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

към процедура на договаряне с предварителна покана за участие/ to negotiated procedure with preliminary call
№ 88-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

Критерии за допускане

1. Кандидатът трябва да е извършил услуги с предмет и обем идентични или сходни* с този на поръчката, най-много за последните три години от датата на подаване на заявлението.

*Под сходен предмет и обем да се разбира предоставяне на услуга за извършване на тестове за сигурност на измервателни уреди и апаратура, ползвани в страни от Европейският съюз – извършени не по-малко от 3 теста на сигурността в системи тип „Smart Grid" и/или „Smart Metering" за последните 3 години.

Представя се списък на услугите, които са идентични или сходни с предмета на поръчката, с посочване на стойностите, датите и получателите, заедно с доказателства за извършените доставки. В описанието на доставките в списъка кандидатът посочва и количествата на доставките.

- при подаването на заявление се попълва Част IV, Раздел В: Технически и професионални способности, т.1б) от ЕЕДОП;

- при условията на чл. 67, ал. 5 и ал. 6 от ЗОП се представя посочения списък, придружен от доказателства за извършените доставки.

2. Кандидатът трябва да разполага с база (лаборатория) със следното минимално техническо оборудване:

* тестови установки за „Smart Grid" и/или „Smart Metering" устройства с G3-PLC, Prime-PLC, SFSK типове комуникация и

* оборудване, което да дава възможност за 3G/GPRS тестове, тестове end-to-end (от край до край), включващи цялата комуникационна верига от електромера, PLC, 3G/GPRS мрежата до системата за управление, с възможни не само тестови атаки върху електромерите, а върху цялата комуникационна и системна верига.

Criteria for admission

1. The applicant must have rendered services with subject and volume identical or similar* with the one of the contract, for the last three years after the date of submission of the application at the most.

*As similar subject and volume is meant provision of a service for testing the security of metering devices and equipment used in EU countries – performed not less than 3 security tests in systems of type „Smart Grid" and/or „Smart Metering" for the past 3 years.

To be provided a list with the services which are identical or similar with the subject of the contract, by stating the values, the dates and the recipients, together with evidences for the performed deliveries. In the description of the deliveries in the list the applicant specifies the volume of the deliveries.

- upon submission of an application is to be completed Part IV, Section C: Technical and professional abilities, item 1b) of the European Single Procurement Document;

- under the terms and procedures of art. 67, para. 5 and para. 6 of the PPA is to be provided the stated list with attached evidences for the deliveries made.

2. The applicant must have a base (laboratory) with the following minimum technical equipment:

*test installations for „Smart Grid" and/or „Smart Metering" devices with G3-PLC, Prime-PLC, SFSK communication types and

*equipment which enables 3G/GPRS tests, end-to-end tests including the whole communication chain from the electric meter, PLC, 3G/GPRS network to the management system, with possible not only test attacks on the electric meters, but on the overall communication and system chain.

Equipment should be designed and able to work with protocols DLMS, GPRS, G3-PLC, PRIME-PLC, M-Bus, HLDC, SFSK, with

Оборудването да е създадено и способно да работи с протоколи DLMS, GPRS, G3-PLC, PRIME-PLC, M-Bus, HLDC, SFSK, с възможност за изследване на допълнителни протоколи по необходимост.

Документ, с който се доказва съответствието с критерия за подбор:

- при подаване на заявление се попълва Част IV, Раздел В: Технически и професионални способности, т.9) от ЕЕДОП;

- при условията на чл. 67, ал. 5 и 6 от ЗОП се представя декларация, подписана от лицето/ата, което/ито представялва участника за инструментите, съоръженията и техническото оборудване в сервизната база (с посочване на точния й адрес), които ще бъдат използвани за изпълнение на поръчката.

possibility to be examined additional protocols, as necessary.

Document which proves the compliance with the selection criteria:

- upon submission of an application is to be completed Part IV, Section C: Technical and professional abilities, item 9) of the European Single Procurement Document;

- under the terms and procedures of art. 67, para. 5 and para. 6 of the PPA is to be provided a declaration signed by the person/s the bidder represents about the tools, the installations and the technical equipment in the service base (by specifying the address) which will be used for the implementation of the contract

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

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

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

- 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 недобронамерени лица
- Да даде оценка относно нивото на знания и компетенции, което е необходимо за изпълнението на

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

откритите рискове
- Да обобщи и раздели рисковете по видове и критичност

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.

Тестовата система да разполага със 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.

risks found
- To summarise and divide the risks by types and criticality

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.

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.