PYSENSE®

Liczniki Energii

Warstwa Bezpieczeństwa w Licznikach LZO

Wprowadzenie

Tomasz Leszczyński, PySENSE Sp. z o.o.

Bezpieczeństwo Liczników LZO a dyrektywy UE

PYSENSE®

- **Dyrektywa MID (Measurement Instrument Directive)** - artykuły 8.1 - 8.5 - nawiązujące do zabezpieczenia funkcji i danych.

- **CSA (Cybersecurity Act)** - framework cyberbezpieczeństwa dla produktów i słuch. W tym zakresie przygotowano odrębne podejście do certyfikacji dla inteligentnych liczników w oparciu o Common Criteria.

- **Dyrektywa RED (Radio Equipment Directive's)** - nowy akt delegowany 6, mający zastosowanie do inteligentnych liczników w zakresie wymogów wysokiego stopnia ochrony.

- **NCCS (Network Code on Cybersecurity)**, jako rozszerzenie dyrektywy NIS/NIS2, mający zastosowanie w szczególności dla sektora energetycznego, proponuje i stosuje nowe wymagania bezpieczeństwa i podejścia do zarządzania ryzykiem dla wszystkich urządzeń wykorzystywanych w systemach energetycznych.

- **CRA (Cyber Resilience Act)**, definiuje podstawowe wymagania cyber-bezpieczeństwa dla różnych rodzajów urządzeń i oprogramowania, wymogów dotyczących zgłaszania podatności na zagrożenia jak i odpowiednich obowiązków podmiotów gospodarczych. CRA określa również wysokie kary za przypadki niezgodności.

European Commission

PYSENSE®

Liczniki inteligentne uznane za infrastrukturę krytyczną (klasy II) - muszą być certyfikowane w ramach CRA

Dodatkowa certyfikacja (poza B+C i H) dla liczników w ramach CRA - schematy certyfikacji (artykuł 18 CRA)

PYSENSE®

Zdalna komunikacja z systemem **HES**

Technologie komunikacyjne **PLC, LTE, LORA, MESH**

Udostępnianie danych do bramy domowej **HAN**

Udostępnianie warstwy aplikacyjnej **DLMS/COSEM**

Billing

Predykcja Zużycia

Zarządzanie Energią

Zdalne Rozłączanie Układu Pomiarowego

Funkcje Inteligentnego Licznika Energii

Funkcja Zdalnego Rozłączania Układu Pomiarowego

=

Infrastruktura Krytyczna !!!

Rozporządzenie w minimalnych wymaganiach dla liczników LZO zakłada, że wszystkie liczniki energii w Polsce będą wyposażone w **rozłącznik umożliwiający zdalne rozłączenie układu elektrycznego.**

Niektóre słabości wymagań dla Liczników LZO

PYSENSE®

PROBLEM	NEGATYWNY REZULTAT	PRZECIWDZIAŁANIE
Brak audytu kodu źródłowego	Celowe lub niecelowe błędy w oprogramowaniu, które mogą doprowadzić np. do masowego rozłączenia układów pomiarowych	Wprowadzenie audytów kodu źródłowego na etapie dostaw w połączeniu z pełną procedurą zapewnienia bezpieczeństwa oprogramowania FW
DLMS Security Suite 0	Zastosowanie tylko szyfrowania symetrycznego w ramach DLMS SS0 naraża na wyciek kluczy dostępowych do liczników na każdym etapie wdrożenia systemu AMI	Wdrożenie infrastruktury klucza publicznego (PKI) w ramach DLMS Security Suite 1 lub 2
DLMS SS0 AES128	Algorytm szyfrujący AES-128 nie powinien być stosowany po 2028 roku. Liczniki LZO w Polsce mają mieć od 2024 roku 12-letnią legalizację.	Możliwość aktualizacji konfiguracji do DLMS Security Suite 2 po 2028 roku
Technologia GSM/2G	Możliwość wymuszenia podłączenia liczników do symulowanej sieci 2G (fake BTS) oraz downgrade'u konfiguracji do zupełnego braku szyfrowania komunikacji.	Zastosowanie technologii LTE oraz odpowiednie zabezpieczenie warstwy aplikacyjnej
Brak szyfrowania pamięci	Możliwość uzyskania dostępu do pamięci licznika i manipulacji FW oraz certyfikatami	Pełne szyfrowanie pamięci na każdym etapie działania urządzenia

PYSENSE®

12 lat czas życia licznika wymaga stosowania najwyższych standardów bezpieczeństwa, które będą mocne w przyszłości

18 milionów liczników w Polsce

18 milionów punktów infrastruktury krytycznej, które powinny być zabezpieczone według najwyższych standardów bezpieczeństwa

PYSENSE®

Standard **DLMS/COSEM - IEC 62056** standaryzuje **3 poziomy** dla mechanizmów bezpieczeństwa, które mogą być stosowane w wymaganiach dla liczników energii.

DLMS Security Suite 0
Podstawowy mechanizm bazujący tylko na szyfrowaniu symetrycznym AES-GCM-128

DLMS Security Suite 1
Zaawansowany mechanizm bazujący na infrastrukturze Klucza Publicznego (PKI)

DLMS Security Suite 2
Zaawansowany mechanizm bazujący na infrastrukturze Klucza Publicznego (PKI)

Poziomy bezpieczeństwa dla DLMS/COSEM

DLMS Security Suite	Szyfrowanie	Podpis Cyfrowy	Wymiana Kluczy	Algorytm Hashujący	Transport Kluczy	Kompresja
0	AES-GCM-128	-	-	-	AES-Wrap z kluczem 128 bit	-
1	AES-GCM-128	ECDSA P-256	ECDH P-256	SHA-256	AES-Wrap z kluczem 128 bit	V.44
2	AES-GCM-256	ECDSA P-384	ECDH P-384	SHA-384	AES-Wrap z kluczem 256 bit	V.44

Zestaw algorytmów znany jako **NSA Suite B**, ostatnio wyewoluował jako **CNSA Suite** (Commercial National Security Algorithms)

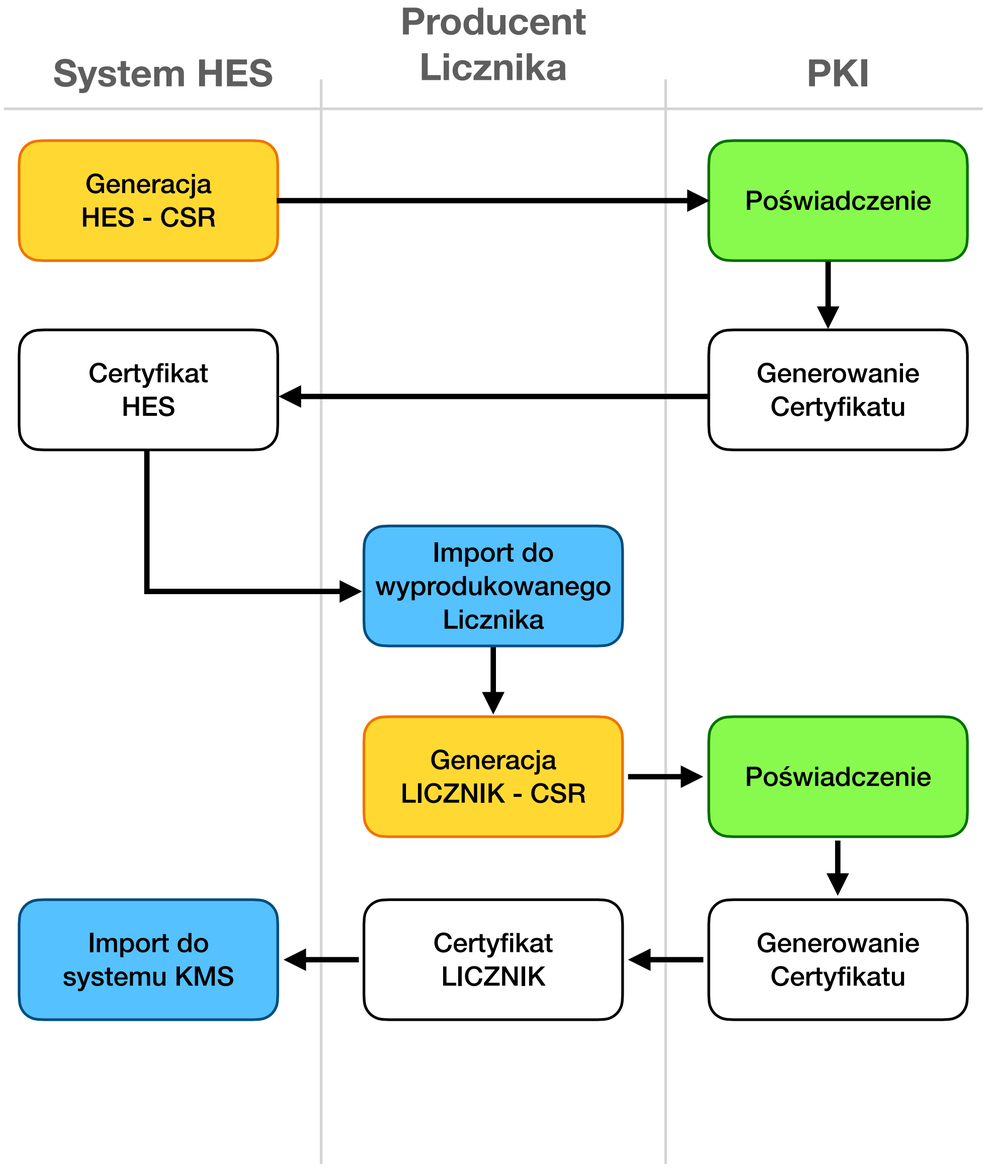
Aby zapewnić odpowiedni poziom bezpieczeństwa dla liczników energii, które będą użytkowane przez **12 lat** należy wdrożyć infrastrukturę klucza publicznego **PKI** oraz zaimplementować mechanizmy opisane w standardzie:

DLMS Security Suite 1 a docelowo
DLMS Security Suite 2

Implementacja PKI, Certyfikatów oraz
infrastruktury do generowania certyfikatów bazująca na specyfikacji **DLMS Green Book: 9.2.6.3**

PYSENSE®

1. Dostawca **HES** generuje **CSR** dla **HES** z wykorzystaniem **root CA**
2. Dostarcza **CSR-HES** do **PKI** aby wygenerować certyfikat dla systemu **HES**
3. Dostarczenie **certyfikatu HES** do producenta liczników
4. Producent liczników powinien zaimportować **certyfikat HES** do urządzeń (licznik, DCU, etc.) podczas produkcji
5. Producent liczników powinien wygenerować **CSR** dla każdego urządzenia z wykorzystaniem swojego **root CA**
6. Producent liczników powinien wysłać plik CSR do PKI aby wygenerować certyfikaty dla urządzeń
7. Dostarczenie certyfikatów urządzeń do KMS
8. Finalnie, system HES może odpytać system KMS o certyfikat jeśli tego potrzebuje



Przykłady wdrożeń Europejskich

TELEKOM AUSTRIA GROUP Smart Metering

Wymagania dla liczników Kaifa w projekcie G3-PLC

Standardy Bezpieczeństwa:
DLMS Security Suite 1 ECC
DLMS Security Suite 2 ECC (opcjonalnie)

Department for Business, Energy & Industrial Strategy

Wymagania dla liczników inteligentnych w zakresie bezpieczeństwa 2017/0350/UK

Standardy Bezpieczeństwa: **DLMS Security Suite 1 ECC**

STADTWERKE SCHWAZ

Wymagania w zakresie bezpieczeństwa dla liczników Kaifa oraz Honeywell wykorzystywanych w infrastrukturze OSD

Standard Bezpieczeństwa: **DLMS Security Suite 1 ECC**

PYSENSE®

Przykłady Liczników Energii

Spełniających wymagania DLMS Security Suite 1 lub Suite 2

Sagemcom

T2XX

iskraemeco
BY ELSEWEDY ELECTRIC

IE.5

ZPA Smart Energy

AM375

Landis+Gyr

E660

KAIFA

MA30X

PYSENSE®

Organizacje i Agencje Rządowe

Określające wytyczne w zakresie cyberbezpieczeństwa w Europie oraz USA również w kontekście liczników energii

NIST
National Institute of Standards and Technology
U.S. Department of Commerce

Agencja rządowa USA
Wydająca tzw.
Cybersecurity Framework

DLMS®

Stowarzyszenie firm
tworzących protokół
DLMS/COSEM

RCB
Rządowe Centrum Bezpieczeństwa

Definiuje standardy
Bezpieczeństwa dla
Infrastruktury krytycznej
w Polsce

ENCS

Organizacja zrzeszająca dystrybutorów OSD
definiująca zasady bezpieczeństwa dla
projektów Smart Grid

PYSENSE®

www.pysense.com

Tomasz Leszczyński
tomasz@pysense.com