Wymagania bezpieczeństwa wobec statycznych bezpośrednich 1-fazowych i 3-fazowych liczników energii elektrycznej

Lp.	Wymaganie techniczne
1.	**Wymagania ogólne**
1.1	Licznik musi posiadać aktywną funkcję Watchdog dla zapewnienia poprawnej pracy licznika oraz modułu komunikacyjnego licznika. Licznik musi zapisywać do dziennika zdarzeń zdarzenie wskazujące na błąd działania Watchdog.
1.2	Licznik musi posiadać mechanizm sprawdzania poprawności sum kontrolnych oprogramowania licznika.
1.3	Licznik musi posiadać zabezpieczenie przed usunięciem i modyfikacją zarejestrowanych danych pomiarowych.
1.4	W liczniku musi istnieć mechanizm zapewniający integralność i niezaprzeczalność przesyłanych do licznika komend w zakresie co najmniej: 1. synchronizacji czasu, 2. sterowania, 3. aktywowania/inicjalizowania trybów pracy licznika.
1.5	1. Proces realizujący aktualizację oprogramowania licznika musi uwzględniać sposoby zabezpieczenia przed nieuprawnioną wymianą oprogramowania oraz mechanizmy zachowania integralności i niezaprzeczalności oprogramowania zgodnie ze standardem DLMS. 2. Wszystkie elementy niezbędne do realizacji ww. aktualizacji oprogramowania winny być dostarczone Zamawiającemu przez Dostawcę. Wykonawca wraz z ofertą musi przedstawić sposób realizacji wymagania.
1.6	Wykonawca przedstawi Zamawiającemu (na żądanie) dokładny opis sposobu, algorytmów oraz technologii stosowanych przy zabezpieczeniu danych w liczniku.
1.7	Wykonawca musi przedstawić: 1. specyfikację zabezpieczeń dostępu do danych przechowywanych i przesyłanych przez licznik 2. specyfikację zabezpieczeń dostępu do wszystkich funkcjonalności licznika poprzez dostępne interfejsy komunikacyjne, w tym wyszczególnienie i opis używanych protokołów komunikacji oraz szyfrowania.
1.8	Licznik oraz moduł komunikacyjny licznika nie mogą w sposób jawny udostępniać haseł oraz kodu PIN karty SIM.
1.9	Licznik oraz moduł komunikacyjny licznika nie może zawierać niezmiennych lub generowanych według określonego algorytmu kont, haseł i kluczy
1.10	W przypadku dostępu do licznika poprzez oprogramowanie narzędziowe, licznik musi rejestrować identyfikator użytkownika uruchamiającego oprogramowanie narzędziowe wraz ze zdarzeniem odpowiadającym wykonaniu komendy, skutkującej wystąpieniem zdarzenia w liczniku: 1. zmiany oprogramowania (firmware) licznika 2. zmiana parametryzacji licznika 3. zmiana stanu elementu wykonawczego
2.	**Uwierzytelnianie, szyfrowanie**

2.1	Dostęp do zasobów i funkcjonalności musi być zabezpieczony co najmniej zabezpieczeniem programowym zdefiniowanym dla poszczególnych ról/poziomów dostępu.
2.2	Dostęp do wszystkich interfejsów komunikacyjnych licznika musi być realizowany wyłącznie po uwierzytelnieniu, z wyłączeniem asocjacji "Public".
2.3	W liczniku musi istnieć mechanizm zdalnej zmiany certyfikatu (klucza) z gotowych plików XML do uwierzytelniania na interfejsach komunikacyjnych.
2.4	Dla poszczególnych interfejsów komunikacyjnych licznika muszą być stosowane wyłącznie różne certyfikaty (klucze), tzn. na każdym z interfejsów nie mogą być takie same certyfikaty (klucze).
2.5	Liczniki muszą mieć zablokowany odczyt i debugowanie poprzez interfejsy procesora do tego celu przeznaczone (SWD, JTAG i inne).
2.6	Komunikacja między modułem komunikacyjnym a systemem odczytowym musi być szyfrowana algorytmem TLS w wersji 1.3.
2.7	Komunikacja na interfejsie komunikacyjnym optozłącze oraz na innych interfejsach komunikacyjnych (o ile występują) musi być szyfrowana algorytmem AES co najmniej128 bit (HLS) dla protokołu odczytu danych zgodnego z DLMS/COSEM.
2.8	Komunikacja bezpośrednia między licznikiem a systemem pomiarowym OSD / oprogramowaniem narzędziowym musi być szyfrowana algorytmem AES co najmniej 128 bit (HLS) dla protokołu odczytu DLMS/COSEM na całej ścieżce komunikacji. Wymagane jest uwierzytelnienie licznika podczas nawiązywania komunikacji z systemem pomiarowym OSD / oprogramowaniem narzędziowym.
2.9	Moduł komunikacyjny licznika musi posiadać możliwość ograniczenia dostępu tylko z wybranych adresów IP lub sieci (tzw. whitelist).
3.	**Alarmowanie i rejestracja zdarzeń**
3.1	Naruszenie bezpieczeństwa dostępu na wszystkich interfejsach komunikacyjnych musi być rejestrowane w dzienniku zdarzeń.
3.2	Naruszenia bezpieczeństwa fizycznego dostępu do licznika musi być sygnalizowane i rejestrowane zgodnie z opisem przedstawionym w dokumencie „Wymagania techniczne dla statycznych bezpośrednich 3-fazowych liczników energii elektrycznej” – pkt.6 oraz 7.1 oraz „Wymagania techniczne dla statycznych bezpośrednich 3-fazowych liczników energii elektrycznej” – pkt.6 oraz 7.1.
4.	**Interfejsy lokalne**
4.1	Licznik musi ignorować niewłaściwe komendy.
4.2	Licznik musi posiadać mechanizmy zabezpieczające przed atakami DoS/DDoS przeprowadzanymi na każdym z interfejsów komunikacyjnych.
4.3	Niedopuszczalne jest implementowanie niezmiennych kluczy fabrycznych/serwisowych umożliwiających lokalny dostęp do licznika.
4.4	Interfejsy lokalne licznika muszą być zabezpieczone mechanizmem zapewniającym, że minimalny okres, w którym można sprawdzić wszystkie kombinacje kluczy wynosi, co najmniej 12 miesięcy (np. poprzez zastosowanie zwłoki w odpowiedzi licznika, wymuszanie minimalnej długości klucza).
4.5	W przypadku posiadania funkcji webGUI, musi istnieć możliwość jej wyłączenia.
5.	**Oprogramowanie narzędziowe**
5.1	Wykonawca dostarczy oprogramowanie narzędziowe dla licznika oraz modułu komunikacyjnego (instalacja na komputerach przenośnych z systemem operacyjnym:

	1. Windows 7 32bit, 2. Windows 7 64bit, 3. Windows 10 32bit, 4. Windows 10 64 bit, umożliwiające: 5. pełną konfigurację, 6. parametryzację, 7. diagnostykę, 8. odczyt danych pomiarowych, 9. odczyt zdarzeń z licznika 10. wymianę firmware 11. obsługę lokalnej wymiany kluczy szyfrujących za pomocą plikuXML
5.2	Oprogramowanie narzędziowe musi zapewnić trzy poziomy dostępu dla kont operatorów: 1. tryb operatorski: tylko odczyt danych pomiarowych (dane bieżące, archiwalne, rejestr zdarzeń, profil obciążenia) i parametrów z licznika, 2. tryb serwisowy: odczyt i parametryzacja licznika za pomocą gotowych plików parametryzacyjnych, ustawienie zegara oraz komend sterujących., 3. tryb administracyjny: odczyt i parametryzacja licznika w pełnym zakresie, tworzenie i przywracanie kopii zapasowej z bieżącej konfiguracji licznika.
5.3	Dostęp do każdego z trybów wymienionych w pkt.5.2 musi być zabezpieczony co najmniej zabezpieczeniem programowym zdefiniowanym dla poszczególnych ról/poziomów dostępu.
5.4	Zmiana metody pomiaru i rejestracji energii z metody arytmetycznej na metodę wektorową oraz zmiana z metody wektorowej na metodę arytmetyczną, musi być możliwa w liczniku wyłącznie w trybie administracyjnym.
5.5	Hasła dostępowe do oprogramowania narzędziowego muszą być zgodne z polityką opisaną w punkcie 6.
5.6	1. Oprogramowanie narzędziowe musi pozwalać na lokalną zmianę firmware licznika (w granicach zapewniających zachowanie zgodności z MID). 2. Proces lokalnej zmiany firmawe licznika nie może trwać dłużej niż 30 minut.
5.7	1. Oprogramowanie narzędziowe musi pozwalać na lokalną zmianę firmware modułu komunikacyjnego. 2. Proces lokalnej zmiany firmware modułu komunikacyjnego nie może trwać dłużej niż 30 minut.
5.8	Oprogramowanie narzędziowe musi posiadać funkcjonalność przechowywania haseł i kluczy w postaci zaszyfrowanej.
5.9	Oprogramowanie narzędziowe musi umożliwiać tworzenie i przywracanie konfiguracji licznika z utworzonej wcześniej kopii zapasowej.
5.10	1. Oprogramowanie narzędziowe musi posiadać zabezpieczenia licencyjne uniemożliwiające instalację bez autoryzacji. 2. Zastosowane klucze licencyjne muszą być autoryzowane podczas każdej (z wyłączeniem upgrade) instalacji oprogramowania. Proces i narzędzia służące do autoryzacji muszą być udostępnione lub przekazane dla Zamawiającego (obsługa tego procesu będzie prowadzona za pośrednictwem Zamawiającego).

	3. Wykonawca wraz z ofertą musi przedstawić sposób realizacji wymagania.
5.11	Klucze licencyjne na oprogramowanie narzędziowe muszą być jednorazowe i generowane na jedną konfigurację sprzętową komputera.
5.12	1. Dostęp do oprogramowania narzędziowego musi być zrealizowany poprzez zastosowanie uwierzytelniania dla kont operatorów. 2. Wykonawca dodatkowo wraz z ofertą musi przedstawić opis sposobu realizacji wymagania oraz dostarczyć wszelkie niezbędne wyposażenie do jego realizacji przez Zamawiającego (m.in. karty, klucze sprzętowe) w ilości określonej przez Zamawiającego.
5.13	Wykonawca musi udostępnić dokumentację w zakresie konfiguracji i procedur aktualizacji oprogramowania narzędziowego.
5.14	1. Oprogramowanie narzędziowe musi umożliwiać przygotowanie plików parametryzacyjnych licznika. 2. Pliki parametryzacyjne ze starszej wersji programu muszą być możliwe do obsłużenia w wersjach nowszych
5.15	Oprogramowanie narzędziowe musi umożliwiać eksport danych pomiarowych, zdarzeń i konfiguracji z liczników do plików tekstowych (TXT, CSV, XML) o udokumentowanej strukturze.
5.16	Oprogramowanie narzędziowe musi być dostarczone w polskiej wersji językowej.
5.17	Oprogramowanie narzędziowe musi wspierać szyfrowanie TLS w wersji zgodnej z wersją TLS w module komunikacyjnym licznika.
5.18	Oprogramowanie narzędziowe musi posiadać możliwość odczytu parametryzacji licznika i zapis jej do pliku, w sposób lokalny i zdalny.
5.19	Oprogramowanie narzędziowe musi umożliwiać ustawienie aktywnego profilu SIM/UICC albo SIM/eUICC.
5.20	Oprogramowanie narzędziowe musi zapewniać odczyt z modułu komunikacyjnego co najmniej następujących informacji: 1. poziom sygnału, 2. adres IP karty SIM, 3. nr IMEI, 4. nr portu TCP/IP.
6.	**Wymagania wobec polityki haseł dla oprogramowania narzędziowego**
6.1	Metody uwierzytelniania dopuszczone do zastosowania: 1. Hasła dostępowe, albo 2. Certyfikaty cyfrowe na kartach mikroprocesorowych, albo 3. Sprzętowe autentykatory haseł jednorazowych.
6.2	Użytkownik musi mieć możliwość samodzielnej zmiany hasła.
6.3	1. Zmiana hasła musi następować na żądanie lub z częstotliwością definiowalną przez Zamawiającego. 2. Zmiana hasła musi być wymuszona przez dostarczone oprogramowanie do obsługi licznika podczas próby uwierzytelnienia.
6.4	Wymagania co do złożoności hasła użytkownika (muszą być wymuszone przez oprogramowanie

	narzędziowe): 1. Co najmniej jedna mała lub wielka litera alfabetu, 2. Co najmniej jeden znak numeryczny, 3. Co najmniej jeden znak specjalny (@,#,$,%,^,&,*,(,_,....), 4. Minimalna długość haseł: 10 znaków.
6.5	Polityka hasła użytkownika (musi być zastosowana w oprogramowaniu narzędziowym): 1. Historia haseł: 5 zapamiętanych haseł, 2. Niemożliwość ustawienia jako nowego hasła jednego z 5 ostatnich haseł zapisanych w historii, 3. Maksymalny okres ważności hasła: 30 dni, 4. Minimalny okres ważności hasła: 2 dni, 5. Hasła muszą być przechowywane w postaci zaszyfrowanej.