BEZPIECZEŃSTWO ZARZĄDZANIA INFRASTRUKTURĄ POMIAROWĄ

Dawid Gruszka

Rozporządzenie MKiŚ z dnia 22 marca 2022 r.

Rozdział 1

Przepisy ogólne

§ 1. Rozporządzenie określa:

1) wymagania funkcjonalne, jakie spełnia system pomiarowy;

2) wymagania w zakresie bezpieczeństwa systemu pomiarowego, w tym ochrony tego systemu przed nieuprawnioną ingerencją w ten system oraz nieuprawnionym dostępem do informacji rynku energii;

3) wymagania, jakie spełniają:

   a) układy pomiarowo-rozliczeniowe w zakresie energii elektrycznej w zależności od miejsca ich instalacji oraz ich przeznaczenia innego niż określone w pkt 9,

   b) dane pomiarowe oraz inne informacje rejestrowane przez licznik zdalnego odczytu,

   c) polecenia odbierane przez licznik zdalnego odczytu, a także warunki ich przesyłania,

   d) dane pomiarowe oraz polecenia wysyłane przez licznik zdalnego odczytu do urządzeń w gospodarstwie domowym, a także warunki ich przesyłania;

4) standardy komunikacji pomiędzy licznikiem zdalnego odczytu a systemem zdalnego odczytu;

5) sposób funkcjonowania liczników zdalnego odczytu w trybie przedpłatowym oraz sposób dokonywania rozliczeń w tym trybie;

Bezpieczeństwo Systemu Pomiarowego oraz Operacyjne

Rozdział 3

Wymagania w zakresie bezpieczeństwa systemu pomiarowego, w tym ochrony tego systemu przed nieuprawnioną ingerencją w ten system oraz nieuprawnionym dostępem do informacji rynku energii

§ 4. 1. System pomiarowy działa w sposób ciągły oraz zapewniający jego ochronę przed nieuprawnioną ingerencją. W tym celu stosuje się środki techniczne i organizacyjne polegające w szczególności na:

1) ustaleniu warunków i sposobu przydzielania uprawnień do dostępu do informacji rynku energii przetwarzanych w systemie pomiarowym;

2) opracowaniu instrukcji bezpieczeństwa systemu pomiarowego, w tym zarządzania ryzykiem oraz procedury bezpiecznej eksploatacji tego systemu umożliwiającej w szczególności jak najszybsze wykrywanie incydentów zagrażających bezpieczeństwu tego systemu;

3) okresowym sprawdzaniu stanu bezpieczeństwa systemu pomiarowego i odpowiednim podnoszeniu poziomu tego bezpieczeństwa;

4) stosowaniu zabezpieczeń na możliwie wielu różnych poziomach organizacji ochrony systemu pomiarowego w celu ograniczenia występowania przypadków, w których przełamanie pojedynczego zabezpieczenia będzie skutkować naruszeniem poufności, integralności lub dostępności danych pomiarowych;

5) opracowaniu procedury postępowania w przypadku awarii elementów systemu pomiarowego;

6) zapewnieniu odporności na awarie systemu pomiarowego, w szczególności przez zapewnienie ciągłości działania jego systemów telekomunikacyjnych i teleinformatycznych przez co najmniej 8 godzin po wystąpieniu awarii;

7) stosowaniu zabezpieczeń przed działaniem złośliwego oprogramowania;

8) zapewnieniu autoryzacji autentyczności i sprawdzeniu integralności aktualizacji oprogramowania systemu pomiarowego;

9) zapewnieniu poufności, integralności oraz dostępności informacji rynku energii;

10) zabezpieczeniu przed nieuprawnionym dostępem do informacji rynku energii oraz przypadkowymi zmianami i celową modyfikacją tych informacji.

2. Licznik zdalnego odczytu spełnia wymagania techniczno-funkcjonalne określone w pkt 10 załącznika nr 1 do rozporządzenia dla danej kategorii.

Bezpieczeństwo LZO

Załącznik nr 1

MINIMALNE WYMAGANIA TECHNICZNO-FUNKCJONALNE DLA LICZNIKÓW ZDALNEGO ODCZYT

10	**Bezpieczeństwo – kategoria 1**
10.1	W pamięci nieulotnej licznika zdalnego odczytu nie mogą znajdować się w postaci jawnej (cleartext) żadne klucze szyfrujące, dane pomiarowe, logi systemowe
10.2	Dane w pamięci nieulotnej, stanowiące podstawę do naliczenia opłat, powinny być zabezpieczone sumami kontrolnymi
10.3	Licznik zdalnego odczytu ma funkcjonalność zabezpieczającą przed nieuprawnioną wymianą oprogramowania oraz mechanizmy zachowania integralności i niezaprzeczalności oprogramowania
10.4	Dostęp do wszystkich interfejsów komunikacyjnych licznika zdalnego odczytu jest realizowany wyłącznie po uwierzytelnieniu. W przypadku interfejsu do komunikacji, o którym mowa w pkt 7.3.2, jest wymagane szyfrowanie komunikacji
10.5	Licznik zdalnego odczytu ma funkcjonalność zdalnej i lokalnej zmiany certyfikatu (klucza) do uwierzytelniania na poszczególnych interfejsach komunikacyjnych
10.6	Licznik zdalnego odczytu jest wyposażony w mechanizm rejestrujący w dzienniku zdarzeń naruszenia bezpieczeństwa w zakresie: a) dostępu na wszystkich interfejsach komunikacyjnych, b) fizycznego dostępu do wewnętrznych elementów oraz osłony skrzynki zaciskowej licznika zdalnego odczytu
10.7	Licznik zdalnego odczytu jest zabezpieczony przed atakami DoS/DDoS przeprowadzanymi na każdym z interfejsów komunikacyjnych. Przez zabezpieczenie przed atakami rozumie się poprawne działanie funkcji pomiarowych licznika zdalnego odczytu w trakcie ataku DoS/DDoS
10.8	Licznik zdalnego odczytu ma funkcjonalność zapewniającą walidację przesyłanych do niego poleceń
10.9	Wszystkie wewnętrzne złącza serwisowe licznika zdalnego odczytu są nieaktywne lub zabezpieczone programowo przed odczytem lub zapisem
10.10	Wszystkie interfejsy komunikacyjne mają możliwość dezaktywacji na definiowalny okres w sposób lokalny i zdalny
10.11	Dwukierunkowa komunikacja między systemem zdalnego odczytu a licznikiem zdalnego odczytu jest uwierzytelniana i szyfrowana algorytmem o długości klucza 128 bitów według specyfikacji AES lub równoważnej zapewniającej ten sam lub wyższy poziom bezpieczeństwa
10.12	Każde polecenie przesyłania między systemem zdalnego odczytu a licznikiem zdalnego odczytu ma zabezpieczenie przed powieleniem, repliką oraz modyfikacją

Standardy komunikacji

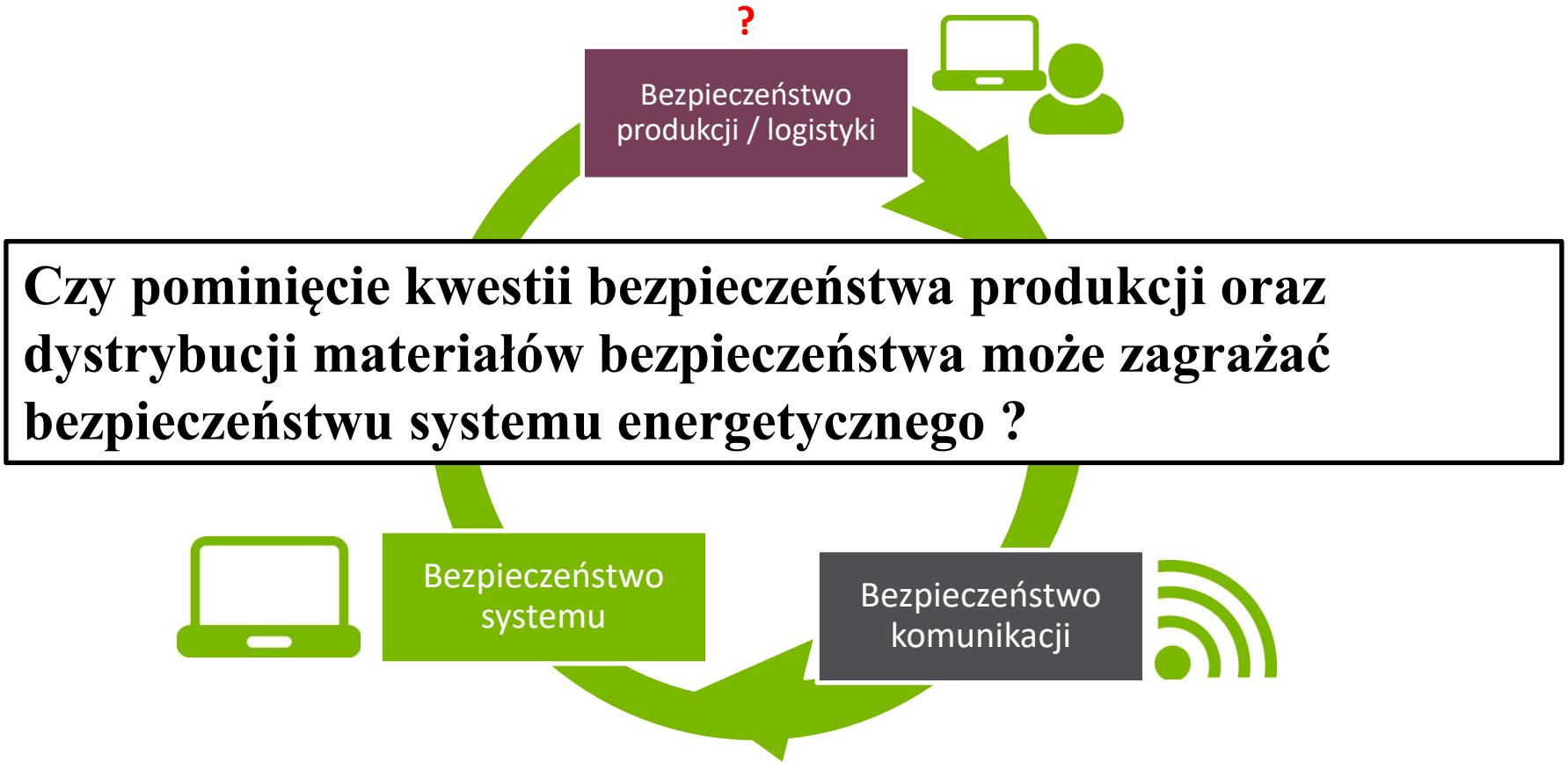
Rozdział 6

Standardy komunikacji między licznikiem zdalnego odczytu a systemem zdalnego odczytu

§ 13. 1. Standardy komunikacji między licznikiem zdalnego odczytu a systemem zdalnego odczytu spełniają w szczególności następujące wymagania:

1) umożliwiają **bezpieczne przekazywanie danych pomiarowych** oraz innych informacji rejestrowanych przez licznik zdalnego odczytu między licznikiem zdalnego odczytu a systemem zdalnego odczytu;
2) komunikacja w systemie zdalnego odczytu odbywa się zgodnie z **najlepszą praktyką** i aktualnym poziomem wiedzy technicznej opisanym w szczególności w odpowiednich Polskich Normach lub normach wydawanych przez krajowe lub międzynarodowe organizacje, zapewniającym interoperacyjność zastosowanego rozwiązania;
3) użyte do komunikacji rozwiązania techniczne i protokoły komunikacyjne zapewniają prawidłową i **bezpieczną komunikację**.
2. Użyte w rozwiązaniach technicznych **standardy protokołów komunikacyjnych** zapewniają możliwość podwyższania tych standardów i są **dostępne publicznie**.

Pełny cykl bezpieczeństwa



Bezpieczeństwo produkcji

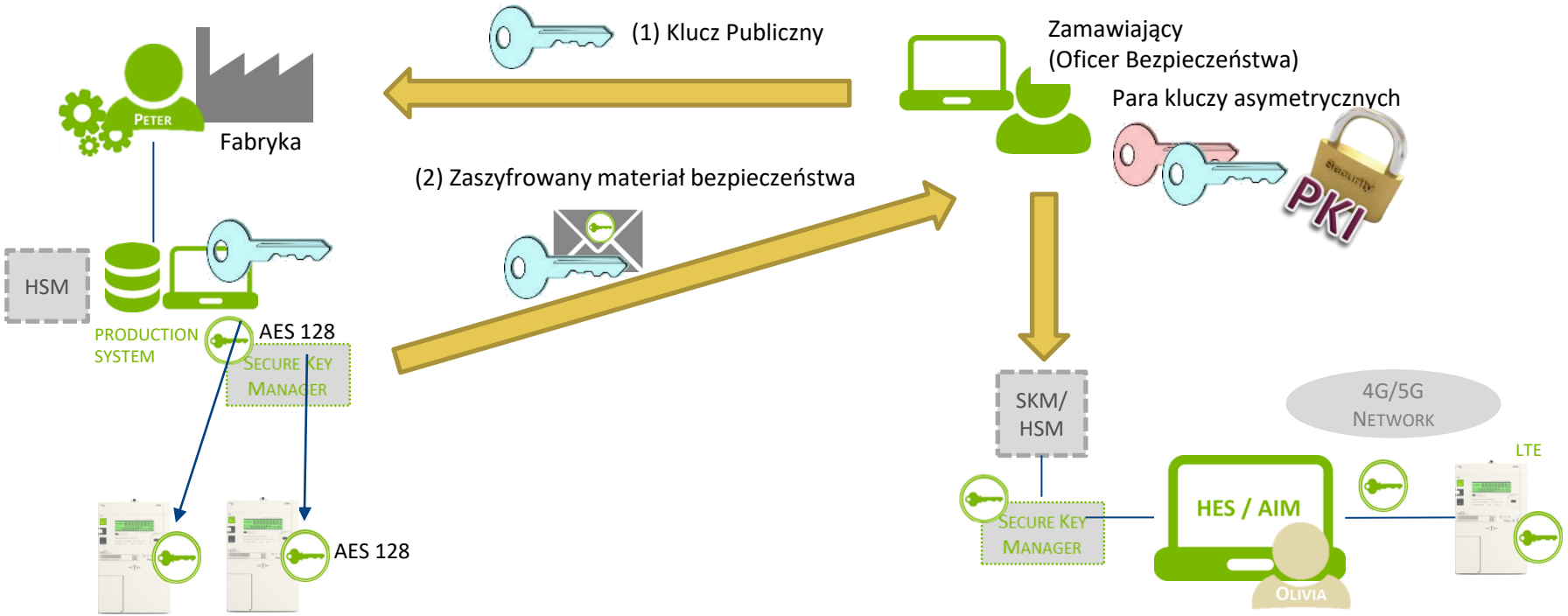
Każdy producent liczników jest odpowiedzialny za produkcję i przechowywanie materiałów bezpieczeństwa związanych z licznikiem, tak aby poufność, integralność i autentyczność materiału bezpieczeństwa nie zostały naruszone podczas produkcji i przetwarzania końcowego licznika w miejscu produkcji

Producent urządzeń musi zapewnić procedury gwarantujące, że tylko odpowiednio upoważniony personel może uzyskać dostęp do bezpiecznych danych i obsługiwać je.

Producent urządzeń powinien utrzymać ścieżkę audytu w zakresie generowania, przechowywania oraz parowania kluczowych materiałów bezpieczeństwa wyprodukowanych przed wysyłką do klienta.

Dystrybucja materiałów bezpieczeństwa

Metoda dystrybucji materiału bezpieczeństwa (zestaw kluczy szyfrujących) musi zagwarantować bezpieczny sposób ich przekazania.



Dystrybucja materiałów bezpieczeństwa
Generic Unit Loader File Format (XML)

```
<tns:Header Manufacturer="Landis+Gyr" Customer="TestCust">
  - <tns:CustomerKey Id="SKCust1">
        <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#rsa-oaep-mgf1p"/>
      - <ds:KeyInfo>
            <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#S
        </ds:KeyInfo>
      - <xenc:CipherData>
            <xenc:CipherValue>V9TSUJT4SQnhohlRXo6GDkbp3Dj99VosZu8mxtcPrrTvxgLtZ7YEdWlzWN
        </xenc:CipherData>
        <xenc:CarriedKeyName>SKCust1</xenc:CarriedKeyName>
    </tns:CustomerKey>
  - <tns:PublicKey>
        <tns:Modulus>pdYczZV/YTcdEDRVK3WgdxO5B68H0vOgWaYA7FsThbGEFNGsruNwg3k1fqx9Ra
        <tns:Exponent>AQAB</tns:Exponent>
    </tns:PublicKey>
</tns:Header>

<tns:General>
  - <tns:Identifiers>
        <tns:Identifier IdentifierName="COSEM_Logical_Name">LGZ1030742032270</tns:Identifier>
        <tns:Identifier IdentifierName="System_Title">4C475A6772815C8E</tns:Identifier>
        <tns:Identifier IdentifierName="Customer_Property_No">SAMPLE42032270</tns:Identifier>
    </tns:Identifiers>
    <tns:Device_Unique_Number>42032270</tns:Device_Unique_Number>
    <tns:Parameterization_ID>EKG0022C.xml</tns:Parameterization_ID>
    <tns:Device_HW_Ver>93101012</tns:Device_HW_Ver>
    <tns:Device_SW_Ver>93.10.10.12</tns:Device_SW_Ver>
    <tns:Human_Readable_Device_Type>E450-3-P</tns:Human_Readable_Device_Type>
    <tns:Device_Type_Designation/>
    <tns:Manufacturing_Date>2018-01-09T09:56:03</tns:Manufacturing_Date>
    <tns:PO_Number/>
</tns:General>
```

```
<tns:Security>
  - <tns:SecurityCredential CredentialType="MK">
      - <tns:Credential>
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
          - <ds:KeyInfo>
                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#SKCust1"/>
                <ds:KeyName>SKCust1</ds:KeyName>
            </ds:KeyInfo>
          - <xenc:CipherData>
                <xenc:CipherValue>NB3aW2twII3KWSQS8QmtdAHQrZvKNNzJefpCKx9csxiag93TkA2K5/KNs33wZxlt</xenc:CipherValue>
            </xenc:CipherData>
        </tns:Credential>
    </tns:SecurityCredential>
  - <tns:SecurityCredential CredentialType="GUEK">
      - <tns:Credential>
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
          - <ds:KeyInfo>
                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#SKCust1"/>
                <ds:KeyName>SKCust1</ds:KeyName>
            </ds:KeyInfo>
          - <xenc:CipherData>
                <xenc:CipherValue>entrfasoQ+703f22/KszPuQzi+St4bZE8Wcf8tuurIcu1ajlykcWEkEM9fx5+qYt</xenc:CipherValue>
            </xenc:CipherData>
        </tns:Credential>
    </tns:SecurityCredential>
  - <tns:SecurityCredential CredentialType="GBEK">
      - <tns:Credential>
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
          - <ds:KeyInfo>
                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#SKCust1"/>
                <ds:KeyName>SKCust1</ds:KeyName>
            </ds:KeyInfo>
          - <xenc:CipherData>
                <xenc:CipherValue>jkxGHKBE2dQgwmNbgmrWc8qrEeiyMgsvUq9Dj3B5sxpoU2EDRgiTEGVhsEh7pgsY</xenc:CipherValue>
            </xenc:CipherData>
        </tns:Credential>
    </tns:SecurityCredential>
  - <tns:SecurityCredential CredentialType="GAK">
      - <tns:Credential>
            <xenc:EncryptionMethod Algorithm="http://www.w3.org/2001/04/xmlenc#aes256-cbc"/>
          - <ds:KeyInfo>
                <ds:RetrievalMethod Type="http://www.w3.org/2001/04/xmlenc#EncryptedKey" URI="#SKCust1"/>
                <ds:KeyName>SKCust1</ds:KeyName>
            </ds:KeyInfo>
          - <xenc:CipherData>
                <xenc:CipherValue>grDPxHoJZidwUrnhU88MB2O/Gat4IZ7GHQUD2haqQTPTn/ky2cEgMbfwk0NvnQyJ</xenc:CipherValue>
            </xenc:CipherData>
        </tns:Credential>
    </tns:SecurityCredential>
</tns:Security>
```

Kilka pytań do... ?

- Czy jest osoba odpowiedzialna za bezpieczeństwo dostępu, przechowywania oraz dystrybucji materiałów bezpieczeństwa ?
- Czy proces zarządzania obiegiem i dystrybucją materiałów bezpieczeństwa jest zdefiniowany dla każdego przypadku użycia ?
- W jaki sposób i gdzie klucze szyfrujące są przechowywane (HW vs SW, HA) ?
- W jaki sposób klucze szyfrujące są dystrybuowane (oprogramowanie serwisowe, aplikacje mobilne obsługi lokalnej, HES) oraz synchronizowane pomiędzy aplikacjami (przypadek zmiany kluczy w liczniku) ?
- Czy na każdym etapie procesu dystrybucji kluczy zapewnione są wymagane zasady bezpieczeństwa (poufność kluczy) ?
- Czy zdefiniowano procedury przypadku zmiany kluczy szyfrujących ?
- Czy zarządzanie procesem bezpieczeństwa jest identyczne dla różnych typów urządzeń ?
- Czy klucze szyfrujące są dostarczane Wam bezpośrednio od producenta urządzeń czy od pośrednika ?

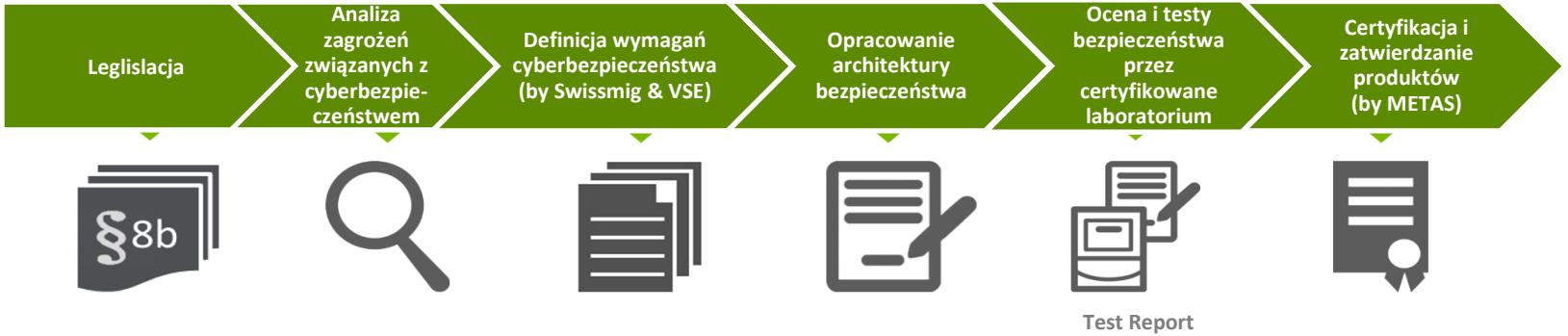
A co z bezpieczeństwem inwestycji ?

- Wybór dostawców zapewniających zaufanie, ciągłość biznesu i dostaw
- Wiarygodność i zdolność
  - Zdolność finansowa
  - Zdolność produkcyjna
- Lokalna obecność
  - Doświadczony i lokalny dział i wsparcie techniczne
  - Europejskie doświadczenie projektowe (referencje)
- Jakość produktu
  - Projektowany czas życia produktu
  - Jakość wykorzystanych komponentów mechanicznych oraz elektronicznych
  - Aspekty środowiskowe (materiały wykorzystane w produkcji urządzeń, tzw. zielony licznik)
  - Kodeks etyczny
  - Społeczna odpowiedzialność biznesu (CSR)
- Standardy produkcji
  - ISO 27001 (Zarządzanie bezpieczeństwem informacji), ISO 9001 (Zarządzanie jakością), ISO 14001 (Zarządzanie środowiskowe), ISO 45001 (Bezpieczeństwo i higiena pracy), ISO 17025 (Laboratoria badawcze i kalibracyjne)
- Certyfikacja

Certyfikacja cyberbezpieczeństwa

Certyfikacja cyberbezpieczeństwa

Rozwiązanie Gridstream (e2e) firmy Landis+Gyr uzyskało certyfikację szwajcarskich standardów bezpieczeństwa jako pierwsze w Szwajcarii



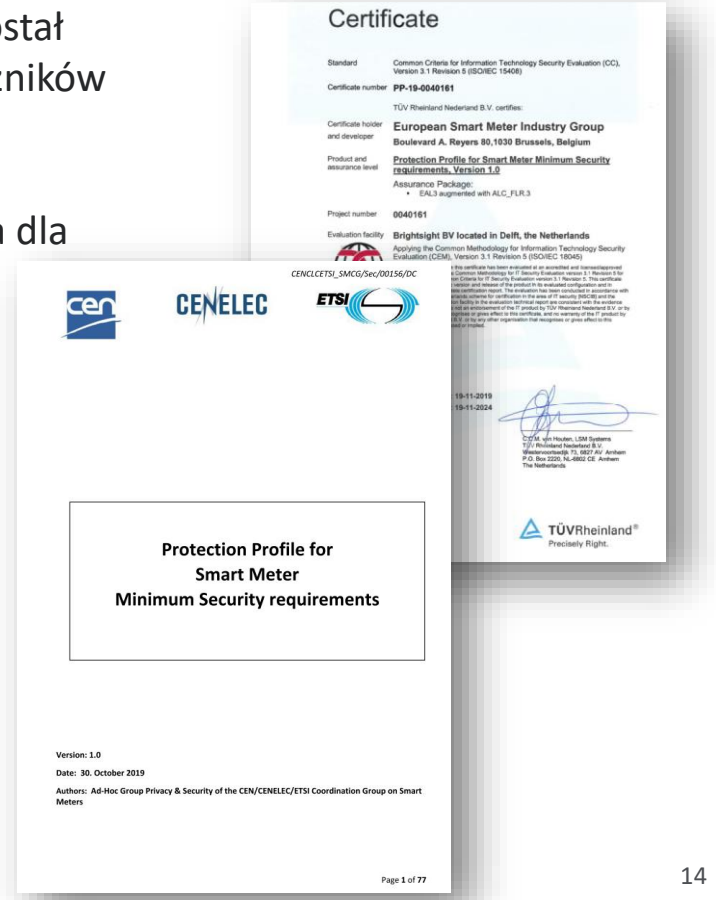
Certyfikacja ISO 27001 zakładów produkcyjnych zapewnia podstawowe bezpieczeństwo etapu projektowania, produkcji jak i dystrybucji urządzeń

Standaryzacja profilu bezpieczeństwa (PP)

Pierwszy europejski profil ochrony inteligentnych liczników został opracowany przez grupę koordynacyjną ds. inteligentnych liczników CEN/CENELEC/ETSI przy wsparciu ESMIG.

Profil ochronny (PP) opisuje zestaw wymagań bezpieczeństwa dla inteligentnych liczników, w oparciu o „minimalne wymagania bezpieczeństwa” dla elementów infrastruktury AMI dla inteligentnych liczników w regionie EMEA.

Celem PP jest wypracowanie europejskiego podejścia do certyfikacji bezpieczeństwa inteligentnych liczników. Ustawa Komisji Europejskiej o cyberbezpieczeństwie wezwała do opracowania europejskich systemów certyfikacji produktów, procesów i usług w celu zapobiegania fragmentacji rynku przez różne krajowe systemy certyfikacji.



Dziękuję za uwagę

Dawid Gruszka
Regionalny Kierownik ds. Sprzedaży

dawid.gruszka@landisgyr.com
Phone +48 606780690

Landis+Gyr Sp. z o.o.
www.landisgyr.com