# Техническа спецификация, Издание: 1
# Technical Specification, Edition: 1

към процедура на договаряне с предварителна покана за участие/ to negotiated procedure with preliminary call
№ 242-ЕР-18-СІ-У-3
с предмет: Извършване на тестове за сигурност на електромери и концентратори на данни /with subject: Security testing of electrical meters and data concentrators

## I. Обща информация

В момента Електроразпределение Юг ЕАД има изградена Система за дистанционно отчитане на електромери, включваща над 850 000 средства за търговско измерване, разположени на цялата лицензионна територия на Дружеството.
Системата е базирана на комуникация по захранващите линии (PLC), което позволява монтаж на крайните и комуникационните устройства без допълнително опроводяване. Използват се S-FSK и Prime модулация на сигналите.
Главен приоритет за Дружеството е сигурността на данните и комуникационните канали. Работи се по подобряване на сигурността, както при внедряване на нови, така и по вече внедрените електромери и комуникационно оборудване към Системата.
За тази е необходимо бъдат извършени съответните тестове за определяне сигурността на горепосоченото оборудване.

## I. Background information

At the moment Elektrorazpredelenie Yug EAD has a developed remote metering system of electric meters, comprising of over 850,000 commercial metering devices, located throughout the license territory of the company.
The system is based on power-line communication (PLC), which allows installation of the end and communication devices without additional wiring. S-FSK and Prime modulation of signals is used.
The main priority for the company is the security of data and communication channels. There are constant activities on security improvement both in the deployment of new and of already deployed electric meters and communication equipment of the System.
This is why it is necessary for the equipment referred above to be carried out the relevant tests for determining the security it meets.

## II. Извършвани тестове и анализ

Преди провеждането на всеки тест, Изпълнителят следва да предостави на Възложителя подробен план за одобрение, който включва минимум следната информация:

- Тестовите сценарии с описание на тестовете които се извършват
- Изисквания за провеждане на теста – необходими мостри на оборудване и апаратура сервизен софтуер, ключове и пароли
- Етапи на провеждане на теста и времеви периоди – възможност при желание на възложителя за предоставяне на предварителни резултати в зависимост от етапа на тестовете
- Адрес за кореспонденция
- Лица за контакт

## II. Performed tests and analysis

Before each test the CONTRACTOR should submit to the CONTRACTING AUTHORITY a detailed plan for approval, which includes at least the following information:

- The test scenarios with a description of the tests which are carried out
- Requirements for the test - needed samples of equipment and apparatus, service software, keys and passwords
- Test stages and time periods - option for provision of preliminary results at the request of the CONTRACTING AUTHORITY depending on the stage of the tests
- Correspondence address
- Contact persons

При възникнала необходимост, Възложителят ще предостави оборудване, върху което трябва да бъдат направени тестове, както следва:

- Опити за претоварване със съобщения по комуникационните канали
- Опити за задръстване на комуникационните канали тип DoS (отказ на услугата) атака
- Сензори за следене на състоянието на електромера при провеждането на теста. Да се ползва интерфейс различен от подложения на тест.
- "Replay attack" атака с повторения на прихванати комуникационни пакети.
- Физическо проникване в устройството
- Тестове дали електромера е устойчив при смущения или липса на захранване
- Тестове върху криптирането и удостоверяването на комуникацията
- Тестове върху удостоверяването на източника на комуникация
- Тестове върху функциите на контрола на достъпа
- Тестове за установяване и одитиране на компрометирани съоръжения

As necessary, the CONTRACTING AUTHORITY will provide equipment on which the following tests should be performed:

- Attempts to overload with messages the communication channels
- Attempts to be blocked the communication channels of type DoS (denial of service) attack
- Sensors for monitoring the condition of the electric meter during the test. To be used interface different from the tested one.
- "Replay attack" - attack with repetitions of caught communications packages.
- Physical penetration into the device
- Tests whether the electric meter is resistant to disturbances or lack of power supply
- Tests on the encryption and authentication of communication
- Tests on the authentication of the source of communication
- Tests on the functions of access control
- Tests for finding and auditing compromised facilities

След провеждане на тестовете, Изпълнителят следва да изготви и предостави оценка и анализ на рисковете, като:

- Даде оценка на рисковете, породени от установените уязвимости;
- Даде оценка относно възможността установените рискове да бъдат приложени от недоброномерени лица
- Да даде оценка относно нивото на знания и компетенции, което е необходимо за изпълнението на откритите рискове
- Да обобщи и раздели рисковете по видове и критичност

After carrying out the tests, the CONTRACTOR should draw up and provide a risk assessment and analysis by:

- providing assessment of the risks driven by the established vulnerabilities;
- Making assessment on the possibility the identified risks to be applied by malicious persons
- To give an assessment on the level of knowledge and competences which is necessary for the implementation of the risks found
- To summarise and divide the risks by types and criticality

**III. Оборудване**

Тестовата установка трябва да е изработена така, че да позволява повтарящи се тестове при устойчива конфигурация, което да даде възможност за регресивни тестове на предоставените устройства.

**III. Equipment**

The setups for testing must be constructed so as to allow repetitive tests at sustainable configuration, to enable regression tests of the devices provided.

Тестовата система да разполага с предефинирани тестове, които да позволяват бързо и систематично сканиране за конкретен спектър от уязвимости по структуриран начин. Да бъде възможно извършването на функционални тестове, тестове за нерегламентирано проникване, тестове за стабилност и устойчива работа. Резултатите от всички тестове трябва да бъдат лесно интерпретирани. Всички тестове трябва да са подробно документирани стъпка по стъпка, което да позволи лесното им повтаряне и детайлно разглеждане.

The test system should have predefined tests to enable quick and systematic scanning for a specific range of vulnerabilities in structured way. To be possible to carry out functional tests, tests for unauthorised penetration, tests for stability and sustainable operation. The results of all tests must be easily interpreted. All tests must be documented in details step by step, to allow for their easy repetition and detailed review.