане повече от това което е изпълнено.

18. Възложителят има право да прехвърли договорното отношение с всичките права и задължения на друго предприятие от концерн EVN. Изпълнителят няма право, освен в случай на предварително писмено съгласие от Възложителя, да прехвърля договора както цяло така и частично на трети лица и/или да ангажира подизпълнители.

19. Всички спорове възникнали във връзка с тълкуването и изпълнението на договора ще бъдат решавани от страните в добронамерен тон чрез преговори, консултации и взаимноизгодни споразумения. Ако такива не бъдат постигнати, спорът ще бъде отнесен за разрешение от компетентния Районен, съответно Окръжен съд по седалището на Възложителя. В сила е материалното право на страната по съдебна регистрация на Възложителя, като се изключва прилагането на Конвенцията на ООН за договорите за международни продажби на стоки и нормите на международното частно право. Езикът на договора е официалният език на страната по съдебна регистрация на Възложителя.

20. Ако някои разпоредби от тези Общи условия на закупуване са, или станат изцяло или отчасти недействителни или неосъществими, то това няма да засегне валидността на останалите разпоредби. На мястото на недействителните или неосъществими разпоредби страните се споразумяват за уреждане на взаимоотношенията по такъв начин, който е възможно най-близък до онова, което страните, са целели чрез станалата недействителна или неосъществима разпоредба от сключеното споразумение.

(Издание Януари 2011)

**Клауза за социална отговорност на дружествата от групата на EVN**

Изпълнителят декларира, че е запознат със съдържанието на по-долу посочените клаузи за социална отговорност, които са в сила също и за дружествата от групата EVN, и ще спазва същите при извършването на доставки/услуги. Възложителят е в правото си по всяко време да проверява спазването на това задължение. В случай на нарушение Възложителят има право да изиска предоговаряне с цел възстановяване на договорното състояние. Ако в рамките на един месец Изпълнителят не изпълни това изискване или ако установеният недостатък не бъде премахнат или отстранен в рамките на определения или двустранно между страните съгласуван срок, Възложителят е в правото си незабавно да прекрати договора. Същото важи и в случай, че Изпълнителят отказва или възпрепятства провеждането на такива проверки. Освен това Изпълнителят се задължава да обвърже с изпълнението на следните основни положения и принципи своите доставчици, както и подизпълнители.

1. Спазване на човешките права. От нашите Изпълнители и техните подизпълнители се очаква те да признават Всеобщата Харта за правата на човека на ООН, както и да гарантират, че те по никакъв начин не са замесени в нарушения на човешките права.
  2. Липса на детски и принудителен труд. Нашите Изпълнители и техните подизпълнители при производството на продуктите си и при извършване на услугите си се задължават да не използват или допускат детски, принудителен или друг недобровolen труд съгл. Конвенциите на Международната Организация на Труда (ILO).
  3. Липса на дискриминация или тормоз на работното място. Към всеки сътрудник следва да бъде подхождано с респект и достойнство. Нито един сътрудник не трябва да бъде физически, психически, сексуално или словесно тормозен, дискриминиран или да бъде злоупотребявано с него поради неговата полава принадлежност, раса, религия, възраст, произход, увреждане, сексуална или политическа ориентация, мироглед.
  4. Безопасни и здравословни условия на труд на работното място. Трябва да се гарантира, че нашите Изпълнители и техните подизпълнители гарантират на сътрудниците си безопасни и здравословни условия на труд, като спазват прилаганите за това закони и правилници. Трябва да се предостави свободен достъп до питейна вода, санитарни помещения, съответната пожарна защита, осветление, вентилация и ако е необходимо - подходящите лични предпазни средства. Сътрудниците се обучават да използват коректно личните предпазни средства и да познават общите разпоредби за сигурност.
  5. Трудово- и социално правни разпоредби. При изпълнение на поръчки нашите Изпълнители и техните подизпълнители са задължени да спазват валидните за съответната страна на изпълнение трудово- и социално правни разпоредби.
  6. Прозрачност на работното време и възнаграждението. Работното време трябва да бъде в съответствие с приложимите закони. Сътрудниците на нашите Изпълнители и техните подизпълнители трябва да имат трудови договори, в които да е фиксирано работното време и възнаграждението.
  7. Защита на околната среда. Ние очакваме от нашите Изпълнители и техните подизпълнители в рамките на тяхната предприемаческа дейност да спазват приложимите закони, подзаконовни нормативни актове и правилници за опазване на околната среда и при предоставяне на услуги/ доставки съответно да преценяват икономическите, екологичните и социалните аспекти и по този начин да вземат предвид принципите на устойчивото развитие.
  8. Намаляване на използването на ресурси, отделяне на отпадъци и емисии. Постоянното подобряване на ефективното използване на ресурсите е важна съставна част на управлението и фирменото ръководство. Нашите Изпълнители и техните подизпълнители трябва да минимизират отделянето на отпадъци от всякакъв вид, както и отделяне на всички емисии във въздуха, водата или почвата.
  9. Високи етични стандарти. Ние очакваме от нашите Изпълнители и техните подизпълнители да демонстрират високи стандарти на фирмена етика, да спазват съответните национални закони (особено трудовоправните и картелните разпоредби, както и разпоредбите за защита на конкуренцията и правата на потребителите) и по никакъв начин да не се въвлечат или да участват в корупционни схеми, лъжа или изнудване.
  10. Прозрачни бизнес отношения. Нашите Изпълнители и техните подизпълнители не трябва нито да предлагат нито да изискват, нито да гарантират, нито да приемат подаръци, плащания или други предимства от подобен род или облаги, които може да са предназначени да подтикнат дадено лице да наруши задълженията си.
  11. Право за провеждане на събрания и стачки. Работниците и служителите на нашите Изпълнители и техните подизпълнители трябва да имат възможност в рамките на законовите разпоредби на страната, в която те работят, да участват в събрания и стачки, без да се страхуват от последствия
- (Издание Януари 2011))

## **Мерки за безопасност при работа на външни фирми на територията на Възложителя**

С Мерките за безопасност се определят изискванията и задълженията, които страните приемат да изпълняват за осигуряване на здравословни и безопасни условия на труд на работниците, назначени от Изпълнителя, както и живота и здравето на други лица, които се намират в района на извършваната от тях дейност.

1. Изпълнителят е задължен да спазва изискванията на Закона за здравословни и безопасни условия на труд, Правилника за безопасност и здраве при работа в електрически и топлофикационни централи и по електрически мрежи, Правилник за безопасност при работа в неелектрически уредби на електрически и топлофикационни централи и по топлопреносни мрежи и хидротехнически съоръжения и други нормативни документи, регламентирани изисквания за безопасно изпълнение на дейността.
2. Преди допускане до работа Изпълнителя предоставя на Възложителя списък на лицата, които ще работят на обекта, в т.ч.: на лицата, имащи право да бъдат изпълнители и/или отговорни ръководители при работа по наряд; на лицата, имащи право да бъдат изпълнители и/или отговорни ръководители при работа по огневи наряд /ако е необходимо издаването на такъв/. В списъка да бъдат вписани притежаваните от тях квалификационни групи по безопасност на труда.
3. Преди допускане до работа Изпълнителя представя на Възложителя валидни удостоверения за притежавана квалификационна група по безопасност на труда на лицата, които ще работят на обекта.
4. Представител на Възложителя провежда начален инструктаж на лицата, които ще работят на обекта в съответствие с мястото и конкретните условия на работа. Инструктажа се документира в съответната Книга за инструктаж.
5. При голяма численост на бригадата началния инструктаж се провежда на отговорния ръководител /отговорник на бригадата/. Преминалият начален инструктаж отговорен ръководител /отговорник на бригадата/ провежда начален инструктаж на работниците от бригадата, документиран в съответния дневник.
6. Не се допускат до работа лица, които ще работят на обекта, които не притежават необходимите знания и умения и/или не са инструктирани по правилата за осигуряване на здравословни и безопасни условия на труд.
7. Лицата, които ще работят на обекта нямат право да преместват и отстраняват средствата за сигнализация и колективна защита /прегради, предупредителни табели, ограждения и др.под./, както и да разширяват работното място извън обозначения и сигнализиран район.
8. Изпълнителят носи пълна отговорност за безопасното изпълнение на работата от неговите работници, вкл. за осигуряване и ползване на подходящи безопасни инструменти, лични предпазни средства, облекла и др., както и за квалификацията, обучението и инструктажите на персонала си.
9. Ежедневно и след окончателното приключване на работата персонала на Изпълнителя, работещ на обекта, почиства работното място.
10. Машините и апаратите, които ще се използват, да са в добро техническо състояние, да са преминали съответно техническо обслужване и да са безопасни за използване.
11. Чрез контролиращ персонал, от страна на Възложителя, се осъществява периодичен контрол по спазване на правилата и изискванията за безопасност на труда. При констатиране на нарушения на правилата за безопасна работа от лицата, които ще работят на обекта, контролиращия персонал следва да уведоми ръководителя на обекта, за вземане на мерки за отстраняване на нарушенията, включително спиране на работата. Констатацията следва да бъде в писмен вид, чрез двустранно подписан констативен протокол.
12. Работата следва да се спре в случай или при вероятност от възникване на опасност за здравето и живота на работещите, до отстраняване на опасността.
13. В случай на трудова злополука, следва да се уведоми веднага Възложителя /група Охрана на труда, отдел Централни операции/, както и да окаже съдействие за изясняване на обстоятелствата и причините за злополуката.
14. Загубите, причинени от влошаване на качеството и/или удължаване сроковете на извършваните работи поради отстраняване на отделни лица или спиране работата на групи за допуснати нарушения на изискванията на Правилниците и инструкциите по безопасността на труда, са за сметка на Изпълнителя.

Настоящите мерки за безопасност са изготвени в изпълнение изискванията на чл.14, чл.16, т.8 и чл.18 от Закона за здравословни и безопасни условия на труд, чл.5 от Правилник за безопасност и здраве при

работа в електрически уредби на електрически и топлофикационни централи и по електрически мрежи, чл.5 от Правилник за безопасност при работа в неелектрически уредби на електрически и топлофикационни централи и по топлопреносни мрежи и хидротехнически съоръжения и за координиране на работата при извършване на дейности от външни фирми и организации за EVN България .

Кандидат:.....

Подпис с правна сила: .....

Дата ..... Гр. ....

С-14-НМ-Д-123