Technical specification

To Improving the security of existing Automatic meter reading (AMR) System - meters and data concentrators, version 7

1. Description:

In EVN Bulgaria Elektrorazpredelenie EAD operated AMR System, produced by ADD Group - Moldova and delivered by ADD Bulgaria. The system includes meters and data concentrators, version 7.
Employer requirements is associated with improving software security of the components of the system - meters and data concentrators to minimize the possibility of abuse by third parties.

It is necessary to ensure the security of power supply to consumers, the proper functioning of these devices, sending and reception of data and commands and limiting any possibility of change (manipulation) of data and commands.

These requirements are based on the conducted in April 2016 security test of components of the AMR System from the European Network for Cyber security (ENCS), described in the test report from 18.04.2016. It is necessary to be taken into consideration findings and recommendations of this report to cover the security requirements.

2. Requirements to improve system security

2.1 System and Device Security Concept

The vendor should provide a system and Device security concept. The security concept should cover design, architecture and policies for the systems and devices provided. The vendor should furthermore provide a concept how the code quality of the meter and data concentrator firmware should be increased.

2.2 DLMS protocol implementation

To fix of vulnerabilities in DLMS protocol should take measures to improve the code quality and the robustness of the meter firmware and data-concentrator application. This should include taking measures to improve the development process, and introducing guidelines for secure coding.
Furthermore, security tests should be part of the development and testing process.

2.3 Entity and Message Authentication

All data send from the meters or the data concentrator should be authenticated. For Message protection in DLMS at least the mode “authenticated only” should be used, for sensitive information (e.g. meter readouts, switching commands,…) “authenticated encryption” should be used. The mode “encrypted only” should not be used in any

Техническа спецификация

За подобряване на сигурността на съществуващата Система за дистанционно отчитане (СДО) – електромери и концентратори за данни, версия 7

1. Описание:

В ЕВН България Електроразпределение ЕАД се експлоатира Система за дистанционно отчитане, произведена от АДД Груп – Молдова и доставена от АДД България. Системата включва електромери и концентратори за данни, версия 7.
Изискванията на Възложителя са свързани с подобряване сигурността на софтуерното осигуряване на компонентите на Системата – електромери и концентратори за данни, с оглед минимизиране на възможността за посегателства от страна на трети лица.
Необходимо е да се гарантира сигурността на захранването на потребителите, нормалното функциониране на всички устройства, предаването и приемането на данните и командите, като се ограничи всяка възможност за промяна (манипулиране) на данните и командите.

Настоящите изисквания са базирани на проведения през м.април 2016г. тест за сигурност на компонентите на Системата за дистанционно отчитане от European Network for Cyber security (ENCS), описани в тестов доклад от 18.04.2016г.
Необходимо е констатациите и препоръките от този доклад да бъдат взети предвид, за да бъдат покрити изискванията за сигурност.

2. Изисквания за подобряване на сигурността на на системата

2.1 Концепция за сигурност на Системата и електромерите

Доставчика трябва да осигури концепция за сигурност на Системата, комуникационните и крайните устройства. Концепцията за сигурност следва да обхваща проектирането, архитектурата и политиките, които са предвидени за Системата и устройствата. Освен това доставчика трябва да предостави концепция как ще бъде подобрено качеството на кода на фърмуера на електромера и концентратора.

2.2 Имплементация на DLMS

За да се отстранят уязвимости в DLMS протокола, трябва да се вземат мерки за подобряване на качеството на кода и надеждността във фърмуера (FW) на електромерите и приложението в концентратора за данни. Това трябва да включва мерки за подобряване в процеса на разработка и въвеждане на кодиране за сигурност.

2.3 Автентикация на заявки и пакети данни

Всички данни, изпратени от електромерите или от концентратора трябва да бъдат автентифицирани . За защита на пакетите в DLMS трябва да се използва най-малко режим " authenticated only ", за чувствителна информация (например регистърни данни, команди за превключване, …) трябва да се използват " authenticated encryption ". Режимът

case.
For mutual authentication of the DLMS Client and the DLMS Server authentication High Level Security (HLS) mechanism 5 (GMAC) should be used, or the system needs to rely on pre-established sessions

2.4 Updating of firmware

Meter firmware updates must be digitally signed by the producer. The meter must check the digital signature of the firmware image and must reject non-genuine or manipulated versions of the firmware.
Data Concentrator firmware updates must be digitally signed by the producer. The Data Concentrator must check the digital signature of the firmware image and must reject non-genuine or manipulated versions of the firmware.

3. Specific requirements to improve security of the Data concentrator (DC)

3.1 DC Web Interface

Fix the input sanitization function used for filtering the user-supplied input, also considering the special case when not url-encoded single quote characters are sent to the ADDAX Administration Web Interface of the data concentrator. Webserver design and configuration shall follow the OWASP guidelines.
Sensible information transmitted as part of HTML code or stored inside log files must be encrypted using state of the art cryptography (ENISA's Algorithms, Key Sizes and Parameters Report provides details on the state of the art in cryptography) and shall neither employ proprietary cryptographic functions nor modify the cryptographic primitives.
The system should not have any hidden or guest accounts. It should be possible to define a password policy with complexity criteria the used passwords has to fulfil.
Require a password to be used for the “sudo” command.
Allow from the web server serving the ADDAX Administrator Web Interface only the known file extensions, block all the others.

3.2 Authentication for Web Services

Access to all network resources and processes must be protected, like the Web Services, through the implementation of appropriate authentication and authorization mechanisms. It is recommended to use TLS for the web services, and to use r client side certificates.

3.3 Keys encryption

Each file containing clear-text passwords or other sensible data (for example, smart meter encryption keys) in filesystem must be encrypted using state of the art cryptography (see 3.1).
All critical resources in the filesystem by assigning strict access permission must be protected. To protect credentials in case of physical access to the data-concentrator, must use one of two options:

- First option - To use a secure element, a chip with strong physical security measures, to store the credentials. This option requires a redesign of the hardware and the change of actual rolled out DCs.

"криптирани само" не трябва да се използва при всички случаи.
За взаимно удостоверяване на DLMS Клиента и удостоверяване на DLMS Сървър трябва да се използва High Level Security (HLS) механизъм 5 (GMAC), или системата трябва да разчита на предварително определени сесии.

2.4 Обновяване на фърмуер

Всеки нов фърмуер на електромера трябва да бъде цифрово подписан от производителя. Електромера трябва да проверява цифровия подпис на фърмуерния имидж и да отхвърля неоригинални или манипулирани версии на фърмуера.
Фърмуерните ъпдейти на концентратора трябва да бъдат цифрово подписани от производителя. Концентратора трябва да проверява цифровия подпис на фърмуерния имидж и да отхвърля неоригинални или манипулирани версии на фърмуера.

3. Специфични изисквания за подобряване за сигурността на концентраторите за данни (DC).

3.1. Web интерфейс

Да се настрои функцията input sanitization за филтриране на потребителския вход, като се има предвид специфични случаи, когато не URL-кодирани единични кавички се изпращат на ADDAX Administration Web интерфейса на концентратора. Дизайна на Web сървъра и конфигурацията трябва да следват указанията на OWASP
Чувствителната информация, която се изпраща като част от HTML кода или се записва в лог файловете трябва да бъде криптирана, съгласно криптографската техника (алгоритми на ENISA, Key Sizes and Parameters Report предоставят информация относно криптографската техника) и не трябва да се използват непатентовани собствени криптографски функции, нито да се променят на криптографски основи..
Системата не трябва да има скрити guest акаунти . Трябва да бъде възможно да се определи политиката за пароли с критерии за сложност на използваните пароли.Необходимо е да има парола за използване на “sudo” команди.
От Web сървъра, обслужващ ADDAX Administrator Web интерфейса да бъдат разрешени само познати файлови разширения. Трябва да се блокират всички останали.

3.2. Автентикация за Web услуги

Достъпа до всички мрежови ресурси и процеси, като Web услугите, трябва да бъде защитен, чрез прилагане на подходящи механизми за автентикация и оторизация.
Препоръчително е да се използва TLS за Web услугите, и да се използват сертификати.

3.3. Кодиране на ключовете

Всички файлове във файловата система, съдържащи пароли или други чувствителни данни (напр. ключове за криптиране на електромерите), трябва да бъдат криптирани, като се използва техниката на криптиране (виж.3.1).
Всички критични ресурси във файловата система, определени като такива със стриктни права за достъп, трябва да бъдат защитени. За да бъдат защитени пълномощията в случай на физически достъп до концентратора, трябва да се използва една от двете възможности:

- Да се използва хардуерен елемент за сигурност, като чип със силни физически мерки за сигурност, в който

- Second option - To use the data-concentrator as a gateway that only routes encrypted and authenticated DLMS messages between the head-end and meter, so that you have end-to-end security. In this way no important credentials or privacy sensitive data is stored on the data-concentrator.

3.4 Encryption on the WAN Interface

To use only network services providing encryption capabilities. Instead of telnet use SSH, instead of HTTP use HTTPS, and instead of FTP use SFTP or FTPS.
To use a VPN between the data-concentrator and the data-center hosting the head-end server using strong encryption algorithmssuch as mentioned in 3.1

3.5 WAN network services and firewall

All unused network services must be disabled. It is necessary to harden configuration of the remaining network services.
Minimize the attack surface area of the data concentrator by binding network services only to the required interfaces and avoiding to use the wildcard address “0.0.0.0”.
To set restrictive firewall configuration for the data concentrator setting the default policy to DROP instead of ACCEPT.

4. HHU

In case we have unfulfilled request (remote connection/disconnection) in HES, operator send this request to terminal. When terminal received the request (using GPRS communications) on the terminal screen is displayed a message that there is a new request and type of request (connection, disconnection, reading). When is sending a request should be sent and cryptographic key for meter. It is absolutely necessary to secure the key export functionality so it shall not be possible to use this functionality for an unauthorized key export. Activating request on the field is with button “Execute” – in this moment terminal execute command, after that delete request and cryptographic key for this meter and send status in HES.

Terminal requirements:

4.1 To be equipped with an optical head for interfacing the maintenance of meters
4.2 To maintain a secure connection with the central system via GPRS communications.
4.3 To be able to set the communication module in terminal (GPRS, DNS).
4.4 Terminal to be register in Central System - registration must be confirmed by the operator.
4.5 Requests send to terminal must be made manually by the operator of the central system and should be able to be canceled (deleted) the operator.
4.6 Cryptographic key to be removed (deleted) from the terminal, immediately after executing command.

да бъдат записани удостоверенията. Тази опция изисква редизайн на хардуера и подмяната на концентраторите
- Да се използва концентратора като гейтуей, който само да маршрутизира криптираните и автентикирани пакети между Централната система и електромерите, при което ще се реализира end-to-end сигурност. По този начин важни удостоверения и чувствителни данни няма да се записват в концентратора.

3.4. Криптиране на WAN интерфейса

Да се използват само такива мрежови услуги, които предлагат възможности за криптиране. Да се използва SSH вместо Telnet, HTTPS вместо HTTP и SFTP или FTPS вместо FTP.
Да се използва VPN между концентратора и Центъра за управление, използвайки силни алгоритми за криптиране, като посочените в т.3.1

3.5 WAN мрежови услуги и защитна стена

Всички неизползвани мрежови услуги трябва да бъдат забранени. Необходимо е да се подобри конфигурацията на останалите мрежови услуги. Да се минимизира областта на атака на концентратора на данни чрез свързване на мрежови услуги само до необходимите интерфейси и да се избягва да се използва адресна маска "0.0.0.0".
Да се установи рестриктивна конфигурация на защитната стена на концентратора с политика по подразбиране „Drop“ вместо „Accept“

4. Преносим терминал

В случай, че има неизпълнена заявка (дистанционно включване/изключване) в Централната система тя се подава от оператор към терминал за изпълнение. При постъпване на заявката в терминала(чрез използване на GPRS комуникация) на екрана на терминала се визуализира съобщение ,че има нова заявка и вида на заявката (включване, изключване, отчитане) .При изпращането на заявката трябва да бъде изпратен и криптографския ключ на електромера. Абсолютно необходимо е да се защити функционалността за експорт на ключове, така, че да не бъде възможно да се използва тази функция за неоторизиран експорт на ключове. Активиране на заявката при посещение на място е посредством бутон „изпълни“ - в този момент терминала изпълнява на командата, след което изтрива заявката и криптографския ключ и връща съобщение в централната система

Изисквания към терминала:

4.1 Да е оборудван с оптична глава, за работа с интерфейса за поддръжка на електромерите
4.2 Да поддържа защитена връзка с Централната система посредством GPRS комуникация.
4.3 Да има възможност за настройване на комуникационния модул на терминала (GPRS, DNS)
4.4 Терминала да се регистрира в централната система – регистрацията му трябва да бъде потвърдена от оператор.
4.5 Заявките към терминала трябва да се подават ръчно от оператора на Централната система и трябва да могат да бъдат отменяни (изтривани) от оператора
4.6 Криптографския ключ да се изтрива от терминала веднага след изпълнение на заявката

4.7 The request must be active in the terminal specified time (e.g..4 hours), then deleted. The active time for every one request should be able to be defined in the central system

4.8 When terminal is start (restart) – automatically have to load the application for work with meter and not be able to access other applications

4.9 HES must have functionality to define groups of terminals, to allow requests to be send to specific terminals.

4.10 To have safety class IP65

4.11 Communication between meter and terminal must be encrypted

4.12 To be shockproof

4.7 Заявката да е активна в терминала определено време (напр.4 часа), след това да се изтрива. Времето за което една заявка е активна трябва да може да бъде дефинирано в централната система

4.8 При стартиране (рестартиране) на терминала автоматично да се зарежда приложението за работа с електромери и да няма възможност достъп до други функции на терминала

4.9 В централната система трябва да има функционалност да се дефинират групи терминали за да може заявките да се насочват към точно определени терминали.

4.10 Да в с клас на защита IP65

4.11.Комуникацията между електромера и терминала да е криптирана.

4.12 Да е удароустойчив

5. Mitigation plan for findings

The vendor has to provide a mitigation plan for each of the findings documented in the Test Report. The mitigation plan should clearly figure out, how and when the vulnerabilities documented in the Test Report will be fixed.

5. План за отстраняване на констатациите

Доставчика трябва да представи план за отстраняване на последиците за всяка една от констатациите документирани в Тестовия протокол. В плана следва ясно да се посочва, как и кога ще бъдат отстранени уязвимостите документирани в тестовия доклад.

Възложител:

.....	.....
Костадин Величков	Роналд Брехелмахер
Kostadin Velichkov	Ronald Brechelmacher

EVN BULGARIA ELEKTRORAZPREDELENIE
ATTN: ANTON GRAMATIKOV
STOYCHO VALCHEV
BELOSLAV STOEV
EVN BULGARIA ELEKTRORAZPREDELENIE

EVN БЪЛГАРИЯ ЕЛЕКТРОРАЗПРЕДЕЛЕНИЕ
НА ВНИМАНИЕТО НА: АНТОН ГРАМАТИКОВ
СТОЙЧО ВЪЛЧЕВ
БЕЛОСЛАВ СТОЕВ
EVN БЪЛГАРИЯ ЕЛЕКТРОРАЗПРЕДЕЛЕНИЕ

PROJECT DESIGN AND IMPLEMENTATION PLAN / СТРУКТУРА НА ПРОЕКТА И ПЛАН ЗА ВНЕДРЯВАНЕ

No:	TASK DESCRIPTION / ОПИСАНИЕ НА ЗАДАЧИТЕ	DELIVERY TIME / ВРЕМЕ ЗА ДОСТАВКА	COMMENTS / КОМЕНТАРИ	RESPONSIBILITY / ОТГОВОРНОСТ
Task 1 Задача 1	DC firmware update from v.7.4.xx up to v.7.6.xx (staying on the same hardware). After completion of Task 1 two goals are achieved: Обновяване на софтуера на концентратора на данни от версия 7.4.xx на версия 7.6.xx (на съществуващия хардуер). След приключване на Задача 1 се постигат две цели : 1. DC firmware v.7.6 is compatible to both SIMS v.6 and SIMS v.8. Софтуера на концентратора на данни версия 7.6 е съвместим със SIMS версия 6 и SIMS версия 8. 2. Set of security vulnerabilities (found in ENCS tests) are removed in v.7.6: Уязвимостите в системата за сигурност (открити в ENCS тестовете) са отстранени във версия 7.6: a. Remove all clear-text credentials exposed via HTML code or on filesystem. Премахване на всички текстови идентификационни данни представени чрез HTML код или на файлова система. b. Remove all unused or not secure network services (FTP, echo, telnet). Премахване на всички неизползвани и несигурни услуги (FTP, echo, telnet). c. Review default firewall and IP-filtering settings. Преглед на фабричните настройки на антивирусните програми и настройките на IP			ADD designs, tests and delivers updated firmware version. АДД проектира, тества и доставя обновена софтуерна версия. Field implementation is out of ADD responsibility scope. Внедряване на полето не е отговорност на АДД.

	адресите за филтриране. d. Review all users access rights to filesystem, tools, etc. Преглед на правата за достъп на всички ползватели до файловата система, инструменти и др. e. Limit admin privileges by using a dedicated application shell. Ограничаване на привилегиите на администратора чрез използване на определен приложен шел. f. Improve WEB server stability to code insertion. Подобряване на стабилността на уеб сървъра за вмъкване на код. g. Use SSH with stronger MAC algorithms. Използване SSH с по-устойчиви MAC алгоритми. h. Configure by default all users with strong passwords. Фабрични настройки с по-сложни пароли на всички ползватели.			
Task 2 Задача 2	SIMS v.6, v.8: implementation of special features for field clean-up and DC hardware v.7 to v.8 migration. Подготовка за миграция от SIMS версия 6 към версия 8: внедряване на специални настройки оптимизиране на работата на полето и подготовка за миграция на концентраторите на данни от версия 7 на версия 8. Before starting special features implementation the following things must be identified: Преди започване на внедряването на специални настройки, следните неща трябва да бъдат идентифицирани: 1. The whole set of meter firmware versions running in the field. Да се уточнят всички софтуерни версии на електромерите, които са инсталирани на полето. 2. Evaluate whether actual PLC performance in all trafostations is sufficient for activating security in future. Оценка дали актуалната PLC комуникация на всички трансформаторни станции е подходяща за активиране на сигурността за в бъдеще. 3. Determine proper S-FSK settings in DC and meters to be make PLC performance sufficient. Определяне на подходящите S-FSK настройки в концентраторите на			ADD is responsible for preparation of recommendation and provision of special software tools for network evaluation. АДД е отговорен за подготовка на препоръка и предоставяне на специален софтуер за оценка на мрежата. The evaluation and clean-up activity is out of ADD responsibility scope Оценката и подготовката за миграцията е извън отговорността на АДД.

	данни и електромерите, за да се оптимизира работата на PLC комуникацията.			
Task 3 Задача 3	Implementation and testing of stable and secure meter firmware v.7.6. This firmware version will implement the following features: Внедряване и тестване на стабилна и сигурна софтуерна версия 7.6 на електромерите. Тази софтуерна версия ще внедри следните функции: ● Basic functionality remains the same as in v.7.2. Основната функционалност остава същата като версия 7.2. ● HLS to be added. Система за сигурност на високо ниво ще бъде добавена. ● DLMS robustness issues (found in the ENCS tests) to be closed or at least mitigated. Въпросът с устойчивостта на DLMS (отбелязан в тестовете на ENCS) ще бъде решен или най-малкото смекчен. ● Meter will accept only firmware image authenticated by manufacturer (GMAC). Електромерите ще приемат само софтуер удостоверен от производителя /GMAC/.		This firmware must be tested in testing environment, in a field pilot before starting massive update. Този софтуер трябва да бъде тестван в тестови условия, в пилотен проект на поле преди масовото обновяване.	ADD is responsible for delivery of meter firmware with functionality mentioned in Task 3 description. АДД е отговорен за доставката на софтуера на електромерите с функционалност описана в Задача 3. Performance of tests shall be responsibility of EVN Bulgaria Отговорността за тестовете ще е на ЕВН България.
Task 4	Pre-update field clean-up. Completion of Task 2 makes it sure that vast majority of meters will have high availability in PLC to achieve high performance in firmware upgrade and data collection with activated security. Подготовка преди обновяване. Приключването на Задача 2 ще гарантира, че повечето от електромерите ще имат висока достъпност в PLC, за да бъде успешно извършена софтуерната актуализация и събираемост на данни с активирана сигурност. Proper S-FSK settings determined in Task 2 will be applied during implementation phase of the Task 4. Подходящите настройки на S-FSK определени в Задача 2 ще бъдат приложени по време на изпълнението на Задача 4.		Prerequisites: Tasks 1 and 2 completed have to be completed. Условия: Необходимо условие: Изпълнението на задачи 1 и 2 да е приключило.	ADD shall be responsible to provide recommendations for Task 4 implementation. АДД е отговорен да предостави предложения за изпълнението на Задача 4. The implementation of Task 4 is out of ADD responsibility scope. Изпълнението на Задача 4 е извън отговорностите на АДД.

Task 5 Задача 5	SIMS v.6 to SIMS v.8 migration. SIMS v.8 will be installed from scratch in a separate environment (e.g., virtual PC) without removing the older version with step-by step transferring DC's and meters from v.6 to v.8. Only DC v.8 (see task 7 below) to be operated in new environment. Миграция от SIMS версия 6 на версия 8. SIMS версия 8 ще бъде инсталиран от нулата в отделна среда (напр., виртуален компютър) без да се премахва по-старата версия с поетапно прехвърляне на концентратори на данни и електромери от SIMS версия 6 към версия 8. Само концентратори на данни версия 8 /виж задача 7 по-долу/ могат да оперират в новата среда.			ADD shall be responsible for delivery of SIMS v.8. АДД е отговорен за доставката на SIMS версия 8. EVN Bulgaria shall be responsible for installation. ЕВН България е отговорен за инсталацията.
Task 6 Задача 6	HHU software implementation and HHU/HES integration (to make it possible to communicate with meters with activated security). HHU/HES integration details are to be agreed with EVN. Внедряване на софтуер за HHU и интеграцията му в софтуера в центъра(HES) /за да може да комуникира с електромери с активирана сигурност/. Подробностите относно интеграцията на HHU и софтуера в центъра(HES) трябва да бъдат съгласувани с ЕВН.		Prerequisites: Task 5 started. Необходимо условие: Изпълнението на Задача 5 да е стартирало.	ADD shall be responsible for delivery of HHU firmware without hardware platform. АДД е отговорен за доставката на софтуера за HHU без хардуерната платформа. EVN must purchase appropriate devices for HHU (Android v.4.1 or higher). ЕВН трябва да закупи съответните устройства за HHU /Андроид версия 4.1 или по-висока/.
Task 7 Задача 7	DC hardware v.7 to v.8 migration. Миграция на концентраторите на данни от версия 7 на версия 8.		It is required physically to exchange RTR7 to RTR8. RTR8 have to be purchased from ADD	ADD is responsible to accept the orders and perform the delivery of DCU RTR8.

			Bulgaria. Изисква се физически да се сменят концентраторите на данни версия 7 с такива от версия 8. Концентраторите на данни версия 8 трябва да бъдат закупени от АДД България.	АДД е отговорен да приеме заявките и изпълни доставките на Концентратори на данни 8-ма серия. EVN is responsible for purchasing of RTR8 ЕВН е отговорен за покупката на Концентратори на данни 8-ма серия.
Task 8 Задача 8	Massive meter firmware upgrade from v.7.2 to v.7.6. Масово обновяване на електромерите с версия 7.2 към версия 7.6.		Prerequisites: Tasks 1, 2, 3 completed, 5, 7 started. Необходимо условие: Задачи 1, 2, 3 завършени, 5, 7 стартирани.	EVN Bulgaria is responsible for meter firmware upgrade ЕВН България е отговорен за обновяването на електромерите.
Task 9 Задача 9	Final clean-up (conditional). Последни настройки (зависещи от условия).		Prerequisites: Tasks 8 started. Необходимо условие: Задача 8 да е започната.	EVN Bulgaria is responsible for clean-up ЕВН България е отговорен за последните настройки.
Task 10 Задача 10	KMS deployment. EVN Bulgaria must purchase two instances of Thales keyAuthority device to be used in the KMS. Внедряване на система за разпределяне на ключове. ЕВН България трябва да закупи две устройства Thales keyAuthority, за да бъдат използвани в системата за раздаване на ключове.		Prerequisites: Task 5 started, two instances of Thales keyAuthority devices are purchased. Необходимо условие: Задача 5 да е започната, две устройства Thales keyAuthority да са доставени.	ADD is responsible to accept the orders and perform the delivery of two instances of Thales keyAuthority devices. АДД е отговорен да приеме заявките и изпълни доставките на две устройства Thales keyAuthority. EVN is responsible for purchasing of two instances of Thales keyAuthority devices. ЕВН е отговорен за покупката на две устройства Thales keyAuthority.
Task	Encryption service activation. Step-by-step process starting in testing		Prerequisites: Tasks 9, 10	ADD is responsible to provide

11 Задача 11	environment and finally coming to massive security activation in production environment. Активиране на услугата за криптиране. Поетапен процес започващ в тестова среда и завършващ с масово активиране на сигурността в продуктивна среда.		completed. Необходимо условие: Задачи 9, 10 да са завършени.	instructions to perform Task 11 АДД е отговорен да предостави инструкции за изпълнението на Задача 11. EVN Bulgaria is responsible for Task 11 implementation ЕВН България е отговорна за внедряването на Задача 11.
Task 12 Задача 12	Implementation and deployment of the archiving subsystem within the SIMS v.8 framework. Внедряване и разгръщане на архивираща подсистема в рамките на SIMS v.8.		Prerequisites: Tasks 5 completed. Необходимо условие: Задача 5 да е завършена.	ADD is responsible to deliver SIMS v.8 with functionality described in Task 12 АДД е отговорен да достави SIMS версия 8 с функционалности описани в Задача 12.

03.08.2016
Plovdiv / Пловдив

Stefan Dikarlo
/Director ADD BULGARIA OOD/

План за повишаване на сигурността на наличната АДД Система изградена от електромери с версия по-ниска от v.7.6 , рутер концентратори v.7 и SIMS6

Съдържание

1 Доставка на хардуер и софтуер

Компоненти на системата	Софтуер и хардуер , описание на необходимите доработки:
SIMS8	Ще се използва един (център) SIMS8 за всички електромери вместо сегашните няколко SIMS6. Към стандартните функции на SIMS8 се добавя възможността за импорт от няколко бази SIMS6 на следните данни : 1. Данни по групи устройства (Group Manager). 2. Балансови групи. 3. Информационни системи (допълнителни инструменти даващи възможност за синхронизиране с външни информационни системи). 4. История на конфигурация на хардуера. 5. Подвързване на електромерите към концентратора (за всеки трафопост).
SIMS8	Архивиране на стари данни.
DCU v.7.6	1. Частично отстраняване на забележките на ENCS касаещи сигурността (колкото позволяват хардуерните устройства). 2. Съвместим със SIMS8 (поддържа четене на всички данни по протокол P3.2, но без HTTPS). 3. Добавена е функцията за експорт на топологията на мрежата PL/LV за импорта в DCU v.8.
DCU v.8	1. Добавена е функцията за импорт на топологията на мрежата PL/LV за импорта в DCU v.8.
Meter FW v.7.6	1. Нужната функционалност на v.7.2 е запазена. 2. Добавена е аутентификация в GCM-AES-128 и HLS. 3. Отстранени са или са смекчени проблемите с DLMS robustness issues, установени от ENCS. 4. Видът на обновяването (FW image) е защитен с помоща на GMAC, електромерът ще приема само правилното обновяване.
HHU на Android	1. Android v.5.1 и по -висока. Хардуерът се доставя от АДД България. 2. HHU може да работи със SIMS8 и електромери v.7.2 и 7.6 (в това число и с включено секюрити).

2 План за обновяване на компонентите на системата

№	Описание	Пояснения и взаимна свързаност
1	ЕВН подготвя необходимия хардуер за инсталиране на SIMS 8 с идеята за изграждане на единен център.	Необходимите сървърни ресурси могат да се добавят в зависимост от нарастването на системата. KMS устройствата трябва да бъдат инсталирани преди началото на Стъпка 9.
2	Обновяване на рутер концентраторите от v.7.4 на v.7.6. Обновеният рутер концентратор продължава да работи под управлението на SIMS6.	Стъпка 2 може да започне независимо от Стъпка 1.
3	Прехвърляне на данните,по групи електромери от SIMS6 в SIMS8	Действието може да се извършва поетапно за тези рутер концентратори при които версията вече е обновена на v.7.6.
4	Прехвърляне на рутер концентраторите от SIMS6 на SIMS8	Действието се извършва с тези рутер концентратори с v.7.6, за които данните по групи електромери вече са прехвърлени в SIMS8/вече е изпълнена Стъпка 3/. След прехвърлянето на електромерите, SIMS8 започва работа с тях.Електромерите все още са с v.7.2.
5	Замяна на рутер концентраторите v.7 с рутер концентратори v.8. При замяната, данните за топологията на мрежата се пренасят в новия рутер концентратор локално/чрез експорт-импорт/.	Действието се извършва с тези рутер концентратори за които е извършена Стъпка 3. Новия концентратор v.8. се прехвърля към SIMS8, старият концентратор v.7.,който е в SIMS8 се поставя в състояние Disabled.
6	Clean-up за подготовка към масово обновяване на електромерите/в зависимост от необходимостта/.	Действието се извършва с тези рутер концентратори с които е приключила Стъпка5. Необходимо е да се постигне добра чуваемост на електромерите и висока производителност при преноса на данни по PLC /availability and performance),с цел да се минимизират ръчните

		операции при обновяването на електромерите.
7	Масово обновяване на електромерите до v.7.6.	Действието се извършва на тези трафопостове на които вече са инсталирани рутер концентратори v.8, които вече са свързани към SIMS8 и е обезпечена добра комуникация по PLC (завършена е Стъпка 6). Възможно е в отделни случаи/поради лоша комуникация по PLC/ да се наложи,посещение на място при електромерите и локална работа.Като краен резултат ще имаме електромери с v.7.6,под управление на концентратори v.8, а концентраторите v.8 под управлението на SIMS8.
8	Проверка за стабилността на работа на комуникационната мрежа преди активирането на security.	Необходимо е известно време да се следи за стабилността на системата.Това действие се извършва за тези рутер концентратори, за които е приключила Стъпка 7.
9	Активиране на security.	Активират се тези рутер концентратори,които успешно са преминали от Стъпка 2 до Стъпка 8.

3 Тестова и продуктивна среда

Преди започването на масово внедряване в продуктивната среда (Production Environment), е необходимо да се тестват всички стъпки в определен от ЕВН тестови участък(Test Environments).

08.03.2017г. Стефан Дикарло

Пловдив Управител на „АДД България“