Raport z konsultacji dotyczących wymagań dla LZO

Wstęp

Raport został opracowany w oparciu o przeprowadzony proces konsultacji technicznych dotyczących zestawu wymagań cyberbezpieczeństwa dla Liczników Zdalnego Odczytu (LZO), stanowiących kluczowy element infrastruktury AMI (Advanced Metering Infrastructure). Jako punkty końcowe sieci elektroenergetycznej, LZO są klasyfikowane jako urządzenia brzegowe o krytycznym znaczeniu dla bezpieczeństwa dostaw energii i integralności danych rozliczeniowych.

Cel konsultacji

Celem konsultacji była weryfikacja pierwszej wersji wymogów (Załącznik nr 6) przez czołowe organizacje, producentów i dostawców rozwiązań AMI. Analiza zgłoszonych uwag pozwoliła na konfrontację teoretycznych założeń bezpieczeństwa z realiami technologicznymi systemów wbudowanych (embedded), ograniczeniami protokołów komunikacyjnych (DLMS/COSEM) oraz rygorystycznymi wymaganiami metrologicznymi (WELMEC 7.2, dyrektywa MID).

Statystyka zgłoszonych uwag

Proces konsultacji charakteryzował się bardzo wysoką aktywnością podmiotów rynkowych. Na 52 zaproponowane wymogi, do 40 z nich (ponad 76%) zgłoszono co najmniej jedną merytoryczną uwagę. Łącznie przeanalizowano 119 komentarzy.

Metodyka i analiza

W toku prac analitycznych każda uwaga została poddana weryfikacji z intencją bezpieczeństwa oraz nadchodzącymi regulacjami unijnymi (Cyber Resilience Act - CRA, NIS2).

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
1	**SLC-1.1**	Oprócz Producentów wymaganie przedstawienia certyfikatu ISO/IEC 27001 powinno być stosowane do Wykonawców. Jednakże ten certyfikat nie zdejmuje odpowiedzialności z Operatorów Systemów.	Vendor 1	Uwzględniono Wymóg w obecnej formie nakłada obowiązek posiadania certyfikatu na oba podmioty (Producenta i Wykonawcę), co zabezpiecza proces dostaw i konfiguracji.
2	**SLC-1.1**	Zamówienia na LZO zwykle są realizowane jako "Dostawa" i dlatego Wykonawcami często nie są "Producenci", których dotyczy to wymaganie. Natomiast to właśnie Wykonawcy mają kluczową m.in. pod względem bezpieczeństwa rolę w realizacji zamówień. Z tego względu sugerujemy rozszerzenie tego lub dodanie osobnego wymagania dla Wykonawców (a nie tylko Producentów), przykładowo o treści: "Wykonawca musi posiadać i utrzymywać certyfikowany na zgodność z normą ISO/IEC 27001 system zarządzania bezpieczeństwem informacji. Zakres certyfikacji musi jawnie obejmować wdrażanie systemów pomiarowych dla branży energetycznej."	Vendor 6	j.w
3	**SLC-1.1**	Whilst Vendor 2 agree that ISO27001 should be referenced, all elements of ISO27001 should not be mandated. This adds considerable investment to the overall process and approval process for ISO27001 and Vendor 2 believe that the manufacturer should be able to define the elements that are appropriate for their implementation.	Vendor 2	Odrzucono Ze względu na charakter infrastruktury krytycznej, kluczowe elementy Systemu Zarządzania Bezpieczeństwem Informacji muszą być obligatoryjne i zweryfikowane przez stronę trzecią (certyfikację), a nie definiowane wyłącznie przez producenta.
4	**SLC-1.2**	Proces powinien być objęty ISO/IEC 27001	Vendor 1	Wyjaśnienie

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
				Proces jest objęty nadzorem Systemu Zarządzania Bezpieczeństwem Informacji zgodnie z SLC-1.1.
5	**SLC-1.2**	Whilst Vendor 2 has a comprehensive and secure software development lifecycle process, this contains intellectual property that we are not comfortable in sharing outside of Vendor 2. The requirement should be changed to the manufacturer shall confirm it has an SDLC but the complete should not be shared with 3rd parties.	Vendor 2	Uwzględniono Wprowadzono możliwość weryfikacji raportów SAST/DAST i szczegółów SDLC pod NDA lub w trakcie audytu lokalnego, chroniąc IP producenta.
6	**SLC-1.2**	Należy odgórnie ustalić, iż dokumentacje przekazywane w celach weryfikacji muszą być obligatoryjnie objęte umową NDA z dwóch powodów: -a) zwiększenia bezpieczeństwa produktu jak i procesów Dostawcy; -b) zapewnienia poufności co do stosowanych rozwiązań technologicznych.	Vendor 3	j.w
7	**SLC-1.2**	Vendor 4 supports the validation of the manufacturer's SDLC process, but not in a way to contain specific and detailed information on tools used and SDLC SAST/DAST reports, but only the outcomes. Tool information, with SAST/DAST reports can be provided during live audits of the functional testing or on-demand basis, but not as part of standard release documentation. As per CRA requirements, manufacturers must produce HW or SW products without known vulnerabilities and providing an outcome of SAST/DAST addresses this requirement.	Vendor 4	j.w.
8	**SLC-1.2**	Proponujemy jako kryterium weryfikacji określenie certyfikacji ISO/IEC 27001, analogicznie do punktu SLC-1.1. Pozwoli to na ocenę przez akredytowaną i niezależną jednostkę certyfikującą. Zapewni to	Vendor 5	Odrzucono Samo ISO 27001 nie zastępuje

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		także transparentność pochodzenia technologii i odpowiedzialności za tworzenie oprogramowania.		weryfikacji technicznej artefaktów takich jak SBOM.
9	**SLC-1.2**	Wymaganie jest zasadne, jednak kosztowne do wprowadzenia oraz co ważniejsze - czasochłonne/trudne w przypadku istniejących rozwiązań. Dlatego też sugerujemy odpowiednio długie "vacatio legis" dla tego wymagania, aby producenci mieli czas na przygotowanie i wprowadzenie opisanych procesów i raportowania.	Vendor 6	Informacja Przyjęto do wiadomości potrzebę vacatio legis
10	**SLC-1.3**	Proces powinien być objęty ISO/IEC 27001	Vendor 1	Wyjaśnienie ISO 27001 jest wymogiem zarządzania bezpieczeństwem informacji w organizacji, a SLC-1.3 jest wymogiem technicznym – są komplementarne.
11	**SLC-1.3**	Vendor 2 believes that the requirement should be changed to specify that manufacturers should use a secure coding standard and that should be referenced in any submittals. However, the requirement should not specify the coding standards that can be used	Vendor 2	Uwzględniono Podkreślono, że standardy są przykładami, a producent ma swobodę w doborze konkretnej metodyki, o ile jest ona uznanym standardem.
12	**SLC-1.3**	Proponujemy jako kryterium weryfikacji określenie certyfikacji ISO/IEC 27001, analogicznie do punktu SLC-1.1. Pozwoli to na ocenę przez akredytowaną i niezależną jednostkę certyfikującą	Vendor 5	Wyjaśnienie ISO 27001 jest wymogiem zarządzania bezpieczeństwem informacji w organizacji, a SLC-1.3 jest wymogiem technicznym – są komplementarne.
13	**SLC-1.3**	Wymaganie jest zasadne, jednak kosztowne do wprowadzenia oraz co ważniejsze - czasochłonne/trudne w przypadku istniejących rozwiązań. Dlatego też sugerujemy odpowiednio długie "vacatio legis" dla tego	Vendor 6	Informacja

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		wymagania, aby producenci mieli czas na przygotowanie i wprowadzenie opisanych procesów i raportowania.		Przyjęto do wiadomości potrzebę vacatio legis
14	**SLC-1.4**	Proces powinien być objęty ISO/IEC 27001. Uwaga - weryfikacja powinna następować w oparciu o konkretny komponent i jego właściwości. Nie wszystkie komponenty mogą być weryfikowane w sposób przykładowo wylistowany, tj. sprawdzanie sum kontrolnych, podpisów cyfrowych.	Vendor 1	<u>Uwzględniono</u> Doprecyzowano, że HBOM dotyczy tylko elementów z logiką cyfrową.
15	**SLC-1.4**	Na dzień dzisiejszy nie ma 100% mechanizmów potrafiących zapewnić autentyczność dostarczanych komponentów sprzętowych. Szacuje się, że rynek elektroniki ponosi straty 100 mld USD rocznie spowodowane obrotem podrabianymi elementami. Przede wszystkim w komponenty należy zaopatrywać się albo wprost u producentów komponentów OEM albo u autoryzowanych dystrybutorów z tzw. pierwszej ręki. np. na rynku polskim Arrow, AVNet, RS Components, Farnell, TME, którzy z kolei muszą zapewnić pełne traceability komponentów wraz ze źródłem pochodzenia. Nie wszystkie komponenty da się też poprawnie oznakować choćby w celu identyfikacji wizualnej ze względu na coraz mniejsze gabaryty obudów komponentów. Odgórnie można wręcz zakazać unikania brokerów, którzy handlują komponentami z niewiadomych źródeł lub też komponentami „starymi" np. z rokiem produkcji sprzed kilku lat. Należy odgórnie ustalić, iż dokumentacje SBOM, HBOM przekazywane w celach weryfikacji muszą być obligatoryjnie objęte umową NDA z dwóch powodów: -a) zwiększenia bezpieczeństwa produktu; -b) zapewnienia poufności co do stosowanych rozwiązań technologicznych.	Vendor 3	<u>Uwzględniono</u> Wprowadzono wymóg NDA. <u>Wyjaśnienie</u> Aspekt identyfikowalności jest w wymogu adresowany.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
16	**SLC-1.4**	Czy w punkcie dotyczącym HBOM można doprecyzować, że chodzi o HBOM w zakresie komponentów zawierających elementy cyfrowe (w odróżnieniu od komponentów "hardware", do których zaliczają się także rezystory i kondensatory)? Proponujemy jako kryterium weryfikacji procesu certyfikację ISO/IEC 27001, analogicznie do punktu SLC-1.1, co umożliwi ocenę przez akredytowaną jednostkę certyfikującą.	Vendor 5	Uwzględniono Doprecyzowano, że HBOM dotyczy tylko elementów z logiką cyfrową.
17	**SLC-1.5**	W przypadku wprowadzenia wymagania dodatkowych audytów w tak kluczowym obszarze, jak software development, mogą być one problematyczne dla producentów ze względu na ochronę tajemnicy przedsiębiorstwa. Sugerujemy zatem przeprowadzanie wspomnianych audytów jedynie lokalnie, w siedzibie producenta, zgodnie z zasadami ochrony informacji, jakie są stosowane - chociazby ze względu na ISO 27001 wymagane w punkcie pierwszym.	Vendor 1	Uwzględniono Doprecyzowano, że audyt odbywa się lokalnie, pod NDA i przez wykwalifikowany personel, co chroni tajemnice producenta.
18	**SLC-1.5**	Skoro Producent zgodnie z SLC-1.1 musi posiadać Certyfikowany System Zarządzania Bezpieczeństwem Informacji zgodnie z ISO/IEC 27001 to zgodnie z zasadą nadrzędności certyfikatu podlega on regularnemu nadzorowi, stanowi niezależne, obiektywne i formalnie uznawane potwierdzenie spełnienia wymagań systemu zarządzania bezpieczeństwem informacji. W przypadku konieczności dopuszczenia OSD (lub wskazanej przez OSD strony trzeciej) do audytu zewnętrznego należy zapewnić podpisanie stosownych umów NDA oraz zapewnić, iż osoby przeprowadzające audyt będą posiadały min. Certyfikat Lead Auditor ISO/IEC 27001 oraz doświadczenie w audytach Systemów Zarządzania Bezpieczeństwem Informacji.	Vendor 3	j.w.
19	**SLC-1.5**	W przypadku wprowadzenia wymagania dodatkowych audytów w tak kluczowym obszarze, jak software development, mogą być one problematyczne dla producentów ze względu na ochronę tajemnicy	Vendor 5	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		przedsiębiorstwa. Sugerujemy zatem przeprowadzanie wspomnianych audytów jedynie lokalnie, w siedzibie producenta, zgodnie z zasadami ochrony informacji, jakie są stosowane - chociazby ze względu na ISO 27001 wymagane w punkcie pierwszym.		
20	**SLC-1.5**	W przypadku wprowadzenia wymagania dodatkowych audytów w tak kluczowym obszarze, jak software development, mogą być one problematyczne dla producentów ze względu na ochronę tajemnicy przedsiębiorstwa. Sugerujemy zatem przeprowadzanie wspomnianych audytów jedynie lokalnie, w siedzibie producenta, zgodnie z zasadami ochrony informacji, jakie są stosowane - chociażby ze względu na ISO 27001 wymagane w punkcie SLC-1.1 lub alternatywnie o weryfikację spełnienia tego wymagania na podstawie zakresu posiadanej przez producenta certyfikacji ISO 27001, gdzie proces powinien być ujęty.	Vendor 6	j.w.
21	**SLC-2.1**	Należy zapewnić Producentom odpowiedni czas na wdrożenie wymagania.	Vendor 1	<u>Informacja</u> Przyjęto do wiadomości potrzebę
22	**SLC-2.1**	Vendor 2 believes that the use of specific hardware for storing the manufacturers key should not be mandated. This not only adds additional cost to the product but also impacts on the overall design of the product. Far more cost-effective methods are available that can be used as an alternative and offer the same level of security.	Vendor 2	<u>Uwzględniono</u> Wyjaśniono, że dopuszczalne są rozwiązania zintegrowane w MCU (np. TrustZone).
23	**SLC-2.1**	Z racji, iż wymogi dotyczą licznika energii elektrycznej, który de facto powinien pracować praktycznie w czasie rzeczywistym, to urządzenie powinno uruchamiać się z ostatnią poprawną wersją oprogramowania. Nie powinno dojść do sytuacji, gdy urządzenie nie wystartuje i przejdzie w stan błędu, powinno po prostu zablokować taki start i powrócić do poprzedniej wersji oprogramowania.	Vendor 3	<u>Uwzględniono</u> Dodano odniesienia do wymogów opisujących procedurę bezpiecznego rozruchu.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		Wymóg praktycznie powiązany z punktem SLC-3.1. – Proponuje się scalić te dwa punkty w jeden.		
24	**SLC-2.1**	Należy zapewnić Producentom odpowiedni czas na wdrożenie tego wymagania.	Vendor 5	Informacja Przyjęto do wiadomości potrzebę
25	**SLC-2.1**	Wprowadzenie zaufanego elementu sprzętowego w LZO oznacza zwykle konieczność istotnej zmiany hardware i firmware obecnie wdrażanych liczników. Sugerujemy odpowiednio długie "vacatio legis" dla tego wymagania, aby producenci mieli czas na przygotowanie i wprowadzenie opisanej zmiany.	Vendor 6	Uwzględniono Wyjaśniono, że dopuszczalne są rozwiązania zintegrowane w MCU (np. TrustZone).
26	**SLC-3.1**	Proponuje się scalenie z punktem SLC-2.1	Vendor 3	Odrzucono Pozostawiono wymogi w rozdzielnej postaci, ze względu na ich odmienną charakterystykę. SLC-2.1 koncentruje się na wbudowanym, zaufanym elemencie sprzętowym, natomiast SLC-3.1 adresuje metodę uwierzytelniania oraz weryfikacji integralności w zakresie aktualizacji oprogramowania układowego.
27	**SLC-3.2**	Proponujemy dopuszczenie możliwości instalacji wersji poprzedniej firmware, jeżeli dany OSD dopuszcza (a nawet oczekuje) takiej możliwości ze względu na specyfikę sieci liczników energii elektrycznej. Uzasadnienie: 1. Standardowym wymaganiem OSD w przetargach jest dostarczenie wraz z wzorcami liczników dodatkowo 2 wersji firmware "N" oraz "N-1", gdzie "N-1" to wersja poprzednia względem "N", celem weryfikacji oczekiwanego przez OSD mechanizmu przywracania	Vendor 5	Uwzględniono Wprowadzono wyjątek pozwalający OSD na wymuszenie downgrade'u w sytuacjach awaryjnych.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		poprzedniej wersji firmware. 2. Po wprowadzeniu "zakazu downgrade'u", w przypadku aktualizacji FW na wersję zawierającą błąd, wykonanej po kilku latach od sprzedaży liczników, OSD będzie chciał przywrócić liczniki do poprawnego działania de facto downgrade'ując FW (do wersji bezbłędnej). OSD zwróci się do producenta o rekompilację poprzedniego FW z numerem wersji większym. Taka rekompilacja FW po kilku latach może być niemożliwa do realizacji (np. stary toolchain nie działa na nowym systemie oper. itp.). Prosimy zwrócić uwagę, że liczniki są częścią infrastruktury krytycznej, OSD muszą zapewnić ciągłość jej działania. W wielu dziedzinach informatyki "pliki aktualizacyjne" są publicznie dostępne. W licznikach energii tak nie jest.		
28	**SLC-3.2**	Sugerujemy dopuszczenie możliwości aktualizacji do wersji poprzedniej firmware, jeżeli OSD zdecyduje się takie wymaganie postawić w danym postępowaniu zakupowym.	Vendor 6	j.w.
29	**SLC-3.3**	Ze względu na wyodrębnione 3 kroki procesu aktualizacji oprogramowania w protokole DLMS zaleca się modyfikację tego punktu, w celu dodatkowego zabezpieczenia procesu: W kroku 1 wykonuje się sam transfer obrazu oprogramowania do licznika. W kroku 2 dokonuje się jego walidacji (sprawdza się zgodność podpisów, sumy kontrolne oraz poprawność zapisu do pamięci) i wyzwala proces aktywacji W kroku 3 dochodzi do fizycznej wymiany oprogramowania w mikrokontrolerze, proces ten może być (a nawet musi) nadzorowany przez bootloader. Jeżeli w tym kroku nastąpi np. zanik zasilania lub zakłócenie przepisania oprogramowania to oprogramowanie	Vendor 3	<u>Uwzględniono</u> Wprowadzono zmiany w wymogu. Ilość prób nie jest regulowana tym wymogiem.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		nadzorujące (np. bootloader) powinno zapewnić kilkukrotną próbę wgrania nowego oprogramowania (np. 3-krotną) przed powróceniem do wersji poprzedniej. Dzięki temu zapewnione zostanie podstawowe bezpieczeństwo na niespodziewane zdarzenia np. na zaniki zasilania. Zalecamy zatem zmianę opisu z „automatycznego powrotu po nieudanej próbie” do „automatycznego powrotu po nieudanych kilku kolejnych próbach”.		
30	**SLC-3.3**	Restoring previous version in case of a failed FW update (e.g. by interrupting power during FW update process) is not the only possible way to mitigate this case. We propose that Fit criterion would be adjusted to not force only one possible solution, but instead other secure update scenarios: Simulation of a failed update (e.g., by interrupting power during it) must not lead to permanent damage to the device. Device must implement a solution to be resilient to those unforeseen problems by either automatically restore the software version, running before the FW update or retry to update the FW again. The device will record this event in the event log if software restore was performed.	Vendor 4	<u>Uwzględniono</u> Wprowadzono zmiany w wymogu. Nie określa się sposobu działania tylko efekt.
31	**SLC-3.3**	Idea wymagania jest słuszna, chociaż w przypadku nieudanej aktualizacji LZO, to urządzenie nie będzie w "nowszej wersji oprogramowania", więc i nie będzie miało skąd wykonywać mechanizmu bezpiecznego powrotu. Nieudana aktualizacja oznacza, że się po prostu nie wykonała.	Vendor 6	<u>Uwzględniono</u> Wprowadzono zmiany w treści wymogu.
32	**SLC-3.3**	Wymaganie powinno być zmienione, ponieważ "Urządzenie" należy rozumieć jako licznik (LZO), który umożliwia zarządzanie uprawnieniami zgodnie ze standardem dlms/cosem. Zewnętrzny KMS jest połączony z systemu HES, a nie bezpośrednio z licznikiem LZO.	Vendor 7	<u>Wyjaśnienie</u> W wymogu wprowadzono zmiany. Wymóg dotyczy odporności logicznej urządzenia na błędy procesu, niezależnie od roli systemów zewnętrznych.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
33	**SLC-3.4**	Liczniki energii elektrycznej w większości przypadków nie mają architektury oprogramowania takiej jak np. routery czy koncentratory, czyli opartej na systemie operacyjnym z powłoką, aplikacjami, bibliotekami i systemem plików. Wykorzystywane systemy operacyjne są bardzo proste, a firmware ma charakter monolityczny, podzielony na kilka części. Stąd wymaganie to należy przeformułować. Wymagana powinna być wymiana oprogramowania w zakresie funkcjonalnym, w tym obejmującym funkcje kryptograficzne i aplikacyjne.	Vendor 1	Uwzględniono Przeformułowano wymóg tak, aby nie wymuszał dynamicznej modułowości (DLL), a skupiał się na możliwości aktualizacji funkcji w ramach obrazu monolitycznego.
34	**SLC-3.4**	Z opisu budowy oprogramowania pomysłodawca zakłada, że budowa oprogramowania licznika oparta jest na systemie typu GPOS stosowanych na systemach mikroprocesorowych. Systemy te charakteryzują się obecnością MMU i dzięki temu umożliwiają one taką organizację oprogramowania np. dzięki procesom w osobnych przestrzeniach, bibliotekom ładowanym dynamicznie itp. Natomiast w realnym wykonaniu, oprogramowanie licznika w dzisiejszych czasach ze względu na koszty, wymogi związane z wyższymi wymogami EMC (dla urządzeń tej klasy) oraz konieczność działania w trybie rzeczywistym z gwarantowanymi opóźnieniami wykonywane są praktycznie jedynie na mikrokontrolerach np. rodziny ARM, które wykonuje się albo pod kontrolą prostego systemu czasu rzeczywistego RTOS dopasowanego do zasobów danego mikrokontrolera albo w oparciu o całe własne dedykowane oprogramowanie z własną maszyną stanów. Oprogramowanie na mikrokontrolery charakteryzuje się tym, iż nie posiada izolowanych procesów działając na wspólnej przestrzeni adresowej z kodem linkowanym statycznie, tym samym nie ma technicznej możliwości modułowej budowy oprogramowania w proponowanym zakresie. W tym przypadku jedyne rozsądne podejście to rozbicie oprogramowania na dwa rodzaje: bootloader oraz oprogramowanie główne, które zawiera w sobie niezbędne funkcjonalności i zawsze jest ładowane pod ten sam adres startowy. Tym	Vendor 3	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		samym możemy rozróżnić dwa moduły. Większa fragmentacja ze względów technicznych i kosztowych nie jest tutaj zalecana. Oczywiście mowa tutaj o programach wykonywalnych ładowanych do mikrokontrolera, a nie o podziale kodów źródłowych, który zwykle posiada odpowiednio wydzielone moduły funkcjonalne. Należy pamiętać o odgórnie ustalonej w WELMEC Guide 7.2 (przywołanym w MID) zasadzie ograniczonej ilości aktualizacji oprogramowania. Po osiągnięciu założonego progu ilości aktualizacji aktualizacja urządzenia ma być niemożliwa w warunkach terenowych, dopiero wyzerowania logu aktualizacji w warunkach laboratoryjnych po fizycznej ingerencji w licznik, może ponownie umożliwić aktualizację oprogramowania.		
35	**SLC-3.4**	Liczniki energii elektrycznej w większości przypadków nie mają architektury oprogramowania takiej jak np. routery czy koncentratory, czyli opartej na systemie operacyjnym z powłoką, aplikacjami, bibliotekami i systemem plików. Wykorzystywane systemy operacyjne są bardzo proste, a firmware licznika podzielony jest na przykład na 2 monolityczne części, zgodnie z obowiązującą w Jednostkach Notyfikowanych praktyką implementacji Dyrektywy MID w zakresie firmware'u licznika, tj. WELMEC Guide 7.2. Wymagana powinna być wymiana oprogramowania w zakresie obejmującym funkcje kryptograficzne i aplikacyjne.	Vendor 5	j.w.
36	**SLC-3.4**	Wymaganie dotyczy urządzeń, które posiadają wymienione komponenty (system operacyjny, biblioteki kryptograficzne, stos komunikacyjny, logika aplikacyjna), czyli np. koncentratory danych czy routery. LZO działają w oparciu o jeden, "monolityczny", skompilowany obraz firmware i nie dają możliwości osobnej aktualizacji wybranych	Vendor 6	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		komponentów. Dodatkowo, jest prawnie zabroniona aktualizacja oprogramowania "metrologicznego" w liczniku wprowadzonym do obrotu. Sugerujemy zatem doprecyzowanie wymagania, że: "Dotyczy urządzeń, które działają w oparciu o system operacyjny i osobne komponenty software'owe".		
37	**SLC-4.1**	Definicja ram czasowych w przypadku liczników energii nie może zostać sztywno ustalona m.in. ze względów na konieczności uzyskania certyfikacji w instytucjach zewnętrznych, np. w JN, na które Producent licznika nie ma wpływu. Należy pamiętać, że licznik energii w odróżnieniu od niektórych urządzeń innej klasy podlega dodatkowym regulacjom.	Vendor 3	Uwzględniono Dodano zapis o uwzględnieniu czasu procesów zewnętrznych (JN) w ramach SLA.
38	**SLC-5.1**	W jaki sposób ma się odbywać przekazanie danych inicjalizacyjnych urządzenia do użytkownika końcowego dla każdej sztuki licznika dla każdego z interfejsów. Jakie środki bezpieczeństwa mają zostać zachowane. Wymóg dostarczenia szczegółowej “dokumentacji środków kontroli logicznej do linii produkcyjnej” w ramach np. Postępowań przetargowych jest ryzykowny , ponieważ zawiera informacje o architekturze sieci wewnętrznej i systemach bezpieczeństwa producenta. Weryfikacja powinna się odbywać wyłącznie za pośrednictwem audytu lokalnego np. w ramach audytów opisanych w punkcie SLC-5.1 lub poprzez uznanie certyfikacji ISO/IEC 27001 z punktu SLC-1.1 za wystarczający dowód zabezpieczenia środowiska produkcyjnego. Znane są nam przypadki, gdy dokumentacja z procesu postępowania zakupowego OSD została przesłana niezaszyfrowaną drogą e-mailową do niewłaściwego adresata poczty elektronicznej.	Vendor 3	Odrzucono Wymóg dotyczy bezpieczeństwa procesu inicjalizacji jako etapu krytycznego dla integralności tożsamości kryptograficznej każdego urządzenia. Ryzyko ujawnienia dokumentacji w toku postępowania przetargowego nie uzasadnia obniżenia wymagań bezpieczeństwa, lecz wskazuje na konieczność wdrożenia przez zamawiającego odpowiednich procedur ochrony informacji wrażliwych na etapie postępowania.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		Proszę spojrzeć na uwagi do punktu ACC-4.1.		
39	**SLC-6.1**	Wymaganie w tej postaci jest niemożliwe do spełnienia. Ze względu na nieprzewidywalny rozwój zagrożeń bezpieczeństwa, algorytmów kryptograficznych, podatności sprzętowych oraz regulacji prawnych, nie jest możliwe rzetelne zaplanowanie wystarczających zasobów sprzętowych i architektury oprogramowania związanych z bezpieczeństwem w horyzoncie 15-20 lat szczególnie, że funkcje kryptograficzne na tak małych platformach bazują na wsparciu sprzętowym, zależnym od obecnie dostępnych na rynku mikrokontrolerów, nie przewidywanych do stosowania przez 15-20 lat. Nieprzewidywalność tego rozwoju potwierdza historia ewolucji wielu urządzeń cyfrowych (np. smartfony - iPhone został wprowadzaony na rynek w 2007 roku). Konieczne jest zawężenie wymagania i ścisłe określenie, jakie funkcje są wymagane do spełnienia w przyszłości (np. AES-256, Security Suite 2), albo określenie wolnych zasobów do wykorzystania w przyszłości (np. procent niewykorzystanego czasu procesora lub pamięci). W innym przypadku wymaganie należy usunąć.	Vendor 1	<u>Uwzględniono</u> Skonkretyzowano wymóg poprzez określenie minimalnej rezerwy (15%) i celu (SS2), co czyni wymóg mierzalnym.
40	**SLC-6.1**	Whilst Vendor 2 make every effort to provide sufficient resource to support future needs, due to advances in technology over the next 15 – 20 years we cannot guarantee that the current meter design cannot support any potential update. For the reference, meters in Poland are specified as having a 12-year lifetime	Vendor 2	j.w.
41	**SLC-6.1**	Odniesienie do budowy oprogramowania jak w SLC-3.4, na tę chwilę brak relatywnie technicznych możliwości budowy oprogramowania w wersji modułowej na mikrokontrolery.	Vendor 3	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		Obecny okres 12 lat od nałożenia cech oceny zgodności to dość długi okres i tym samym precyzyjne i jednoznaczne określenie przyszłej odporności kryptograficznej nie jest możliwe z przyczyn obiektywnych, biorąc pod uwagę dzisiejszy rozwój techniki i mocy obliczeniowych, a także potencjalnego rozwoju komputerów kwantowych trudno jest określić jakie będą wystarczające zasoby o ile w ogóle budowa licznika na mikrokontrolerach będzie nadal możliwa w sposób bezpieczny przy oferowanych przez niego zasobach. Jedynym realnym podejściem wydaje się być pozostawienie pewnych rezerw pamięci i mocy obliczeniowej np. 10% oraz ewentualne umożliwienie przyszłego zmniejszenia funkcjonalności licznika poprzez wymianę FW w celu wygospodarowania dodatkowych zasobów na platformie sprzętowej. Próba zagwarantowania pełnej kompatybilności z nieznanymi przyszłymi standardami kryptograficznymi prowadziłaby do nierzetelnych deklaracji projektowych, które nie mogą być technicznie zweryfikowane. Jednocześnie nie jest możliwe i nie jest uzasadnione deklarowanie zdolności obsługi nieokreślonych przyszłych algorytmów kryptograficznych w horyzoncie kilkunastu lat, gdyż wykracza to poza możliwości techniczne platformy oraz poza aktualny stan wiedzy.		
42	**SLC-6.1**	Ze względu na nieprzewidywalny rozwój zagrożeń bezpieczeństwa, algorytmów kryptograficznych, podatności sprzętowych oraz regulacji prawnych, nie jest możliwe rzetelne zaplanowanie wystarczających zasobów sprzętowych i architektury oprogramowania związanych z bezpieczeństwem w horyzoncie 15-20 lat szczególnie, że funkcje kryptograficzne na tak małych platformach bazują na wsparciu sprzętowym, zależnym od obecnie dostępnych na rynku mikrokontrolerów, nie przewiduwanych do stosowania na 15-20 lat Nieprzewidywalność tego rozwoju potwierdza historia ewolucji wielu	Vendor 5	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		urządzeń cyfrowych (np. smartfony - iPhone został wprowadzaony na rynek w 2007 roku). Dodatkowym przykładem jest rozwój specyfikacji DLMS w zakresie bezpieczeństwa (Security Suite 1 i 2 pojawił się dopiero w edycji 8 Green Book z 2014r.). Stosowanie platform, których koszt jest wielokrotnie wyższy, nie ma uzasadnienia ekonomicznego, a przedsiębiorstwa prowadzące ostrożniejszą politykę inwestycyjną ponoszą nieproporcjonalnie większe wydatki. Prosimy również o uwzględnienie uwag z pkt. SLC-3.4 dot. monolityczności firmware.		
43	**SLC-6.1**	W celu określenia rezerwy mocy obliczeniowej i pamięci potrzebne jest precyzyjne określenie na co ma być gotowa ta rezerwa. Sugerujemy zatem obligatoryjne umieszczenie w wymaganiu takich przykładów, np. wspomnianych mechanizmów Security Suite 1 i 2 dla protokołu DLMS.	Vendor 6	j.w.
44	**CRY-1.1**			<u>Nie zmieniono zapisu</u> Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
45	**CRY-1.2**	Wymaganie w tej postaci jest niemożliwe do spełnienia. Ze względu na nieprzewidywalny rozwój zagrożeń bezpieczeństwa, algorytmów kryptograficznych, podatności sprzętowych oraz regulacji prawnych, nie jest możliwe rzetelne zaplanowanie wystarczających zasobów sprzętowych i architektury oprogramowania związanych z bezpieczeństwem w horyzoncie 15-20 lat szczególnie, że funkcje kryptograficzne na tak małych platformach bazują na wsparciu sprzętowym, zależnym od obecnie dostępnych na rynku mikrokontrolerów, nie przewidywanych do stosowania przez 15-20 lat.	Vendor 1	<u>Uwzględniono</u> Uwzględniono, że w przypadku systemów monolitycznych aktualizacja mechanizmów następuje poprzez wymianę całego obrazu firmware, a nie pojedynczych plików bibliotek. Odniesiono się do realiów architektury mikrokontrolerów, usuwając wymóg

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		Nieprzewidywalność tego rozwoju potwierdza historia ewolucji wielu urządzeń cyfrowych (np. smartfony - iPhone został wprowadzony na rynek w 2007 roku). Konieczne jest zawężenie wymagania i ścisłe określenie, jakie funkcje są wymagane do spełnienia w przyszłości (np. AES-256, Security Suite 2), albo określenie wolnych zasobów do wykorzystania w przyszłości (np. procent niewykorzystanego czasu procesora lub pamięci). W innym przypadku wymaganie należy usunąć. Dodatkowo, liczniki energii elektrycznej w większości przypadków nie mają architektury oprogramowania takiej jak np. routery czy koncentratory, czyli opartej na systemie operacyjnym z aplikacjami i bibliotekami i systemem plików. Wykorzystywane systemy operacyjne są bardzo proste, a firmware ma charakter monolityczny, podzielony na kilka części. Stąd wymaganie związane z modułami/bibliotekami kryptograficznymi należy przeformułować. Wymagana powinna być wymiana oprogramowania obejmująca funkcje kryptograficzne.		"modułowości" w sensie systemowym (dynamicznym) na rzecz funkcjonalnym.
46	**CRY-1.2**	Odniesienie do budowy oprogramowania jak w SLC-3.4, na tę chwilę brak relatywnie technicznych możliwości budowy oprogramowania w wersji modułowej na mikrokontrolery.	Vendor 3	j.w.
47	**CRY-1.2**	Ze względu na nieprzewidywalny rozwój zagrożeń bezpieczeństwa, algorytmów kryptograficznych, podatności sprzętowych oraz regulacji prawnych, nie jest możliwe rzetelne zaplanowanie architektury oprogramowania związanych z bezpieczeństwem w horyzoncie 15-20 lat. Architektura, która jest wystarczająca na dzisiaj, prawdopodobnie okaże się niewystarczająca w perspektywie 15-20 lat szczególnie, że funkcje kryptograficzne na tak małych platformach bazują na wsparciu sprzętowym, zależnym od szczególnie, że funkcje kryptograficzne na tak małych platformach bazują na wsparciu sprzętowym, zależnym od obecnie dostępnych na rynku mikrokontrolerów, nie	Vendor 5	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		przewiduwanych do stosowania na 15-20 lat. Prosimy również o uwzględnienie uwag z pkt. SLC-3.4 dot. monolityczności firmware.		
48	**CRY-1.2**	Wymaganie można postawić dla urządzeń, które posiadają wymienione komponenty (system operacyjny, biblioteki kryptograficzne, stos komunikacyjny, logika aplikacyjna), czyli np. koncentratory danych czy routery. LZO działają w oparciu o jeden, "monolityczny", skompilowany obraz firmware i nie dają możliwości osobnej aktualizacji wybranych komponentów. Dodatkowo, jest prawnie zabroniona aktualizacja oprogramowania "metrologicznego" w liczniku wprowadzonym do obrotu. Sugerujemy zatem doprecyzowanie wymagania, że "Dotyczy urządzeń, które działają w oparciu o system operacyjny i osobne komponenty software'owe".	Vendor 6	j.w.
49	**CRY-2.1**	Proponujemy usunięcie testów statystycznych, ponieważ ze względu na architekturę firmware licznika może być to niemożliwe do przeprowadzenia, również ze względu na ochronę własności intelektualnej Producenta i konieczność udostępniania środowiska developerskiego.	Vendor 1	<u>Uwzględniono</u> Zrezygnowano z przeprowadzania testów statystycznych entropii na gotowym urządzeniu, które są trudne do realizacji w warunkach produkcyjnych. Zamiast tego postawiono na weryfikację dokumentacji platformy sprzętowej (MCU) oraz deklarację producenta dotyczącą wykorzystania TRNG w procesach kryptograficznych.
50	**CRY-2.1**	Proponujemy, aby kryterium weryfikacji opierało się na sprawdzeniu, czy wymieniona w HBOM platforma sprzętowa posiada określony wymaganiem RNG oraz deklarację producenta, że jest on wykorzystywany przy wymagających tego operacjach kryptograficznych.	Vendor 5	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		Uzasadnienie: w praktyce odróżnienie RNG od PRNG jest trudne bez długotrwałych testów.		
51	**CRY-2.1**	Proponujemy, aby kryterium weryfikacji opierało się na sprawdzeniu, czy wymieniona w HBOM platforma sprzętowa posiada określony wymaganiem RNG oraz deklarację producenta, że jest on wykorzystywany przy wymagających tego operacjach kryptograficznych. W praktyce odróżnienie RNG od PRNG jest trudne bez długotrwałych testów.	Vendor 6	j.w.
52	**CRY-3.1**	Analogicznie jak w SLC-5.1: W jaki sposób ma się odbywać przekazanie danych inicjalizacyjnych urządzenia do użytkownika końcowego dla każdej sztuki licznika dla każdego z interfejsów. Jakie środki bezpieczeństwa mają zostać zachowane.	Vendor 3	Odrzucono Pytania dotyczące sposobu przekazania danych inicjalizacyjnych użytkownikowi końcowemu są kwestią proceduralną i logistyczną, która nie stanowi przesłanki do modyfikacji wymagania o charakterze fundamentalnym dla bezpieczeństwa kryptograficznego liczników. Zasada unikalności kluczy jest absolutnym minimum bezpieczeństwa w systemach rozproszonych i nie podlega kompromisowi niezależnie od złożoności jej wdrożenia.
53	**CRY-3.2**	Prosimy o doprecyzowanie czy sformułowanie "bezpieczne usuwanie" kluczy, dotyczy tylko tymczasowych kluczy oraz zmienionych (starych) kluczy po wymianie na nowe? Usunięcie kluczy obowiązujących w liczniku spowoduje utratę dostępu do urządzenia.	Vendor 1	Uwzględniono Doprecyzowano pojęcie "bezpiecznego usuwania" – dotyczy ono kluczy tymczasowych (RAM) oraz starych kluczy, które zostały zastąpione nowymi w procesie rotacji.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
54	**CRY-3.2**	Jak często (regularnie) klucze powinny być zmieniane. Zakładając, że OSD posiada na swoim terenie 5 milionów liczników, z którego każdy posiada 3 interfejsy i do każdego interfejsu przypisane są 3 klucze (autentykacji, szyfrujący i master) z prostego rachunku wychodzi, że każdorazowo, cyklicznie, wymianie powinno podlegać 15 milionów kluczy, które oprócz tego, że muszą zostać wymienione w samych licznika to będą musiały także podlegać wymianie we wszystkich systemach do obsługi liczników. Co więcej, każdorazowa pomyłka, czy błąd ludzki, czy błąd systemu (np. zapis niepoprawnych kluczy itp.) może spowodować, że utracony zostanie bezpowrotnie dostęp do interfejsów licznika. Należy także pamiętać, że w celu zapewnienia wymogów z punktów CRY-3.1 dotyczących unikalności kluczy pomiędzy licznikami każdorazowa akcji wymiany kluczy będzie ze sobą niosła dość duże nakłady czasowe.	Vendor 3	<u>Wyjaśnienie</u> Skala rotacji kluczy (np. 15 mln) jest wyzwaniem dla systemów nadrzędnych OSD (HES/KMS), jednak licznik musi technicznie wspierać taką operację, aby umożliwić realizację polityk bezpieczeństwa (np. wynikających z Cyber Resilience Act).
55	**CRY-3.2**	Prosimy o doprecyzowanie czy sformułowanie "bezpieczne usuwanie" kluczy, dotyczy tylko tymczasowych kluczy oraz zmienionych (starych) kluczy po wymianie na nowe? Usunięcie kluczy obowiązujących w liczniku spowoduje utratę dostępu do urządzenia.	Vendor 5	<u>Uwzględniono</u> Doprecyzowano pojęcie "bezpiecznego usuwania" – dotyczy ono kluczy tymczasowych (RAM) oraz starych kluczy, które zostały zastąpione nowymi w procesie rotacji.
56	**CRY-3.2**	Sugerujemy doprecyzowanie sformułowania o "bezpiecznym usuwaniu" kluczy, że dotyczy tylko tymczasowych kluczy oraz zmienionych (starych) kluczy po wymianie na nowe. Usunięcie kluczy obowiązujących w liczniku spowoduje utratę dostępu do urządzenia.	Vendor 6	j.w.
57	**CRY-3.3**	Wymaganie należy zmienić: "Urządzenie" należy rozumieć jako licznik (LZO). Zewnętrzny KMS jest połączony z systemem HES, a nie bezpośrednio z licznikiem LZO. Sama funkcjonalność licznika umożliwia	Vendor 1	<u>Uwzględniono</u> Zmieniono przykłady protokołów (usunięto SCEP/EST jako nieadekwatne

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		natomiast zarządzanie kluczami zgodnie z funkcjami przewidzianymi w standardzie DLMS/COSEM.		dla LZO) na rzecz mechanizmów specyficznych dla DLMS/COSEM (Security Suite). Wyjaśniono, że wymóg dotyczy zdolności licznika do współpracy w procesie KMS, a nie samej komunikacji licznika bezpośrednio z systemem KMS.
58	**CRY-3.3**	Whilst Vendor 2 agree on principles and benefits of KMS system application, Vendor 2 would strongly recommend that the KMS is provided by a third party, not associated with a specific meter manufacturer. Choosing an open standard/system supplier will not affect future tender competitiveness and removes the potential risk of sourcing a proprietary solution. Such closed solution greatly restricts the ability to migrate to an alternative solution.	Vendor 2	Nie uwzględniono Nie stoi to w sprzeczności z wymogiem.
59	**CRY-3.3**	Już w punkcie CRY-3.2 zdefiniowano, że wymiana kluczy odbywać się będzie w protokole DLMS, zatem ten punkt wydaje się bezzasadny i przeczy punktowi CRY-3.2. Jak nawet widać w opisie punkt CRY-3.3 dotyczy systemu centralnego a nie LZO i nie powinno stanowić wpisu w wymogach do LZO.	Vendor 3	Uwzględniono Zmieniono przykłady protokołów (usunięto SCEP/EST jako nieadekwatne dla LZO) na rzecz mechanizmów specyficznych dla DLMS/COSEM (Security Suite). Wyjaśniono, że wymóg dotyczy zdolności licznika do współpracy w procesie KMS, a nie samej komunikacji licznika bezpośrednio z systemem KMS.
60	**CRY-3.3**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Protokół ten obejmuje specyfikacje dotyczące bezpiecznej wymiany kluczy, również w skali masowej	Vendor 5	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		automatyzowanej. Prosimy więc o modyfikację i odniesienie do DLMS w tym wymaganiu - implementacja innych, przytaczanych w wymaganiu protokołów jest bezcelowa. Dodatkowo odwołanie do systemu KMS wykracza poza zakres wymagań dla liczników, gdyż systemy KMS nie komunikują się bezpośrednio z licznikami (przekazują zlecenia do systemów HES).		
61	**CRY-3.3**	LZO są zarządzane protokołem DLMS, również w zakresie bezpieczeństwa, gdzie dostępy i uprawnienia są oparte na szczegółowo opisanych asocjacjach. Przedstawione wymaganie może dotyczyć innych urządzeń OSD, ale nie LZO.	Vendor 6	j.w.
62	**CRY-4.1**	Wymagany czas na wprowadzenie dla Producentów	Vendor 1	Wyjaśnienie Przyjęto argument o potrzebie vacatio legis dla zmian w konstrukcji sprzętowej.
63	**CRY-4.1**	Vendor 2 believes that the use of specific hardware for storing any key should not be mandated. This not only adds additional cost to the product but also impacts on the overall design of the product. Far more cost-effective methods are available that can be used as an alternative and offer the same level of security	Vendor 2	Wyjaśnienie Wyjaśniono, że "izolowane środowisko" nie musi oznaczać zewnętrznego chipa (Secure Element), ale może być realizowane przez funkcje wewnętrzne MCU. Przyjęto argument o potrzebie vacatio legis dla zmian w konstrukcji sprzętowej.
64	**CRY-4.1**	Należy zapewnić Producentom odpowiedni czas na wdrożenie tego wymagania.	Vendor 5	Wyjaśnienie Przyjęto argument o potrzebie vacatio legis dla zmian w konstrukcji sprzętowej.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
65	**CRY-4.1**	Wprowadzenie zaufanego elementu sprzętowego w LZO oznacza zwykle konieczność istotnej zmiany hardware i firmware obecnie wdrażanych liczników. Sugerujemy odpowiednio długie "vacatio legis" dla tego wymagania, aby producenci mieli czas na przygotowanie i wprowadzenie opisanej zmiany.	Vendor 6	Wyjaśnienie Wyjaśniono, że "izolowane środowisko" nie musi oznaczać zewnętrznego chipa (Secure Element), ale może być realizowane przez funkcje wewnętrzne MCU. Przyjęto argument o potrzebie vacatio legis dla zmian w konstrukcji sprzętowej.
66	**CRY-5.1**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Protokół ten obejmuje specyfikacje dotyczące certyfikatów cyfrowych (od Security Suite 1), prosimy o odniesienie się do tego standardu. Proponujemy także wpisanie do wymagania, że "Niedopuszczalne jest implementowanie w LZO protokołów komunikacyjnych, które pozwalają na komunikację zdalną lub lokalną z LZO z użyciem słabszego uwierzytelniania, niż to zapewniane przez protokół DLMS/COSEM. Zwracamy także uwagę na to, że: - dla części technologii komunikacyjnych, takich jak np. PLC, NB-IoT autoryzacja certyfikatami może istotnie wpływać na skuteczność odczytu danych pomiarowych i może być problematyczna do wykorzystania ze względu na niską przepustowość kanału - w przypadku wykorzystania CA należącego do OSD, infrastruktura produkcyjna OT dostawcy musi być zintegrowana z infrastrukturą informatyczną OSD.	Vendor 1	Uwzględniono Odniesiono wymóg do nomenklatury DLMS/COSEM. Uwzględniono kanały o niskiej przepustowości.
67	**CRY-5.1**	Kto dostarcza certyfikaty do inicjalizacji urządzeń? Kto jest wystawcą certyfikatu (jaki urząd)?	Vendor 3	Wyjaśnienie Za PKI odpowiedzialność ponosi OSD.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
68	**CRY-5.1**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Protokół ten obejmuje specyfikacje dotyczące certyfikatów cyfrowych (od Security Suite 1). Prosimy więc o modyfikację i odniesienie do DLMS w tym wymaganiu - implementacja innych, przytaczanych w wymaganiu protokołów jest bezcelowa. Zwracamy także uwagę na to, że w przypadku wykorzystania CA należącego do OSD, infrastruktura produkcyjna OT dostawcy musi być zintegrowana z infrastrukturą informatyczną OSD. Ponadto proponujemy dopuszczenie fallbacku na sieci do Security Suite 0 w kanałach transmisji o niskich możliwościach (np. PLC, NBIoT)- decyzję taką podejmowałby OSD	Vendor 5	<u>Uwzględniono</u> Odniesiono wymóg do nomenklatury DLMS/COSEM. Uwzględniono kanały o niskiej przepustowości.
69	**CRY-5.1**	LZO są zarządzane protokołem DLMS, również w zakresie bezpieczeństwa, gdzie dostępy i uprawnienia są oparte na szczegółowo opisanych asocjacjach. Przedstawione wymaganie może dotyczyć innych urządzeń OSD, ale nie LZO. Dodatkowo zwracamy uwagę, że wykorzystywanie certyfikatów do uwierzytelniania nie jest realnie możliwe w niektórych stosowanych w Polsce technologiach komunikacyjnych, na przykład liczniki PLC lub technologiach LTE Narrowband. W takich miejscach przepustowość kanału komunikacji jest wystarczająca do uwierzytelniania kluczami (symetrycznie) oraz do przesyłania danych pomiarowych i realizacji innych wymagań Rozporządzenia ws systemu pomiarowego. Sugerujemy zatem doprecyzowanie wymagania: "Dotyczy urządzeń i kanałów komunikacji, które umożliwiają stosowanie X.509 / PKI / TLS."	Vendor 6	j.w.
70	**COM-1.1**	Wymaganie wykracza poza wymagania dotyczące liczników i dotyczy działania systemu i koncentratorów, prosimy o usunięcie tych wzmianek	Vendor 1	<u>Odrzucono</u>

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		- definiowanie gdzie kończy się szyfrowana sesja jest niezależne od licznika i przekracza zakres wymagań na liczniki. Licznik musi wspierać bezpieczną komunikację, z autoryzacją i szyfrowanym kanałem komunikacyjnym.		W sytuacji kiedy licznik nawiązuję bezpośrednie połączenie z system centralnym, wymaganie dotyczy licznika.
71	**COM-1.1**	Prosimy o doprecyzowanie wymagania także od strony licznika - funkcje bezpieczeństwa w liczniku powinny być wyizolowane do procesora licznika odpowiedzialnego za bezpieczeństwo end-to-end (zabroniona jest implementacja takich funkcji np. w procesorach modułów komunikacyjnych). Dodatkowo zwracamy uwagę, że wymaganie wykracza poza wymagania dotyczące liczników i dotyczy działania systemu i koncentratorów, prosimy o usunięcie tych wzmianek - definiowanie, gdzie kończy się szyfrowana sesja jest niezależne od licznika i przekracza zakres wymagań na liczniki.	Vendor 5	<u>Wyjaśnienie</u> Za ochronę integralności danych odpowiedzialna jest osobna grupa wymagań. W sytuacji kiedy licznik nawiązuję bezpośrednie połączenie z system centralnym, wymaganie dotyczy licznika.
72	**COM-1.1**	Wykorzystywanie certyfikatów (czyli Security Suite 1 lub 2) do uwierzytelniania może nie być realnie możliwe w niektórych stosowanych w Polsce technologiach komunikacyjnych, na przykład licznikach PLC lub technologiach LTE Narrowband. W takich miejscach przepustowość kanału komunikacji jest wystarczająca do uwierzytelniania kluczami (symetrycznie) oraz do przesyłania danych pomiarowych i realizacji innych wymagań Rozporządzenia ws. systemu pomiarowego. Ponadto, wszystkie wdrożone w Polsce technologie PLC (PRIME, G3-PLC) opierają się na działaniu koncentratora danych PLC, który zarządza lokalnie siecią PLC i dokonuje akwizycji danych pomiarowych z liczników, wg aktualnych możliwości na danej stacji nN, a później udostępnia je do Systemu Centralnego. Nie jest to komunikacja bezpośrednia, "online" między Systemem Centralnym a LZO, jak wydaje się zakładać wymaganie, gdyż taka komunikacja nie jest możliwa w technologiach	Vendor 6	<u>Uwzględniono:</u> Doprecyzowano wymaganie do W sytuacji kiedy licznik nawiązuję bezpośrednie połączenie z system centralnym, wymaganie dotyczy licznika - doprecyzowano wymaganie.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		PLC. Sugerujemy zatem doprecyzowanie wymagania: "Dotyczy kanałów komunikacji, które umożliwiają ich stosowanie przy jednoczesnym spełnieniu wymagań Rozporządzenia ws. systemu pomiarowego."		
73	**COM-2.1**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Protokół ten obejmuje specyfikacje dotyczące certyfikatów cyfrowych (od Security Suite 1). Inne kanały komunikacji (np. z modułem LTE w zakresie monitoringu) także powinny być uwierzytelnione / ograniczone do odczytu danych.	Vendor 1	Uwzględniono Wskazano mechanizmy DLMS.
74	**COM-2.1**	Punkt pokrywa się w większości z CRY-5.1, proponuje się scalenie punktów. Czy po stronie licznika dla każdego interfejsu ma być przypisany osobny certyfikat (w połączeniu z punktem ACC-1.1)?	Vendor 3	Wyjaśnienie Certyfikat dotyczy licznika jako całości, nie każdego interfejsu z osobna.
75	**COM-2.1**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Protokół ten obejmuje specyfikacje dotyczące certyfikatów cyfrowych (od Security Suite 1). Prosimy więc o modyfikację i odniesienie do DLMS w tym wymaganiu - implementacja innych, przytaczanych w wymaganiu protokołów jest bezcelowa. Zwracamy także uwagę na to, że w przypadku wykorzystania CA należącego do OSD, infrastruktura produkcyjna OT dostawcy musi być zintegrowana z infrastrukturą informatyczną OSD. Ponadto proponujemy dopuszczenie fallbacku na sieci do Security Suite 0 w kanałach transmisji o niskich możliwościach (np. PLC, NBIoT)- decyzję taką podejmowałby OSD.	Vendor 5	Uwzględniono Wskazano mechanizmy DLMS.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
76	**COM-2.1**	LZO są zarządzane protokołem DLMS, również w zakresie bezpieczeństwa, gdzie dostępy i uprawnienia są oparte na szczegółowo opisanych asocjacjach. Przedstawione wymaganie może dotyczyć innych urządzeń OSD, ale nie LZO.	Vendor 6	Wyjaśnienie Wymaganie dotyczy LZO.
77	**COM-3.1**			Nie zmieniono zapisu Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
78	**COM-3.2**			Nie zmieniono zapisu Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
79	**ACC-1.1**	LZO są zarządzane protokołem DLMS, również w zakresie bezpieczeństwa, gdzie dostępy i uprawnienia są oparte na szczegółowo opisanych asocjacjach. Przedstawione wymaganie może dotyczyć innych urządzeń OSD, ale nie LZO. Dodatkowo, nie może być mowy o „anonimowym dostępie dla interfejsu do infrastruktury domowej", podczas gdy Rozporządzenie ws systemu pomiarowego z 2022 roku jasno definiuje, że dla użytkownika końcowego liczniki LZO mają oferować interfejs ISD, gdzie dane są wysyłane przez licznik do ISD, a użytkownik nie ma możliwości łączenia się do licznika.	Vendor 6	Uwzględniono Wyjaśniono, że interfejs ISD (tryb *push*) nie jest interfejsem dostępowym, więc wymóg uwierzytelnienia go nie dotyczy.
80	**ACC-1.1**	Należy podkreślić, że normy DLMS/COSM pozwalają na zdefiniowanie użytkownika jako „public client" bez uprawnień, ale tylko w zakresie informacji o urządzeniu niezbędnej do nawiązania sesji komunikacyjnej z urządzeniem	Vendor 7	Uwzględniono

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
				Dopisano wyjątek dla asocjacji „public client” w zakresie niezbędnym do identyfikacji urządzenia.
81	**ACC-2.1**			Nie zmieniono zapisu Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
82	**ACC-3.1**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy model danych COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Poziomy uprawnień w tym modelu są oparte na asocjacjach, które predefiniują zakres dostępu na danym poziomie. Prosimy o odniesienie się w tym wymaganiu do asocjacji COSEM	Vendor 1	Uwzględniono Dostosowano terminologię do standardu DLMS/COSEM, zamieniając "role/konta" na "asocjacje".
83	**ACC-3.1**	Opis wskazuje, jakoby w samym liczniku miało następować, raz definiowanie ról, dwa definiowanie użytkowników na poziomie licznika, trzy przypisywanie ról tym użytkownikom. W aktualnie stosowanych rozwiązaniach definiowanie użytkowników oraz przypisywanie do nich stosownych uprawnień realizowane jest w oprogramowaniu do zarządzania licznikiem. Taki model postępowania jest zgodny z Rozporządzeniem MKiŚ z 22 marca 2022. Jeśli takie uprawnienia i definiowanie ról oraz użytkowników miało by się odbywać na poziomie licznika, to w jaki sposób miałby się on autoryzować ? Dla każdej roli i użytkownika niezbędny byłby stosowny certyfikat w celu zarejestrowania nieautoryzowanej operacji. Niosłoby to ze sobą także konieczność multiplikacji certyfikatów dla każdej zdefiniowanej roli oraz konieczność zarządzania nimi z poziomy aplikacji do obsługi technicznej jak i aplikacji centralnych do odczytów i zarządzania pomiarami.	Vendor 3	Odrzucono Wymóg dotyczy egzekwowania uprawnień przez licznik (jako punkt końcowy), a nie sposobu zarządzania certyfikatami w systemach nadrzędnych.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		Opis wskazuje, jakoby w samym liczniku miało następować, raz definiowanie ról, dwa definiowanie użytkowników na poziomie licznika, trzy przypisywanie ról tym użytkownikom. Obecnie takie operacje definiuje się w oprogramowaniu do zarządzania licznikiem i w nim nadaje się stosowne uprawnienia, co wyszczególniono w Rozporządzeniu MKiŚ z 22 marca. Jeśli takie uprawnienia i definiowanie ról oraz użytkowników miało by się odbywać na poziomie licznika, to w jaki sposób miałby się on autoryzować. Dla każdej roli i użytkownika niezbędny byłby stosowny certyfikat w celu zarejestrowania nieautoryzowanej operacji. Niosłoby to ze sobą także konieczność multiplikacji certyfikatów dla każdej zdefiniowanej roli oraz konieczność zarządzania nimi z poziomy aplikacji do obsługi technicznej jak i aplikacji centralnych do odczytów i zarządzania pomiarami. Czy opisana funkcjonalność nie powinna stanowić funkcji oprogramowania nadrzędnego a nie samego LZO, a tym samym zostać wyniesiona poza proponowany załącznik definiujący funkcje LZO ?		
84	**ACC-3.1**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy model danych COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Poziomy uprawnień w tym modelu są oparte na asocjacjach, które predefiniują zakres dostępu na danym poziomie. Prosimy o odniesienie się w tym wymaganiu do asocjacji COSEM.	Vendor 5	Uwzględniono Dostosowano terminologię do standardu DLMS/COSEM, zamieniając "role/konta" na "asocjacje".
85	**ACC-3.1**	LZO są zarządzane protokołem DLMS, również w zakresie bezpieczeństwa, gdzie dostępy i uprawnienia są oparte na szczegółowo opisanych asocjacjach. Przedstawione wymaganie może dotyczyć innych urządzeń OSD, ale nie LZO.	Vendor 6	j.w.
86	**ACC-3.2**	Wymaganie opisuje zbyt szczegółowo trzy poziomy uprawnień. W licznikach energii elektrycznej w Polsce stosowany jest powszechnie	Vendor 1	Uwzględniono

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. W modelu COSEM do definiowania poziomów uprawnień wykorzystane są asocjacje. O tym jaka jest struktura i uprawnienia dla poszczególnych ról użytkowników decyduje OSD i OSD musi dbać o spójność i interoperacyjność wszystkich rodzajów liczników w swoim systemie AMI.		Zmniejszono stopień szczegółowości do 2 typowo stosowanych poziomów asocjacji.
87	**ACC-3.2**	Level 1 and Level 3 are provided as standard; however, Level 2 is a nonstandard client. The specific requirements for Level 2 will have to be clearly defined.	Vendor 2	<u>Uwzględniono</u> Wspomniany poziom asocjacji nie będzie przywoływany w wymogu.
88	**ACC-3.2**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. W specyfikacji DLMS/COSEM role użytkowników nazywane są "asocjacjami". Wymaganie niepotrzebnie i błędnie zdefiniowało 3 poziomy dostępu, powinno ograniczyć się do samego stwierdzenia, że role muszą być zdefiniowane, natomiast o ich wymaganym zestawie w liczniku powinien decydować OSD -zależy to m.in. od użytej technologii transmisji itp.	Vendor 5	<u>Częściowo uwzględniono</u> Zmniejszono stopień szczegółowości do 2 typowo stosowanych poziomów asocjacji które dalej zgodnie z wymogiem mają być predefiniowane.
89	**ACC-3.2**	LZO są zarządzane protokołem DLMS, również w zakresie bezpieczeństwa, gdzie dostępy i uprawnienia są oparte na szczegółowo opisanych asocjacjach. Przedstawione wymaganie może dotyczyć innych urządzeń OSD, ale nie LZO. Szczególnie, że wymaganie mówi o dostępie dla "użytkownika końcowego", podczas gdy Rozporządzenie ws systemu pomiarowego z 2022 roku jasno definiuje, że dla użytkownika końcowego liczniki LZO	Vendor 6	<u>Wyjaśnienie</u> Zmieniono w treści wymogu nazwę z użytkownika końcowego na publiczny, aby nie myliła się z ISD.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		mają oferować interfejs ISD, gdzie dane są wysyłane przez licznik, a użytkownik nie ma możliwości łączenia się do licznika.		
90	**ACC-3.3**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Model COSEM standardowo specyfikuje asocjacje, które określają poziomy uprawnień. Asocjacje te są dostosowane do specyfiki liczników energii elektrycznej. Standard DLMS/COSEM nie przewiduje w licznikach energii obsługi "kont użytkowników". Proponujemy więc w tym wymaganiu odniesienie do asocjacji COSEM.	Vendor 1	<u>Wyjaśnienie</u> Wymogi precyzowane dla kont mają na celu zabezpieczenie przed implementacją niebezpiecznych mechanizmów wykraczających poza standard DLMS (konta inżynierskie, hasła). W ramach DLMS wymóg jest spełniony.
91	**ACC-3.3**	W licznikach energii elektrycznej w Polsce stosowany jest powszechnie standardowy protokół DLMS/COSEM, który przywoływany jest w tych wymaganiach wielokrotnie. Model COSEM standardowo specyfikuje asocjacje, które reprezentują poziomy uprawnień. Asocjacje te są dostosowane do specyfiki liczników energii elektrycznej. Standard DLMS/COSEM nie przewiduje w licznikach energii obsługi "kont użytkowników". Proponujemy więc w tym wymaganiu odniesienie do asocjacji COSEM.	Vendor 5	j.w.
92	**ACC-3.3**	LZO są zarządzane protokołem DLMS, również w zakresie bezpieczeństwa, gdzie dostępy i uprawnienia są oparte na szczegółowo opisanych asocjacjach. Przedstawione wymaganie może dotyczyć innych urządzeń OSD, ale nie LZO.	Vendor 6	j.w.
93	**ACC-4.1**	Zgodnie z propozycją licznik powinien posiadać aktywny jedynie interfejs OPTO z możliwością odczytu i programowania parametrów z wyłączonymi wszystkimi poleceniami wykonawczymi oraz wyłączoną funkcją wymiany FW. Pozostałe interfejsy licznika powinny być	Vendor 3	<u>Nie zmieniono zapisu</u> Wymaganie określa stan domyślny urządzenia w momencie dostawy i nie

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		nieaktywne a wszystkie uprawnienia na nich powinny być dodatkowo wyłączone (brak możliwości, odczytu, zapisu, wykonania poleceń oraz wymiany FW)? Idąc dalej za wymogami, powstaje pytanie o sens narażania na ewentualną kompromitację i trudności logistyczne w procesie inicjalizacji liczników. Czy zgodnie z powyższym punktem, wszystkie liczniki nie powinny przejść przez odpowiednie służby OSD, które aktywują w liczniku niezbędne interfejsy i funkcje oraz nadadzą unikatowe klucze/certyfikaty, które już będą wygenerowane przez system nadrzędny OSD zgodnie z polityką danego OSD i wymogami punktów SLC-5.1, CRY-3.1, CRY-3.2, CRY-3.3 ?		przesądza o ostatecznej konfiguracji operacyjnej - aktywacja interfejsów przez OSD jest procesem następczym, zgodnym z wymaganiem, a nie alternatywą dla niego. Propozycja przeniesienia inicjalizacji kluczy do OSD jest odrębną kwestią architektoniczną.
94	**ACC-4.2**			Nie zmieniono zapisu Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
95	**ACC-4.3**	W celu zachowania zgodności z dyrektywami UE dot. naprawialności urządzeń, proponujemy modyfikację tego wymagania. W przypadku niektórych napraw licznika, istnieje konieczność ponownego produkcyjnego zaprogramowania procesora licznika. Oczywiście taki mechanizm musi być zabezpieczony kryptograficznie i możliwy do wykonania tylko u producenta licznika, po jego otwarciu. Prosimy więc o dopuszczenie takiej możliwości z zachowaniem pełnego bezpieczeństwa	Vendor 1	Odrzucono Podtrzymano wymóg trwałego wyłączenia fizycznych interfejsów debugowania w urządzeniach produkcyjnych. Naprawialność urządzenia powinna być realizowana poprzez bezpieczne mechanizmy logiczne, a nie pozostawianie otwartych furtek sprzętowych.
96	**ACC-4.3**	W celu zachowania zgodności z dyrektywami UE dot. naprawialności urządzeń, proponujemy modyfikację tego wymagania.	Vendor 5	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		W przypadku niektórych napraw licznika, istnieje konieczność ponownego produkcyjnego zaprogramowania procesora licznika. Oczywiście taki mechanizm musi być zabezpieczony kryptograficznie i możliwy do wykonania tylko u producenta licznika, po jego otwarciu. Prosimy więc o dopuszczenie takiej możliwości z zachowaniem pełnego bezpieczeństwa.		
97	**ACC-4.3**	W celu zachowania zgodności z dyrektywami UE dot. naprawialności urządzeń, proponujemy modyfikację tego wymagania. W przypadku niektórych napraw licznika, istnieje konieczność ponownego produkcyjnego zaprogramowania procesora licznika. Oczywiście taki mechanizm musi być zabezpieczony kryptograficznie i możliwy do wykonania tylko u producenta licznika, po jego otwarciu. Prosimy więc o dopuszczenie takiej możliwości z zachowaniem pełnego bezpieczeństwa.	Vendor 6	j.w.
98	**ACC-5.1**	Wymaganie COM-2.1 nie dopuszcza uwierzytelniania na tak niskim poziomie jak opartego na hasłach dla liczników energii. Wymaganie raczej dotyczy systemu a nie funkcji LZO. Prosimy o usunięcie tego wymagania / przesunięcie do wymagań dotyczących systemów.	Vendor 1	<u>Wyjaśnienie</u> Wymóg zdefiniowany w kontekście licznika: Wymóg zabezpieczający przed implementacją niebezpiecznych mechanizmów wykraczających poza standard DLMS (konta inżynierskie, hasła). W ramach DLMS spełniony.
99	**ACC-5.1**	Powyższy punkt odnosi się raczej do systemu nadrzędnego i powinien zostać wyniesiony poza zakres załącznika dotyczącego LZO. Zgodnie z wymogami licznik ma korzystać z pełnego uwierzytelniania i szyfrowania	Vendor 3	j.w.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		co znosi możliwość stosowania haseł, dodatkowo w wymogach mowa także o prezentacji komunikatów dotyczących haseł.		
100	**ACC-5.1**	Wymaganie COM-2.1 nie dopuszcza uwierzytelniania na tak niskim poziomie jak opartego na hasłach dla liczników energii. Proponujemy więc usunięcie tego wymagania lub wpisanie wprost braku możliwości uwierzytelniania hasłem.	Vendor 5	j.w.
101	**ACC-5.1**	Niektóre z wymagań nie mają zastosowania do komunikacji maszyna-maszyna (IoT). Proponujemy ich sformułowanie następująco: • Dane uwierzytelniające fabryczne muszą być unikalne dla każdego urządzenia i wymuszać zmianę przy pierwszym logowaniu. • Musi istnieć możliwość zdefiniowania polityki złożoności danych uwierzytelniających (minimalna długość, wymagane klasy znaków) oraz polityki starzenia się danych uwierzytelniających (maksymalny okres ważności). Definiowalna polityka danych uwierzytelniających musi być zgodna z aktualnie obowiązującymi standardami bezpieczeństwa. • Dane uwierzytelniające muszą być przesyłane wyłącznie za pośrednictwem kanałów szyfrowanych. • W każdym interfejsie graficznym użytkownika (GUI) dane uwierzytelniające muszą być maskowane podczas wprowadzania. • Zmiana danych uwierzytelniających musi generować wpis w dzienniku zdarzeń.	Vendor 7	Wyjaśnienie Wymóg zdefiniowany w kontekście licznika: Wymóg zabezpieczający przed implementacją niebezpiecznych mechanizmów wykraczających poza standard DLMS (konta inżynierskie, hasła). W ramach DLMS spełniony.
102	**ACC-5.2**			Nie zmieniono zapisu Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
103	**INT-1.1**	Proponujemy, aby wymaganie odnosiło się do integralności danych: - bieżące stany liczydeł energii - klucze uwierzytelniające i szyfrujące	Vendor 1	Uwzględniono

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		Uzasadnienie: Ten zakres danych stanowi podstawę rozliczeń z odbiorcami oraz zapewnia bezpieczeństwo dostępu do licznika.		Doprecyzowano listę danych krytycznych objętych kodami MAC.
104	**INT-1.1**	Proponujemy, aby wymaganie odnosiło się do integralności danych: - bieżące stany liczydeł energii - klucze uwierzytelniające i szyfrujące Uzasadnienie: Ten zakres danych stanowi podstawę rozliczeń z odbiorcami oraz zapewnia bezpieczeństwo dostępu do licznika.	Vendor 5	Uwzględniono Doprecyzowano listę danych krytycznych objętych kodami MAC.
105	**INT-1.2**			Nie zmieniono zapisu Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
106	**INT-2.1**	Takie zachowanie wymusza już WELMEC Guide 7.2 (wymagany prze MID) dotyczący budowy oprogramowania urządzeń metrologicznych.	Vendor 3	Odrzucono Wymaganie INT-2.1 funkcjonuje w zestawie wymagań bezpieczeństwa jako samodzielna kontrola, której zakres i cel weryfikacji są odrębne od wymagań metrologicznych wynikających z MID. WELMEC Guide 7.2 adresuje integralność oprogramowania metrologicznego z perspektywy zgodności prawno-metrologicznej, natomiast INT-2.1 adresuje odporność na celowe działania atakującego w środowisku sieciowym, co jest domeną cyberbezpieczeństwa, nie metrologii. Pokrywanie się zakresów dwóch wymagań z różnych reżimów

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
				regulacyjnych nie eliminuje żadnego z nich.
107	**INT-2.2**			Nie zmieniono zapisu Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
108	**INT-2.3**	Vendor 2 believes that this requirement should not be mandatory regarding security checks. If the meters fail, we record an appropriate event in the nominated event log	Vendor 2	Odrzucono Całkowitą rezygnację z przedmiotowego wymogu uznano za niezasadną, gdyż brak mechanizmów autotestów funkcji kryptograficznych stanowiłby naruszenie wymagań IEC 62443-3-3 oraz pozostawałby w sprzeczności z zasadą fail-secure.
109	**INT-2.3**	Wymóg z kryterium weryfikacji tj. blokada uruchamiania, jest sprzeczny z normami dotyczącymi urządzeń tej klasy. Podstawową funkcją licznika energii jest pomiar mocy i energii elektrycznej, który musi wystartować tak wcześnie jak to tylko możliwe. Działanie funkcji pobocznych nie może powodować, że pomiar nie będzie realizowany. Ten wymóg to kolejny przykład iż, część założeń przyjętych w tym załączniku odnosi się do urządzeń nie tej klasy co licznik energii.	Vendor 3	Uwzględniono Doprecyzowano wymóg o procesy jakie muszą mieć miejsce w urządzeniu w przypadku wykrycia błędu autotestu. Ponadto dodano, iż błąd funkcji bezpieczeństwa musi alarmować, ale nie może przerywać pomiaru. Urządzenie w takiej sytuacji będzie wymagało interwencji lokalnej (wymiany).
110	**INT-3.1**	Proponujemy dopisanie w wymaganiu, że nie dotyczy to liczników (LZO) które posiadają nie otwieralną obudowę.	Vendor 1	Uwzględniono

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
				Zgodnie z propozycją Dostawcy, modyfikacja wymogu została uwzględniona, a zapis doprecyzowano poprzez wskazanie, że wymóg nie dotyczy liczników wyposażonych w nierozbieralną obudowę.
111	**INT-3.1**	In the point INT-3.1 you require device equipped with sensor to detect opening of the meter case, with the exception of the meters with non-dismountable meter cases. We design and manufacture this kind of meter cases (non-dismountable) and fully support your approach here. However, in the point LOG-5.1 “Fit criterion” you stated (e,g, case opening). We propose clarifying it by adding: (e.g. case opening, if applicable). In this point you listed the events that should be detected by physical sensors. We propose to add here the following event: opening of the communication module cover (with the exception of integrated meters).	Vendor 4	Uwzględniono Zgodnie z propozycją Dostawcy, modyfikacja wymogu została uwzględniona, a zapis poszerzono o zdarzenie dotyczące otwarcia osłony modułu komunikacyjnego, które musi zostać wykryte przez czujniki.
112	**INT-3.1**	Proponujemy dopisanie w wymaganiu, że nie dotyczy to liczników (LZO) które posiadają nieotwieralną obudowę.	Vendor 5	Uwzględniono Zgodnie z propozycją Dostawcy, modyfikacja wymogu została uwzględniona, a zapis doprecyzowano poprzez wskazanie, że wymóg nie dotyczy liczników wyposażonych w nierozbieralną obudowę.
113	**INT-4.1**			Nie zmieniono zapisu

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
				Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
114	**LOG-1.1**	Rejestracja „udanych” prób uwierzytelniania bardzo szybko spowoduje nadpisanie logu. Jaka ma być głębokość logu? Rejestracja zmiany czasu systemowego to zdarzenie powszechne. Zgodnie z wymogami Rozporządzenia MKiŚ z 22 marca 2022 r. podstawowym źródłem czasu dla LZO jest system OSD, w związku z tym można założyć, że czas powinien być kontrolowany i korygowany przynajmniej raz na dobę. Tym samym log ten będzie szybko zapełniany. Jak duża powinna być głębokość tego logu ? Rejestracja aktualizacji oprogramowania – należy określić zgodnie z wytycznymi WELMEC Guide 7.2 (jako wytyczną nadrzędną dla liczników energii). Zgodnie z zapisami WELMEC Guide 7.2 licznik ma umożliwić tylko „rozsądną” ilość aktualizacji. Po zapełnieniu logu aktualizacji, aktualizacja nie może być już możliwa, a log można wykasować jedynie w warunkach laboratoryjnych. Wymóg ten wręcz wymusza, odgórne ograniczenie ilości tych operacji. Należy także pamiętać, że przy normalnej operacji aktualizacji wpis w logach powinien zawierać dwie pozycje (operację przesłania aktualizacji i jej weryfikacji, oraz operację jej uruchomienia), gdyż aktualizację w protokole DLMS przeprowadza się w dwóch właściwie krokowo.	Vendor 3	<u>Uwzględniono</u> Wszystkie zastrzeżenia wymienione w komentarzu zostały uwzględnione w treści wymogu. Treść wymogu została dostosowana i zostały w niej zaadresowane kwestie dotyczące mechanizmu uwierzytelnień sesji automatycznych, dwupoziomowej architektury retencji (centralna i lokalna) oraz dwuetapowej rejestracji aktualizacji.
115	**LOG-1.2**			<u>Nie zmieniono zapisu</u> Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
116	**LOG-2.1**	Wnosimy o usunięcie tego wymaganie w całości, ponieważ zostało najprawdopodobniej zaadoptowane z innych urządzeń IT opartych na systemach operacyjnych z powłoką, systemem plików, etc, do których mogą być dostępne na rynku narzędzia deweloperskie pozwalające na głębokie przegladanie struktury wewnętrznej urządzenia i zmienianie np. statusów wpisów. W licznikach nie ma żadnego "API", kasowanie logów jest dopuszczone wyłącznie w szczególnych przypadkach na odpowiednich poziomach dostępu (np. całkowita rekonfiguracja urządzenia) zgodnie z wymaganiem LOG-2.2.	Vendor 1	Odrzucono Zasada niezmienialności dziennika zdarzeń jest wymaganiem powszechnie stosowanym w urządzeniach OT i jest adresowana przez standardy dedykowane tej klasie urządzeń. Fakt, że licznik nie posiada powłoki systemowej ani ogólnodostępnego API, nie eliminuje zagrożenia nieautoryzowanej modyfikacji logów a zmienia jedynie wektor ataku. Powołanie się na wymaganie LOG-2.2 jako regulację wystarczającą nie jest zasadne, ponieważ oba wymagania adresują odrębne aspekty ochrony dziennika zdarzeń i są wobec siebie komplementarne, nie substytucyjne.
117	**LOG-2.1**	Czy ochrona wpisów loga przed wyczyszczeniem lub nadpisaniem ma także dotyczyć samego trybu pracy loga (bufor okrężny). Jak ma się zachować licznik po zapełnieniu całej pamięci na dany log zdarzeń. Idąc dalej, atak może doprowadzić do wygenerowania takiej ilości zdarzeń, które usuną zdarzenia wcześniejsze wskazujące jakie operacje przeprowadzono, gdy log będzie pracował w trybie bufora okrężnego. Należy zdefiniować jak ma się zachowywać licznik w takim trybie. Należy określić jakieś odgórne rozsądne ilości wpisów w logach zdarzeń. Należy pamiętać, że liczniki to urządzenia o dość ograniczonych zasobach.	Vendor 3	Odrzucono Kwestie zawarte w komentarzu są odrębną klasą problemu w stosunku do treści wymagania, które adresuje wyłącznie ochronę przed nieautoryzowaną modyfikacją i selektywnym usunięciem istniejących wpisów przez atakującego, nie politykę retencji przy przepełnieniu bufora.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
118	**LOG-2.1**	Wnosimy o usuniecie tego wymaganie w całości, ponieważ zostało najprawdopodobniej zaadoptowane z innych urządzeń IT opartych na systemach operacyjnych z powłoką, systemem plików, etc., do których mogą być dostępne na rynku narzędzia deweloperskie pozwalające na głębokie przeglądanie struktury wewnętrznej urządzenia i zmienianie np. statusów wpisów. W licznikach nie ma żadnego "API", kasowanie logów jest dopuszczone wyłącznie w szczególnych przypadkach na odpowiednich poziomach dostępu (np. całkowita rekonfiguracja urządzenia) zgodnie z wymaganiem LOG-2.2.	Vendor 5	Odrzucono Zasada niezmienialności dziennika zdarzeń jest wymaganiem powszechnie stosowanym w urządzeniach OT i jest adresowana przez standardy dedykowane tej klasie urządzeń. Fakt, że licznik nie posiada powłoki systemowej ani ogólnodostępnego API, nie eliminuje zagrożenia nieautoryzowanej modyfikacji logów a zmienia jedynie wektor ataku. Powołanie się na wymaganie LOG-2.2 jako regulację wystarczającą nie jest zasadne, ponieważ oba wymagania adresują odrębne aspekty ochrony dziennika zdarzeń i są wobec siebie komplementarne, nie substytucyjne.
119	**LOG-2.1**	Zgadzamy się z wymaganiem zablokowania możliwości edycji/kasowania dzienników zdarzeń. Z tego względu sugerujemy usunięcie z wymagania LOG-2.2 zapisów o takiej możliwości.	Vendor 6	Odrzucono Ze względu na potencjalny scenariusz w zakresie uzasadnionych operacji administracyjnych polegających na m.in. wyczyszczeniu dziennika podczas prac serwisowych wspomnianym w LOG-2.2, proponujemy, aby wymóg nie został usunięty.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
120	**LOG-2.2**	W związku z niedopuszczaniem modyfikacji wpisów w dzienniku zdarzeń proponujemy następujący zapis wymagania: "Dostęp do odczytu i usuwania wpisów w dzienniku zdarzeń musi być kontrolowany i ograniczony do autoryzowanych ról (zgodnie z modelem separacji uprawnień)."	Vendor 1	Uwzględniono Propozycja zmiany zawarta w komentarzu została uwzględniona w treści wymogu.
121	**LOG-2.2**	Należy uściślić czy mówimy tu o dzienniku zdarzeń w pojęciu ogólnym czy tylko o dzienniku bezpieczeństwa. Współczesne liczniki energii posiadają po kilka logów zdarzeń z podziałem na funkcje np.: Ogólny, Sieciowy, Antykradzieżowy, Parametryzacji, Wymiany oprogramowania, Serwisowy itd. Wymogiem WELMEC Guide 7.2 jest np. osobny log aktualizacji oprogramowania, który w normalnych warunkach pracy ma być niemożliwy do skasowania, a możliwość wykonywania aktualizacji ma być dostępna tylko do jego zapełnienia.	Vendor 3	Uwzględniono Komentarz został uwzględniony na w treści wymogu. Wymóg jednoznacznie rozróżnia trzy kategorie dzienników: dziennik zdarzeń bezpieczeństwa, dzienniki objęte prawną kontrolą metrologiczną w tym dziennik aktualizacji oprogramowania oraz pozostałe dzienniki operacyjne.
122	**LOG-2.2**	W związku z niedopuszczaniem modyfikacji wpisów w dzienniku zdarzeń proponujemy następujący zapis wymagania: "Dostęp do odczytu i usuwania wpisów w dzienniku zdarzeń musi być kontrolowany i ograniczony do autoryzowanych ról (zgodnie z modelem separacji uprawnień). "	Vendor 5	Uwzględniono Propozycja zmiany zawarta w komentarzu została uwzględniona w treści wymogu.
123	**LOG-2.2**	Zgadzamy się z wymaganiem zablokowania możliwości edycji/kasowania dzienników zdarzeń. Z tego względu sugerujemy usunięcie z wymagania zapisów o takiej możliwości, a pozostawienia jedynie możliwości odczytu.	Vendor 6	Częściowo uwzględniono Kwestia blokowania możliwości edycji i usuwania dzienników zdarzeń nie została w pełni zastosowana ze względu na istnienie uzasadnionych operacji administracyjnych, które mogą być niezbędne.

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
124	**LOG-3.1**	Należy uściślić jaka powinna być „odpowiednia” pamięć z „rozsądnego okresu”. Pamiętajmy, że zdarzenia mogą wystąpi zarówno raz na miesiąc jak i co sekundę. Rozporządzenie MKiŚ mówi o minimum 250 zdarzeniach, wymogi OSD nawet o 1000. Współczesne liczniki energii posiadają po kilka logów zdarzeń z podziałem na funkcje np.: Ogólny, Sieciowy, Antykradzieżowy, Parametryzacji, Wymiany oprogramowania, Serwisowy itd. Wymogiem WELMEC Guide 7.2 jest osobny log aktualizacji oprogramowania, który ma działać tylko do zapełnienia po tym okresie nie może być już wykonana aktualizacja a log można skasować tylko w warunkach laboratoryjnych. Zatem wskazany wymóg pracy w trybie FIFO dla tego logu jest sprzeczny z prawem dla liczników zgodnych z MID. Jak rozwiązać problem wymogu LOG-2.1 przy buforze FIFO. Jak ma się zachować licznik po zapełnieniu całej pamięci na dany log zdarzeń. Idąc dalej, atak może doprowadzić do wygenerowania takiej ilości zdarzeń, które usuną zdarzenia wcześniejsze wskazujące jakie operacje przeprowadzono, gdy log będzie pracował w trybie bufora okrężnego.	Vendor 3	<u>Wyjaśnienie</u> Wymóg został doprecyzowany poprzez dodanie zasad dotyczących zarządzania pamięcią nieulotną. Zgodnie z komentarzem zastosowano również odpowiednie odwołanie do wymagań WELMEC Guide 7.2 W zakresie zarządzania zapełnieniem dziennika oraz mechanizmu blokowania kolejnych aktualizacji po osiągnięciu jego maksymalnej pojemności.
125	**LOG-4.1**			<u>Nie zmieniono zapisu</u> Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.
126	**LOG-5.1**	In the point INT-3.1 you require device equipped with sensor to detect opening of the meter case, with the exception of the meters with non-dismountable meter cases. We design and manufacture this kind of meter cases (non-dismountable) and fully support your approach here.	Vendor 4	<u>Uwzględniono</u> Opis wymagania został uzupełniony zdarzenie zaproponowane przez Dostawcę. Doprecyzowano w kryterium

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
		However, in the point LOG-5.1 “Fit criterion” you stated (e,g, case opening). We propose clarifying it by adding: (e.g. case opening, if applicable). In this point you listed the events that should be detected by physical sensors. We propose to add here the following event: opening of the communication module cover (with the exception of integrated meters).		weryfikacji kwestię dotyczącą budowy urządzenia.
127	**PHY-1.1**	Proponujemy dopisanie w wymaganiu, że nie dotyczy to liczników (LZO) które posiadają nieotwieralną obudowę.	Vendor 1	Uwzględniono Zgodnie z propozycjami zmian zgłoszonymi przez Dostawców, w opisie wymogów zamieszczono wyjątek dotyczący liczników posiadających nierozbieralną obudowę.
128	**PHY-1.1**	In the point PHY-1.1 you requested enabling of sealing. Due to the fact that we have non-dismountable meter cases, we propose to change this point to the following: The meter case (with the exception of meters with non-dismountable meter cases), terminal cover and communication module cover (if applicable) must be constructed in a way that enables their sealing. The construction must prevent access to the interior of the device, the terminals and the communication module, without breaking or visibly damaging the seals or without breaking and visible damaging of the meter cover.	Vendor 4	Uwzględniono Zgodnie z propozycjami zmian zgłoszonymi przez Dostawców, w opisie wymogów zamieszczono wyjątek dotyczący liczników posiadających nierozbieralną obudowę.
129	**PHY-1.1**	Proponujemy dopisanie w wymaganiu, że nie dotyczy to liczników (LZO) które posiadają nieotwieralną obudowę.	Vendor 5	Uwzględniono Zgodnie z propozycjami zmian zgłoszonymi przez Dostawców, w opisie wymogów zamieszczono wyjątek

Lp.		Treść uwagi wraz z uzasadnieniem	Zgłaszający uwagę	Stanowisko PTPIREE
				dotyczący liczników posiadających nierozbieralną obudowę.
130	**PHY-2.1**	Co rozumiemy pod pojęciem portów serwisowych? Jak mniemamy chodzi o interfejsy komunikacyjne (w poprzednich punktach posługujemy się terminem interfejsów). Należy ujednolicić nazewnictwo elementów w całym załączniku.	Vendor 3	<u>Uwzględniono</u> Zgodnie z propozycją zmiany zgłoszoną przez Dostawcę, zostało zastosowane ujednolicenie nazewnictwa poprzez zmianę określenia z „portów serwisowych” na „interfejsy komunikacyjne”.
131	**PHY-3.1**			<u>Nie zmieniono zapisu</u> Brzmienie wymogu pozostaje niezmienione; nie odnotowano uwag ze strony Dostawców.