**Specyfikacja komunikacji za pośrednictwem protokołu DLMS dla liczników energii elektrycznej i koncentratorów danych  
do zastosowań w ENERGA-OPERATOR SA**

**Opis zastosowań protokołu DLMS**

**z uwzględnieniem mechanizmów bezpieczeństwa**

Gdańsk, 2016

ENERGA-Operator SA

październik 2016, wersja 1.3.3

**Spis treści**

1. Uwagi wstępne 5

2. Komunikacja z licznikami 6

2.1. Asocjacje DLMS 6

2.2. Profile komunikacyjne 7

2.2.1. Profil PLC PRIME 7

2.2.2. Profil HDLC 7

2.2.3. Profile TCP/IP 9

2.3. Obiekty COSEM modelu bezpieczeństwa w liczniku 10

2.4. Typy kluczy 11

2.5. Liczniki ramek 13

2.6. Czas życia kluczy i haseł LLS 14

2.7. Zabezpieczenie dostępu do danych (autentykacja) 14

2.8. Szyfrowanie i uwierzytelnianie przesyłanych danych 14

3. Komunikacja koncentratora z licznikami 16

3.1. Asocjacja i rodzaj komunikacji nawiązywany między koncentratorem a licznikiem 16

3.2. Obsługa obiektów liczników ramek urządzeń pomiarowych 17

3.3. Rozszerzenia DCSAP 18

*3.3.1.* Klasa *DLMS Security Setup* 18

3.3.2. Kody błędów DCSAP 19

3.3.3. Obiekty COSEM w koncentratorze związane z bezpieczeństwem 20

3.3.3.1. Globalne obiekty koncentratora 21

3.3.3.2. Globalne obiekty liczników realizowane przez koncentrator 21

3.4. Komunikacja w procesie aktualizacji oprogramowania liczników 24

3.5. Obsługa komunikatów Emergency 24

4. Funkcjonalności związane z bezpieczeństwem w centralnym systemie AMI 26

4.1. Komunikacja w TAN B 26

4.2. Komunikacja w TAN C 27

4.3. Inne krytyczne funkcjonalności 29

5. Materiały źródłowe 31

6. Załączniki (przekazywane jedynie partnerom realizującym dostawy urządzeń pomiarowych do ENERGA-Operator) 32

Załącznik nr 1. Procedura generowania domyślnego hasła LLS dla asocjacji Management i Firmware Update 33

Załącznik nr 2. Domyślne klucze szyfrujące i hasła LLS 35

**Spis tabel**

Tabela 1 Macierz powiązań asocjacji DLMS z portami interfejsu licznika 6

Tabela 2 Identyfikatory asocjacji DLMS 6

Tabela 3 Obiekty licznika związane z bezpieczeństwem komunikacji 10

Tabela 4 Rodzaje transmisji (broadcast/unicast) dostępne w kontekście asocjacji 11

Tabela 5 Klucze dostępne dla poszczególnych asocjacji 11

Tabela 6 Klucze kryptograficzne wykorzystywane w komunikacji między komponentami infrastruktury pomiarowej i systemem AMI 12

Tabela 7 Liczności i unikalność kluczy w licznikach i systemie AMI 13

Tabela 8 Asocjacje i rodzaj komunikacji w przypadku komunikacji realizowanej autonomicznie przez koncentrator 16

Tabela 9 Asocjacje i rodzaj komunikacji realizowanej w sytuacji komunikacji bezpośredniej 17

Tabela 10 Klasy interfejsów wprowadzone na potrzeby zarządzania bezpieczeństwem komunikacji z licznikami. 18

Tabela 11 Opis klasy DLMS Security Setup 19

Tabela 12 Kody błędów DCSAP związane z bezpieczeństwem komunikacji. 19

Tabela 13 Wartość domyślna klucza master licznika 35

Tabela 14 Wartości domyślne parametrów bezpieczeństwa dla asocjacji Management 35

Tabela 15 Wartości domyślne parametrów bezpieczeństwa dla asocjacji Read Only 35

Tabela 16 Wartości domyślne parametrów bezpieczeństwa dla asocjacji Firmware Update 35

Tabela 17 Wartości domyślne parametrów bezpieczeństwa dla asocjacji HAN 36

Tabela 18 Wartości domyślne parametrów bezpieczeństwa dla asocjacji Pre-Established 36

**Spis rysunków**

Rysunek 1 Nagłówek protokołu LLC w profilu PRIME PLC 7

Rysunek 2 Nagłówek protokołu LLC w profilu HDLC 7

Rysunek 3 Nagłówek ramki MAC protokołu HDLC (format typu 3) 8

Rysunek 4 Nagłówek WPDU dla profili TCP/IP 9

# **Uwagi wstępne**

W warstwie aplikacyjnej komunikacja z licznikami odbywa się za pośrednictwem protokołu DLMS opisanego w [1], która to specyfikacja w sposób rozbudowany opisuje role poszczególnych stron jak i zasady wymiany informacji między uczestnikami.

Z natury jednak tego dokumentu jest to opis często ogólny, obejmujący jak najszerszy zakres zastosowań, przy czym w wielu przypadkach funkcjonalności określane są jako opcjonalne bądź opisane są w sposób bardzo ogólny.

Niniejszy dokument ma za zadanie wskazać te opcje, których obecność w infrastrukturze pomiarowej ENERGA-Operator jest wymagana, jak również ma doprecyzować zagadnienia co do których przytoczona specyfikacja protokołu DLMS jest niewystarczająca.

Szczególny nacisk położono na wymagania bezpieczeństwa w odniesieniu do liczników i koncentratorów, a także powiązane z tym funkcjonalności Centralnego Systemu AMI.

Mechanizmy bezpieczeństwa w komunikacji z licznikami bazują na Security Suite ID = 0 oznaczającym Galois/Counter Mode z algorytmem szyfrowania AES-128. W tym przypadku zarówno do kontroli dostępu jak i uwierzytelniania oraz szyfrowania danych wykorzystywany jest algorytm AES-128. Analogicznie do transportu kluczy globalnych wykorzystywane jest kodowanie („key wrapping”) w oparciu o AES-128 zgodnie z [3]. Mechanizm ten bazuje na kryptografii z wykorzystaniem kluczy symetrycznych.

W kolejnych wydaniach specyfikacji, kiedy już zostaną opublikowane w [2] zestandaryzowane klasy i obiekty COSEM przechowujące certyfikaty oparte o kryptografię z wykorzystaniem kluczy asymetrycznych oraz w miarę dostępności zweryfikowanych rozwiązań w licznikach wykorzystujących kryptografię asymetryczną – przewiduje się ich wykorzystanie i integrację centralnego systemu AMI z centralnym systemem PKI w ENERGA-Operator.

# **Komunikacja z licznikami**

# **Asocjacje DLMS**

Zgodnie z [1] protokół DLMS jest protokołem sesyjnym wymagającym między stroną klienta a serwerem (licznikiem) ustanowienia asocjacji (sesji).

Możliwe są następujące rodzaje tworzonych asocjacji, tworzone w kontekście określonych ról klienta:

1. do zarządzania (tj. odczytu i zapisu danych) – Management (M),
2. do odczytu – Reading (R),
3. publiczna – Public (P),
4. do wymiany oprogramowania licznika – Firmware Update (F),
5. HAN (H).

Z uwagi na konieczność obsługi komunikacji typu broadcast – licznik w roli serwera DLMS musi obsługiwać również specjalną asocjację Pre-Established (PE). Komunikacja ta może zajść jedynie w sytuacji, kiedy klient DLMS jest klientem zdalnym. Wobec tego pełna tabela powiązań możliwych asocjacji z interfejsami licznika zgodnie z [5] wygląda następująco:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **port/asocjacja** | **Management**  **(M)** | **Reading**  **(R)** | **Public**  **(P)** | **Firmware update (F)** | **HAN (H)** | **Pre-Established (PE)** |
| PLC |  |  |  |  |  |  |
| opto |  |  |  |  |  |  |
| USB – tryb „DATA PUSH” |  |  |  |  |  |  |
| USB – tryb „DLMS/COSEM modem” |  |  |  |  |  |  |
| USB – tryb „DLMS/COSEM HAN” |  |  |  |  |  |  |
| 3GPP |  |  |  |  |  |  |
| Ethernet |  |  |  |  |  |  |

Tabela Macierz powiązań asocjacji DLMS z portami interfejsu licznika

Identyfikatory poszczególnych asocjacji powinny przyjmować następujące wartości:

|  |  |
| --- | --- |
| **asocjacja** | **ID** |
| Management (M) | 1 |
| Reading (R) | 2 |
| Firmware Update (F) | 3 |
| HAN (H) | 4 |
| Public (P) | 16 |
| Pre-Established (PE) | 102 |

Tabela Identyfikatory asocjacji DLMS

Asocjację protokołu DLMS (z wyjątkiem Pre-Established) nawiązuje klient poprzez wysłanie do serwera (licznika) AARQ APDU.

W procesie przekazywania danych przez stos protokołów – dla profili komunikacji PLC PRIME i HDLC – występuje podwarstwa LLC (Logical Link Control – opisanej w [6]), będąca częścią warstwy łącza danych (DLL), dodająca 3-bajtowy nagłówek do APDU xDLMS. Dla profilu komunikacyjnego bazującego na TCP/IP (GPRS, Ethernet) występuje tworząc 8-bajtowy nagłówek jednostka WPDU (Wrapper Protocol Data Unit).

# **Profile komunikacyjne**

Szczegóły implementacyjne nagłówków komunikacji różnią się w zależności od fizycznej realizacji transportu danych. Poniże doprecyzowano pewne niuanse poszczególnych profili stosowanych z licznikami w ENERGA-Operator.

# **Profil PLC PRIME**

W profilu komunikacyjnym PLC PRIME nagłówek LLC ma analogicznie jak dla profilu PLC   
S-FSK opisanego w [1] postać:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Control field | | | | | | | | DSAP address field | | | | | | | | SSAP address field | | | | | | | |
| MSB | |  |  |  |  | LSB | | MSB | |  |  |  |  | LSB | | MSB | |  |  |  |  | LSB | |
| 1 | 0 | 0 | 1 | 0 | 0 | 0 | 0 | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A | A |
| 0x90 | | | | | | | | association ID | | | | | | | | association ID | | | | | | | |

Rysunek Nagłówek protokołu LLC w profilu PRIME PLC

* pole Control field ma wartość 0x90 (DL-Data.request),
* w polach DSAP/SSAP address field należy wprowadzić ID asocjacji (np. dla Management będzie to wartość 0x01).

Specjalna asocjacja Pre-Established ma zastosowanie jedynie w wysyłaniu komunikatów Emergency i jest realizowana poprzez transmisję broadcast. Z tego powodu po stronie licznika nie jest ona jawnie otwierana – jest ona zawsze otwarta i nie może zostać zamknięta. W przypadku gdy otrzymana jednostka protokołu DLMS ma w nagłówku LLC użytą asocjację o ID równym 102 (0x66) jest dorozumiana jako polecenie przesyłane w kontekście asocjacji Pre-Established.

# **Profil HDLC**

W profilu komunikacyjnym HDLC (wykorzystywanym w komunikacji przez port opto oraz port USB w trybach DLMS/COSEM modem / DLMS/COSEM HAN) nagłówek LLC ma zgodnie z [1] i [8] postać:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Destination (remote) LSAP | | | | | | | | Source (local) LSAP | | | | | | | | LLC\_Quality | | | | | | | |
| MSB | |  |  |  |  | LSB | | MSB | |  |  |  |  | LSB | | MSB | |  |  |  |  | LSB | |
| 1 | 1 | 1 | 0 | 0 | 1 | 1 | 0 | 1 | 1 | 1 | 0 | 0 | 1 | 1 | X | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| 0xE6 | | | | | | | | 0xE6-request / 0xE7-response | | | | | | | | 0x00 | | | | | | | |

Rysunek Nagłówek protokołu LLC w profilu HDLC

* pole Destination (remote) LSAP ma wartość 0xE6,
* w polu Source (local) LSAP najmniej znaczący bit (LSB) służy do rozróżnienia komendy (0xE6) od odpowiedzi (0xE7),
* ostatnie pole LLC\_Quality ma stałą wartość 0x00.

W profilu tym w warstwie MAC używany jest protokół HDLC, którego nagłówek zgodnie z [8] ma postać (format typu 3):

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Flag | Frame format | | Dest. address | | Source address | | Control | | HCS | | | | |
| B1 | B2 | B1 |  | |  | | B1 | | B2 | | B1 | | |
| 0x7E | XX | XX | 1 or 2 bytes | | 1 or 2 bytes | | XX | | XX | | XX | | |
| 0x7E |  |  |  |  |  |  |  |  |  |  |  |  |

Rysunek Nagłówek ramki MAC protokołu HDLC (format typu 3)

* pole Flag ma stałą wartość 0x7E,
* w polu Frame format kodowany jest zarówno typ ramki jak i jej długość,
* w polach Destination address / Source address w zależności od kierunku transmisji występują adresy strony serwera (licznika) i klienta:
  + adres klienta to zawsze 1 bajt, przy czym najmłodszy bit (LSB) ma zawsze wartość 1, pozostałe 7 bitów są co do wartości równe ID asocjacji DLMS (przykładowo dla asocjacji Management wartość pola adresu klienta będzie wynosić 0x03) niezależnie od kierunku transmisji,
  + adres serwera jest kodowany na 2 bajtach (w starszym bajcie 7 starszych bitów tworzy Upper HDLC address, w młodszym 7 starszych bitów tworzy Lower HDLC address). W starszym bajcie najmłodszy bit (LSB) ma wartość 0, w młodszym bajcie najmłodszy bit (LSB) ma wartość 1:
    - w komunikacji kierowanej do licznika w części Upper HDLC (destination) address powinien być kodowany Management Logical Device Address (0x01), młodszy bajt może zawierać np. ALL\_STATION Address (0x7F), wtedy całe pole Destination address miałoby wartość 0x02FF,
    - w komunikacji kierowanej od licznika w części Upper HDLC (source) address powinien być kodowany Management Logical Device Address (0x01),
* pole Control o długości jednego bajta, identyfikuje typ zapytania / odpowiedzi oraz zawiera nadawczy/odbiorczy numer sekwencyjny ramki,
* HCS – Header Check Sequence – suma kontrolna nagłówka (stanowi element ramki tylko wtedy, jeśli w ramce HDLC występuje pole Information field).

UWAGA: oczekiwana jest realizacja protokołu HDLC z następującymi parametrami:

* ustawienia protokołu negocjowane podczas negocjacji SNRM/UA (Set normal response mode command / Unnumbered acknowledge response):
  + maximum information field length - transmit = minimum 200 (bajtów)
  + maximum information field length - receive = minimum 200 (bajtów)
  + window size, transmit = 1
  + window size, receive = 1
* wymiana ramek potwierdzeń (RR - Receive ready command and response) po każdorazowej wymianie ramek informacyjnych (I - Information transfer command and response)

# **Profile TCP/IP**

Dla profili TCP/IP (GPRS, Ethernet) – w miejsce LLC PDU występuje WPDU (Wrapper Protocol Data Unit) i zgodnie z [7] i jego 8-bajtowy nagłówek ma postać:

|  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| Version | | Source wPort | | | | Destination wPort | | | | Length | |
| B2 | B1 | B2 | | B1 | | B2 | | B1 | | B2 | B1 |
| 0x00 | 0x01 | 0x00 | | assoc.-ID | | 0x00 | | 0x01 | | XX | XX |
| 0x0001 | |  |  |  |  |  |  |  |  | APDU length | |

Rysunek Nagłówek WPDU dla profili TCP/IP

* pole Version ma stałą wartość 0x0001,
* w polu Source wPort starszy bajt B2 przenosi stałą wartość 0x00, zaś jako wartość młodszego bajtu B1 należy wprowadzić ID asocjacji (np. dla Management będzie to wartość 0x01),
* w polu Destination wPort występuje stała wartość 0x0001 (Management Logical Device),
* w ostatnim polu Length jest przekazywany rozmiar przenoszonego APDU.

# **Obiekty COSEM modelu bezpieczeństwa w liczniku**

Liczniki w ENERGA-Operator mają możliwość komunikowania się przez swoje interfejsy zarówno w sposób niezabezpieczony (stosowany głównie podczas testów dla ułatwienia diagnostyki oraz na początkowym etapie wdrożenia) jak i zabezpieczony z wykorzystaniem mechanizmów bezpieczeństwa dostępu do danych oraz szyfrowania i uwierzytelniania transportu danych (tryb produkcyjny pracy systemu AMI).

W modelu obiektów COSEM opisanym w [5] dla liczników przewidziano cały szereg obiektów parametryzujących związanych z bezpieczeństwem, spośród których najistotniejsze są:

|  |  |  |  |
| --- | --- | --- | --- |
| Obiekt | class\_ID COSEM | Kod OBIS | Uwagi |
| Asocjacja – klient publiczny | 15 | 0-0:40.0.1.255 |  |
| Asocjacja - klient uprawniony do odczytu | 15 | 0-0:40.0.2.255 |  |
| Asocjacja – klient uprawniony do zarządzania | 15 | 0-0:40.0.3.255 |  |
| Asocjacja – klient uprawniony do wymiany oprogramowania | 15 | 0-0:40.0.4.255 |  |
| Asocjacja – klient HAN | 15 | 0-0:40.0.5.255 |  |
| Asocjacja – klient Pre-Established | 15 | 0-0:40.0.6.255 |  |
| Obiekt ustawień bezpieczeństwa dla klienta uprawnionego do odczytu | 64 | 0-0:43.0.2.255 | R |
| Obiekt ustawień bezpieczeństwa dla klienta uprawnionego do zarządzania | 64 | 0-0:43.0.3.255 | M |
| Obiekt ustawień bezpieczeństwa dla klienta uprawnionego do wymiany oprogramowania | 64 | 0-0:43.0.4.255 | F |
| Obiekt ustawień bezpieczeństwa dla klienta HAN | 64 | 0-0:43.0.5.255 | H |
| Obiekt ustawień bezpieczeństwa dla klienta Pre-Established | 64 | 0-0:43.0.6.255 | PE |
| Licznik ramek dla klienta uprawnionego do odczytu | 1 | 0-1:43.1.2.255 | global unicast |
| Licznik ramek dla klienta uprawnionego do zarządzania | 1 | 0-1:43.1.3.255 | global unicast |
| Licznik ramek dla klienta uprawnionego do wymiany oprogramowania | 1 | 0-x:43.1.4.255 | x= 1 – global unicast x= 2 – global broadcast |
| Licznik ramek dla klienta HAN | 1 | 0-1:43.1.5.255 | global unicast |
| Licznik ramek dla klienta Pre-Established | 1 | 0-2:43.1.6.255 | global broadcast |

Tabela 3 Obiekty licznika związane z bezpieczeństwem komunikacji

# **Typy kluczy**

Model zabezpieczeń licznika w sytuacji komunikacji z wykorzystaniem koncentratorów danych bazuje na kluczach globalnych (klucze dedykowane nie są wspierane). W związku z tym mechanizm autentykacji dostępu jak i szyfrowania oraz uwierzytelniania transmitowanych danych wykorzystuje klucze:

* globalny klucz szyfrujący komunikacji unicast (global unicast encryption key - GUEK),
* globalny klucz szyfrujący komunikacji broadcast (global broadcast encryption key - GBEK),
* (globalny) klucz autentykujący ((global) authentication key - GAK).

Dodatkowo konieczny jest klucz główny (master: key-encryption key - KEK), który służy do szyfrowania i bezpiecznego transferu innych kluczy globalnych (w tym również nowego klucza master).

W praktycznym zastosowaniu w kontekście danej asocjacji mogą zajść tylko wybrane rodzaje komunikacji broadcast/unicast:

|  |  |  |
| --- | --- | --- |
| **asocjacja** | **unicast** | **broadcast** |
| Management (M) |  |  |
| Reading (R) |  |  |
| Firmware Update (F) |  |  |
| HAN (H) |  |  |
| Public (P) |  |  |
| Pre-Established (PE) |  |  |

Tabela Rodzaje transmisji (broadcast/unicast) dostępne w kontekście asocjacji

stąd – konsekwentnie dla poszczególnych asocjacji dostępne są klucze:

|  |  |
| --- | --- |
| **asocjacja** | **klucz** |
| Management (M) | global unicast encryption key  authentication key |
| Reading (R) | global unicast encryption key  authentication key |
| Firmware Update (F) | global unicast encryption key  global broadcast encryption key  authentication key |
| HAN (H) | global unicast encryption key  authentication key |
| Public (P) | - |
| Pre-Established (PE) | global broadcast encryption key  authentication key |

Tabela Klucze dostępne dla poszczególnych asocjacji

Poszczególne typy kluczy mają zastosowanie:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **klucz** | **miejsce generacji** | **zastosowanie** | **wymiana w liczniku** | **lokalizacja** |
| master key | system AMI | klucz kodujący inny klucze globalne oraz nową wersję klucza master | poprzez wywołanie metody global\_key\_transfer obiektu ustawień bezpieczeństwa asocjacji Management z zakodowanym nowym kluczem (przez stary klucz master) jako parametr | system AMI, licznik |
| global unicast encryption key | system AMI | szyfrowanie unicast’owych xDLMS APDU | poprzez wywołanie metody global\_key\_transfer obiektu ustawień bezpieczeństwa właściwej asocjacji z zakodowanym nowym kluczem (przez klucz master) jako parametr | system AMI, koncentrator, licznik |
| global broadcast encryption key | system AMI | szyfrowanie broadcast’owych xDLMS APDU | poprzez wywołanie metody global\_key\_transfer obiektu ustawień bezpieczeństwa właściwej asocjacji z zakodowanym nowym kluczem (przez klucz master) jako parametr | system AMI, koncentrator, licznik |
| (global) authentication key | system AMI | autentykacja HLS,  uwierzytelnianie xDLMS APDU | poprzez wywołanie metody global\_key\_transfer obiektu ustawień bezpieczeństwa właściwej asocjacji z zakodowanym nowym kluczem (przez klucz master) jako parametr | system AMI, koncentrator, licznik |

Tabela Klucze kryptograficzne wykorzystywane w komunikacji między komponentami infrastruktury pomiarowej i systemem AMI

Dostarczenie tzw. kontekstu bezpieczeństwa (tj. haseł, kluczy globalnych i innych informacji niezbędnych do prowadzenia zabezpieczonej komunikacji z licznikami) do koncentratorów odbywać się powinna poprzez mechanizmy protokołu DCSAP z wykorzystaniem dedykowanych globalnych obiektów liczników realizowanych przez koncentrator. Szczegóły są opisane w rozdziale 3.

Z uwagi na zastosowanie liczność i unikalność poszczególnych kluczy przedstawia się następująco:

|  |  |  |  |
| --- | --- | --- | --- |
| **klucz** | **liczność** | **unikalność** | **uwagi** |
| master key | 1 klucz w danym liczniku | unikalne w całym systemie AMI | wymiana w kontekście obiektu ustawień bezpieczeństwa asocjacji Management |
| global unicast encryption key | 4 klucze w danym liczniku | różne klucze dla wszystkich 4 asocjacji i unikalne w całym systemie AMI | dla asocjacji Management, Reading, Firmware Update i HAN |
| global broadcast encryption key | 2 klucze w danym liczniku | różne klucze dla obu asocjacji, w ramach danej asocjacji wspólne dla wszystkich w systemie AMI | dla asocjacji Firmware Update i Pre-Established |
| (global) authentication key | 5 kluczy w danym liczniku | różne klucze dla wszystkich 5 asocjacji i unikalne w całym systemie AMI | dla asocjacji Management, Reading, Firmware Update, HAN i Pre-Established |

Tabela Liczności i unikalność kluczy w licznikach i systemie AMI

Kontrola unikalności kluczy i ich dystrybucja do liczników jest zadaniem systemu AMI. W szczególności zatem w liczniku mogą się znaleźć różne klucze o identycznych wartościach, licznik nie kontroluje ani ich unikalności ani innych właściwości (siła, reguła budowy, historia użycia) poza weryfikacją formalnej poprawności.

Wartości domyślne kluczy są zamieszczone w: Załącznik nr 2. Domyślne klucze szyfrujące i hasła LLS.

# **Liczniki ramek**

Zarówno w procesie autentykacji dostępu do danych jak i szyfrowania i uwierzytelniania przesyłanych danych wykorzystywane są liczniki ramek (Frame Counter, FC), zwane również licznikami wywołań (Invocation Counter, IC).

Licznik energii elektrycznej przechowuje numer ostatniej odebranej (Rx) ramki w kontekście każdej asocjacji, interfejsu i typu transmisji niezależnie (oprócz asocjacji Public).

Każda kolejna ramka w ramach danej asocjacji, interfejsu i typu transmisji) powinna mieć numer większy od poprzedniej, inaczej zostanie odrzucona, a asocjacja (z wyjątkiem Pre-Established) zamknięta.

W sytuacji osiągnięcia maksymalnego numeru ramki wynikającego z typu danych (0xFFFFFFFF) licznik nadal powinien umożliwiać nawiązanie asocjacji Management i realizację procedury wymiany kluczy na nowe wartości (wywołanie metod global\_key\_transfer() obiektów klasy class\_id=64).

Liczniki odebranych ramek są dostępne do odczytu również przez asocjację Public, jest to wykorzystywane w procesie synchronizacji liczników ramek poszczególnych urządzeń z koncentratorami (ewentualnie z system centralnym AMI w przypadku komunikacji bezpośredniej) w celu prowadzenia poprawnej komunikacji z wykorzystaniem mechanizmów bezpieczeństwa.

Sposób obsługi liczników ramek przez koncentratory opisany jest w rozdziale 3.2.

Liczniki ramek są zerowane w sytuacji wymiany kluczy szyfrujących na nową wartość różną od poprzedniej (w tym samym kontekście asocjacji i rodzaju komunikacji broadcast/unicast). W szczególnym przypadku wymiana klucza na identyczną wartość z poprzednią – jest poprawnie obsługiwana przez licznik, jednak nie zeruje licznika ramek.

# **Czas życia kluczy i haseł LLS**

Czas życia i procedury generacji oraz wymiany haseł LLS należą do kompetencji centralnego systemu AMI. Zakłada się, że w produkcyjnym funkcjonowaniu systemu klucze domyślne zastaną wymienione i następnie zgodnie z wytycznymi Biura Ryzyka i Systemów Bezpieczeństwa ENERGA-Operator będą cyklicznie aktualizowane.

Niezależnie od czasu życia kluczy szyfrujących wynikającego z reguł centralnego systemu AMI – wymiana klucza szyfrującego musi być zainicjowana po przekroczeniu połowy zakresu danego licznika ramek. Algorytm ten jest w kompetencji centralnego systemu AMI na podstawie informacji o przekroczeniu połowy zakresu liczników ramek pozyskanych z koncentratorów lub bezpośrednio z urządzeń pomiarowych. Z punktu widzenia licznika energii elektrycznej wszystkie ramki o numerach powyżej połowy zakresu są przetwarzane w standardowy sposób, natomiast koncentrator nie może realizować w takiej sytuacji innej komunikacji niż proces wymiany klucza. Po wymianie klucza na nową (różną od poprzedniej) wartość licznika ramek jest zerowana i koncentrator może wznowić normalną komunikację z licznikiem.

# **Zabezpieczenie dostępu do danych (autentykacja)**

W zakresie zabezpieczeń dostępu do danych możliwe są tryby tworzonej asocjacji:

* „no security” – brak zabezpieczeń (tylko dla asocjacji Public)
* „LLS – Low Level Security” – podstawowy poziom bezpieczeństwa (etap wdrażania i uruchamiania, minimalny poziom zabezpieczeń w przypadku asocjacji innych niż Public i Pre-Established)
* „HLS – High Level Security” – wysoki poziom bezpieczeństwa (etap stabilizacji, praca produkcyjna jedynie z tym poziomem zabezpieczenia uwierzytelniania).

Domyślne wartości haseł LLS (wartości atrybutu nr 7 - LSS\_secret obiektu asocjacji (klasy 15)) dla poszczególnych asocjacji zawiera załącznik: Załącznik nr 2. Domyślne klucze szyfrujące i hasła LLS.

Mechanizm HLS zaimplementowany w liczniku powinien bazować na mechanism\_id(5) HLS GMAC (COSEM\_High\_Level\_Security\_Mechanism\_Name\_Using\_GMAC), gdzie sekwencjami „challenge” klienta do serwera (CtoS) oraz serwera do klienta (StoC) są losowe łańcuchy znaków o długości od 8 do 64 oktetów.

# **Szyfrowanie i uwierzytelnianie przesyłanych danych**

Zgodnie z przyjętym zestawem ustawień bezpieczeństwa (Security Suite ID = 0 oznaczającym Galois/Counter Mode) do szyfrowania i uwierzytelniania wykorzystywany jest algorytm AES-128.

Do szyfrowania/uwierzytelniania wykorzystywane są klucze globalne, przy czym obsługiwana jest zarówno komunikacja unicast jak i broadcast.

Zależnie od ustawienia parametru security\_policy obiektu ustawień bezpieczeństwa danej asocjacji – przesyłane dane mogą być niezależnie szyfrowane / uwierzytelniane (lub jednocześnie szyfrowane i uwierzytelniane – praca produkcyjna jedynie w tym trybie).

# **Komunikacja koncentratora z licznikami**

Koncentrator realizuje polecenia wysłane przez centralny system AMI poprzez protokół DCSAP.

Komunikaty DCSAP zawierające dane kierowane do / odbierane z liczników w polu dlms-data mają zawsze postać nieszyfrowaną:

* get-request/get-response,
* set-request/set-response,
* action-request/action-response,
* event-notification-request.

przy czym muszą być wspierane mechanizmy selective-access i multiple-references.

W zależności od ustawień bezpieczeństwa komunikacji koncentratora z licznikami komunikaty te mogą zostać przetransponowane na odpowiedniki szyfrowane / uwierzytelniane z wykorzystaniem kluczy globalnych:

* glo-get-request/glo-get-response,
* glo-set-request/glo-set-response,
* glo-action-request/glo-action-response,
* glo-event-notification-request.

Ustawienia bezpieczeństwa komunikacji koncentratora z licznikami decydują również o rodzaju autentykacji wykorzystywanego podczas nawiązywania asocjacji z licznikami.

# **Asocjacja i rodzaj komunikacji nawiązywany między koncentratorem a licznikiem**

W komunikacji inicjowanej i realizowanej autonomicznie z licznikami koncentrator samodzielnie wybiera właściwą asocjację i rodzaj komunikacji (broadcast / unicast). Reguły są następujące:

|  |  |  |
| --- | --- | --- |
| **działanie** | **asocjacja** | **rodzaj komunikacji** |
| pobieranie informacji identyfikacyjnych (ID, paszport) | Public | unicast |
| synchronizacja liczników ramek | Public | unicast |
| realizacja procesu aktualizacji firmware licznika | Firmware Update | unicast/broadcast |
| inne operacje | Management | unicast |

Tabela Asocjacje i rodzaj komunikacji w przypadku komunikacji realizowanej autonomicznie przez koncentrator

W komunikacji inicjowanej z systemu centralnego, które są realizowane poprzez komunikację bezpośrednią z licznikami koncentrator wybiera następującą asocjację i rodzaj komunikacji:

|  |  |  |
| --- | --- | --- |
| **działanie** | **asocjacja** | **rodzaj komunikacji** |
| operacje dotyczące obiektu ogranicznika mocy licznika (obiekt 0-0:17.0.1.255) w trybie Emergency (poprzez wysłanie specjalnego komunikatu dotyczącego dedykowanego obiektu 0-100:2.0.0.255 koncentratora) | Pre-Established | broadcast |
| inne operacje | Management | unicast |

Tabela 9 Asocjacje i rodzaj komunikacji realizowanej w sytuacji komunikacji bezpośredniej

# **Obsługa obiektów liczników ramek urządzeń pomiarowych**

W sytuacji kiedy z licznikiem ma być prowadzona komunikacja szyfrowana / uwierzytelniana – zgodnie z [1] w komunikatach są wykorzystywane liczniki ramek. Ponieważ urządzenia pomiarowe mogą nawiązywać komunikację z różnymi koncentratorami w związku zarówno z montażami / demontażami jak i w zależności od aktualnej topologii sieci PLC – sytuacja jest zmienna w czasie. Dlatego też wymagana jest znajomość przez koncentrator aktualnych wartości obiektów liczników ramek urządzeń pomiarowych – czyli następuje konieczność synchronizacji tych wartości między urządzeniami pomiarowymi a koncentratorami.

Funkcjonalność synchronizacji liczników ramek między koncentratorem a urządzeniami pomiarowymi jest realizowana z wykorzystaniem asocjacji Public.

Koncentrator nadaje numery ramek kolejnych komunikatów kierowanych do danego licznika inkrementując je o 1.

W sytuacji przekroczenia połowy zakresu licznika ramek (wartości większe od 0x7FFFFFFF) uważa się, że odpowiadający szyfrujący klucz globalny traci ważność. W związku z tym koncentrator powinien zgłosić błąd DCSAP *EFCLIMITREACHED* i zaprzestać obsługi innych poleceń DLMS niż wymiana właściwego klucza global unicast/broadcast encryption key (polecenie ACTION wywołania metody global\_key\_transfer(data)). Wymiana klucza jak to opisano w 2.5 skutkuje również wyzerowaniem odpowiadającego licznika ramek i szyfrowana / uwierzytelniana komunikacja między koncentratorem a urządzeniem pomiarowym wraca do normalnego trybu działania.

# **Rozszerzenia DCSAP**

Dla umożliwienia autentykacji HLS jak i komunikacji szyfrowanej / uwierzytelnionej zostały zaproponowane poniższe rozszerzenia w stosunku do specyfikacji DCSAP opisanej w [4].

Do realizacji tych zadań konieczne było zdefiniowanie obiektów przechowujących ustawienia związane z mechanizmami bezpieczeństwa liczników, co pociągało konieczność opracowania także definicji nowej klasy:

|  |  |  |  |
| --- | --- | --- | --- |
| Nazwa klasy interfejsu | Numer klasy (class\_id) | Kardynalność w koncentratorze | Kardynalność w liczniku |
| *DLMS Security Setup* | 40199 | 1..n | 1..n |

Tabela Klasy interfejsów wprowadzone na potrzeby zarządzania bezpieczeństwem komunikacji z licznikami.

# **Klasa *DLMS Security Setup***

Klasa definiuje parametry bezpieczeństwa komunikacji DLMS związane z odpowiednimi obiektami COSEM obecnymi w licznikach:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| DLMS Security Setup | | 0..n | class\_id=40199, version=0 | | |
| *Atrybuty* | | *Typ danych* | *Min.* | *Max.* | *Def.* |
| 1. | logical\_name | octet-string |  |  |  |
| 2. | security\_policy | enum | 0 | 3 | 0 |
| 3. | authentication\_mechanism\_id | unsigned | 0 | 5 | 1 |
| 4. | secret | octet-string |  |  | (pusty) |
| 5. | global unicast encryption key | octet-string |  |  | (pusty) |
| 6. | global broadcast encryption key | octet-string |  |  | (pusty) |
| 7. | global authentication key | octet-string |  |  | (pusty) |

|  |  |
| --- | --- |
| **Opis atrybutów** |  |
| **logical\_name** | identyfikuje instancję obiektu klasy „DLMS Security setup” |
| **security\_policy** | określa włączenie mechanizmów szyfrowania i/lub uwierzytelniania transmisji w kontekście Security Suite ID = 0 (Galois/Counter Mode z algorytmem szyfrowania AES-128):  enum: 0 - brak  1 - wszystkie wiadomości są uwierzytelniane   2 - wszystkie wiadomości są szyfrowane  3 - wszystkie wiadomości są uwierzytelniane i  szyfrowane |
| **authentication\_ mechanism\_id** | identyfikator mechanizmu dostępu do danych (autentykacji):  unsigned: 0 - COSEM\_lowest\_level\_security\_mechanism\_name  1 - COSEM\_low\_level\_security\_mechanism\_name  5 - COSEM\_High\_Level\_Security\_Mechanism\_Name\_Using\_GMAC |
| **secret** | hasło wykorzystywane w trybie autentykacji LLS z licznikiem |
| **global\_unicast\_ encryption\_key** | wartość klucza global unicast encryption key - GUEK |
| **global\_broadcast\_ encryption\_key** | wartość klucza global broadcast encryption key - GBEK |
| **global\_authentication\_ key** | wartość klucza (global) authentication key - GAK |

Tabela Opis klasy DLMS Security Setup

# **Kody błędów DCSAP**

Do automatyzacji procesów związanych z zabezpieczeniem dostępu i transferu danych konieczne było wprowadzenie dodatkowych kodów błędów DCSAP, które pozwolą diagnozować problemy z funkcjonowaniem mechanizmów zabezpieczeń w komunikacji między licznikiem a koncentratorem.

|  |  |  |
| --- | --- | --- |
| KB | Symbol | Opis |
| -7 | *ELLSERROR* | Błąd podczas podczas nawiązywania asocjacji LLS z licznikiem |
| -8 | *EHLSERROR* | Błąd podczas podczas nawiązywania asocjacji HLS z licznikiem |
| -9 | *ESECURITYERROR* | Błąd podczas transmisji szyfrowanej/uwierzytelnianej |
| -10 | *EFCLIMITREACHED* | Przekroczono dopuszczalny limit wartości licznika ramek (górna połowa zakresu) |

Tabela Kody błędów DCSAP związane z bezpieczeństwem komunikacji.

W sytuacji kiedy wystąpią wyżej wymienione błędy w komunikacji z konkretnym licznikiem, centralny system AMI porównuje dane dotyczące zabezpieczeń danego licznika zapisane w systemie AMI i w koncentratorze, i w przypadku wykrycia różnic – uaktualnia dane w koncentratorze. Jeśli błędy nadal występują mimo zgodności parametrów między systemem AMI a koncentratorem – oznacza to, że problem nie wiąże się ze zdezaktualizowanymi danymi przechowywanymi po stronie koncentratora i sytuacja musi zostać zasygnalizowana operatorom systemu AMI do dalszego rozstrzygnięcia.

# **Obiekty COSEM w koncentratorze związane z bezpieczeństwem**

W koncentratorach przechowywane są informacje związane z obsługą mechanizmów bezpieczeństwa, dzięki czemu koncentrator jest w stanie nawiązać asocjację w trybie HLS i prowadzić komunikację z transmisją szyfrowaną / uwierzytelnianą.

Wprowadzone zostały dodatkowe grupy obiektów związanych z mechanizmami zabezpieczeń:

* globalne obiekty koncentratora, umożliwiające zarządzanie rozsyłaniem komunikatów Emergency w trybie broadcast:

|  |  |  |  |
| --- | --- | --- | --- |
| Obiekt | class\_ID COSEM | Kod OBIS | Uwagi |
| Emergency broadcast | 1 | 0-100:2.0.0.255 |  |

* globalne obiekty liczników realizowane przez koncentrator, przechowują ustawienia bezpieczeństwa w komunikacji z konkretnym licznikiem dla poszczególnych asocjacji:

|  |  |  |  |
| --- | --- | --- | --- |
| Obiekt | class\_ID COSEM | Kod OBIS | Uwagi |
| Meter DLMS Security Setup - Reading association | 40199 | 0-100:65.0.2.255 |  |
| Meter DLMS Security Setup - Management association | 40199 | 0-100:65.0.3.255 |  |
| Meter DLMS Security Setup - Firmware Update association | 40199 | 0-100:65.0.4.255 |  |
| Meter DLMS Security Setup - Pre-Established association | 40199 | 0-100:65.0.6.255 |  |
| Frame counter - Read Only association | 1 | 0-100:66.0.2.255 | global unicast |
| Frame counter - Management association | 1 | 0-100:66.0.3.255 | global unicast |
| Frame counter - Firmware Update association | 1 | 0-100:66.x.4.255 | x= 0 – global unicast x= 1 – global broadcast |
| Frame counter - Pre-Established association | 1 | 0-100:66.1.6.255 | global broadcast |

# **Globalne obiekty koncentratora**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **LP** | **Obiekt/Nazwa atrybutu** | **Cl** | **Typ** | **Wartość** | **Znaczenie** | **Uwagi** |
|
|  | Emergency broadcast | 1 | (version=0) | 0-100:2.0.0.255 |  |  |
| 1 | logical\_name |  | octet-string[6] | 0064020000FF |  |  |
| 2 | emergency\_profile |  | emergency\_profile |  | emergency\_profile ::= structure {  emergency\_profile\_id: long-unsigned,  emergency\_activation\_time: octet-string,  emergency\_duration: double-long-unsigned } znaczenie jak dla atrybutu emergency\_profile klasy Limiter (class\_id=71) |  |

# **Globalne obiekty liczników realizowane przez koncentrator**

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
| **LP** | **Obiekt/Nazwa atrybutu** | **Cl** | **Typ** | **Wartość** | **Znaczenie** | **Uwagi** |
|
|  | Meter DLMS Security Setup - Reading association | 40199 | (version=0) | 0-100:65.0.2.255 |  |  |
| 1 | logical\_name |  | octet-string[6] | 0064410002FF |  |  |
| 2 | security\_policy |  | enum | 0 | (brak bezpieczeństwa) |  |
| 3 | authentication\_mechanism\_id |  | unsigned | 1 | LLS |  |
| 4 | secret |  | octet-string[8] | (zgodnie z Załącznikiem nr 2) |  |  |
| 5 | global\_unicast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 6 | global\_broadcast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 7 | global\_authentication\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
|  | Meter DLMS Security Setup - Management association | 40199 | (version=0) | 0-100:65.0.3.255 |  |  |
| 1 | logical\_name |  | octet-string[6] | 0064410003FF |  |  |
| 2 | security\_policy |  | enum | 0 | (brak bezpieczeństwa) |  |
| 3 | authentication\_mechanism\_id |  | unsigned | 1 | LLS |  |
| 4 | secret |  | octet-string[8] | (zgodnie z Załącznikiem nr 2) |  |  |
| 5 | global\_unicast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 6 | global\_broadcast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 7 | global\_authentication\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
|  | Meter DLMS Security Setup - Firmware Update association | 40199 | (version=0) | 0-100:65.0.4.255 |  |  |
| 1 | logical\_name |  | octet-string[6] | 0064410004FF |  |  |
| 2 | security\_policy |  | enum | 0 | (brak bezpieczeństwa) |  |
| 3 | authentication\_mechanism\_id |  | unsigned | 1 | LLS |  |
| 4 | secret |  | octet-string[8] | (zgodnie z Załącznikiem nr 2) |  |  |
| 5 | global\_unicast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 6 | global\_broadcast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 7 | global\_authentication\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
|  | Meter DLMS Security Setup - Pre-Established association | 40199 | (version=0) | 0-100:65.0.6.255 |  |  |
| 1 | logical\_name |  | octet-string[6] | 0064410006FF |  |  |
| 2 | security\_policy |  | enum | 0 | (brak bezpieczeństwa) |  |
| 3 | authentication\_mechanism\_id |  | unsigned | 0 |  |  |
| 4 | secret |  | octet-string[8] | (pusty) |  |  |
| 5 | global\_unicast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 6 | global\_broadcast\_encryption\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
| 7 | global\_authentication\_key |  | octet-string[16] | (zgodnie z Załącznikiem nr 2) |  |  |
|  | Frame counter - Read Only association | 1 | (version=0) | 0-100:66.0.2.255 | global unicast |  |
| 1 | logical\_name |  | octet-string[6] | 0064420002FF |  |  |
| 2 | value |  | double-long-unsigned |  |  |  |
|  | Frame counter - Management association | 1 | (version=0) | 0-100:66.0.3.255 | global unicast |  |
| 1 | logical\_name |  | octet-string[6] | 0064420003FF |  |  |
| 2 | value |  | double-long-unsigned |  |  |  |
|  | Frame counter - Firmware Update association | 1 | (version=0) | 0-100:66.x.4.255 | x= 0 – global unicast x= 1 – global broadcast |  |
| 1 | logical\_name |  | octet-string[6] | 006442xx04FF |  |  |
| 2 | value |  | double-long-unsigned |  |  |  |
|  | Frame counter - Pre-Established association | 1 | (version=0) | 0-100:66.1.6.255 | global broadcast |  |
| 1 | logical\_name |  | octet-string[6] | 0064420106FF |  |  |
| 2 | value |  | double-long-unsigned |  |  |  |

# **Komunikacja w procesie aktualizacji oprogramowania liczników**

Zgodnie z [2] proces aktualizacji oprogramowania obsługiwany jest przez obiekt klasy Image transfer (class\_ID=18) i przebiega w 7 krokach:

1. (opcjonalnie) pobranie rozmiaru transferowanego bloku firmware akceptowanego przez licznik
2. inicjalizacja procesu transferu nowego firmware
3. transfer sekwencji bloków nowego firmware
4. weryfikacja kompletności przesłania nowego firmware do licznika
5. weryfikacja firmware przez licznik
6. (opcjonalnie) weryfikacja gotowości do aktywacji nowego firmware w licznku
7. aktywacja nowego firmware przez licznik

Zakłada się, że:

* cała komunikacja związana z realizacją powyższego algorytmu jest realizowana w kontekście asocjacji Firmware Update,
* kroki 1-2 oraz 4-7 wykorzystują komunikację typu unicast,
* krok 3:
  + w pierwszej fazie (realizowanej globalnie w ramach danego koncentratora) jest realizowany za pomocą mechanizmu broadcast (dla zwiększenia skuteczności propagacji emisja danego bloku powinna być ponawiana kilkukrotnie),
  + w drugiej fazie, w wyniku realizacji kroku nr 4 i przy stwierdzeniu niekompletności firmware w danym liczniku – indywidualnie poprzez komunikację unicast do danego licznika są transferowane brakujące bloki.

W sytuacji broadcast’owej transmisji bloków firmware:

* w bajcie Invoke-Id-And-Priority bit nr 6 (service-class) powinien mieć ustawioną wartość = 0 (Unconfirmed),
* jeżeli dodatkowo z ustawień bezpieczeństwa wynika konieczność zastosowania mechanizmów szyfrowania / uwierzytelniania – ponieważ w komunikatach DLSM wykorzystywane są liczniki ramek – wybierana jest maksymalna wartość atrybutu value odpowiedniego obiektu licznika ramek spośród wszystkich układów pomiarowych zarejestrowanych w danym koncentratorze do których jest kierowana transmisja broadcast.

# **Obsługa komunikatów Emergency**

Komunikaty Emergency służy do masowego ustanowienia ograniczenia mocy w wyselekcjonowanej grupie liczników (które zostaną odpowiednio sparametryzowane do akceptacji takiego komunikatu).

W sytuacji konieczności wysłania komunikatu Emergency następuje sekwencja zdarzeń:

* centralny system AMI za pośrednictwem protokołu DCSAP przesyła odpowiedni komunikat do właściwych koncentratorów dotyczący dedykowanego obiektu koncentratora (0-100:2.0.0.255) ustawiając nim operacją SET wartość atrybutu emergency\_profile, która następnie zostanie wykorzystana do przygotowania i wysłania operacji SET dotyczących atrybutu emergency\_profile obiektu ogranicznika mocy liczników (obiekt 0-0:17.0.1.255),
* koncentrator wysyła do wszystkich liczników operację SET dotyczącą atrybutu emergency\_profile obiektu ogranicznika mocy licznika (obiekt 0-0:17.0.1.255) w trybie broadcast o następujących właściwościach:
  + wykorzystana jest asocjacja Pre-Established (odpowiednio ustawiony nagłówek LLC)
  + w bajcie Invoke-Id-And-Priority bit nr 6 (service-class) powinien mieć ustawioną wartość = 0 (Unconfirmed),
  + jeżeli dla tej asocjacji włączone są mechanizmy szyfrowania / uwierzytelniania – to analogicznie jak w przypadku komunikat broadcast podczas procedury aktualizacji firmware opisanej w rozdziale 3.4 – wybierana jest maksymalna wartość atrybutu value obiektu licznika ramek 0-2:43.1.6.255 spośród wszystkich układów pomiarowych zarejestrowanych w danym koncentratorze do których jest kierowana transmisja komunikatów Emergency,
  + dla zwiększenia skuteczności propagacji emisja komunikatu Emergency powinna być ponawiana kilkukrotnie.

# **Funkcjonalności związane z bezpieczeństwem w centralnym systemie AMI**

W niniejszym rozdziale opisano jedynie te funkcjonalności systemu AMI, które odnoszą się do bezpieczeństwa komunikacji w TAN B (do koncentratora) i TAN C (do liczników).

# **Komunikacja w TAN B**

Zabezpieczenie komunikacji w TAN B leży poza zakresem odpowiedzialności centralnego systemu AMI.

W produkcyjnym trybie działania centralnego systemu AMI zakłada się, że protokół DCSAP będzie zabezpieczony podstawowym mechanizmem w postaci tunelu IPsec, gdzie odpowiednie certyfikaty będą dystrybuowane za pośrednictwem protokołu SCEP.

Istnieją dwa dopuszczalne warianty realizacji zaufania do koncentratora, jako elementu poprzedzającego licznik:

1. koncentrator stanowi samodzielne urządzenie komunikacyjne WAN (posiada odpowiednie moduły radiowe)
2. koncentrator komunikuje się z wykorzystaniem sieci Ethernet z urządzeniem integrującym funkcjonalność rutera i modemu.

W przypadku (a) w koncentratorze wymagana jest funkcjonalność zestawiania tuneli VPN w technice IPsec z wykorzystaniem certyfikatów. Tunel zestawiany jest do urządzenia pełniącego rolę koncentratora VPN znajdującego się wewnątrz sieci DMZ ENERGA-Operator. Certyfikaty powinny funkcjonować w dwóch rozłącznych trybach: dostarczonych inicjalnie przez producenta oraz dopuszczonych produkcyjnie do akwizycji danych pomiarowych. Pierwszy z wymienionych trybów powinien zezwalać jedynie na komunikację w celu uzyskania certyfikatów zabezpieczających pracę w trybie drugim. Wymiana certyfikatów powinna zostać zrealizowana w oparciu o protokół SCEP. Protokół SCEP będzie wykorzystany zarówno do inicjalnej wymiany certyfikatów po instalacji koncentratora od producenta, jak również do rotacji certyfikatów w trakcie eksploatacji – proaktywnie (upływający czas życia) i reaktywnie (kompromitacja materiału kryptograficznego).

W przypadku (b) koncentrator, podłączany jako urządzenie zewnętrzne siecią Ethernet, powinien pomyślnie przejść proces uwierzytelniania, realizowany przez ruter. Do tego celu należy wykorzystać protokół IEEE 802.1X wraz z rozwiązaniami towarzyszącymi – protokołem EAP i metodą uwierzytelniania EAP-TLS, protokołem EAPOL i protokołami Diameter (dopuszczalnie RADIUS). Ruter z jednej strony pełni rolę klienta protokołu Diameter/RADIUS, z drugiej strony odpowiada za uwierzytelnienie koncentratora, który na potrzeby tego procesu posługuje się certyfikatem. Po stronie koncentratora wymagana jest implementacja protokołu IEEE 802.1X oraz protokołu SCEP. Pierwszy z nich pozwala uwierzytelnić koncentrator w roli suplikanta protokołu Diameter/RADIUS, drugi odpowiada za obsługę certyfikatów – ich dostarczanie i rotację.

W przypadku (b) to ruter pełni rolę urządzenia zestawiającego tunel VPN – ze wszystkimi funkcjonalnościami opisywanymi dla przypadku (a).

Proces uwierzytelniania zarówno na potrzeby protokołów 802.1X oraz IPsec powinien obejmować uwierzytelnianie wzajemne. Oznacza to, że zanim urządzenie wyniesione (koncentrator i ruter) rozpocznie proces własnego uwierzytelniania, musi zweryfikować tożsamość części serwerowej/infrastrukturalnej systemu na bazie certyfikatu zaufanej trzeciej strony – urzędu certyfikacji (CA).

W sytuacji kiedy podstawowy mechanizm (tunel IPsec) nie jest wspierany przez ruter dopuszczalne jest zastosowanie mechanizmu zapasowego – szyfrowania komunikacji za pomocą protokołu SSL na poziomie połączenia TCP/IP. Pozostałe założenia dotyczące wszystkich protokołów (SCEP, IEEE 802.1X) oraz wzajemnego uwierzytelniania pozostają w mocy.

We wszystkich przypadkach wymagana jest obsługa certyfikatów podpisywanych przez urząd certyfikacji Energa-Operator. Implementacja powinna pozwalać na zastosowanie hierarchii urzędów certyfikacji o minimalnym dwukrotnym poziomie zagłębienia (CA -> CA -> certyfikat urządzenia).

Centralny system PKI (zewnętrzny w stosunku do centralnego systemu AMI) będzie w pełni odpowiadał za generowanie, zarządzanie i proaktywną wymianę certyfikatów w koncentratorach i innych urządzeniach infrastruktury komunikacyjnej przed wygaśnięciem terminu ich ważności (generowanie i instalacja i rotacja odpowiednich certyfikatów leży poza zakresem odpowiedzialności centralnego systemu AMI).

# **Komunikacja w TAN C**

Zarządzanie kryptografią symetryczną w oparciu o algorytm AES-128 w komunikacji między koncentratorami a licznikami jest w pełnym zakresie odpowiedzialności centralnego systemu AMI (przy czym możliwe jest wykorzystanie zewnętrznych komponentów, np. zewnętrznego generatora liczb pseudolosowych).

W związki z tym oczekiwane są następujące funkcjonalności centralnego systemu AMI:

* zarządzanie poziomem bezpieczeństwa komunikacji z poszczególnymi licznikami (indywidualnie dla liczników i globalnie w skali systemu), w szczególności umożliwienie:
  + definiowania stosowanego mechanizmu zabezpieczenia dostępu do danych licznika (autentykacji): LLS / HLS,
  + definiowania stosowanego mechanizmu zabezpieczenia przesyłania danych (brak / szyfrowanie i/lub uwierzytelnianie),
  + definiowanie zestawu parametrów (asocjacja, poziom bezpieczeństwa) dla wszystkich zadań wymagających komunikacji z licznikami z możliwością podawania indywidualnych reguł dla poszczególnych przypadków (regularna akwizycja harmonogramowa, zapytania na żądanie, zapytania wynikające ze zleceń od systemów zewnętrznych – np. windykacyjne zmiana stanu stycznika, zdalna parametryzacja układu, wysyłka żądania ograniczenia mocy DSM / Emergency, itp.),
* zarządzanie hasłami LLS asocjacji DLMS (Management, Reading, Firmware Update, HAN), przy czym:
  + docelowo hasła do wszystkich asocjacji powinny być unikalne w każdym liczniku,
  + system AMI powinien umożliwiać definiowanie parametrów generowanego hasła (złożoność i zmienność znaków, długość historii itp.) oraz jego czas ważności,
  + system AMI powinien zgodnie z cyklem czasu ważności hasła dokonywać jego zmiany w liczniku (a także uaktualniać tę informację w koncentratorach komunikujących się z danym licznikiem),
  + system AMI powinien również dokonywać zmiany hasła w liczniku na żądanie uprawnionego operatora,

*UWAGA: biorąc pod uwagę docelową liczbę liczników AMI w ENERGA-Operator ok. 3 mln daje to ok. 12 mln haseł bieżąco obowiązujących do obsłużenia. W sytuacji zarządzania historią haseł liczbę tę należy pomnożyć przez długość historii (np. przy historii 10 ostatnich haseł system powinien być zdolny do zarządzania 120 mln haseł).*

* zarządzanie kluczami szyfrującymi (global unicast encryption key, global broadcast encryption key, authentication key) dla odpowiednich asocjacji (zgodnie z Tabela 5) oraz kluczami master dla każdego z liczników, przy czym:
  + klucze global unicast encryption key, authentication key powinny być unikalne dla każdego licznika i dla każdej asocjacji,
  + klucze master powinny być unikalne dla każdego licznika,
  + klucze global broadcast encryption key powinny być różne dla asocjacji, ale identyczne w każdym liczniku,
  + system AMI powinien umożliwiać definiowanie parametrów generowanego klucza (złożoność i zmienność znaków, długość historii itp.) oraz jego czas ważności,
  + system AMI powinien zgodnie z cyklem czasu ważności klucza dokonywać jego zmiany w liczniku (a także uaktualniać tę informację w koncentratorach komunikujących się z danym licznikiem),
  + system AMI powinien również dokonywać zmiany kluczy w liczniku na żądanie uprawnionego operatora lub w sytuacji sygnalizacji takiej potrzeby przez koncentrator (przekroczenie połowy zakresu licznika ramek odpowiadającego danemu kluczowi),

*UWAGA: biorąc pod uwagę docelową liczbę liczników AMI w ENERGA-Operator ok. 3 mln i liczności poszczególnych kluczy przedstawiają się zgodnie z Tabela 7 następująco:*

* *3 mln kluczy master key*
* *12 mln kluczy global unicast encryption key*
* *2 klucze global broadcast encryption key*
* *15 mln kluczy (global) authentication key*

*- w sumie daje to ok. 30 mln kluczy bieżąco obowiązujących do obsłużenia. W sytuacji zarządzania historią kluczy liczbę tę należy pomnożyć przez długość historii (np. przy historii 10 ostatnich kluczy system powinien być zdolny do zarządzania 300 mln kluczy). Należy przy tym zauważyć, że zakłada się wstępnie iż maksymalny czas ważności kluczy (parametr aplikacji AMI) będzie wynosić 1 rok – czyli każdy klucz będzie musiał być wymieniony co najmniej w cyklu jednorocznym.*

* monitorowanie i diagnostyka zdarzeń związanych z bezpieczeństwem:
  + sygnalizacja wszelkich niepowodzeń i anomalii związanych z zabezpieczoną komunikacją (np. niemożność autentykacji bądź prowadzenia zabezpieczonej komunikacji z określeniem rodzaju i potencjalnej przyczyny błędu),
  + zarządzanie parametryzacją i gromadzenie informacji z innych obiektów związanych z bezpieczeństwem z modelu danych COSEM licznika [5], w szczególności:
    - parametryzacja zachowania licznika w sytuacji przekroczenia progu błędnych logowań (określenie progu, okresu blokowania),
    - ewidencjonowanie i prezentacja liczby logowań zakończonych sukcesem/błędem przez poszczególne interfejsy,
    - ewidencjonowanie i prezentacja zdarzeń oraz alertów z Rejestru zdarzeń związanych z bezpieczeństwem (0-0:99.98.3.255),
  + integracja z zewnętrznymi systemami monitorowania i diagnostyki funkcjonującymi w ENERGA-Operator.

# **Inne krytyczne funkcjonalności**

Niezależnie od funkcjonalności związanych z zabezpieczeniem komunikacji w TAN C do szczególnie wrażliwych funkcjonalności systemu AMI należą mechanizmy zarządzania aktualizacjami oprogramowania urządzeń oraz obsługa zleceń komunikatów Emergency.

Stąd do mechanizmów krytycznych systemu AMI zaliczono również wymagania:

* zarządzanie i automatyzacja procesu aktualizacji oprogramowania urządzeń (zarówno liczników jak i koncentratorów/ZKB):
  + ewidencjonowanie informacji o zainstalowanej aktualnej wersji oprogramowania funkcjonującej na urządzeniach,
  + zarządzanie bazą plików z aktualizacjami oprogramowania,
  + możliwość manualnego zainicjowania jak i zarządzanie harmonogramami zaplanowanych procesów aktualizacji, przy czym możliwość zdefiniowania co najmniej:
    - obszaru urządzeń do aktualizacji,
    - listy docelowych urządzeń (poprzez filtr typu urządzeń i obecnie funkcjonującej wersji oprogramowania z możliwością ręcznego wykluczenia/uzupełnienia urządzeń),
    - momentu startu procedury aktualizacji,
  + powinna istnieć możliwość monitorowania przebiegu i przerwania/wycofania trwającej aktualizacji,
  + gromadzenie i prezentacja statystyk przebiegu aktualizacji (powodzenia, niepowodzenia, zestawienia funkcjonujących wersji oprogramowania itp.),
* zarządzanie i automatyzacja procesu realizacji komunikatów Emergency:
  + zarządzanie parametryzacją obiektu ogranicznika mocy (0-0:17.0.1.255) w zakresie atrybutów związanych z funkcjonalnością Emergency,
  + udostępnienie metody umożliwiającej przesłanie przez uprawniony zewnętrzny system zlecenia wysłania komunikatu Emergency w wytypowanym obszarze,
  + realizacja wysyłki za pośrednictwem protokołu DCSAP komunikatu Emergency do koncentratorów zgodnie z przekazanymi parametrami,
  + gromadzenie i prezentacja statystyk skuteczności wysyłki komunikatu Emergency (przez porównanie list liczników skonfigurowanych do odbioru danego komunikatu Emergency w wytypowanym obszarze z listą liczników, które odebrały i przetworzyły komunikat – na podstawie analizy Rejestru zdarzeń związanych ze stycznikiem 0-0:99.98.2.255).

# **Materiały źródłowe**

1. Green Book 8th edition, TECHNICAL REPORT, Companion Specification for Energy Metering, DLMS/COSEM Architecture and Protocols, DLMS User Association. Reference number: DLMS UA 1000-2 Ed. 8.0, 2014-07-07,
2. Blue Book 11th edition, TECHNICAL REPORT, Companion Specification for Energy Metering, COSEM Interface classes and OBIS identification system, DLMS User Association. Reference number: DLMS UA 1000-1 Ed. 11.0, 2013-08-27,
3. RFC 3394, Advanced Encryption Standard (AES) Key Wrap Algorithm, 2002, http://tools.ietf.org/html/rfc3394,
4. Data Concentrator Simple Acquisition Protocol - wersja: 1.0.4, 2014-10-17, opracowanie ENERGA-Operator, http://www.energa-operator.pl/dcsap.xml,
5. Specyfikacja obiektów COSEM dla liczników energii elektrycznej do zastosowań w ENERGA-Operator SA, październik 2016, wersja 6.2.6,
6. Norma PN-EN 61334-4-32:2004, Automatyzacja sieci rozdzielczej z użyciem łączności wykorzystującej tę sieć. Część 4-32: Protokoły transmisji danych. Warstwa łącza danych. Sterowanie łączem logicznym LLC, maj 2004,
7. Norma PN-EN 62056-47:2007, Pomiary energii elektrycznej -- Wymiana danych w celu odczytu liczników, sterowania taryfami i obciążeniem -- Część 47: COSEM warstwa transportowa dla sieci IPv4, czerwiec 2007,
8. Norma PN-EN 62056-46:2003, Pomiary elektryczne - wymiana danych w celu odczytu liczników, sterowania taryfami i obciążeniem - Część 46: Warstwa łącza danych przy użyciu protokołu HDLC, czerwiec 2003.

# **Załączniki (przekazywane jedynie partnerom realizującym dostawy urządzeń pomiarowych do ENERGA-Operator)**

Z uwagi na krytyczną z punktu widzenia bezpieczeństwa zawartość załączników, precyzujących domyślne ustawienia zabezpieczeń – załączniki powinny być przekazywane jedynie partnerom realizującym dostawy urządzeń pomiarowych do ENERGA-Operator.

# **Załącznik nr 1. Procedura generowania domyślnego hasła LLS dla asocjacji Management i Firmware Update**

Hasła składają się z 8 znaków. Opisane zostały dwa algorytmy generowania haseł: MAC\_HASH\_1 i MAC\_HASH\_2 – opisane poniżej.

Podstawowym mechanizmem jest MAC\_HASH\_1.

**Mechanizm MAC\_HASH\_1**

Procedura generowania domyślnego hasła LLS dla asocjacji Management i Firmware Update bazuje na przekształceniu adresu MAC interfejsu PRIME Service Node licznika (ten zaś powstaje przez konkatenację identyfikatora OUI producenta oraz na numeru seryjnego licznika ID 1 w postaci szesnastkowej).

**Hasło LLS dla asocjacji Management**

Na podstawie opisanej wyżej metody MAC\_HASH\_1 (algorytm zostanie udostępniony po podpisaniu umowy)

**Hasło LLS dla asocjacji Reading**

Hasło jest stałe i ma wartość ciągu 8 cyfr np. „12345678”.

**Hasło LLS dla asocjacji Firmware Update**

Na podstawie opisanej wyżej metody MAC\_HASH\_1 (algorytm zostanie udostępniony po podpisaniu umowy)

**Hasło LLS dla asocjacji HAN**

Hasło jest stałe i ma wartość ciągu 8 cyfr np. „12345678”.

**Mechanizm MAC\_HASH\_2**

Procedura generowania domyślnego hasła LLS dla asocjacji Management i Firmware Update bazuje na przekształceniu numeru seryjnego ID 1, którego postać jest następująca: SAG + YY + X + 0cdefgh.

**Hasło LLS dla asocjacji Management**

Na podstawie opisanej wyżej metody MAC\_HASH\_1 ((algorytm zostanie udostępniony po podpisaniu umowy)

**Hasło LLS dla asocjacji Reading**

Hasło jest stałe i ma wartość ciągu 8 cyfr np. „12345678”.

**Hasło LLS dla asocjacji Firmware Update**

Na podstawie opisanej wyżej metody MAC\_HASH\_1 ((algorytm zostanie udostępniony po podpisaniu umowy)

**Hasło LLS dla asocjacji HAN**

Hasło jest stałe i ma wartość ciągu 8 cyfr np. „12345678”.

# **Załącznik nr 2. Przykładowe klucze szyfrujące i hasła LLS**

**Parametry globalne dla licznika**

|  |  |
| --- | --- |
| **parametr bezpieczeństwa** | **Wartość** |
| master key | 0x00 33 33 33 44 44 44 66 66 99 AB DD DD DD GH FF |

Tabela Wartość przykładowa klucza master licznika

**Asocjacja Management**

|  |  |
| --- | --- |
| **parametr bezpieczeństwa** | **Wartość** |
| hasło LLS | zgodnie z Załącznik nr 1. Procedura generowania domyślnego hasła LLS dla asocjacji Management i Firmware Update (MAC\_HASH\_1) |
| global unicast encryption key | 0x00 01 01 01 01 01 01 01 01 01 0A 0A 0A 0A 0A 0A |
| (global) authentication key | 0xD0 D1 D1 D2 D1 D2 D3 D1 D1 D2 DA DB DC DD DE DF |

Tabela Wartości przykładowa parametrów bezpieczeństwa dla asocjacji Management

**Asocjacja Reading**

|  |  |
| --- | --- |
| **parametr bezpieczeństwa** | **Wartość** |
| hasło LLS | „12345678” (bez znaku cudzysłowu) |
| global unicast encryption key | 0x00 01 01 01 01 01 01 01 01 01 0A 0A 0A 0A 0A 0A |
| global broadcast encryption key | 0x0F 1B 0B 0A 0A 0A 01 01 01 01 01 02 04 05 02 11 |
| (global) authentication key | 0xD0 D1 D1 D2 D1 D1 D2 D1 D1 D9 DA DB DC DD DE DF |

Tabela Wartości przykładowa parametrów bezpieczeństwa dla asocjacji Read Only

**Asocjacja Firmware Update**

|  |  |
| --- | --- |
| **parametr bezpieczeństwa** | **Wartość** |
| hasło LLS | zgodnie z Załącznik nr 1. Procedura generowania domyślnego hasła LLS dla asocjacji Management i Firmware Update (MAC\_HASH\_1) |
| global unicast encryption key | 0x00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F |
| global broadcast encryption key | 0x0F 0A 0A 0A 0B 0C 01 02 01 03 01 02 01 02 03 00 |
| (global) authentication key | 0xD0 D1 D2 D1 D1 D1 D4 D5 D7 D7 DD DC DD DD DF DF |

Tabela Wartości przykładowa parametrów bezpieczeństwa dla asocjacji Firmware Update

**Asocjacja HAN**

|  |  |
| --- | --- |
| **parametr bezpieczeństwa** | **Wartość** |
| hasło LLS | „12345678” (bez znaku cudzysłowu) |
| global unicast encryption key | 0x00 01 01 02 02 02 02 02 02 02 02 0B 0C 0D 0E 0F |
| (global) authentication key | 0xD0 D1 D2 D3 D4 D5 D6 D7 D8 D9 DA DB DC DD DE DF |

Tabela Wartości przykładowa parametrów bezpieczeństwa dla asocjacji HAN

**Asocjacja Pre-Established**

|  |  |
| --- | --- |
| **parametr bezpieczeństwa** | **Wartość** |
| global broadcast encryption key | 0x0F 0E 0D 0C 0B 0A 09 08 07 06 05 04 03 02 01 00 |
| (global) authentication key | 0xD0 D1 D2 D1 D2 D1 D2 D1 D8 D9 DD DD DD DD DD DD |

Tabela Wartości przykładowa parametrów bezpieczeństwa dla asocjacji Pre-Established