KOMISJA
EUROPEJSKA

Bruksela, dnia 13.3.2019 r.
C(2019) 1789 final

ANNEX 3

ZAŁĄCZNIK

do

rozporządzenia delegowanego Komisji

uzupełniającego dyrektywę Parlamentu Europejskiego i Rady 2010/40/UE w odniesieniu do wdrażania i eksploatacji współpracujących inteligentnych systemów transportowych

{SEC(2019) 100 final} - {SWD(2019) 95 final} - {SWD(2019) 96 final}

SPIS TREŚCI

1. Wprowadzenie 9
1.1. Przegląd i zakres niniejszej polityki 9
1.2. Definicje i skróty 11
1.3. Uczestnicy infrastruktury klucza publicznego 13
1.3.1. Wprowadzenie 13
1.3.2. Organ ds. polityki certyfikacji C-ITS 16
1.3.3. Zarządzający zaufaną listą 17
1.3.4. Akredytowany audytor infrastruktury klucza publicznego 17
1.3.5. Punkt kontaktowy ds. C-ITS (CPOC) 17
1.3.6. Role operacyjne 18
1.4. Zastosowanie certyfikatu 18
1.4.1. Obowiązujące dziedziny stosowania 18
1.4.2. Ograniczenia odpowiedzialności 19
1.5. Zarządzanie polityką certyfikacji 19
1.5.1. Aktualizacja CPS urzędów certyfikacji wymienionych na ECTL 19
1.5.2. Procedury przyjmowania CPS 20
2. Obowiązki związane z publikacją i repozytorium 20
2.1. Metody publikowania informacji o certyfikatach 20
2.2. Czas lub częstotliwość publikacji 21
2.3. Repozytoria 21
2.4. Kontrole dostępu do repozytoriów 21
2.5. Publikacja informacji o certyfikacie 22
2.5.1. Publikacja informacji o certyfikacie przez TLM 22
2.5.2. Publikacja informacji o certyfikacie przez urzędy certyfikacji 22
3. Identyfikacja i uwierzytelnianie 23
3.1. Nadawanie nazwy 23
3.1.1. Rodzaje nazw 23
3.1.1.1. Nazwy TLM, głównych urzędów certyfikacji, organów ds. rejestracji, organów autoryzujących 23
3.1.1.2. Nazwy jednostek końcowych 23
3.1.1.3. Identyfikacja certyfikatów 23
3.1.2. Potrzeba nadania nazw posiadających znaczenie 23
3.1.3. Anonimowość i pseudonimizacja jednostek końcowych 23
3.1.4. Zasady interpretowania różnych form nazw 23

3.1.5. Niepowtarzalność nazw 24
3.2. Pierwsza walidacja tożsamości 24
3.2.1. Metoda udowodnienia posiadania klucza prywatnego 24
3.2.2. Uwierzytelnianie tożsamości organizacji 24
3.2.2.1. Uwierzytelnianie tożsamości organizacji głównych urzędów certyfikacji 24
3.2.2.2. Uwierzytelnianie tożsamości organizacji TLM 25
3.2.2.3. Uwierzytelnianie tożsamości organizacji podporządkowanych urzędów certyfikacji 25
3.2.2.4. Uwierzytelnianie organizacji abonenta jednostek końcowych 26
3.2.3. Uwierzytelnianie pojedynczej jednostki 26
3.2.3.1. Uwierzytelnianie pojedynczej jednostki TLM / urzędu certyfikacji 26
3.2.3.2. Uwierzytelnianie tożsamości abonenta stacji C-ITS 27
3.2.3.3. Uwierzytelnianie tożsamości stacji C-ITS 27
3.2.4. Niezweryfikowane informacje o abonencie 27
3.2.5. Walidacja organu 27
3.2.5.1. Walidacja TLM, głównego urzędu certyfikacji, organu ds. rejestracji, organu autoryzującego 27
3.2.5.2. Walidacja abonentów stacji C-ITS 28
3.2.5.3. Walidacja stacji C-ITS 28
3.2.6. Kryteria interoperacyjności 28
3.3. Identyfikacja i uwierzytelnianie w przypadku wniosków o ponowne wprowadzenie kluczy 28
3.3.1. Identyfikacja i uwierzytelnianie w przypadku zwykłych wniosków o ponowne wprowadzenie kluczy 28
3.3.1.1. Certyfikaty TLM 28
3.3.1.2. Certyfikaty głównego urzędu certyfikacji 28
3.3.1.3. Przedłużenie lub ponowne wprowadzenie certyfikatu organu ds. rejestracji / organu autoryzującego 28
3.3.1.4. Dane uwierzytelniające rejestrację jednostek końcowych 29
3.3.1.5. Bilety autoryzacyjne jednostek końcowych 29
3.3.2. Identyfikacja i uwierzytelnianie w przypadku wniosków o ponowne wprowadzenie kluczy po ich unieważnieniu 29
3.3.2.1. Certyfikaty urzędu certyfikacji 29
3.3.2.2. Dane uwierzytelniające rejestrację jednostek końcowych 29
3.3.2.3. Wnioski o autoryzację jednostek końcowych 29
3.4. Identyfikacja i uwierzytelnianie wniosku o unieważnienie 29

3.4.1. Certyfikaty głównego urzędu certyfikacji / organu ds. rejestracji / organu autoryzującego 29
3.4.2. Dane uwierzytelniające rejestrację stacji C-ITS 30
3.4.3. Bilety autoryzacyjne stacji C-ITS 30
4. Wymogi operacyjne cyklu życia certyfikatu 30
4.1. Wniosek o wydanie certyfikatu 30
4.1.1. Kto może złożyć wniosek o wydanie certyfikatu 30
4.1.1.1. Główne urzędy certyfikacji 30
4.1.1.2. Zarządzający zaufaną listą 31
4.1.1.3. Organ ds. rejestracji i organ autoryzujący 31
4.1.1.4. Stacja C-ITS 31
4.1.2. Proces rejestracji i zakres odpowiedzialności 31
4.1.2.1. Główne urzędy certyfikacji 31
4.1.2.2. Zarządzający zaufaną listą 32
4.1.2.3. Organ ds. rejestracji i organ autoryzujący 32
4.1.2.4. Stacja C-ITS 32
4.2. Przetwarzanie wniosku o wydanie certyfikatu 33
4.2.1. Realizacja czynności związanych z identyfikacją i uwierzytelnianiem 33
4.2.1.1. Identyfikacja i uwierzytelnianie głównych urzędów certyfikacji 33
4.2.1.2. Identyfikacja i uwierzytelnianie TLM 33
4.2.1.3. Identyfikacja i uwierzytelnianie organu ds. rejestracji i organu autoryzującego 33
4.2.1.4. Identyfikacja i uwierzytelnianie abonenta jednostki końcowej 34
4.2.1.5. Bilety autoryzacyjne 34
4.2.2. Przyjmowanie lub odrzucanie wniosków o wydanie certyfikatu 34
4.2.2.1. Przyjmowanie lub odrzucanie certyfikatów głównego urzędu certyfikacji 34
4.2.2.2. Przyjmowanie lub odrzucanie certyfikatów TLM 34
4.2.2.3. Przyjmowanie lub odrzucanie certyfikatów organu ds. rejestracji i organu autoryzującego 34
4.2.2.4. Przyjmowanie lub odrzucanie danych uwierzytelniających rejestrację 34
4.2.2.5. Przyjmowanie lub odrzucanie biletu autoryzacyjnego 35
4.2.3. Czas na przetworzenie wniosku o wydanie certyfikatu 35
4.2.3.1. Wniosek o wydanie certyfikatu przez główny urząd certyfikacji 35
4.2.3.2. Wniosek o wydanie certyfikatu przez TLM 35
4.2.3.3. Wniosek o wydanie certyfikatu organu ds. rejestracji i organu autoryzującego 35
4.2.3.4. Wniosek o dane uwierzytelniające rejestrację 35
4.2.3.5. Wniosek o bilet autoryzacyjny 35

4.3. Wydanie certyfikatu 35
4.3.1. Czynności urzędu certyfikacji wykonywane podczas wydawania certyfikatu 35
4.3.1.1. Wydanie certyfikatu przez główny urząd certyfikacji 35
4.3.1.2. Wydanie certyfikatu przez TLM 36
4.3.1.3. Wydanie certyfikatu przez organ ds. rejestracji i organ autoryzujący 36
4.3.1.4. Wydanie danych uwierzytelniających rejestrację 36
4.3.1.5. Wydanie biletu autoryzacyjnego 36
4.3.2. Powiadomienie abonenta o wydaniu certyfikatów przez urząd certyfikacji 36
4.4. Akceptacja certyfikatu 37
4.4.1. Przeprowadzanie akceptacji certyfikatu 37
4.4.1.1. Główny urząd certyfikacji 37
4.4.1.2. Zarządzający zaufaną listą 37
4.4.1.3. Organ ds. rejestracji i organ autoryzujący 37
4.4.1.4. Stacja C-ITS 37
4.4.2. Publikacja certyfikatu 37
4.4.3. Powiadomienie o wydaniu certyfikatu 37
4.5. Zastosowanie pary kluczy i certyfikatów 37
4.5.1. Zastosowanie klucza prywatnego i certyfikatu 37
4.5.1.1. Zastosowanie klucza prywatnego i certyfikatu przez TLM 37
4.5.1.2. Stosowanie klucza prywatnego i certyfikatów przez główne urzędy certyfikacji 37
4.5.1.3. Zastosowanie klucza prywatnego i certyfikatu przez organy ds. rejestracji i organy autoryzujące 37
4.5.1.4. Zastosowanie klucza prywatnego i certyfikatu w przypadku jednostki końcowej 38
4.5.2. Zastosowanie klucza publicznego i certyfikatu przez stronę ufającą 38
4.6. Przedłużenie certyfikatu 38
4.7. Ponowne wprowadzenie certyfikatu 38
4.7.1. Okoliczności ponownego wprowadzenia certyfikatu 38
4.7.2. Kto może złożyć wniosek o ponowne wprowadzenie certyfikatu 38
4.7.2.1. Główny urząd certyfikacji 38
4.7.2.2. Zarządzający zaufaną listą 38
4.7.2.3. Organ ds. rejestracji i organ autoryzujący 38
4.7.2.4. Stacja C-ITS 39
4.7.3. Proces ponownego wprowadzenia certyfikatu 39
4.7.3.1. Certyfikat zarządzającego zaufaną listą 39
4.7.3.2. Certyfikat głównego urzędu certyfikacji 39
4.7.3.3. Certyfikaty organu ds. rejestracji i organu autoryzującego 39

4.7.3.4. Certyfikaty stacji C-ITS 40
4.8. Zmiana certyfikatu 40
4.9. Unieważnienie i zawieszenie certyfikatu 40
4.10. Usługi związane ze statusem certyfikatu 40
4.10.1. Charakterystyka użytkowania 40
4.10.2. Dostępność usługi 40
4.10.3. Cechy fakultatywne 40
4.11. Zakończenie abonamentu 40
4.12. Deponowanie i odzyskiwanie klucza 40
4.12.1. Abonent 40
4.12.1.1. Jaką parę kluczy można zdeponować 40
4.12.1.2. Kto może złożyć wniosek o odzyskanie klucza 40
4.12.1.3. Proces odzyskiwania i zakres odpowiedzialności 40
4.12.1.4. Identyfikacja i uwierzytelnianie 40
4.12.1.5. Przyjęcie lub odrzucenie wniosków o odzyskanie klucza 40
4.12.1.6. Operacje wykonywane przez szablony KEA i KRA podczas odzyskiwania pary kluczy 41
4.12.1.7. Dostępność szablonów KEA i KRA 41
4.12.2. Polityka i praktyki w zakresie hermetyzacji i odzyskiwania klucza sesji 41
5. Kontrole obiektów i zarządzania oraz kontrole operacyjne 41
5.1. Kontrole fizyczne 41
5.1.1. Lokalizacja i konstrukcja 41
5.1.1.1. Główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą 41
5.1.1.2. Organ ds. rejestracji / organ autoryzujący 42
5.1.2. Dostęp fizyczny 42
5.1.2.1. Główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą 42
5.1.2.2. Organ ds. rejestracji / organ autoryzujący 43
5.1.3. Zasilanie i klimatyzacja 43
5.1.4. Narażenie na działanie wody 43
5.1.5. Ochrona przeciwpożarowa 44
5.1.6. Zarządzanie nośnikami danych 44
5.1.7. Usuwanie odpadów 44
5.1.8. Kopie zapasowe poza obiektem 44
5.1.8.1. Główny urząd certyfikacji, centralny punkt kontaktowy i zarządzający zaufaną listą 44
5.1.8.2. Organ ds. rejestracji / organ autoryzujący 45

5.2. Kontrole proceduralne 45
5.2.1. Zaufane role 45
5.2.2. Liczba osób wymaganych do realizacji zadania 45
5.2.3. Identyfikacja i uwierzytelnianie każdej roli 46
5.2.4. Role wymagające podziału obowiązków 46
5.3. Nadzorowanie personelu 47
5.3.1. Wymogi w zakresie kwalifikacji, doświadczenia i poświadczeń 47
5.3.2. Procedury sprawdzania przeszłości 47
5.3.3. Wymogi szkoleniowe 48
5.3.4. Częstotliwość i wymogi powtarzania szkoleń 48
5.3.5. Częstotliwość i kolejność rotacji stanowisk 48
5.3.6. Sankcje z tytułu nieuprawnionych działań 48
5.3.7. Wymogi dotyczące niezależnego wykonawcy 49
5.3.8. Dokumentacja przekazana personelowi 49
5.4. Procedury rejestracji kontroli 49
5.4.1. Rodzaje zdarzeń rejestrowanych i zgłaszanych przez każdy urząd certyfikacji 49
5.4.2. Częstotliwość przetwarzania dziennika 50
5.4.3. Okres przechowywania dziennika kontroli 50
5.4.4. Ochrona dziennika kontroli 51
5.4.5. Procedury tworzenia kopii zapasowych dzienników kontroli 51
5.4.6. System zbierania danych z audytu (wewnętrzny lub zewnętrzny) 51
5.4.7. Powiadamianie jednostki odpowiedzialnej za zdarzenie 51
5.4.8. Ocena luk w zabezpieczeniach 51
5.5. Archiwizacja zapisów 52
5.5.1. Rodzaje archiwizowanych zapisów 52
5.5.2. Okres przechowywania archiwum 53
5.5.3. Ochrona archiwum 53
5.5.4. Archiwum systemu i jego przechowywanie 53
5.5.5. Wymogi dotyczące oznaczania czasu zapisów 54
5.5.6. System zbierania zapisów archiwalnych (wewnętrzny lub zewnętrzny) 54
5.5.7. Procedury uzyskiwania dostępu do informacji archiwalnych i ich weryfikacji 54
5.6. Zmiana klucza dla elementów modelu zaufania C-ITS 54
5.6.1. Zarządzający zaufaną listą 54
5.6.2. Główny urząd certyfikacji 54
5.6.3. Certyfikat organu ds. rejestracji / organu autoryzującego 54

5.6.4. Audytor 55
5.7. Naruszenie ochrony i przywrócenie gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej 55
5.7.1. Postępowanie w przypadku incydentu i naruszenia ochrony 55
5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania lub danych 56
5.7.3. Procedury w przypadku ujawnienia klucza prywatnego jednostki 56
5.7.4. Zapewnienie ciągłości działania po wystąpieniu katastrofy 56
5.8. Zakończenie i przekazanie działalności 57
5.8.1. Zarządzający zaufaną listą 57
5.8.2. Główny urząd certyfikacji 57
5.8.3. Organ ds. rejestracji / organ autoryzujący 58
6. Kontrola bezpieczeństwa technicznego 58
6.1. Generowanie pary kluczy i jej instalacja 58
6.1.1. Zarządzający zaufaną listą, główny urząd certyfikacji, organ ds. rejestracji, organ autoryzujący 58
6.1.2. Jednostka końcowa – ruchoma stacja C-ITS 58
6.1.3. Jednostka końcowa – stała stacja C-ITS 59
6.1.4. Wymogi kryptograficzne 59
6.1.4.1. Długość algorytmu i klucza – algorytmy podpisu 59
6.1.4.2. Długość algorytmu i klucza – algorytmy szyfrujące do celów rejestracji i autoryzacji 60
6.1.4.3. Zręczność kryptograficzna 61
6.1.5. Bezpieczne przechowywanie kluczy prywatnych 61
6.1.5.1. Poziom głównego urzędu certyfikacji, podporządkowanego urzędu certyfikacji i zarządzającego zaufaną listą 61
6.1.5.2. Jednostka końcowa 62
6.1.6. Kopie zapasowe kluczy prywatnych 63
6.1.7. Niszczenie kluczy prywatnych 63
6.2. Dane aktywacyjne 63
6.3. Zabezpieczenia komputerowe 63
6.4. Techniczne kontrole cyklu życia 63
6.5. Zabezpieczenia sieci 63
7. Profile certyfikatów, CRL i CTL 63
7.1. Profil certyfikatu 63
7.2. Ważność certyfikatu 64
7.2.1. Certyfikaty z zastosowaniem pseudonimu 65
7.2.2. Bilety autoryzacyjne dla stałych stacji C-ITS 65

7.3. Unieważnianie certyfikatów 65
7.3.1. Unieważnianie certyfikatów urzędu certyfikacji, organu ds. rejestracji i organu autoryzującego 65
7.3.2. Unieważnianie danych uwierzytelniających rejestrację 66
7.3.3. Unieważnianie biletów autoryzacyjnych 66
7.4. Lista unieważnionych certyfikatów 66
7.5. Europejska zaufana lista certyfikatów 66
8. Audyt zgodności i inne oceny 66
8.1. Tematy objęte audytem i podstawa audytu 66
8.2. Częstotliwość audytów 67
8.3. Tożsamość/kwalifikacje audytora 67
8.4. Powiązania audytora z audytowaną jednostką 67
8.5. Działania podjęte w wyniku uchybienia 68
8.6. Ogłoszenie wyników 68
9. Pozostałe przepisy 68
9.1. Opłaty 68
9.2. Odpowiedzialność finansowa 69
9.3. Poufność informacji biznesowych 69
9.4. Plan ochrony prywatności 69
10. Odniesienia 69

ZAŁĄCZNIK III

1. WPROWADZENIE

1.1. Przegląd i zakres tej polityki

Niniejsza polityka certyfikacji określa europejski model zaufania C-ITS oparty na infrastrukturze klucza publicznego w ramach ogólnego unijnego systemu zarządzania danymi uwierzytelniającymi C-ITS (EU CCMS). Określa wymogi w zakresie zarządzania certyfikatami klucza publicznego w przypadku wniosków dotyczących C-ITS składanych przez jednostki wydające i w zakresie ich wykorzystania przez jednostki końcowe w Europie. Na najwyższym poziomie infrastruktura klucza publicznego składa się z zestawu głównych urzędów certyfikacji „uaktywnianych" w wyniku zamieszczenia ich certyfikatów przez zarządzającego zaufaną listą (TLM) na europejskiej zaufanej liście certyfikatów (ECTL), która jest wydawana i publikowana przez jednostkę centralną TLM (zob. sekcje 1.2 i 1.3).

Polityka ta jest obowiązująca dla wszystkich jednostek uczestniczących w zaufanym systemie C-ITS w Europie. Ułatwia ona ocenę poziomu zaufania, jaki można ustalić w informacjach otrzymanych przez dowolnego odbiorcę komunikatu uwierzytelnionego certyfikatem infrastruktury klucza publicznego jednostki końcowej. Aby umożliwić ocenę zaufania do certyfikatów wydawanych przez EU CCMS, określono w niej wiążący zestaw wymogów dotyczących funkcjonowania TLM centralnej jednostki oraz opracowywania ECTL i zarządzania nią. W związku z tym niniejszy dokument dotyczy następujących aspektów ECTL:

- identyfikacji i uwierzytelniania osób obejmujących dane role w infrastrukturze klucza publicznego w odniesieniu do TLM, w tym zestawień uprawnień przypisanych do każdej roli;
- minimalnych wymagań w zakresie lokalnych praktyk bezpieczeństwa w odniesieniu do TLM, w tym kontroli fizycznych, kontroli personelu i kontroli proceduralnych;
- minimalnych wymogów w zakresie praktyk bezpieczeństwa technicznego w odniesieniu do TLM, w tym zabezpieczeń komputerowych, zabezpieczeń sieci oraz kontroli technicznych modułu kryptograficznego;
- minimalnych wymogów w zakresie praktyk operacyjnych w odniesieniu do TLM, w tym rejestracji nowych certyfikatów głównego urzędu certyfikacji, tymczasowego lub trwałego wyrejestrowania istniejących zarejestrowanych urzędów certyfikacji oraz publikacji i dystrybucji aktualizacji ECTL;
- profilu ECTL, w tym wszystkich obowiązkowych i fakultatywnych pól danych w ECTL, algorytmów kryptograficznych, z których należy korzystać, dokładnego formatu ECTL i zaleceń dotyczących jej przetwarzania;
- zarządzania cyklem życia certyfikatu ECTL, w tym dystrybucji, aktywacji, wygaszania i unieważniania certyfikatów znajdujących się na ECTL;
- w stosownych przypadkach, zarządzania unieważnieniem zaufania dla głównych urzędów certyfikacji.

Z uwagi na fakt, że wiarygodność ECTL nie zależy wyłącznie od samej ECTL, ale w dużym stopniu również od głównych urzędów certyfikacji, które tworzą

infrastrukturę klucza publicznego, i ich podporządkowanych urzędów certyfikacji, w ramach przedmiotowej polityki określono również minimalne wymogi, które są obowiązkowe dla wszystkich uczestniczących urzędów certyfikacji (głównych urzędów certyfikacji i ich podporządkowanych urzędów certyfikacji). Obszary objęte wymogami są następujące:

- identyfikacja i uwierzytelnianie osób obejmujących dane role w infrastrukturze klucza publicznego (np. inspektor ds. bezpieczeństwa, inspektor ds. ochrony prywatności, administrator ds. bezpieczeństwa, administrator rejestru i użytkownik końcowy), w tym określenie obowiązków, zakresu odpowiedzialności, zobowiązań i uprawnień związanych z każdą rolą;
- zarządzanie kluczami, w tym możliwe do przyjęcia i obowiązkowe algorytmy podpisywania certyfikatów i danych, oraz okresy ważności certyfikatu;
- minimalne wymogi w zakresie lokalnych praktyk bezpieczeństwa, w tym kontrole fizyczne, kontrole personelu i kontrole proceduralne;
- minimalne wymogi w zakresie praktyk bezpieczeństwa technicznego, takie jak zabezpieczenia komputerowe, zabezpieczenia sieci oraz kontrole inżynieryjne modułu kryptograficznego;
- minimalne wymogi w zakresie praktyk operacyjnych urzędu certyfikacji, organu ds. rejestracji, organu autoryzującego i jednostek końcowych, w tym aspekty dotyczące rejestracji, wyrejestrowania (tj. skreślenia z listy), unieważnienia, ujawnienia klucza, zwolnienia z określonego powodu, aktualizacji certyfikatu, praktyk audytowych i nieujawniania informacji objętych ochroną prywatności;
- profil certyfikatu i profil CRL, w tym formaty, akceptowane algorytmy, obowiązkowe i fakultatywne pola danych oraz ich ważne zakresy wartości oraz sposób, w jaki weryfikatorzy mają przetwarzać certyfikaty;
- regularne monitorowanie, sprawozdawczość, ostrzeganie i przywracanie obowiązków jednostek modelu zaufania C-ITS w celu zapewnienia bezpiecznego działania, także w przypadkach niewłaściwego zachowania.

Oprócz tych wymogów minimalnych jednostki prowadzące główne urzędy certyfikacji i ich podporządkowane urzędy certyfikacji mogą podejmować decyzje w sprawie własnych dodatkowych wymogów i określać je w odpowiednich oświadczeniach dotyczących praktyk w zakresie certyfikacji (CPS), o ile nie są one sprzeczne z wymogami określonymi w polityce certyfikacji. Szczegółowe informacje na temat audytu i publikacji CPS znajdują się w sekcji 1.5.

W polityce certyfikacji określono również cele, do jakich można wykorzystywać główne urzędy certyfikacji, ich podporządkowane urzędy certyfikacji oraz wydawane przez nie certyfikaty. Określono w niej zobowiązania przyjęte przez:

- TLM;
- każdy główny urząd certyfikacji, którego certyfikaty są wymienione na ECTL;
- urzędy certyfikacji podporządkowane głównemu urzędowi certyfikacji (organ ds. rejestracji i organ autoryzujący);
- każdego członka lub organizację odpowiedzialnych za jedną z jednostek modelu zaufania C-ITS lub stosujących taki model.

W polityce certyfikacji określono również obowiązki mające zastosowanie do:

- TLM;
- każdy główny urząd certyfikacji, którego certyfikaty są wymienione na ECTL;
- każdego urzędu certyfikacji podporządkowanego urzędowi certyfikacji certyfikowanemu przez główny urząd certyfikacji;
- wszystkich jednostek końcowych;
- każdego członka organizacji odpowiedzialnego za jedną z jednostek modelu zaufania C-ITS lub prowadzącego go.

Ponadto w polityce certyfikacji określono wymogi dotyczące dokumentowania ograniczeń w zakresie zobowiązań i obowiązków w CPS każdego głównego urzędu certyfikacji, którego certyfikaty są wymienione w ECTL.

Niniejsza polityka certyfikacji jest zgodna z polityką certyfikacji i ramami praktyk certyfikacji przyjętymi przez grupę zadaniową ds. inżynierii internetowej (ang. Internet Engineering Task Force – IETF) [3].

1.2. Definicje i skróty

Stosuje się definicje podane w [2], [3] i [4].

AA	organ autoryzujący
AT	bilet autoryzacyjny
CA	urząd certyfikacji
CP	polityka certyfikacji
CPA	organ ds. polityki certyfikacji C-ITS
CPOC	punkt kontaktowy ds. C-ITS
CPS	oświadczenie dotyczące praktyk w zakresie certyfikacji
CRL	lista unieważnionych certyfikatów
EA	organ ds. rejestracji
EC	dane uwierzytelniające rejestrację
ECIES	zintegrowany system kryptograficzny oparty na krzywych eliptycznych
EE	jednostka końcowa (tj. stacja C-ITS)
ECTL	europejska zaufana lista certyfikatów
EU CCMS	unijny system zarządzania danymi uwierzytelniającymi C-ITS
RODO	Ogólne rozporządzenie o ochronie danych

HSM	moduł zabezpieczeń sprzętu
PKI	infrastruktura klucza publicznego
RA	organ ds. rejestracji
podporządkowany urząd certyfikacji	organ ds. rejestracji i organ autoryzujący
Zarządzający zaufaną listą	zarządzający zaufaną listą

Glosariusz

wnioskodawca	Osoba fizyczna lub prawna, która ubiega się o wydanie (lub o przedłużenie) certyfikatu. Po utworzeniu pierwszego certyfikatu (inicjalizacji), wnioskodawca jest zwany abonentem. W przypadku certyfikatów wydawanych jednostkom końcowym abonent (wnioskujący o certyfikat) jest jednostką, która sprawuje kontrolę nad jednostką końcową, której wydany zostaje certyfikat, lub kieruje jej działaniami, nawet jeżeli to jednostka końcowa wysyła rzeczywisty wniosek o wydanie certyfikatu.
organ autoryzujący	W niniejszym dokumencie termin „organ autoryzujący" odnosi się nie tylko do konkretnej funkcji organu autoryzującego, ale także do podmiotu prawnego lub operacyjnego, który zarządza tym organem.
urząd certyfikacji	Główny urząd certyfikacji, organ ds. rejestracji i organ autoryzujący są zbiorczo nazywane „urzędem certyfikacji".
model zaufania C-ITS	Model zaufania C-ITS odpowiada za nawiązanie relacji wzajemnego zaufania między stacjami C-ITS. Jest on wdrażany poprzez stosowanie infrastruktury klucza publicznego składającego się z głównych urzędów certyfikacji, CPOC, TLM, organów ds. rejestracji, organów autoryzujących i bezpiecznej sieci.
zręczność kryptograficzna	Zdolność jednostek modelu zaufania C-ITS do dostosowania polityki certyfikacji do zmieniających się środowisk lub do nowych przyszłych wymogów, np. poprzez zmianę algorytmów kryptograficznych i długości klucza z biegiem czasu.
moduł kryptograficzny	Bezpieczny element oparty na sprzęcie służący do generowania lub przechowywania kluczy, generowania numerów losowych oraz podpisywania lub szyfrowania danych.
organ ds. rejestracji	W niniejszym dokumencie termin „organ ds. rejestracji" odnosi się nie tylko do konkretnej funkcji organu ds. rejestracji, ale także do osoby prawnej lub jednostki operacyjnej zarządzających tym organem.
Uczestnicy infrastruktury klucza publicznego	Jednostki modelu zaufania C-ITS, tj. TLM, główne urzędy certyfikacji, organy ds. rejestracji, organy autoryzujące i stacje C-ITS.
ponowne wprowadzenie certyfikatu	Ten podkomponent służy do opisu pewnych szczegółów dotyczących abonenta lub innego uczestnika, który generuje nową parę kluczy i składa wniosek o wydanie nowego certyfikatu, który poświadcza nowy klucz publiczny określony w [3].
repozytorium	Repozytorium wykorzystywane do przechowywania certyfikatów i informacji na temat certyfikatów dostarczonych przez jednostki modelu zaufania C-ITS zgodnie z definicją podaną w sekcji 2.3.
główny urząd certyfikacji	W niniejszym dokumencie termin „główny urząd certyfikacji" odnosi się nie tylko do konkretnej funkcji głównego urzędu certyfikacji, ale także do osoby prawnej lub jednostki operacyjnej zarządzających tym organem.
podmiot	Osoba fizyczna, urządzenie, system, komórka lub osoba prawna wskazana w certyfikacie jako podmiot, tj. abonent albo urządzenie znajdujące się pod kontrolą abonenta lub obsługiwane przez niego.
abonent	Osoba fizyczna lub prawna, której wydawane jest świadectwo i która jest prawnie związana umową abonencką lub umową użytkowania.

umowa abonencka	Umowa między urzędem certyfikacji a wnioskodawcą/abonentem, w której określono prawa i obowiązki stron.

1.3. Uczestnicy infrastruktury klucza publicznego

1.3.1. Wprowadzenie

Uczestnicy infrastruktury klucza publicznego odgrywają w niej rolę określoną w przedmiotowej polityce. Uczestnik może jednocześnie pełnić kilka ról, chyba że jest to wyraźnie zabronione. Może istnieć zakaz pełnienia poszczególnych ról w tym samym czasie, aby uniknąć konfliktów interesów lub zapewnić podział obowiązków.

Uczestnicy mogą również przekazać część swojej roli innym jednostkom w ramach umowy o świadczenie usług. Jeżeli na przykład informacje o statusie unieważnienia przekazywane są z wykorzystaniem CRL, urząd certyfikacji jest również emitentem CRL, ale może przekazać odpowiedzialność za wystawianie CRL innej jednostce.

Role infrastruktury klucza publicznego obejmują:

- role autorytatywne, tj. każda funkcja jest utworzona w sposób jednoznaczny;
- role operacyjne, tj. role, które można stworzyć w co najmniej jednej jednostce.

Na przykład główny urząd certyfikacji może zostać powołany przez podmiot komercyjny, grupę mającą przedmiot wspólnego zainteresowania, organizację krajową lub organizację europejską.

Rysunek 1 przedstawia strukturę modelu zaufania C-ITS opartą na [2]. W tym miejscu strukturę przedstawiono jedynie pokrótce, zaś główne elementy opisano bardziej szczegółowo w sekcjach 1.3.2–1.3.6.

Organ ds. polityki certyfikacji C-ITS wyznacza TLM, który w związku z tym staje się zaufanym podmiotem dla wszystkich uczestników infrastruktury klucza publicznego. Organ ds. polityki certyfikacji C-ITS zatwierdza działania głównego urzędu certyfikacji i potwierdza, że TLM może zaufać głównemu urzędowi certyfikacji (głównym urzędom certyfikacji). TLM wydaje ECTL, która wzbudza zaufanie wszystkich uczestników infrastruktury klucza publicznego do zatwierdzonych głównych urzędów certyfikacji. Główny urząd certyfikacji wydaje certyfikaty organowi ds. rejestracji i organowi autoryzującemu, okazując w ten sposób zaufanie do ich działań. Organ ds. rejestracji wydaje certyfikaty rejestracji nadającym i pośredniczącym stacjom C-ITS (jako jednostkom końcowym), okazując w ten sposób zaufanie do ich działań. Na podstawie zaufania do organu ds. rejestracji organ autoryzujący wydaje bilety autoryzacyjne stacjom C-ITS.

Odbierająca i przekazująca stacja C-ITS (jako strona pośrednicząca) może mieć zaufanie do innych stacji C-ITS, ponieważ bilety autoryzacyjne są wydawane przez organ autoryzujący cieszący się zaufaniem głównego urzędu certyfikacji, któremu z kolei ufają TLM i organ ds. polityki certyfikacji C-ITS.

Należy zauważyć, że na rys. 1 pokazano jedynie poziom głównego urzędu certyfikacji w modelu zaufania C-ITS. Szczegółowe informacje na temat niższych poziomów przedstawiono w kolejnych sekcjach przedmiotowej polityki certyfikacji lub w CPS dotyczącym poszczególnych głównych urzędów certyfikacji.

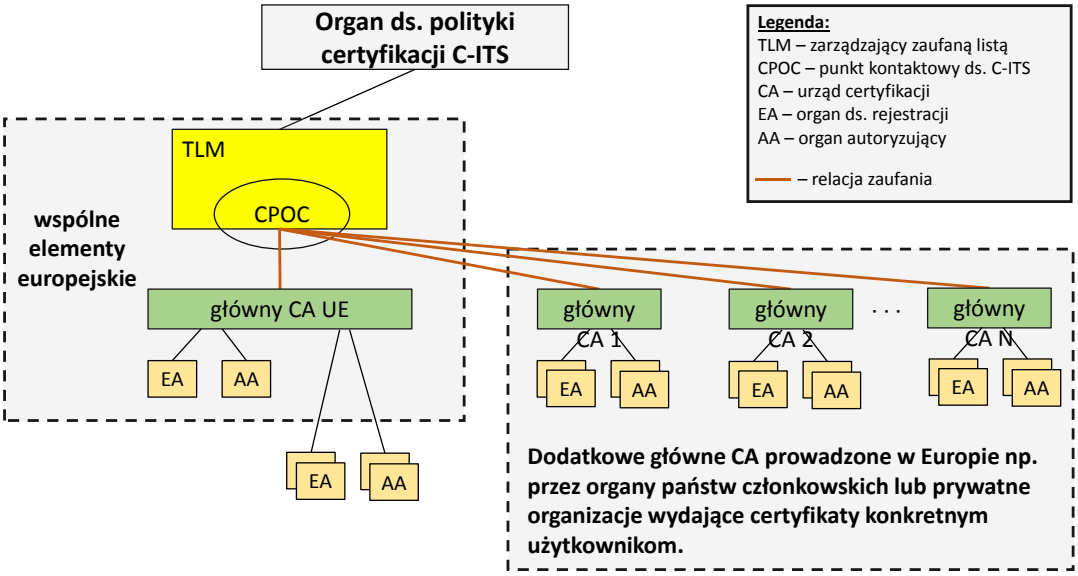
Rys. 2 przedstawia przegląd przepływów informacji między uczestnikami infrastruktury klucza publicznego. Zielone kropki oznaczają przepływy, które

wymagają komunikacji między maszynami. Przepływy informacji oznaczone kolorem czerwonym mają określone wymogi w zakresie ochrony.

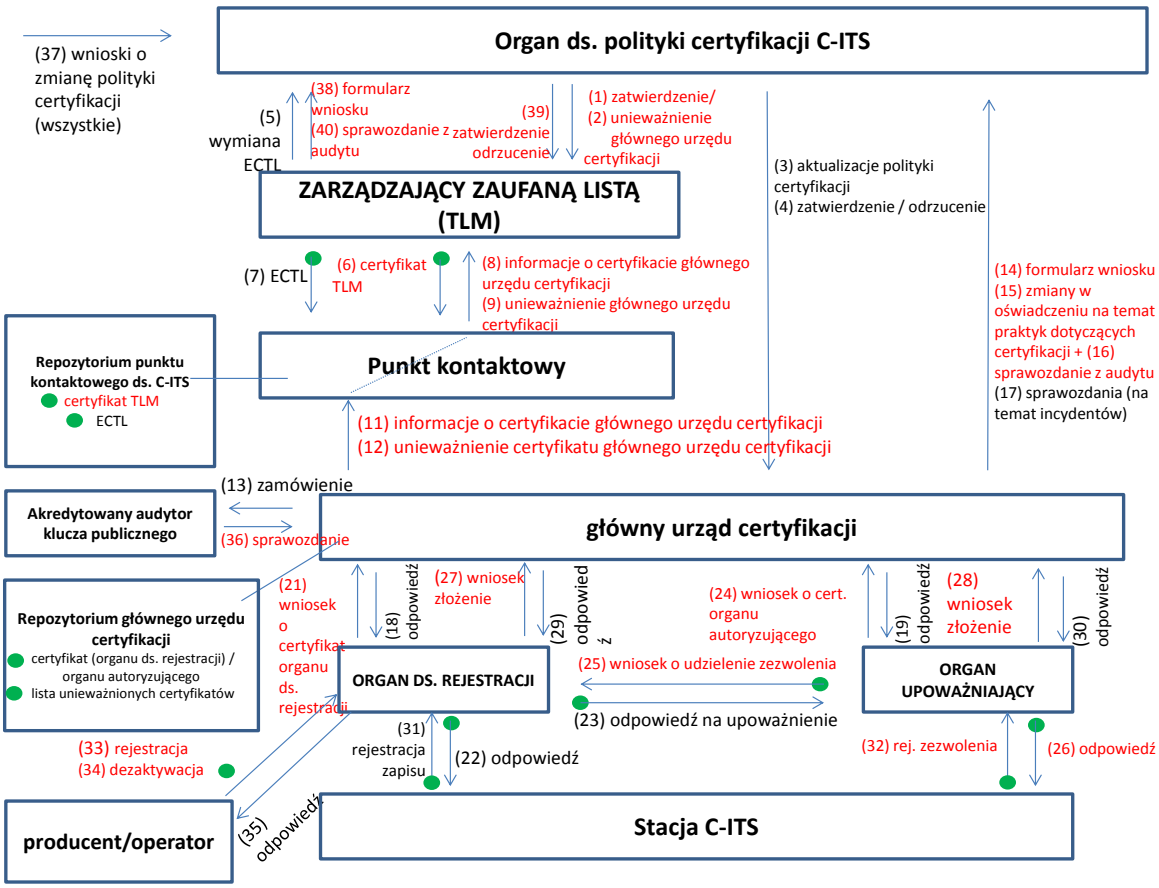
Model zaufania C-ITS opiera się na strukturze wielu głównych urzędów certyfikacji, gdzie certyfikaty wydawane przez główny urząd certyfikacji są przekazywane okresowo (jak przedstawiono poniżej) do centralnego punktu kontaktowego za pomocą bezpiecznego protokołu (np. certyfikatów łączących) określonego przez ten punkt.

Głównym urzędem certyfikacji może zarządzać organizacja rządowa lub prywatna. Architektura modelu zaufania C-ITS obejmuje co najmniej jeden główny urząd certyfikacji (unijny główny urząd certyfikacji na tym samym poziomie, co inny główny urząd certyfikacji). Wszystkie jednostki uczestniczące w modelu zaufania C-ITS, które nie chcą zakładać własnych głównych urzędów certyfikacji, wyznaczają unijny główny urząd certyfikacji. CPOC przekazuje otrzymane certyfikaty głównego urzędu certyfikacji do TLM, który odpowiada za gromadzenie i podpisywanie listy certyfikatów wydanych przez główny urząd certyfikacji, oraz przesyłanie ich z powrotem do CPOC, co sprawia, że są one publicznie dostępne (zob. poniżej).

Relacje zaufania między jednostkami w modelu zaufania C-ITS przedstawiono na poniższych wykresach, w tabelach i sekcjach.



Rysunek 1: Struktura modelu zaufania C-ITS



Rysunek 2: Przepływy informacji w modelu zaufania C-ITS

Identyfikator przepływu	Nadawca	Odbiorca	Treść	Odniesienie
1)	CPA	Zarządzający zaufaną listą	zatwierdzenie wniosku głównego CA	8
2)	CPA	Zarządzający zaufaną listą	informacje o unieważnieniu głównego CA	8.5
3)	CPA	główny CA	aktualizacje polityki certyfikacji	1.5
4)	CPA	główny CA	zatwierdzenie/odrzucenie wniosku głównego CA lub zmiany we wniosku CPS lub proces audytu	8.5, 8.6
5)	Zarządzający zaufaną listą	CPA	powiadomienie o zmianie ECTL	4, 5.8.1
6)	Zarządzający zaufaną listą	CPOC	Certyfikat zarządzającego zaufaną listą	4.4.2.
7)	Zarządzający zaufaną listą	CPOC	ECTL	4.4.2.
8)	CPOC	Zarządzający zaufaną listą	informacje o certyfikacie głównego CA	4.3.1.1.
9)	CPOC	Zarządzający zaufaną listą	unieważnienie certyfikatu głównego CA	7.3
10)	CPOC	wszystkie jednostki końcowe	Certyfikat zarządzającego zaufaną listą	4.4.2.
11)	główny CA	CPOC	informacje o certyfikacie głównego CA	4.3.1.1.
12)	główny CA	CPOC	unieważnienie certyfikatu głównego CA	7.3
13)	główny CA	audytor	zlecenie audytu	8
14)	główny CA	CPA	formularz wniosku głównego CA – pierwszy wniosek	4.1.2.1.
15)	główny CA	CPA	formularz wniosku głównego CA – zmiany w CPS	1.5.1.
16)	główny CA	CPA	formularz wniosku głównego CA – sprawozdanie z audytu	8.6
17)	główny CA	CPA	sprawozdania głównego CA z incydentów, w tym unieważnienie podporządkowanych CA (EA, AA)	załącznik III, 7.3.1
18)	główny CA	EA	odpowiedź na certyfikat EA	4.2.2.3.
19)	główny CA	AA	odpowiedź na certyfikat AA	4.2.2.3.
20)	główny CA	wszystkie	certyfikat EA/AA, CRL	4.4.2.
21)	EA	główny CA	wniosek o certyfikat EA	4.2.2.3.

22)	EA	Stacja C-ITS	odpowiedź na dane uwierzytelniające rejestrację	4.3.1.4.
23)	EA	AA	odpowiedź na upoważnienie	4.2.2.5.
24)	AA	główny CA	wniosek o certyfikat AA	4.2.2.3.
25)	AA	EA	wniosek o upoważnienie	4.2.2.5.
26)	AA	Stacja C-ITS	odpowiedź na bilet autoryzacyjny	4.3.1.5.
27)	EA	główny CA	złożenie wniosku	4.1.2.3.
28)	AA	główny CA	złożenie wniosku	4.1.2.3.
29)	główny CA	EA	odpowiedź	4.12 i 4.2.1
30)	główny CA	AA	odpowiedź	4.12 i 4.2.1
31)	Stacja C-ITS	EA	wniosek o dane uwierzytelniające rejestrację	4.2.2.4.
32)	Stacja C-ITS	AA	wniosek o bilet autoryzacyjny	4.2.2.5.
33)	producent/operator	EA	rejestracja	4.2.1.4.
34)	producent/operator	EA	dezaktywacja	7.3
35)	EA	producent/operator	odpowiedź	4.2.1.4.
36)	audytor	główny CA	sprawozdanie	8.1
37)	wszystkie	CPA	wnioski w sprawie zmiany polityki certyfikacji	1.5
38)	Zarządzający zaufaną listą	CPA	formularz wniosku	4.1.2.2.
39)	CPA	Zarządzający zaufaną listą	przyjęcie/odrzucenie	4.1.2.2.
40)	Zarządzający zaufaną listą	CPA	sprawozdanie z audytu	4.1.2.2.

Tabela 1: Szczegółowy opis przepływów informacji w modelu zaufania C-ITS

1.3.2. Organ ds. polityki certyfikacji C-ITS

1) W skład organu ds. polityki certyfikacji C-ITS wchodzą przedstawiciele zainteresowanych stron publicznych i prywatnych (np. państw członkowskich, producentów pojazdów itp.) uczestniczących w modelu zaufania C-ITS. Odpowiada on za dwie role składowe:

   1) zarządzanie polityką certyfikacji, w tym:

      - zatwierdzanie bieżących i przyszłych wniosków w sprawie zmiany polityki certyfikacji;

- podejmowanie decyzji w sprawie przeglądu wniosków o zmianę polityki certyfikacji i zaleceń przedstawionych przez innych uczestników lub jednostki infrastruktury klucza publicznego;
- podejmowanie decyzji o wydaniu nowych wersji polityki certyfikacji;

2) zarządzanie uwierzytelnianiem infrastruktury klucza publicznego, w tym:

- określanie i publikowanie zatwierdzeń CPS oraz procedur audytu urzędu certyfikacji (zwanych łącznie „procedurami zatwierdzania urzędu certyfikacji"), a także podejmowanie decyzji w ich sprawie;
- upoważnianie CPOC do działalności i regularnej sprawozdawczości;
- upoważnianie TLM do działalności i regularnej sprawozdawczości;
- zatwierdzanie CPS głównego urzędu certyfikacji, jeżeli jest zgodne ze wspólną i ważną polityką certyfikacji;
- weryfikacja sprawozdań z audytu sporządzonych przez akredytowanego audytora infrastruktury klucza publicznego w odniesieniu do wszystkich głównych urzędów certyfikacji;
- powiadamianie TLM o liście zatwierdzonych lub niezatwierdzonych głównych urzędów certyfikacji i ich certyfikatach na podstawie otrzymanych sprawozdań zatwierdzających sporządzonych przez główne urzędy certyfikacji i regularnych sprawozdań działalności.

2) Upoważniony przedstawiciel organu ds. polityki certyfikacji C-ITS odpowiada za uwierzytelnianie upoważnionego przedstawiciela TLM i zatwierdzenie formularza wniosku o rejestrację TLM. Organ ds. polityki certyfikacji C-ITS jest odpowiedzialny za upoważnianie TLM do działania zgodnie z niniejszą sekcją.

1.3.3. Zarządzający zaufaną listą

3) TLM jest pojedynczą jednostką wyznaczoną przez organ ds. polityki certyfikacji C-ITS.

4) TLM odpowiada za:

- obsługę ECTL zgodnie ze wspólną ważną polityką certyfikacji i regularną sprawozdawczością z działalności przed organem ds. polityki certyfikacji C-ITS w odniesieniu do ogólnego bezpiecznego działania modelu zaufania C-ITS;
- otrzymywanie certyfikatów głównego urzędu certyfikacji od CPOC;
- włączanie certyfikatów głównego urzędu certyfikacji do ECTL lub wyłączanie ich z ECTL po otrzymaniu powiadomienia od organu ds. polityki certyfikacji C-ITS;
- podpisywanie ECTL;
- regularne i terminowe przekazywanie ECTL do CPOC.

1.3.4. Akredytowany audytor infrastruktury klucza publicznego

5) Akredytowany audytor infrastruktury klucza publicznego odpowiada za:

- przeprowadzanie lub organizowanie audytów w głównym urzędzie certyfikacji, TLM i podporządkowanych urzędach certyfikacji;
- przekazanie sprawozdania z audytu (wstępnego lub okresowego) do organu ds. polityki certyfikacji C-ITS zgodnie z wymogami określonymi w sekcji 8 poniżej. Sprawozdanie z audytu powinno zawierać zalecenia akredytowanego audytora infrastruktury klucza publicznego;
- powiadamianie jednostki zarządzającej głównym urzędem certyfikacji o pomyślnej lub nieudanej realizacji wstępnego lub okresowego audytu podporządkowanych urzędów certyfikacji;
- ocenę zgodności CPS z przedmiotową polityką certyfikacji.

1.3.5. Punkt kontaktowy ds. C-ITS (CPOC)

6) CPOC jest pojedynczą jednostką wyznaczoną przez organ ds. polityki certyfikacji C-ITS. Upoważniony przedstawiciel organu ds. polityki certyfikacji C-ITS odpowiada za uwierzytelnienie upoważnionego przedstawiciela CPOC i zatwierdzenie formularza wniosku o rejestrację CPOC. Organ ds. polityki certyfikacji C-ITS jest odpowiedzialny za upoważnienie CPOC do działania zgodnie z niniejszą sekcją.

7) CPOC odpowiada za:

- ustanawianie bezpiecznej wymiany komunikatów między wszystkimi jednostkami w ramach modelu zaufania C-ITS i przyczynianie się do tej wymiany w skuteczny i szybki sposób;
- przegląd wniosków o wprowadzenie zmian proceduralnych i zaleceń przedstawionych przez pozostałych uczestników modelu zaufania (np. główne urzędy certyfikacji);
- przekazywanie certyfikatów wydanych przez główny urząd certyfikacji do TLM;
- publikowanie wspólnej kotwicy zaufania (ang. trust anchor – aktualnego klucza publicznego i certyfikatu łączącego TLM);
- publikowanie ECTL.

Wszystkie szczegóły dotyczące ECTL można znaleźć w sekcji 7.

1.3.6. Role operacyjne

8) Następujące jednostki określone w [2] odgrywają rolę operacyjną, zgodnie z definicją w RFC 3647:

Element funkcjonalny	rola PKI ([3] oraz [4])	rola szczegółowa ([2])
główny urząd certyfikacji	CA/RA (organ ds. rejestracji)	Dostarcza EA i AA dowód na to, że mogą wydawać EC lub AT.
organ ds. rejestracji	abonent głównego urzędu certyfikacji / podmiot certyfikatu organu ds. rejestracji CA/RA	Uwierzytelnia stację C-ITS i daje jej dostęp do komunikatów ITS.
organ autoryzujący	abonent głównego urzędu certyfikacji / podmiot certyfikatu organu autoryzującego CA/RA	Dostarcza stacji C-ITS miarodajny dowód na to, że może korzystać ze szczególnych usług ITS.
nadająca stacja C-ITS	podmiot certyfikatu jednostki końcowej dane uwierzytelniające rejestrację)	Nabywa prawa od EA w celu uzyskania dostępu do komunikatów ITS. Negocjuje z AA prawa do przywołania usług ITS. Wysyła komunikaty bez urządzeń pośredniczących i przez stacje pośredniczące.
pośrednicząca stacja C-ITS	strona pośrednicząca / podmiot certyfikatu jednostki końcowej	Otrzymuje komunikat od nadającej stacji C-ITS i przekazuje je do odbierającej stacji C-ITS, jeżeli jest to wymagane.
odbierająca stacja C-ITS	strona pośrednicząca	Odbiera komunikaty z nadającej lub pośredniczącej stacji C-ITS.
producent	abonent EA	Wprowadza informacje niezbędne do zarządzania bezpieczeństwem do stacji C-ITS na etapie produkcji.
operator	abonent EA/AA	Wgrywa i aktualizuje informacje niezbędne do zarządzania bezpieczeństwem do stacji C-ITS na etapie eksploatacji.

Tabela 2: Role operacyjne

Uwaga: zgodnie z [4] w niniejszej polityce certyfikacji stosuje się różne terminy w odniesieniu do „abonenta", który zawiera umowę z urzędem certyfikacji dotyczącą wydania certyfikatów oraz w odniesieniu do „podmiotu", którego dotyczy certyfikat. Abonenci to wszystkie jednostki, które zawarły stosunek umowny z urzędem certyfikacji. Podmioty to jednostki, których dotyczą certyfikaty. Organy ds. rejestracji / organy autoryzujące są abonentami oraz jednostkami głównego urzędu certyfikacji i mogą składać wnioski o wydanie certyfikatów do organu ds. rejestracji / organu autoryzującego. Stacje C-ITS są podmiotami i mogą składać wnioski o wydanie certyfikatów jednostek końcowych.

9) Organy ds. rejestracji:

Organ ds. rejestracji ma pełnić rolę organu ds. rejestracji dla jednostek końcowych. Jedynie uwierzytelniony i upoważniony abonent może zarejestrować nowe jednostki końcowe (stacje C-ITS) w organie ds. rejestracji. Odpowiednie główne urzędy certyfikacji mają pełnić rolę organów ds. rejestracji w odniesieniu do organów ds. rejestracji i organów autoryzujących.

1.4. Zastosowanie certyfikatu

1.4.1. Obowiązujące dziedziny stosowania

10) Certyfikaty wydane na podstawie niniejszej polityki certyfikacji mają być wykorzystywane do walidacji podpisów cyfrowych w kontekście komunikacji współpracujących inteligentnych systemów transportowych zgodnie z architekturą referencyjną określoną w [2].

11) Profile certyfikatów w [5] określają zastosowania certyfikatów dla zarządzających zaufaną listą, głównych urzędów certyfikacji, organów ds. rejestracji, organów autoryzujących i jednostek końcowych.

1.4.2. Ograniczenia odpowiedzialności

12) Nie zezwala się na stosowanie, ani nie planuje wykorzystania certyfikatów w:

- okolicznościach złamania, przekroczenia lub naruszenia dowolnego obowiązującego przepisu prawa, rozporządzenia (np. ogólnego rozporządzenia o ochronie danych), decyzji lub zarządzenia rządu;
- okolicznościach przekroczenia lub naruszenia praw innych osób;
- przypadku naruszenia przedmiotowej polityki certyfikacji lub odpowiedniej umowy abonenckiej;
- wszelkich okolicznościach, w których ich zastosowanie mogłoby bezpośrednio prowadzić do śmierci, uszkodzenia ciała lub poważnych szkód w środowisku (np. w wyniku awarii obiektów jądrowych, nawigacji lub komunikacji lotniczej lub systemów sterowania uzbrojeniem);
- okolicznościach, które stoją w sprzeczności z ogólnymi celami zwiększenia bezpieczeństwa ruchu drogowego i zwiększenia efektywności transportu drogowego w Europie.

1.5. Zarządzanie polityką certyfikacji

1.5.1. Aktualizacja CPS urzędów certyfikacji wymienionych na ECTL

13) Każdy główny urząd certyfikacji wymieniony na ECTL publikuje własne CPS, które musi być zgodne z tą polityką. Główny urząd certyfikacji może przewidzieć dodatkowe wymogi, ale zapewnia, aby wszystkie wymogi zawarte w przedmiotowej polityce certyfikacji były spełnione przez cały czas.

14) Każdy główny urząd certyfikacji wymieniony na ECTL wdraża odpowiedni proces zmiany dokumentu CPS. Kluczowe właściwości procesu zmiany są dokumentowane w publicznej części CPS.

15) Proces zmiany służy zapewnieniu, aby wszystkie zmiany tej polityki certyfikacji były starannie zbadane i, jeżeli jest to konieczne ze względu na zgodność ze zmienioną polityką certyfikacji, aby CPS było aktualizowane zgodnie z harmonogramem przewidzianym dla etapu wdrażania w ramach procesu zmiany polityki certyfikacji. W szczególności proces zmiany obejmuje procedury zmiany w przypadku sytuacji nadzwyczajnej, które zapewniają terminowe wdrożenie zmian w polityce certyfikacji istotnych z punktu widzenia bezpieczeństwa.

16) Proces zmiany obejmuje odpowiednie środki służące weryfikacji zgodności wszystkich zmian w CPS z polityką certyfikacji. Wszelkie zmiany w CPS muszą być jasno dokumentowane. Przed wdrożeniem nowej wersji CPS akredytowany audytor infrastruktury klucza publicznego musi potwierdzić jego zgodność z polityką certyfikacji.

17) Główny urząd certyfikacji powiadamia organ ds. polityki certyfikacji C-ITS o wszelkich zmianach CPS obejmujących co najmniej następujące informacje:

- dokładny opis zmiany;
- uzasadnienie zmiany;
- sprawozdanie akredytowanego audytora infrastruktury klucza publicznego potwierdzające jego zgodność z polityką certyfikacji;
- dane kontaktowe osoby odpowiedzialnej za CPS;
- planowane ramy czasowe wdrożenia.

1.5.2. Procedury przyjmowania CPS

18) Przed rozpoczęciem działalności potencjalny urząd certyfikacji przedstawia swoje CPS akredytowanemu audytorowi infrastruktury klucza publicznego w ramach nakazu przeprowadzenia audytu w zakresie zgodności (przepływ 13) i organowi ds. polityki certyfikacji C-ITS do zatwierdzenia (przepływ 15).

19) Główny urząd certyfikacji przedstawia zmiany swojego CPS akredytowanemu audytorowi infrastruktury klucza publicznego w ramach nakazu przeprowadzenia audytu w zakresie zgodności (przepływ 13) i organowi ds. polityki certyfikacji C-ITS do zatwierdzenia (przepływ 15) przed wejściem w życie tych zmian.

20) Organ ds. rejestracji/organ autoryzujący przedstawia swoje oświadczenie dotyczące praktyk w zakresie certyfikacji lub zmiany tego oświadczenia głównemu urzędowi certyfikacji. Główny urząd certyfikacji może zażądać certyfikatu zgodności od organu krajowego lub podmiotu prywatnego odpowiedzialnego za zatwierdzenie organu ds. rejestracji/organu autoryzującego, jak określono w sekcjach 4.1.2 i 8.

21) Akredytowany audytor infrastruktury klucza publicznego ocenia oświadczenie dotyczące praktyk w zakresie certyfikacji zgodnie z sekcją 8.

22) Akredytowany audytor infrastruktury klucza publicznego przekazuje wyniki oceny oświadczenia dotyczącego praktyk w zakresie certyfikacji jako część sprawozdania z audytu, jak określono w sekcji 8.1. Oświadczenie dotyczące praktyk w zakresie certyfikacji zostaje przyjęte lub odrzucone w ramach procedury przyjęcia sprawozdania z audytu o której mowa w sekcjach 8.5 i 8.6.

2. OBOWIĄZKI ZWIĄZANE Z PUBLIKACJĄ I REPOZYTORIUM

2.1. Metody publikowania informacji o certyfikatach

23) Informacje o certyfikatach mogą być publikowane zgodnie z sekcją 2.5:

- w sposób regularny lub okresowy; lub
- w odpowiedzi na wniosek jednej z uczestniczących jednostek.

W każdym przypadku do publikacji zastosowanie mają różne stopnie pilności, a w związku z tym również inne harmonogramy, jednak jednostki muszą być przygotowane na oba rodzaje ustaleń.

24) Regularna publikacja informacji o certyfikacie umożliwia określenie maksymalnego terminu, do którego informacje o certyfikacie są aktualizowane dla wszystkich węzłów sieci C-ITS. Częstotliwość publikacji wszystkich informacji o certyfikatach jest określona w sekcji 2.2.

25) Na wniosek jednostek uczestniczących w sieci C-ITS dowolny uczestnik może rozpocząć publikowanie informacji o certyfikacie w dowolnym momencie i, w zależności od jego statusu, wystąpić z wnioskiem o aktualny zestaw informacji o certyfikacie, aby stać się w pełni zaufanym węzłem sieci C-ITS. Celem takiej publikacji jest głównie zaktualizowanie danych posiadanych przez jednostki w zakresie ogólnego aktualnego statusu informacji o certyfikacie w sieci oraz umożliwienie im komunikacji na zasadzie zaufania do czasu kolejnej regularnej publikacji informacji.

26) Pojedynczy główny urząd certyfikacji może również rozpocząć publikację informacji o certyfikacie w dowolnym momencie poprzez wysłanie uaktualnionego zestawu certyfikatów do wszystkich „członków-abonentów" sieci C-ITS, którzy są regularnymi odbiorcami takich informacji. Wspiera to funkcjonowanie urzędów certyfikacji i umożliwia im komunikację z członkami między regularnymi i zaplanowanymi terminami publikacji certyfikatów.

27) W sekcji 2.5 określono mechanizm i wszystkie procedury dotyczące publikowania certyfikatów głównego urzędu certyfikacji i ECTL.

28) CPOC publikuje certyfikaty głównego urzędu certyfikacji (w takiej formie jak na ECTL, przeznaczonej do wykorzystania publicznego), certyfikaty TLM i ECTL, które wydaje.

29) Główne urzędy certyfikacji publikują swoje certyfikaty organu ds. rejestracji / organu autoryzującego i listy unieważnionych certyfikatów i są w stanie wspierać wszystkie trzy mechanizmy, o których mowa, w celu ich opublikowania wśród „członków-abonentów" i stron ufających, podejmując wszelkie niezbędne kroki w celu zapewnienia bezpiecznej transmisji, o której mowa w sekcji 4.

2.2. Czas lub częstotliwość publikacji

30) Wymogi dotyczące harmonogramu publikacji certyfikatów i CRL muszą zostać określone w świetle różnych ograniczających czynników dotyczących pojedynczych węzłów C-ITS, przy czym ogólnym celem jest prowadzenie „sieci zaufania" i jak najszybsze publikowanie aktualizacji dla zaangażowanych stacji C-ITS.

- W przypadku regularnej publikacji uaktualnionych informacji o certyfikatach (np. zmianach w treści ECTL lub CRL) wymagany jest maksymalny okres trzech miesięcy na osiągnięcie bezpiecznego działania sieci C-ITS.
- Główne urzędy certyfikacji publikują certyfikaty urzędów certyfikacji i CRL najszybciej jak to możliwe po ich wydaniu.
- W celu publikacji CRL korzysta się z repozytorium głównego urzędu certyfikacji.

Ponadto w CPS każdego urzędu certyfikacji wyznacza się okres, w którym certyfikat zostanie opublikowany po jego wydaniu przez urząd certyfikacji.

W niniejszej sekcji określono jedynie czas lub częstotliwość regularnej publikacji. Środki łączności służące aktualizacji stacji C-ITS o dane z ECTL i CRL w ciągu tygodnia od ich publikacji (w normalnych warunkach działalności, np. przy zasięgu sieci komórkowej, w pojazdach w trakcie rzeczywistej eksploatacji itp.) należy wdrożyć zgodnie z wymogami określonymi w niniejszym dokumencie.

2.3. Repozytoria

31) Dla pojedynczych jednostek wymogi dotyczące struktury repozytorium przechowywania certyfikatów oraz informacji dostarczonych przez jednostki sieci C-ITS są następujące:

- zasadniczo każdy urząd certyfikacji powinno posługiwać się repozytorium aktualnie posiadanych informacji o aktywnych certyfikatach organu ds. rejestracji / organu autoryzującego i CRL w celu publikacji certyfikatów dla pozostałych uczestników infrastruktury klucza publicznego (np. usługi katalogowe oparte na LDAP). Repozytorium każdego głównego urzędu certyfikacji obsługuje wszelkie wymagane kontrole dostępu (sekcja 2.4) i czas transmisji (sekcja 2.2) dla każdej metody dystrybucji informacji związanych z C-ITS.
- Repozytorium TLM (które przechowuje certyfikaty ECTR i TLM publikowane przez CPOC) powinno opierać się na mechanizmie publikacji, który jest w stanie zapewnić czas transmisji określony w sekcji 2.2 w odniesieniu do każdej metody dystrybucji.

Wymogi dotyczące organów autoryzujących nie zostały określone, jednak muszą wspierać te same poziomy bezpieczeństwa, co inne jednostki, a poziomy te muszą zadeklarować w swoich CPS.

2.4. Kontrole dostępu do repozytoriów

32) Wymogi dotyczące kontroli dostępu do repozytoriów informacji o certyfikacie muszą spełniać co najmniej ogólne normy bezpiecznego przetwarzania informacji określone w normie ISO/IEC 27001, a także wymogi określone w sekcji 4. Ponadto odzwierciedlają one potrzeby związane z bezpieczeństwem przetwarzania danych, które należy ustanowić dla poszczególnych etapów procesu w ramach publikacji informacji o certyfikacie.

- Obejmuje to wdrożenie repozytorium dla certyfikatów TLM oraz ECTL w TLM/CPOC. Każdy urząd certyfikacji lub operator repozytorium wdraża kontrole dostępu w odniesieniu do wszystkich jednostek C-ITS i podmiotów zewnętrznych na co najmniej trzech różnych poziomach (np. publicznym, ograniczonym do jednostek C-ITS, głównego urzędu certyfikacji), aby zapobiec dodawaniu, zmienianiu i usuwaniu wpisów do repozytoriów przez podmioty nieupoważnione.
- Konkretne mechanizmy kontroli dostępu dla pojedynczej jednostki powinny wchodzić w skład odpowiedniego CPS.
- W odniesieniu do każdego głównego urzędu certyfikacji repozytoria organu ds. rejestracji i organu autoryzującego spełniają te same wymogi

dotyczące procedur kontroli dostępu, niezależnie od miejsca i stosunku umownego z usługodawcą obsługującym repozytorium.

Jako punkt wyjścia dla poziomów kontroli dostępu każdy główny urząd certyfikacji lub operator repozytorium powinien zapewniać co najmniej trzy różne poziomy (np. publiczny, ograniczony do jednostek C-ITS, głównego urzędu certyfikacji).

2.5. Publikacja informacji o certyfikacie

2.5.1. Publikacja informacji o certyfikacie przez TLM

33) TLM w europejskiej wspólnej dziedzinie zaufania C-ITS publikuje następujące informacje za pośrednictwem CPOC:

- wszystkie aktualnie ważne certyfikaty TLM na następny okres działania (certyfikat bieżący i łączący, jeżeli są dostępne);
- informacje na temat punktu dostępu repozytorium centralnego punktu kontaktowego w celu przedłożenia podpisanego wykazu głównych urzędów certyfikacji (ECTL);
- ogólny punkt informacyjny dla wdrażania ECTL i C-ITS.

2.5.2. Publikacja informacji o certyfikacie przez urzędy certyfikacji

34) Główne urzędy certyfikacji w europejskiej wspólnej dziedzinie zaufania C-ITS publikują następujące informacje:

- Wydane (aktualnie ważne) certyfikaty głównego urzędu certyfikacji (aktualne i prawidłowo ponownie wprowadzone certyfikaty, w tym certyfikat łączący) w repozytorium, o którym mowa w sekcji 2.3;
- wszystkie ważne jednostki organów ds. rejestracji oraz organów autoryzujących, wraz z ich identyfikatorem operatora i planowanym okresem działania;
- wydane certyfikaty urzędu certyfikacji w repozytoriach, o których mowa w sekcji 2.3;
- CRL wszystkich unieważnionych certyfikatów urzędów certyfikacji obejmujące podlegające im organy ds. rejestracji i organy autoryzujące;
- informacje dotyczące punktu dostępu głównego urzędów certyfikacji do CRL i informacji na temat urzędu certyfikacji.

Wszystkie informacje kategoryzuje się zgodnie z trzema poziomami poufności, a dokumenty przeznaczone dla ogółu społeczeństwa muszą być dostępne publicznie bez żadnych ograniczeń.

3. IDENTYFIKACJA I UWIERZYTELNIANIE

3.1. Nadawanie nazwy

3.1.1. Rodzaje nazw

3.1.1.1. Nazwy TLM, głównych urzędów certyfikacji, organów ds. rejestracji, organów autoryzujących

35) Nazwa na certyfikacie TLM składa się z jednego atrybutu subject_name o wartości zastrzeżonej „EU_TLM”.

36) Nazwa głównego urzędu certyfikacji składa się z jednego atrybutu subject_name o wartości przyznanej przez organ ds. polityki certyfikacji C-ITS (ang. C-ITS certificate policy authority, CPA). Za zachowanie niepowtarzalności nazw odpowiedzialny jest wyłącznie CPA, a TLM prowadzi rejestr nazw głównych urzędów certyfikacji w następstwie powiadomienia go przez ten organ (zatwierdzenie, unieważnienie/likwidacja głównego urzędu certyfikacji). Nazwy podmiotów umieszczonych w certyfikatach nie powinny przekraczać 32 bajtów. Każdy główny urząd certyfikacji składa do CPA propozycję swojej nazwy za pośrednictwem formularza wniosku (przepływ 14). CPA odpowiada za kontrolę niepowtarzalności. Jeżeli nazwa nie jest niepowtarzalna, formularz wniosku zostaje odrzucony (przepływ 4).

37) Nazwa w każdym certyfikacie organu ds. rejestracji / organu autoryzującego może składać się z pojedynczego atrybutu subject_name o wartości wygenerowanej przez wystawcę certyfikatu. Odpowiedzialność za niepowtarzalność nazw leży wyłącznie w gestii głównego urzędu certyfikacji wystawiającego certyfikat.

38) W certyfikatach organu ds. rejestracji / organu autoryzującego nie stosuje się nazw o rozmiarze większym niż 32 bajty, ponieważ rozmiar atrybutów subject_name w certyfikatach ogranicza się do 32 bajtów.

39) Bilet autoryzacyjny nie zawiera nazwy.

3.1.1.2. Nazwy jednostek końcowych

40) Na każdej stacji C-ITS przydziela się dwa rodzaje niepowtarzalnego identyfikatora:

- identyfikator kanoniczny, który jest przechowywany podczas pierwszej rejestracji stacji C-ITS w ramach odpowiedzialności producenta. Zawiera on podłańcuch identyfikujący producenta lub operatora, tak aby identyfikator ten mógł być niepowtarzalny;
- atrybut subject_name, który może stanowić część danych uwierzytelniających rejestrację stacji C-ITS, wchodzący w zakres odpowiedzialności organu ds. rejestracji.

3.1.1.3. Identyfikacja certyfikatów

41) Certyfikaty zgodne z formatem [5] identyfikuje się przez obliczenie wartości HashedId8, zgodnie z definicją w [5].

3.1.2. Potrzeba nadania nazw posiadających znaczenie

Brak zastrzeżeń.

3.1.3. Anonimowość i pseudonimizacja jednostek końcowych

42) Organ autoryzujący zapewnia, aby pseudonimizacja stacji C-ITS wprowadzana była poprzez dostarczenie do stacji C-ITS biletów autoryzacyjnych, które nie zawierają żadnych nazw lub informacji mogących powiązać podmiot z jego prawdziwą tożsamością.

3.1.4. Zasady interpretowania różnych form nazw

Brak zastrzeżeń.

3.1.5. Niepowtarzalność nazw

43) Nazwy TLM, głównych urzędów certyfikacji, organów ds. rejestracji, organów autoryzujących i identyfikatorów kanonicznych stacji C-ITS są niepowtarzalne.

44) TLM zapewnia w procesie rejestracji danego głównego urzędu certyfikacji na europejskiej zaufanej liście certyfikatów, aby jego identyfikator certyfikatu (HashedId8) był niepowtarzalny. Główny urząd certyfikacji zapewnia w procesie wydawania certyfikatu, aby identyfikator certyfikatu (HashedId8) każdego podlegającego mu urzędu certyfikacji był niepowtarzalny.

45) HashedId8 danych uwierzytelniających rejestrację jest niepowtarzalny w obrębie urzędu certyfikacji wydającego certyfikat. HashedId8 biletu autoryzacyjnego nie musi być niepowtarzalny.

3.2. Pierwsza walidacja tożsamości

3.2.1. Metoda udowodnienia posiadania klucza prywatnego

46) Główny urząd certyfikacji dowodzi, że ma prawo do posiadania klucza prywatnego odpowiadającego kluczowi publicznemu w autonomicznym certyfikacie. Centralny punkt kontaktowy sprawdza ten dowód.

47) Organ ds. rejestracji / organ autoryzujący dowodzi, że ma prawo do posiadania klucza prywatnego odpowiadającego, który ma być wykazany w certyfikacie. Główny urząd certyfikacji sprawdza ten dowód.

48) Posiadania nowego klucza prywatnego (dla celów ponownego wprowadzenia certyfikatu) dowodzi się, podpisując wniosek za pomocą nowego klucza prywatnego (podpisu wewnętrznego), po czym następuje wygenerowanie zewnętrznego podpisu na podpisanym wniosku za pomocą aktualne ważnego klucza prywatnego (aby zagwarantować autentyczność wniosku). Wnioskodawca przedkłada podpisany wniosek o wydanie certyfikatu do urzędu certyfikacji wydającego certyfikat za pośrednictwem bezpiecznej wymiany komunikatów. Urząd certyfikacji wydający certyfikat sprawdza, czy podpis cyfrowy wnioskodawcy w komunikacie dotyczącym wniosku złożono za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu załączonemu do wniosku o wydanie certyfikatu. Główny urząd certyfikacji określa, który wniosek o wydanie certyfikatu i udzielone odpowiedzi popiera w swoim oświadczeniu dotyczącym praktyk w zakresie certyfikacji.

3.2.2. Uwierzytelnianie tożsamości organizacji

3.2.2.1. Uwierzytelnianie tożsamości organizacji głównych urzędów certyfikacji

49) W formularzu wniosku do CPA (tj. przepływ 14) główny urząd certyfikacji podaje tożsamość organizacji i informacje dotyczące rejestracji, w których skład wchodzi:

- nazwa organizacji;
- adres pocztowy;
- adres poczty elektronicznej;
- nazwa osoby fizycznej wyznaczonej do kontaktów w organizacji;
- numer telefonu;
- cyfrowy odcisk palca w formie drukowanej (tj. wartość skrótu SHA 256) certyfikatu głównego urzędu certyfikacji;
- informacje kryptograficzne (tj. algorytmy kryptograficzne, długości klucza) w certyfikacie głównego urzędu certyfikacji;
- wszelkiego rodzaju zezwolenia, z których może korzystać główny urząd certyfikacji, i które może przekazywać do podporządkowanych urzędów certyfikacji.

50) CPA sprawdza tożsamość organizacji i inne informacje dotyczące rejestracji udzielone przez wnioskującego o certyfikat w celu wprowadzenia certyfikatu głównego urzędu certyfikacji na europejską zaufaną listę certyfikatów.

51) CPA gromadzi bezpośrednie dowody, albo poświadczenia pochodzące z odpowiedniego i autoryzowanego źródła, dotyczące tożsamości (np. nazwy) oraz, w stosownych przypadkach, wszelkie szczegółowe atrybuty podmiotów, którym wydawany jest certyfikat. Dowody można przedłożyć w formie dokumentacji papierowej lub elektronicznej.

52) Tożsamość podmiotu sprawdza się w trakcie rejestracji za pomocą odpowiednich środków i zgodnie z obecną polityką certyfikacji.

53) Przy składaniu każdego wniosku o wydanie certyfikatu należy przedłożyć dowody potwierdzające:

- pełną nazwę jednostki organizacyjnej (organizacji prywatnej, instytucji rządowej lub jednostki niekomercyjnej);
- uznaną na szczeblu krajowym rejestrację lub inne cechy, które można w miarę możliwości wykorzystać, aby odróżnić jednostkę organizacyjną od innych o tej samej nazwie.

Powyższe zasady opierają się na TS 102 042 [4]: *Urząd certyfikacji zapewnia, aby dowody potwierdzające tożsamość abonenta i podmiotu oraz dokładność ich nazw/imion i nazwisk oraz powiązanych danych zostały odpowiednio zbadane w ramach określonej usługi lub, w stosownych przypadkach, potwierdzone w wyniku analizy poświadczeń z odpowiednich i autoryzowanych źródeł oraz aby wnioski o certyfikat były dokładne, zatwierdzone i kompletne zgodnie ze zgromadzonymi dowodami lub poświadczeniem.*

3.2.2.2. Uwierzytelnianie tożsamości organizacji TLM

54) Organizacja obsługująca TLM przedstawia dowody identyfikacji i dokładności nazwy oraz związanych z nią danych w celu umożliwienia właściwej weryfikacji przy początkowym tworzeniu i ponownym wprowadzaniu certyfikatu TLM.

55) Tożsamość podmiotu sprawdza się w trakcie tworzenia certyfikatu lub ponownego wprowadzania go za pomocą odpowiednich środków i zgodnie z obecną polityką certyfikacji.

56) Dowody dotyczące organizacji dostarcza się zgodnie z sekcją 3.2.2.1.

3.2.2.3. Uwierzytelnianie tożsamości organizacji podporządkowanych urzędów certyfikacji

57) Główny urząd certyfikacji sprawdza tożsamość organizacji i inne informacje dotyczące rejestracji dostarczone przez wnioskujących o certyfikaty podporządkowanego urzędu certyfikacji (organu ds. rejestracji / organu autoryzującego).

58) Główny urząd certyfikacji co najmniej:

- stwierdza, czy organizacja istnieje, korzystając z co najmniej jednej usługi weryfikacji tożsamości osoby trzeciej lub bazy danych lub, alternatywnie, dokumentacji organizacyjnej wydanej przez lub złożonej w odpowiedniej agencji rządowej lub w uznawanym organie, które potwierdzają istnienie organizacji;
- korzysta z usług poczty tradycyjnej lub stosuje porównywalną procedurę wymagającą od wnioskującego o certyfikat potwierdzenia określonych informacji na temat organizacji tj. tego, że autoryzował wniosek o certyfikat, oraz że osoba przedkładająca wniosek w imieniu wnioskodawcy jest do tego upoważniona. W przypadku gdy certyfikat zawiera nazwę osoby fizycznej jako upoważnionego przedstawiciela organizacji potwierdza ona również, że zatrudnia tę osobę i upoważnia ją do działania w jej imieniu.

59) Procedury walidacji dotyczące wydawania certyfikatów urzędu certyfikacji dokumentuje się w oświadczeniu głównego urzędu certyfikacji dotyczącym praktyk w zakresie certyfikacji.

3.2.2.4. Uwierzytelnianie organizacji abonenta jednostek końcowych

60) Zanim abonent jednostek końcowych (producenta/operatora) będzie mógł zarejestrować się w zaufanym organie ds. rejestracji w celu umożliwienia jednostkom końcowym wysyłania wniosków o certyfikat danych uwierzytelniających rejestrację, organ ds. rejestracji:

- sprawdza tożsamość organizacji-abonenta i inne informacje dotyczące rejestracji udzielone przez wnioskującego o certyfikat;
- sprawdza, czy typ stacji C-ITS (tj. konkretny produkt oparty na marce, modelu i wersji stacji C-ITS) spełnia wszystkie kryteria oceny zgodności.

61) Organ ds. rejestracji co najmniej:

- stwierdza, czy organizacja istnieje, korzystając z co najmniej jednej usługi weryfikacji tożsamości osoby trzeciej lub bazy danych lub, alternatywnie, dokumentacji organizacyjnej wydanej przez lub złożonej w odpowiedniej agencji rządowej lub w uznawanym organie, które potwierdzają istnienie organizacji;
- korzysta z usług poczty tradycyjnej lub porównywalnej procedury wymagającej od wnioskującego o certyfikat potwierdzenia określonych informacji na temat organizacji, że autoryzował wniosek o certyfikat oraz

że osoba przedkładająca wniosek w jego imieniu jest do tego upoważniona. W przypadku gdy certyfikat zawiera imię i nazwisko osoby fizycznej jako upoważnionego przedstawiciela organizacji, wnioskodawca potwierdza również, że zatrudnia tę osobę i upoważnia ją do działania w jego imieniu.

62) Procedury walidacji dotyczące rejestracji stacji C-ITS przez abonenta dokumentuje się w oświadczeniu dotyczącym praktyk w zakresie certyfikacji organu ds. rejestracji.

3.2.3. Uwierzytelnianie pojedynczej jednostki

3.2.3.1. Uwierzytelnianie pojedynczej jednostki TLM / urzędu certyfikacji

63) W celu uwierzytelnienia pojedynczej jednostki (osoby fizycznej) zidentyfikowanej w związku z osobą prawną lub jednostką organizacyjną (np. abonentem) przedstawia się dowody potwierdzające:

- pełne nazwisko i imiona podmiotu (nazwisko i nadane imiona, zgodnie z obowiązującymi przepisami i krajowymi praktykami identyfikacyjnymi);
- datę i miejsce urodzenia, odniesienie do uznawanego w kraju dokumentu tożsamości lub inne cechy abonenta, które można w miarę możliwości wykorzystać w celu odróżnienia tej osoby od innych osób o tym samym imieniu i nazwisku;
- pełną nazwę i status prawny powiązanej osoby prawnej lub innej jednostki organizacyjnej (np. abonenta);
- wszelkie istotne informacje dotyczące rejestracji (np. rejestracji przedsiębiorstwa) powiązanej osoby prawnej lub innej jednostki organizacyjnej;
- dowody, że podmiot jest powiązany z osobą prawną lub inną jednostką organizacyjną.

Dowody można przedłożyć w formie dokumentacji papierowej lub elektronicznej.

64) Upoważniony przedstawiciel głównego urzędu certyfikacji, organu ds. rejestracji, organu autoryzującego lub abonenta, aby zweryfikować swoją tożsamość dostarcza dokumentację dowodzącą, że pracuje on dla organizacji (certyfikat autoryzacji). Osoba ta przedstawia również oficjalny dowód tożsamości.

65) W przypadku początkowego procesu rejestracji (przepływ 31/32) przedstawiciel organu ds. rejestracji / organu autoryzującego dostarcza odpowiedniemu głównemu urzędowi certyfikacji wszystkie niezbędne informacje (zob. sekcja 4.1.2).

66) Personel głównego urzędu certyfikacji dokonuje weryfikacji tożsamości przedstawiciela wnioskującego o certyfikat i wszystkich powiązanych dokumentów, stosując wymogi dotyczące „zaufanego personelu”, o których mowa w sekcji 5.2.1. (Proces walidacji informacji dotyczących wniosku i generowania certyfikatu przez główny urząd certyfikacji jest przeprowadzany przez „zaufane osoby” w głównym urzędzie certyfikacji, co najmniej pod

podwójnym nadzorem, ponieważ są to wrażliwe operacje w rozumieniu sekcji 5.2.2).

3.2.3.2. Uwierzytelnianie tożsamości abonenta stacji C-ITS

67) Abonentów reprezentują upoważnieni użytkownicy końcowi w organizacji; są oni zarejestrowani w organach wystawiających certyfikaty – organie ds. rejestracji i organie autoryzującym. Ci wyznaczeni przez organizacje użytkownicy końcowi (producenci lub operatorzy) potwierdzają swoją tożsamość i autentyczność przed:

- rejestracją jednostki końcowej w odpowiednim organie ds. rejestracji, w tym jej kanonicznego klucza publicznego, identyfikatora kanonicznego (niepowtarzalnego identyfikatora) oraz zezwoleń zgodnych z jednostką końcową;
- rejestracją w organie autoryzującym i zabezpieczeniem dowodu zawarcia umowy z abonentem, który to dowód można wysłać do organu ds. rejestracji.

3.2.3.3. Uwierzytelnianie tożsamości stacji C-ITS

68) Podmioty uwierzytelnienia rejestracji jednostek końcowych uwierzytelniają się, gdy występują o te dane uwierzytelniające rejestrację (przepływ 31), wykorzystując do ich pierwszego uwierzytelnienia kanoniczny klucz prywatny. Organ ds. rejestracji sprawdza uwierzytelnienie, wykorzystując kanoniczny klucz publiczny odpowiadający jednostce końcowej. Kanoniczne klucze publiczne jednostek końcowych przekazuje się do organu ds. rejestracji przed wykonaniem pierwszego wniosku; dokonuje się tego za pośrednictwem bezpiecznego kanału między producentem lub operatorem stacji C-ITS a organem ds. rejestracji (przepływ 33).

69) Podmioty biletów autoryzacyjnych jednostek końcowych uwierzytelniają się, gdy występują o te bilety (przepływ 32), wykorzystując ich niepowtarzalny klucz prywatny służący do rejestracji. Organ autoryzujący w celu walidacji przekazuje podpis do organu ds. rejestracji (przepływ 25); organ ds. rejestracji zatwierdza go i potwierdza wynik w organie autoryzującym (przepływ 23).

3.2.4. Niezweryfikowane informacje o abonencie

Brak zastrzeżeń.

3.2.5. Walidacja organu

3.2.5.1. Walidacja TLM, głównego urzędu certyfikacji, organu ds. rejestracji, organu autoryzującego

70) Każda organizacja wskazuje w oświadczeniu dotyczącym praktyk w zakresie certyfikacji co najmniej jednego przedstawiciela (np. inspektora ds. bezpieczeństwa) odpowiedzialnego za wnioskowanie o nowe certyfikaty lub o przedłużenia certyfikatów. Zastosowanie mają przepisy dotyczące nazw określone w sekcji 3.2.3.

3.2.5.2. Walidacja abonentów stacji C-ITS

71) Co najmniej jedna osoba fizyczna odpowiedzialna za rejestrację stacji C-ITS w organie ds. rejestracji (np. urzędnik ds. bezpieczeństwa) jest znana i zatwierdzona przez urząd ds. rejestracji (zob. sekcja 3.2.3).

3.2.5.3. Walidacja stacji C-ITS

72) Abonent stacji C-ITS może zarejestrować stacje C-ITS w określonym organie ds. rejestracji (przepływ 33), o ile ten organ uwierzytelnił go.

W przypadku gdy stacja C-ITS jest zarejestrowana w organie ds. rejestracji posiadającym niepowtarzalny kanoniczny identyfikator i kanoniczny klucz publiczny, może wnioskować o dane uwierzytelniające rejestrację stosując wniosek podpisany kanonicznym kluczem prywatnym powiązanym z wcześniej zarejestrowanym kanonicznym kluczem publicznym.

3.2.6. Kryteria interoperacyjności

73) W przypadku komunikacji między stacjami C-ITS i organami ds. rejestracji (lub organami autoryzującymi) stacja C-ITS musi być w stanie zapewnić bezpieczną komunikację z organami ds. rejestracji (lub organami autoryzującymi), tj. wykonywać funkcje uwierzytelniania, poufności i integralności, jak określono w [1]. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1]. Organ ds. rejestracji i organ autoryzujący wspierają tą bezpieczną komunikację.

74) Organ ds. rejestracji i organ autoryzujący obsługują wnioski o certyfikat i odpowiedzi, które są zgodne z [1]; w [1] przewidziano bezpieczny protokół wniosku AT /odpowiedzi na wniosek AT, wspierający anonimowość wnioskującego wnioskodawcy względem AT oraz rozdział obowiązków organu ds. rejestracji i organu autoryzującego. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1]. Aby zapobiec ujawnieniu długoterminowej tożsamości stacji C-ITS komunikacja między ruchomą stacją C-ITS a organem ds. rejestracji ma charakter poufny (np. dane dotyczące komunikacji muszą być w pełni zaszyfrowane).

75) Organ autoryzujący przedkłada wniosek o zatwierdzenie autoryzacji (przepływ 25) w odniesieniu do każdego wniosku o autoryzację otrzymywanego od podmiotu certyfikatu jednostki końcowej. Organ ds. rejestracji zatwierdza ten wniosek w odniesieniu do:

- statusu jednostki końcowej w organie ds. rejestracji;
- ważności podpisu;
- wnioskowanych identyfikatorów aplikacji ITS (ITS-AID) oraz zezwoleń;
- statusu świadczenia usługi przez organ autoryzujący na rzecz abonenta.

3.3. Identyfikacja i uwierzytelnianie w przypadku wniosków o ponowne wprowadzenie kluczy

3.3.1. Identyfikacja i uwierzytelnianie w przypadku zwykłych wniosków o ponowne wprowadzenie kluczy

3.3.1.1. Certyfikaty TLM

76) TLM generuje parę kluczy i dwa certyfikaty: jeden certyfikat autonomiczny i jeden certyfikat łączący, o których mowa w sekcji 7.

3.3.1.2. Certyfikaty głównego urzędu certyfikacji

Nie dotyczy.

3.3.1.3. Przedłużenie lub ponowne wprowadzenie certyfikatu organu ds. rejestracji / organu autoryzującego

77) Przed wygaśnięciem świadectwa organu ds. rejestracji / organu autoryzującego, dany organ zwraca się z wnioskiem o wydanie nowego certyfikatu (przepływ 21 / przepływ 24) w celu zachowania ciągłości stosowania certyfikatu. Organ ds. rejestracji / organ autoryzujący generuje nową parę kluczy, aby zastąpić wygasającą parę kluczy i podpisać wniosek o ponowne wprowadzenie zawierający nowy klucz publiczny wraz z aktualnym ważnym kluczem prywatnym („ponowne wprowadzenie"). Organ ds. rejestracji lub organ autoryzujący generuje nową parę kluczy i podpisuje wniosek za pomocą nowego klucza prywatnego (wewnętrznego podpisu), aby potwierdzić fakt posiadania nowego klucza prywatnego. Cały wniosek podpisuje się (podpisuje całościowo) za pomocą aktualnego ważnego klucza prywatnego (zewnętrznego podpisu), aby zapewnić integralność i autentyczność wniosku. Jeżeli używa się pary kluczy szyfrujących i deszyfrujących, należy wykazać posiadanie prywatnych kluczy deszyfrujących (szczegółowy opis ponownego wprowadzania znajduje się w sekcji 4.7.3.3).

78) Metoda identyfikacji i uwierzytelniania do celów rutynowego ponownego wprowadzania jest taka sama, jak w przypadku pierwszego wydania zatwierdzenia certyfikatu głównego urzędu certyfikacji, jak określono w sekcji 3.2.2.

3.3.1.4. Dane uwierzytelniające rejestrację jednostek końcowych

79) Przed wygaśnięciem istniejących danych uwierzytelniających rejestrację jednostka końcowa żąda wydania nowego certyfikatu (przepływ 31) w celu zachowania ciągłości stosowania certyfikatu. Jednostka końcowa generuje nową parę kluczy, aby zastąpić istniejącą parę kluczy i złożyć wniosek o nowy certyfikat zawierający nowy klucz publiczny; żądanie zostaje podpisane za pomocą obecnie aktualnego klucza prywatnego danych uwierzytelniających rejestrację.

80) Jednostka końcowa może podpisać wniosek za pomocą nowo utworzonego klucza prywatnego (podpis wewnętrzny), aby potwierdzić posiadanie nowego klucza prywatnego. Następnie cały wniosek podpisuje się (podpisuje całościowo) za pomocą aktualnego ważnego klucza prywatnego (zewnętrznego podpisu) i szyfruje się do przyjmującego organu ds. rejestracji, jak określono w [1], aby zapewnić poufność integralność i autentyczność wniosku. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

3.3.1.5. Bilety autoryzacyjne jednostek końcowych

81) Ponowne wprowadzenie certyfikatu dla AT opiera się na tym samym procesie, co pierwsza autoryzacja, jak określono w [1]. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

3.3.2. Identyfikacja i uwierzytelnianie w przypadku wniosków o ponowne wprowadzenie kluczy po ich unieważnieniu

3.3.2.1. Certyfikaty urzędu certyfikacji

82) Uwierzytelnienie organizacji urzędu certyfikacji w odniesieniu do ponownego wprowadzenia certyfikatu głównego urzędu certyfikacji, organu ds. rejestracji

i organu autoryzującego po unieważnieniu jest traktowane w taki sam sposób, jak pierwsze wydanie certyfikatu urzędu certyfikacji, jak określono w sekcji 3.2.2.

3.3.2.2. Dane uwierzytelniające rejestrację jednostek końcowych

83) Uwierzytelnienie jednostki końcowej w odniesieniu do ponownego wprowadzenia certyfikatu danych uwierzytelniających rejestrację po unieważnieniu stosuje się w taki sam sposób, jak pierwsze wydanie certyfikatu jednostki końcowej, jak określono w sekcji 3.2.2.

3.3.2.3. Wnioski o autoryzację jednostek końcowych

Nie dotyczy, ponieważ bilety autoryzacyjne nie podlegają unieważnianiu.

3.4. Identyfikacja i uwierzytelnianie wniosku o unieważnienie

3.4.1. Certyfikaty głównego urzędu certyfikacji / organu ds. rejestracji / organu autoryzującego

84) Wnioski dotyczące wykreślenia certyfikatu głównego urzędu certyfikacji z europejskiej zaufanej listy certyfikatów uwierzytelnia główny urząd certyfikacji do TLM (przepływ 12 i 9). Wnioski dotyczące unieważniania certyfikatów organu ds. rejestracji / organu autoryzującego uwierzytelnia odpowiedni główny urząd certyfikacji oraz sam podporządkowany urząd certyfikacji.

85) Dopuszczalne procedury uwierzytelniania wniosków o unieważnienie rejestracji abonenta obejmują:

- podpisany komunikat w formie pisemnej umieszczony na firmowym papierze listowym sporządzony przez abonenta wnioskującego o unieważnienie, zawierający odniesienie do unieważnianego certyfikatu;
- komunikację z abonentem dającą uzasadnione zapewnienie, że osoba lub organizacja składająca wniosek o unieważnienie jest w rzeczywistości abonentem. W zależności od okoliczności taka komunikacja może obejmować co najmniej jedną z poniższych form komunikacji: pocztę elektroniczną, tradycyjną lub kurierską.

3.4.2. Dane uwierzytelniające rejestrację stacji C-ITS

86) Abonent stacji C-ITS może unieważnić dane uwierzytelniające rejestrację poprzednio zarejestrowanej stacji C-ITS, zwracając się w tej kwestii do organu ds. rejestracji (przepływ 34). Wnioskujący abonent tworzy wniosek o unieważnienie danej stacji C-ITS lub wykazu stacji C-ITS. Organ ds. rejestracji uwierzytelnia wniosek o unieważnienie przed rozpoczęciem jego przetwarzania oraz potwierdza unieważnienie stacji C-ITS oraz związanych z nimi danych uwierzytelniających rejestrację.

87) Organ ds. rejestracji może unieważnić dane uwierzytelniające rejestrację stacji C-ITS zgodnie z sekcją 7.3.

3.4.3. Bilety autoryzacyjne stacji C-ITS

88) Ponieważ biletów autoryzacyjnych nie unieważnia się, ich ważność ogranicza się do konkretnego okresu. Zakres dopuszczalnych okresów ważności w niniejszej polityce certyfikacji jest określony w sekcji 7.

4. WYMOGI OPERACYJNE CYKLU ŻYCIA CERTYFIKATU

4.1. Wniosek o wydanie certyfikatu

89) W tej sekcji określono wymagania dotyczące pierwszego wniosku o wydanie certyfikatu.

90) Pojęcie „wniosek o wydanie certyfikatu” odnosi się do następujących procesów:

- rejestracji i ustanowienia relacji zaufania między TLM a CPA;
- rejestracji i ustanowienia relacji zaufania między głównym urzędem certyfikacji, CPA i TLM, w tym wprowadzenie pierwszego certyfikatu głównego urzędu certyfikacji na europejską zaufaną listę certyfikatów;
- rejestracji i ustanowienia relacji zaufania między organem ds. rejestracji / organem autoryzującym a głównym urzędem certyfikacji, w tym wydanie nowego certyfikatu organu ds. rejestracji / organu autoryzującego;
- rejestracji przez producenta/operatora stacji C-ITS w organie ds. rejestracji;
- żądania stacji C-ITS dotyczącego danych uwierzytelniających rejestrację / biletu autoryzacyjnego.

4.1.1. Kto może złożyć wniosek o wydanie certyfikatu

4.1.1.1. Główne urzędy certyfikacji

91) Główne urzędy certyfikacji generują własne pary kluczy i same wydają certyfikaty główne. Główny urząd certyfikacji może przedłożyć wniosek o wydanie certyfikatu za pośrednictwem wyznaczonego przedstawiciela (przepływ 14).

4.1.1.2. Zarządzający zaufaną listą

92) TLM generuje własną parę kluczy i sam wydaje certyfikat. Pierwsze utworzenie certyfikatu TLM przetwarza przedstawiciel organizacji TLM pod kontrolą CPA.

4.1.1.3. Organ ds. rejestracji i organ autoryzujący

93) Upoważniony przedstawiciel organu ds. rejestracji lub organu autoryzującego może przedłożyć formularz wniosku o wydanie certyfikatu podporządkowanego urzędu certyfikacji (organu ds. rejestracji lub organu autoryzującego) do upoważnionego przedstawiciela właściwego urzędu certyfikacji (przepływ 27/28).

4.1.1.4. Stacja C-ITS

94) Abonenci rejestrują każdą stację C-ITS w organie ds. rejestracji zgodnie z sekcją 3.2.5.3.

95) Każda stacja C-ITS zarejestrowana w organie ds. rejestracji może wysyłać wnioski dotyczące danych uwierzytelniających rejestrację (przepływ 31).

96) Każda stacja C-ITS może wysyłać żądania biletu autoryzacyjnego (przepływ 32), nie żądając żadnej interakcji ze strony abonenta. Zanim stacja C-ITS

zażąda biletu autoryzacyjnego, musi posiadać dane uwierzytelniające rejestrację.

4.1.2. Proces rejestracji i zakres odpowiedzialności

97) Zezwoleń dla głównych urzędów certyfikacji i podporządkowanych urzędów certyfikacji wystawiających certyfikaty do specjalnych (rządowych) celów (tj. specjalnych ruchomych i stałych stacji C-ITS) mogą udzielać wyłącznie państwa członkowskie, na terenie których znajdują się te organizacje.

4.1.2.1. Główne urzędy certyfikacji

98) Po przeprowadzeniu audytu (przepływ 13 i 36, sekcja 8), główne urzędy certyfikacji mogą złożyć w organie ds. polityki certyfikacji C-ITS wniosek o wprowadzenie ich certyfikatów do ECTL (przepływ 14). Proces rejestracji opiera się na podpisanym ręcznym formularzu wniosku, fizycznie dostarczonym do organu ds. polityki certyfikacji C-ITS przez upoważnionego przedstawiciela głównego urzędu certyfikacji i zawierającym co najmniej informacje określone w sekcjach 3.2.2.1, 3.2.3 i 3.2.5.1.

99) Formularz wniosku głównego urzędu certyfikacji podpisuje jego upoważniony przedstawiciel.

100) Oprócz formularza wniosku upoważniony przedstawiciel głównego urzędu certyfikacji dostarcza egzemplarz oświadczenia głównego urzędu certyfikacji dotyczącego praktyk w zakresie certyfikacji (przepływ 15), a także, w celu zatwierdzenia przez CPA (przepływ 16), swojego sprawozdania z audytu. CPA, w przypadku zatwierdzenia, generuje i wysyła certyfikat zgodności do CPOC/TLM oraz do odpowiedniego głównego urzędu certyfikacji.

101) Następnie upoważniony przedstawiciel głównego urzędu certyfikacji przedstawia CPOC/TLM swój formularz wniosku (zawierający odcisk palca (ang. fingerprint) autonomicznego certyfikatu), oficjalny dowód tożsamości i dowód autoryzacji. Autonomiczny certyfikat do CPOC/TLM dostarcza się drogą elektroniczną. CPOC/TLM sprawdza wszystkie dokumenty oraz autonomiczny certyfikat.

102) W przypadku pozytywnego wyniku kontroli TLM umieszcza certyfikat głównego urzędu certyfikacji na europejskiej zaufanej liście certyfikatów w oparciu o powiadomienie otrzymane od CPA (przepływy 1 i 2). Szczegółowy proces opisano w oświadczeniu TLM dotyczącym praktyk w zakresie certyfikacji.

103) Należy udostępnić dodatkową procedurę, aby w organie krajowym konkretnego państwa zdobyć zatwierdzenie oświadczenia dotyczącego praktyk w zakresie certyfikacji oraz sprawozdania z audytu głównego urzędu certyfikacji.

4.1.2.2. Zarządzający zaufaną listą

104) TLM po przeprowadzeniu audytu może zarejestrować się w CPA. Proces rejestracji opiera się na podpisanym ręcznym formularzu, fizycznie dostarczonym do organu ds. polityki certyfikacji C-ITS (przepływ 38) przez upoważnionego przedstawiciela TLM i zawierającym co najmniej informacje, o których mowa w sekcjach 3.2.2.2 i 3.2.3.

105) Formularz wniosku TLM podpisuje jego upoważniony przedstawiciel.

106) TLM generuje najpierw autonomiczny certyfikat i przekazuje go w sposób bezpieczny do CPA. Następnie TLM składa do CPA formularz wniosku (zawierający odcisk palca autonomicznego certyfikatu), egzemplarz oświadczenia dotyczącego praktyk w zakresie certyfikacji, oficjalny dowód tożsamości, dowód autoryzacji i sprawozdanie z audytu (przepływ 40). CPA sprawdza wszystkie dokumenty i autonomiczny certyfikat. W przypadku pozytywnej weryfikacji wszystkich dokumentów, autonomicznego certyfikatu i odcisku palca CPA potwierdza przeprowadzenie procesu rejestracji poprzez przesłanie zatwierdzenia do TLM i CPOC (przepływ 39). CPA przechowuje informacje dotyczące wniosku przesłane przez TLM. Następnie za pośrednictwem CPOC wystawia się certyfikat TLM.

4.1.2.3. Organ ds. rejestracji i organ autoryzujący

107) W trakcie procesu rejestracji organ ds. rejestracji / organ autoryzujący, w celu zatwierdzenia, składa odpowiednie dokumenty (np. oświadczenie dotyczące praktyk w zakresie certyfikacji i sprawozdanie z audytu) do odpowiedniego głównego urzędu certyfikacji (przepływ 27/28). W przypadkach pozytywnej kontroli dokumentów główny urząd certyfikacji przesyła zatwierdzenie do odpowiednich głównych podporządkowanych urzędów certyfikacji (przepływ 29/30). Podporządkowany urząd certyfikacji (organ ds. rejestracji lub organ autoryzujący) następnie przekazuje swój podpisany wniosek w formie elektronicznej oraz fizycznie dostarcza formularz wniosku (zgodnie z sekcją 3.2.2.1), dowód autoryzacji i dokument tożsamości do odpowiedniego głównego urzędu certyfikacji. Główny urząd certyfikacji weryfikuje wniosek i otrzymane dokumenty (formularz wniosku zawierający odcisk palca, stanowiący wartość skrótu SHA 256 podporządkowanego urzędu certyfikacji, dowód autoryzacji i dokument tożsamości). Jeżeli wszystkie kontrole prowadzą do uzyskania pozytywnego wyniku, główny urząd certyfikacji wydaje odpowiedni certyfikat podporządkowanego urzędu certyfikacji. Szczegółowe informacje dotyczące sposobu, w jaki składa się pierwszy wniosek opisano w konkretnym oświadczeniu dotyczącym praktyk w zakresie certyfikacji.

108) Oprócz formularza wniosku podporządkowanego urzędu certyfikacji, upoważniony przedstawiciel tego urzędu załącza egzemplarz oświadczenia dotyczącego praktyk w zakresie certyfikacji skierowany do głównego urzędu certyfikacji.

109) Akredytowanemu audytorowi infrastruktury klucza publicznego przekazuje się informacje do celów audytu zgodnie z sekcją 8.

110) Jeżeli właścicielem podporządkowanego urzędu certyfikacji jest jednostka inna niż jednostka, która jest właścicielem głównego urzędu certyfikacji, przed wystawieniem wniosku o wydanie certyfikatu podporządkowanego urzędu certyfikacji, jednostka, która jest właścicielem podporządkowanego urzędu certyfikacji podpisuje umowę dotyczącą usług głównego urzędu certyfikacji.

4.1.2.4. Stacja C-ITS

111) Pierwsza rejestracja podmiotów jednostek końcowych (stacji C-ITS) dokonywana jest przez odpowiedzialnego abonenta (producenta/operatora) za pośrednictwem organu ds. rejestracji (przepływy 33 i 35) po skutecznym

uwierzytelnieniu organizacji abonenta i jednego z jej przedstawicieli zgodnie z sekcjami 3.2.2.4 i 3.2.5.2.

112) Stacja C-ITS może wygenerować parę kluczy organu ds. rejestracji (zob. sekcja 6.1) i utworzyć podpisany wniosek o dane uwierzytelniające rejestrację zgodnie z [1]. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

113) Podczas rejestracji zwykłej stacji C-ITS (w odróżnieniu do specjalnej ruchomej lub stałej stacji C-ITS) organ ds. rejestracji musi sprawdzić, czy zezwolenia zawarte w pierwszym wniosku nie są przeznaczone do użytku rządowego. Zezwolenia przeznaczone do użytku rządowego określają odpowiednie państwa członkowskie. Szczegółową procedurę rejestracji i udzielania odpowiedzi organu ds. rejestracji producentowi/operatorowi (przepływy 33 i 35) określa się w odpowiednim oświadczeniu organu ds. rejestracji dotyczącym praktyk w zakresie certyfikacji.

114) Stacja C-ITS jest rejestrowana w organie ds. rejestracji (sekcja 3.2.5.3), poprzez przesłanie pierwszego wniosku o dane uwierzytelniające rejestrację zgodnie z [1].

115) Po pierwszej rejestracji przez upoważnionego przedstawiciela abonenta organ ds. rejestracji zatwierdza, które bilety autoryzacyjne może uzyskać podmiot jednostki końcowej (tj. stacja C-ITS). Ponadto każdej jednostce końcowej przypisuje się poziom zaufania, związany z certyfikacją jednostki końcowej zgodnie z jednym z profili zabezpieczenia wymienionych w sekcji 6.1.5.2.

116) Standardowe pojazdy posiadają tylko jedną stację C-ITS, która jest zarejestrowana w jednym organie ds. rejestracji. Pojazdy specjalnego przeznaczenia (takie jak samochody policyjne oraz inne pojazdy specjalnego przeznaczenia posiadające szczególne przywileje) można zarejestrować w dodatkowym organie ds. rejestracji lub mogą posiadać dodatkową stację C-ITS na potrzeby autoryzacji w ramach specjalnego przeznaczenia. Pojazdy, do których zastosowanie ma takie wyłączenie, wyznaczają odpowiedzialne państwa członkowskie. Zezwolenia na specjalne ruchome i stałe stacje C-ITS przyznają wyłącznie odpowiedzialne państwa członkowskie. Oświadczenie dotyczące praktyk w zakresie certyfikacji głównego urzędu certyfikacji lub podporządkowanego urzędu certyfikacji wydającego certyfikaty na takie pojazdy w tych państwach członkowskich określa sposób, w jaki proces certyfikacji ma zastosowanie do takich pojazdów.

117) W przypadku gdy abonent jest w trakcie przenoszenia stacji C-ITS z jednego organu ds. rejestracji do innego, stację C-ITS można zarejestrować w dwóch (podobnych) organach ds. rejestracji.

118) Stacja C-ITS generuje parę kluczy AT (zob. sekcja 6.1) i tworzy wniosek AT zgodnie z [1]. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

119) Stacje C-ITS przesyłają wniosek o autoryzację na adres URL organu autoryzującego (przepływy 32 i 26) przesyłając co najmniej wymagane informacje, o których mowa w sekcji 3.2.3.3). Organ ds. rejestracji / organ autoryzujący zatwierdzają autoryzację każdego wniosku zgodnie z sekcją 3.2.6 i 4.2.2.5.

4.2. Przetwarzanie wniosku o wydanie certyfikatu

4.2.1. Realizacja czynności związanych z identyfikacją i uwierzytelnianiem

4.2.1.1. Identyfikacja i uwierzytelnianie głównych urzędów certyfikacji

120) Upoważniony przedstawiciel organu ds. polityki certyfikacji C-ITS odpowiada za uwierzytelnianie upoważnionego przedstawiciela głównego urzędu certyfikacji i zatwierdzenie jego procesu rejestracji zgodnie z sekcją 3.

4.2.1.2. Identyfikacja i uwierzytelnianie TLM

121) Upoważniony przedstawiciel organu ds. polityki certyfikacji C-ITS odpowiada za uwierzytelnienie upoważnionego przedstawiciela TLM i zatwierdzenie jego formularza wniosku dotyczącego procesu rejestracji zgodnie z sekcją 3.

4.2.1.3. Identyfikacja i uwierzytelnianie organu ds. rejestracji i organu autoryzującego

122) Odpowiedni główny urząd certyfikacji odpowiada za uwierzytelnienie upoważnionego przedstawiciela organu ds. rejestracji / organu autoryzującego i zatwierdzenie jego formularza wniosku dotyczącego procesu rejestracji zgodnie z sekcją 3.

123) Główny urząd certyfikacji potwierdza organowi ds. rejestracji / organowi autoryzującemu pomyślną walidację formularza wniosku. Organ ds. rejestracji / organ autoryzujący może następnie wysłać wniosek o wydanie certyfikatu do głównego urzędu certyfikacji (przepływ 21/24), który wydaje certyfikaty odpowiedniemu organowi ds. rejestracji / organowi autoryzującemu (przepływ 18/19).

4.2.1.4. Identyfikacja i uwierzytelnianie abonenta jednostki końcowej

124) Zanim stacja C-ITS będzie mogła zwrócić się o certyfikat danych uwierzytelniających rejestrację, abonent jednostki końcowej w bezpieczny sposób przekaże informacje dotyczące identyfikatora stacji C-ITS do organu ds. rejestracji (przepływ 33). Organ ds. rejestracji sprawdza wniosek i w przypadkach pozytywnej weryfikacji rejestruje informacje na temat stacji C-ITS w bazie danych, a abonentowi jednostki końcowej przekazuje potwierdzenie tego działania (przepływ 35). Producent lub operator wykonuje tę operację wyłącznie raz w odniesieniu do każdej stacji C-ITS. Gdy organ ds. rejestracji zarejestruje stację C-ITS, może ona wtedy zażądać pojedynczego certyfikatu danych uwierzytelniających rejestrację (przepływ 31). Organ ds. rejestracji uwierzytelnia i sprawdza, czy informacje zawarte we wniosku o wydanie certyfikatu danych uwierzytelniających rejestrację są ważne w odniesieniu do stacji C-ITS.

4.2.1.5. Bilety autoryzacyjne

125) W trakcie składania wniosków autoryzację (przepływ 32), zgodnie z [1], organ autoryzujący musi dokonać uwierzytelnienia organu ds. rejestracji, z którego stacja C-ITS otrzymała dane uwierzytelniające rejestrację. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1]. Wniosek odrzuca się, jeżeli organ autoryzujący nie jest w stanie uwierzytelnić organu ds. rejestracji (przepływ 26). Jako wymóg organ autoryzujący posiada certyfikat organu ds. rejestracji w celu uwierzytelnienia organu ds. rejestracji i weryfikacji jego odpowiedzi (przepływy 25 i 23, sekcja 3.2.5.3).

126) Organ ds. rejestracji uwierzytelnia stację C-ITS żądającą biletu autoryzacyjnego, weryfikując jej dane uwierzytelniające rejestrację (przepływy 25 i 23).

4.2.2. Przyjmowanie lub odrzucanie wniosków o wydanie certyfikatu

4.2.2.1. Przyjmowanie lub odrzucanie certyfikatów głównego urzędu certyfikacji

127) TLM, zgodnie z zatwierdzeniem CPA, dokonuje wprowadzenia/usunięcia certyfikatów głównego urzędu certyfikacji w odniesieniu do europejskiej zaufanej listy certyfikatów (przepływ 1/2).

128) TLM po uzyskaniu zatwierdzenia przez CPA sprawdza podpis, informacje oraz kodowanie certyfikatów głównego urzędu certyfikacji (przepływ 1). TLM, po pomyślnej walidacji i zatwierdzeniu przez CPA, umieszcza odpowiedni certyfikat główny na europejskiej zaufanej liście certyfikatów, a następnie powiadamia o tym CPA (przepływ 5).

4.2.2.2. *Przyjmowanie lub odrzucanie certyfikatów TLM*

129) CPA jest odpowiedzialny za zatwierdzanie lub odrzucanie certyfikatów TLM.

4.2.2.3. *Przyjmowanie lub odrzucanie certyfikatów organu ds. rejestracji i organu autoryzującego*

130) Główny urząd certyfikacji weryfikuje wnioski podporządkowanego urzędu certyfikacji o certyfikat (przepływ 21/24) i odpowiednie sprawozdania (wydane przez akredytowanego audytora infrastruktury klucza publicznego) w momencie ich otrzymania (przepływ 36, sekcja 8) od odpowiedniego podporządkowanego urzędu certyfikacji głównego urzędu certyfikacji. Jeżeli kontrola wniosku zakończy się wynikiem pozytywnym, odpowiedni główny urząd certyfikacji wydaje certyfikat organowi ds. rejestracji / organowi autoryzującemu (przepływ 18/19); w przeciwnym wypadku żądanie zostaje odrzucone, a organowi ds. rejestracji / organowi autoryzującemu nie wydaje się żadnego certyfikatu.

4.2.2.4. Przyjmowanie lub odrzucanie danych uwierzytelniających rejestrację

131) Organ ds. rejestracji weryfikuje i zatwierdza wniosek o dane uwierzytelniające rejestrację zgodnie z sekcją 3.2.3.2 i 3.2.5.3.

132) Jeżeli wniosek o certyfikat zgodnie z [1] jest poprawny i ważny, organ ds. rejestracji generuje żądany certyfikat.

133) Jeżeli wniosek o certyfikat jest nieważny, organ ds. rejestracji odmawia jego wydania i przesyła odpowiedź określającą przyczynę odmowy zgodnie z [1]. Jeżeli stacja C-ITS wciąż domaga się danych uwierzytelniających rejestrację, występuje z nowym żądaniem certyfikatu. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

4.2.2.5. Przyjmowanie lub odrzucanie biletu autoryzacyjnego

134) Organ ds. rejestracji sprawdza żądanie certyfikatu. Organ autoryzujący komunikuje się z organem ds. rejestracji w celu zatwierdzenia żądania (przepływ 25). Organ ds. rejestracji uwierzytelnia żądającą stację C-ITS i sprawdza, czy jest ona, zgodnie z polityką certyfikacji, upoważniona do otrzymywania żądanego biletu autoryzacyjnego (np. przez sprawdzenie statusu unieważnienia i zatwierdzenie ważności daty/regionu certyfikatu, zezwoleń,

poziomu ufności itp.). Organ ds. rejestracji zwraca odpowiedź dotyczącą walidacji (przepływ 23) oraz, jeżeli odpowiedź ta jest pozytywna, organ autoryzujący generuje żądany certyfikat, a następnie przesyła go do stacji C-ITS. Jeżeli żądanie biletu autoryzacyjnego jest niepoprawne lub odpowiedź organu ds. rejestracji dotycząca walidacji jest negatywna, organ autoryzujący odrzuca żądanie. Jeżeli stacja C-ITS nadal wymaga biletu autoryzacyjnego, tworzy nowe żądanie o autoryzację.

4.2.3. Czas na przetworzenie wniosku o wydanie certyfikatu

4.2.3.1. Wniosek o wydanie certyfikatu przez główny urząd certyfikacji

135) Proces identyfikacji i uwierzytelnienia wniosku o wydanie certyfikatu ma miejsce w ciągu dnia roboczego i podlega maksymalnemu terminowi określonemu w oświadczeniu głównego urzędu certyfikacji dotyczącym praktyk w zakresie certyfikacji.

4.2.3.2. Wniosek o wydanie certyfikatu przez TLM

136) Przetwarzanie wniosku o wydanie certyfikatu TLM podlega maksymalnemu ograniczeniu czasowemu określonemu w oświadczeniu TLM dotyczącym praktyk w zakresie certyfikacji.

4.2.3.3. Wniosek o wydanie certyfikatu organu ds. rejestracji i organu autoryzującego

137) Proces identyfikacji i uwierzytelniania wniosku o wydanie certyfikatu ma miejsce w ciągu dnia roboczego zgodnie z porozumieniem i umową zawartymi między państwem członkowskim / organizacją prywatną głównego urzędu certyfikacji a podporządkowanym urzędem certyfikacji. Czas na przetworzenie wniosków o wydanie certyfikatu podporządkowanego urzędu certyfikacji nie może przekraczać maksymalnego terminu określonego w oświadczeniu podporządkowanego urzędu certyfikacji dotyczącym praktyk w zakresie certyfikacji.

4.2.3.4. Wniosek o dane uwierzytelniające rejestrację

138) Przetwarzanie wniosków o dane uwierzytelniające rejestrację podlega maksymalnemu terminowi określonemu w oświadczeniu organu ds. rejestracji dotyczącym praktyk w zakresie certyfikacji.

4.2.3.5. Wniosek o bilet autoryzacyjny

139) Przetwarzanie wniosków o bilet autoryzacyjny podlega maksymalnemu terminowi określonemu w oświadczeniu organu autoryzującego dotyczącym praktyk w zakresie certyfikacji.

4.3. Wydanie certyfikatu

4.3.1. Czynności urzędu certyfikacji wykonywane podczas wydawania certyfikatu

4.3.1.1. Wydanie certyfikatu przez główny urząd certyfikacji

140) Główne urzędy certyfikacji wydają własne autonomiczne certyfikaty głównych urzędów certyfikacji, certyfikaty łączące, certyfikaty podporządkowanego urzędu certyfikacji oraz listy unieważnionych certyfikatów.

141) Po zatwierdzeniu przez CPA (przepływ 4) główny urząd certyfikacji przekazuje TLM za pośrednictwem CPOC certyfikat, który ma zostać dodany do ECTL (przepływy 11 i 8) (zob. sekcja 4.1.2.1). TLM sprawdza, czy CPA zatwierdził certyfikat (przepływ 1).

4.3.1.2. *Wydanie certyfikatu przez TLM*

142) TLM wydaje własny autonomiczny certyfikat TLM i certyfikat łączący, a następnie przesyła go do CPOC (przepływ 6).

4.3.1.3. Wydanie certyfikatu przez organ ds. rejestracji i organ autoryzujący

143) Podporządkowane urzędy certyfikacji generują podpisany wniosek o wydanie certyfikatu i przekazują go do odpowiedniego głównego urzędu certyfikacji (przepływy 21 i 24). Główny urząd certyfikacji weryfikuje wniosek i wydaje wnioskującemu podporządkowanemu urzędowi certyfikacji certyfikat zgodnie z [5] jak najszybciej, jak określono w oświadczeniu dotyczącym praktyk w zakresie certyfikacji w odniesieniu do zwykłej praktyki operacyjnej, jednak nie później niż w terminie pięciu dni roboczych od otrzymania wniosku.

144) Główny urząd certyfikacji aktualizuje repozytorium zawierające certyfikaty podporządkowanych urzędów certyfikacji.

4.3.1.4. Wydanie danych uwierzytelniających rejestrację

145) Stacja C-ITS przesyła wniosek o dane uwierzytelniające rejestrację organowi ds. rejestracji zgodnie z [1]. Organ ds. rejestracji uwierzytelnia i sprawdza, czy informacje zawarte we wniosku o wydanie certyfikatu są ważne w odniesieniu do stacji C-ITS. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

146) W przypadku pozytywnego zatwierdzenia organ ds. rejestracji wydaje certyfikat zgodnie z rejestracją stacji C-ITS (zob. 4.2.1.4) i przesyła go do stacji C-ITS przy użyciu komunikatu odpowiedzi EC zgodnie z [1]. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

147) W przypadku braku rejestracji organ ds. rejestracji generuje kod błędu i przesyła go do stacji C-ITS przy użyciu komunikatu odpowiedzi EC zgodnie z [1]. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

148) Wnioski oraz odpowiedzi w sprawie danych uwierzytelniających rejestrację szyfruje się, aby zapewnić poufność, a także podpisuje się, aby je uwierzytelnić i zapewnić ich integralność.

4.3.1.5. Wydanie biletu autoryzacyjnego

149) Stacja C-ITS wysyła organowi autoryzującemu komunikat w wnioskiem o AT zgodnie z [1]. Organ autoryzujący przesyła wniosek o zatwierdzenie AT zgodnie z [1] do organu ds. rejestracji. Organ ds. rejestracji przesyła do organu autoryzującego odpowiedź dotyczącą zatwierdzenia AT. W przypadku pozytywnej odpowiedzi organ autoryzujący tworzy bilet autoryzacyjny i przesyła go do stacji C-ITS przy użyciu komunikatu odpowiedzi AT zgodnie z [1]. W przypadku negatywnej odpowiedzi organ autoryzujący generuje kod błędu i przesyła go do stacji C-ITS przy użyciu komunikatu odpowiedzi AT zgodnie z [1]. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

150) Wnioski i odpowiedzi dotyczące biletu autoryzacyjnego szyfruje się (wyłącznie w przypadku ruchomych stacji C-ITS), aby zapewnić poufność oraz podpisuje się, aby je uwierzytelnić i zapewnić ich integralność.

4.3.2. Powiadomienie abonenta o wydaniu certyfikatów przez urząd certyfikacji

Nie dotyczy.

4.4. Akceptacja certyfikatu

4.4.1. Przeprowadzanie akceptacji certyfikatu

4.4.1.1. Główny urząd certyfikacji

Nie dotyczy.

4.4.1.2. Zarządzający zaufaną listą

Nie dotyczy.

4.4.1.3. Organ ds. rejestracji i organ autoryzujący

151) Organ ds. rejestracji / organ autoryzujący sprawdza rodzaj certyfikatu, podpis oraz informacje zawarte w otrzymanym certyfikacie. Organ ds. rejestracji / organ autoryzujący odrzuca wszystkie certyfikaty organu ds. rejestracji / organu autoryzującego, których nie sprawdzono w sposób prawidłowy oraz wydaje nowy wniosek.

4.4.1.4. Stacja C-ITS

152) Stacja C-ITS sprawdza odpowiedź w sprawie danych uwierzytelniających rejestrację / biletu autoryzacyjnego otrzymaną od organu ds. rejestracji/organu autoryzującego na jej pierwotne żądanie, w tym podpis i łańcuch certyfikatów. Odrzuca wszystkie nieprawidłowo zweryfikowane odpowiedzi dotyczące danych uwierzytelniających rejestrację / biletów autoryzacyjnych. W takich przypadkach stacja wysyła nowy wniosek o dane uwierzytelniające rejestrację / bilet autoryzacyjny.

4.4.2. Publikacja certyfikatu

153) Certyfikaty TLM i ich certyfikaty łączące udostępnia się wszystkim uczestnikom za pośrednictwem CPOC.

154) Certyfikaty głównego urzędu certyfikacji publikuje CPOC za pośrednictwem europejskiej zaufanej listy certyfikatów, którą podpisuje TLM.

155) Certyfikaty podporządkowanych urzędów certyfikacji (organów ds. rejestracji i organów autoryzujących) publikuje główny urząd certyfikacji.

156) Nie publikuje się danych uwierzytelniających rejestrację oraz biletów autoryzacyjnych.

4.4.3. Powiadomienie o wydaniu certyfikatu

Nie istnieją powiadomienia o wydaniu certyfikatu.

4.5. Zastosowanie pary kluczy i certyfikatów

4.5.1. Zastosowanie klucza prywatnego i certyfikatu

4.5.1.1. Zastosowanie klucza prywatnego i certyfikatu przez TLM

157) TLM wykorzystuje klucze prywatne do podpisywania własnych certyfikatów (TLM i certyfikatów łączących), a także europejskiej zaufanej listy certyfikatów.

158) Certyfikat TLM wykorzystują uczestnicy infrastruktury klucza publicznego w celu weryfikacji europejskiej zaufanej listy certyfikatów i uwierzytelnienia TLM.

4.5.1.2. Stosowanie klucza prywatnego i certyfikatów przez główne urzędy certyfikacji

159) Główne urzędy certyfikacji wykorzystują swoje klucze prywatne do podpisywania własnych certyfikatów, CRL, certyfikatów łączących oraz certyfikatów organów ds. rejestracji i organów autoryzujących.

160) Certyfikaty głównych urzędów certyfikacji są wykorzystywane przez uczestników infrastruktury klucza publicznego do weryfikacji powiązanych certyfikatów organów ds. rejestracji i organów autoryzujących, certyfikatów łączących oraz CRL.

4.5.1.3. Zastosowanie klucza prywatnego i certyfikatu przez organy ds. rejestracji i organy autoryzujące

161) Organy ds. rejestracji wykorzystują swoje klucze prywatne do podpisywania danych uwierzytelniających rejestrację oraz do odszyfrowywania wniosków o rejestrację.

162) Certyfikaty organów ds. rejestracji wykorzystuje się do weryfikacji podpisu powiązanych danych uwierzytelniających rejestrację oraz do szyfrowania wniosków o dane uwierzytelniające rejestrację i bilet autoryzacyjny przez jednostkę końcową, jak określono w [1].

163) Organy autoryzujące wykorzystują swoje klucze prywatne do podpisywania biletów autoryzacyjnych oraz do odszyfrowywania wniosków o wydanie takich biletów.

164) Jednostki końcowe stosują certyfikaty organów autoryzujących, aby zweryfikować powiązane bilety autoryzacyjne oraz do szyfrowania wniosków o takie bilety, jak określono w [1].

4.5.1.4. Zastosowanie klucza prywatnego i certyfikatu w przypadku jednostki końcowej

165) Jednostki końcowe stosują prywatny klucz odpowiadający ważnym danym uwierzytelniającym rejestrację w celu podpisania nowego wniosku o rejestrację, jak określono w [1]. Nowy klucz prywatny jest wykorzystywany do tworzenia podpisu wewnętrznego we wniosku o potwierdzenie posiadania klucza prywatnego odpowiadającego nowemu kluczowi publicznemu w przypadku danych uwierzytelniających rejestrację.

166) Jednostki końcowe wykorzystują klucz prywatny odpowiadający ważnym danym uwierzytelniającym rejestrację do podpisania wniosku o uwierzytelnienie, jak określono w [1]. Nowy klucz prywatny odpowiadający nowemu biletowi autoryzacyjnemu powinien być wykorzystywany do tworzenia podpisu wewnętrznego we wniosku o potwierdzenie posiadania klucza prywatnego odpowiadającego nowemu kluczowi publicznemu w przypadku danych uwierzytelniających rejestrację.

167) Jednostka końcowa wykorzystuje klucz prywatny odpowiadający właściwemu biletowi autoryzacyjnemu do podpisywania komunikatu C-ITS, jak określono w [5].

4.5.2. ***Zastosowanie klucza publicznego i certyfikatu przez stronę ufającą***

168) Strony ufające korzystają z zaufanej ścieżki certyfikacji i powiązanych kluczy publicznych do celów, o których mowa w certyfikatach, oraz do uwierzytelniania zaufanej, wspólnej tożsamości w przypadku danych uwierzytelniających rejestrację oraz biletów autoryzacyjnych.

169) Certyfikaty głównych urzędów certyfikacji, organów ds. rejestracji i organów autoryzujących, a także dane uwierzytelniające rejestrację i bilety autoryzacyjne nie mogą być wykorzystywane bez wstępnej kontroli przeprowadzonej przez stronę ufającą.

4.6. Przedłużenie certyfikatu

Niedozwolone.

4.7. Ponowne wprowadzenie certyfikatu

4.7.1. Okoliczności ponownego wprowadzenia certyfikatu

170) Ponowne wprowadzenie certyfikatu ma miejsce, gdy kończy się czas obowiązywania certyfikatu lub nastąpi koniec użytkowania klucza prywatnego, ale nadal istnieje relacja zaufania z urzędem certyfikacji. We wszystkich przypadkach generowana jest i wydawana nowa para kluczy oraz odpowiedni certyfikat.

4.7.2. Kto może złożyć wniosek o ponowne wprowadzenie certyfikatu

4.7.2.1. Główny urząd certyfikacji

171) Główny urząd certyfikacji nie składa wniosku o ponowne wprowadzenie certyfikatu. Proces ponownego wprowadzania certyfikatu jest procesem wewnętrznym głównego urzędu certyfikacji, ponieważ urząd ten wydaje certyfikat autonomiczny. Główny urząd certyfikacji dokonuje ponownego wprowadzenia certyfikatu za pomocą certyfikatów łączących albo wydając nowy certyfikat (zob. sekcja 4.3.1.1).

4.7.2.2. Zarządzający zaufaną listą

172) Zarządzający zaufaną listą nie składa wniosku o ponowne wprowadzenie certyfikatu. Proces ponownego wprowadzania certyfikatu jest procesem wewnętrznym zarządzającego zaufaną listą, ponieważ podmiot ten wydaje certyfikat autonomiczny.

4.7.2.3. Organ ds. rejestracji i organ autoryzujący

173) Wniosek o wydanie certyfikatu przez podporządkowany urząd certyfikacji musi zostać złożony w terminie, aby zapewnić uzyskanie nowego certyfikatu podporządkowanego urzędu certyfikacji oraz aktywną parę kluczy tego urzędu przed wygaśnięciem aktualnego klucza prywatnego podporządkowanego urzędu certyfikacji. Termin na złożenie wniosku musi uwzględniać również czas potrzebny na zatwierdzenie.

4.7.2.4. Stacja C-ITS

Nie dotyczy.

4.7.3. Proces ponownego wprowadzenia certyfikatu

4.7.3.1. Certyfikat zarządzającego zaufaną listą

174) Zarządzający zaufaną listą podejmuje decyzję o ponownym wprowadzeniu certyfikatu w oparciu o wymogi sekcji 6.1 i 7.2. Szczegółowy proces został przedstawiony w oświadczeniu dotyczącym praktyk w zakresie certyfikacji.

175) Zarządzający zaufaną listą przeprowadza proces ponownego wprowadzania certyfikatu w odpowiednim czasie w celu umożliwienia dystrybucji nowego certyfikatu zarządzającego zaufaną listą i certyfikatu łączącego wśród wszystkich uczestników przed wygaśnięciem aktualnego certyfikatu zarządzającego zaufaną listą.

176) Zarządzający zaufaną listą wykorzystuje certyfikaty łączące w celu ponownego wprowadzenia certyfikatu oraz aby zagwarantować relację zaufania w przypadku nowego certyfikatu autonomicznego. Nowo wygenerowany certyfikat zarządzającego zaufaną listą i certyfikat łączący jest przekazywany do centralnego punktu kontaktowego.

4.7.3.2. Certyfikat głównego urzędu certyfikacji

177) Główny urząd certyfikacji podejmuje decyzję o ponownym wprowadzeniu certyfikatu w oparciu o wymogi sekcji 6.1.5 i 7.2. Szczegółowy proces powinien być zdefiniowany w oświadczeniu dotyczącym praktyk w zakresie certyfikacji tego urzędu.

178) Główny urząd certyfikacji przeprowadza proces ponownego wprowadzania certyfikatu w odpowiednim czasie (przed wygaśnięciem bieżącego certyfikatu głównego urzędu certyfikacji) w celu umożliwienia wprowadzenia nowego certyfikatu na europejską zaufaną listę certyfikatów przed uzyskaniem ważności przez certyfikat głównego urzędu certyfikacji (zob. sekcja 5.6.2). Proces ponownego wprowadzania certyfikatu przeprowadza się za pomocą certyfikatów łączących albo tak, jak w przypadku pierwszego wniosku.

4.7.3.3. Certyfikaty organu ds. rejestracji i organu autoryzującego

179) Organ ds. rejestracji lub organ autoryzujący żądają nowego certyfikatu w następujący sposób:

Etap	Oznaczenie	Wniosek o ponowne wprowadzenie certyfikatu
1	**Wygenerowanie pary kluczy**	Podporządkowane urzędy certyfikacji (organy ds. rejestracji i organy autoryzujące) generują nowe pary kluczy zgodnie z sekcją 6.1.
2	**Wygenerowanie wniosku o wydanie certyfikatu i podpisu wewnętrznego**	Podporządkowany urząd certyfikacji generuje wniosek o wydanie certyfikatu z nowo wygenerowanego klucza publicznego z uwzględnieniem schematu nazewnictwa (subject_info) z sekcji 3, algorytmu podpisu, specjalnych zezwoleń dotyczących usług (SSP) oraz opcjonalnych parametrów dodatkowych, a także generuje podpis wewnętrzny z odpowiednim nowym kluczem prywatnym. Jeżeli wymagany jest klucz szyfrujący, podporządkowany urząd certyfikacji musi również udowodnić posiadanie odpowiednich deszyfrujących kluczy prywatnych.
3	**Wygenerowanie podpisu zewnętrznego**	Aby zagwarantować autentyczność podpisanego wniosku, cały wniosek należy podpisać aktualnym i ważnym kluczem prywatnym.
4	**Przesłanie wniosku do**	Podpisany wniosek należy przekazać do odpowiedniego głównego

	głównego urzędu certyfikacji	urzędu certyfikacji.
5	**Weryfikacja wniosku**	Odpowiedni główny urząd certyfikacji weryfikuje integralność i autentyczność wniosku. W pierwszej kolejności urząd ten sprawdza podpis zewnętrzny. Jeżeli wynik weryfikacji jest pozytywny, sprawdza podpis wewnętrzny. W przypadku istnienia dowodu posiadania deszyfrującego klucza prywatnego, główny urząd certyfikacji sprawdza również ten dowód.
6	**Przyjęcie lub odrzucenie wniosku**	Jeżeli wszystkie kontrole zakończą się wynikiem pozytywnym, główny urząd certyfikacji przyjmuje wniosek, w przeciwnym razie wniosek zostaje odrzucony.
7	**Wygenerowanie i wydanie certyfikatu**	Główny urząd certyfikacji generuje nowy certyfikat i przekazuje go podporządkowanemu urzędowi certyfikacji, który złożył wniosek.
8	**Wysłanie odpowiedzi**	Podporządkowany urząd certyfikacji wysyła do głównego urzędu certyfikacji komunikat o statusie (informujący o otrzymaniu lub o nieotrzymaniu certyfikatu.)

Tabela 3: Proces ponownego wprowadzenia certyfikatu w przypadku organów ds. rejestracji i organów autoryzujących

180) W czasie automatycznego ponownego wprowadzania certyfikatu przez podporządkowane urzędy certyfikacji główny urząd certyfikacji dopilnowuje, aby podmiot składający wniosek faktycznie posiadał swój klucz prywatny. Należy zastosować odpowiednie protokoły potwierdzające posiadanie deszyfrujących kluczy prywatnych, jak określono np. w RFC 4210 i 4211. W przypadku kluczy prywatnych podpisu należy używać podpisu wewnętrznego.

4.7.3.4. Certyfikaty stacji C-ITS

Nie dotyczy biletu autoryzacyjnego.

4.8. Zmiana certyfikatu

Niedozwolone.

4.9. Unieważnienie i zawieszenie certyfikatu

Zob. sekcja 7.

4.10. Usługi związane ze statusem certyfikatu

4.10.1. Charakterystyka użytkowania

Nie dotyczy.

4.10.2. Dostępność usługi

Nie dotyczy.

4.10.3. Cechy fakultatywne

Nie dotyczy.

4.11. Zakończenie abonamentu

Nie dotyczy.

4.12. Deponowanie i odzyskiwanie klucza

4.12.1. Abonent

4.12.1.1. Jaką parę kluczy można zdeponować

Nie dotyczy.

4.12.1.2. Kto może złożyć wniosek o odzyskanie klucza

Nie dotyczy.

4.12.1.3. Proces odzyskiwania i zakres odpowiedzialności

Nie dotyczy.

4.12.1.4. Identyfikacja i uwierzytelnianie

Nie dotyczy.

4.12.1.5. Przyjęcie lub odrzucenie wniosków o odzyskanie klucza

Nie dotyczy.

4.12.1.6. Operacje wykonywane przez szablony KEA i KRA podczas odzyskiwania pary kluczy

Nie dotyczy.

4.12.1.7. Dostępność szablonów KEA i KRA

Nie dotyczy.

4.12.2. Polityka i praktyki w zakresie hermetyzacji i odzyskiwania klucza sesji

Nie dotyczy.

5. KONTROLE OBIEKTÓW I ZARZĄDZANIA ORAZ KONTROLE OPERACYJNE

181) Na infrastrukturę klucza publicznego składają się: główny urząd certyfikacji, organ ds. rejestracji / organ autoryzujący, centralny punkt kontaktowy oraz zarządzający zaufaną listą, wraz z elementami składowymi ich ICT (np. sieciami i serwerami).

182) W niniejszej sekcji jednostka odpowiedzialna za element infrastruktury klucza publicznego jest identyfikowana za pomocą samego elementu. Innymi słowy, zdanie „urząd certyfikacji jest odpowiedzialny za przeprowadzenie audytu" jest równoznaczne ze zdaniem „jednostka kierująca urzędem certyfikacji lub personel kierujący tym urzędem jest odpowiedzialna/odpowiedzialny za przeprowadzenie...".

183) Termin „elementy składowe modelu zaufania C-ITS" obejmuje główny urząd certyfikacji, zarządzającego zaufaną listą, organ ds. rejestracji / organ autoryzujący, centralny punkt kontaktowy oraz sieć zabezpieczoną.

5.1. Kontrole fizyczne

184) Wszystkie operacje związane z modelem zaufania C-ITS należy przeprowadzać w środowisku objętym fizyczną ochroną, która powstrzymuje przed nieuprawnionym dostępem do informacji i systemów szczególnie chronionych lub ich nieuprawnionym użytkowaniem i ujawnianiem, a także zapobiega takiemu działaniu i zapewnia jego wykrywanie. W przypadku

elementów składowych modelu zaufania C-ITS stosuje się kontrole bezpieczeństwa fizycznego zgodnie z ISO 27001 i ISO 27005.

185) Jednostki zarządzające elementami składowymi modelu zaufania C-ITS opisują kontrole fizyczne, proceduralne i kontrole bezpieczeństwa osobowego w swoich oświadczeniach dotyczących praktyk w zakresie certyfikacji. Oświadczenie dotyczące praktyk w zakresie certyfikacji musi zawierać w szczególności informacje o lokalizacji i budowie budynków oraz na temat kontroli ich bezpieczeństwa fizycznego gwarantujących kontrolowany dostęp do wszystkich pomieszczeń wykorzystywanych w obiektach jednostek modelu zaufania C-ITS.

5.1.1. Lokalizacja i budowa

5.1.1.1. Główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą

186) Lokalizacja i konstrukcja obiektu, w którym znajdują się urządzenia i dane (moduł zabezpieczeń sprzętu – HSM, dane aktywacyjne, kopie zapasowe pary kluczy, komputer, dziennik, skrypt procedury generowania klucza, wniosek o wydanie certyfikatu itp.) głównego urzędu certyfikacji, centralnego punktu kontaktowego oraz zarządzającego zaufaną listą muszą być spójne z obiektami wykorzystywanymi do przechowywania informacji o wysokiej wartości oraz informacji szczególnie chronionych. Główny urząd certyfikacji działa na specjalnie do tego przeznaczonym obszarze fizycznym oddzielonym od obszarów fizycznych innych elementów składowych infrastruktury klucza publicznego.

187) Główny urząd certyfikacji, centralny punkt kontaktowy oraz zarządzający zaufaną listą wdrażają politykę i procedury zapewniające utrzymanie wysokiego poziomu bezpieczeństwa środowiska fizycznego, w którym zainstalowane są urządzenia głównego urzędu certyfikacji, aby zagwarantować:

- ich odizolowanie od sieci działających poza modelem zaufania;
- ich podzielenie na serię (co najmniej dwóch) parametrów fizycznych o rosnącym bezpieczeństwie;
- przechowywanie danych wrażliwych (HSM, kopii zapasowej pary kluczy, danych aktywacyjnych itp.) w specjalnie do tego przeznaczonym obszarze fizycznym w bezpiecznej lokalizacji z zastosowaniem wielopoziomowej kontroli dostępu.

188) Stosowane techniki bezpieczeństwa muszą być zaprojektowane w taki sposób, aby były odporne na dużą liczbę i kombinacje różnych form ataku. Stosowane mechanizmy muszą obejmować co najmniej:

- alarm obwodowy, telewizję przemysłową, wzmocnione ściany i czujniki ruchu;
- uwierzytelnianie dwuskładnikowe (np. za pomocą smartcard i PIN) w przypadku każdej osoby oraz identyfikatora, pozwalające na wejście na teren obiektów i bezpiecznego (zabezpieczonego kontrolą fizyczną) obszaru głównego urzędu certyfikacji oraz na ich opuszczenie.

189) Główny urząd certyfikacji, centralny punkt kontaktowy i zarządzający zaufaną listą wyznaczają upoważniony personel na potrzeby ciągłego monitorowania znajdujących się w obiekcie urządzeń w systemie 7x24x365. Środowisko operacyjne (np. obiekt fizyczny) nie może pozostać bez nadzoru. Personel środowiska operacyjnego nigdy nie może mieć dostępu do zabezpieczonych obszarów głównych lub podporządkowanych urzędów certyfikacji, chyba że został do tego upoważniony.

5.1.1.2. Organ ds. rejestracji / organ autoryzujący

190) Zastosowanie mają te same przepisy sekcji 5.1.1.1.

5.1.2. Dostęp fizyczny

5.1.2.1. Główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą

191) Urządzenia i dane (HSM, dane aktywacyjne, kopia zapasowa pary kluczy, komputer, dziennik, skrypt procedury generowania klucza, wniosek o wydanie certyfikatu itp.) muszą być zawsze zabezpieczone przed nieuprawnionym dostępem. Mechanizmy bezpieczeństwa fizycznego w odniesieniu wyposażenia muszą zapewniać co najmniej:

- ciągłe monitorowanie, ręczne lub elektroniczne, pod kątem nieuprawnionego wtargnięcia;
- aby nie był możliwy nieuprawniony dostęp do sprzętu komputerowego i danych aktywacyjnych;
- przechowywanie w bezpiecznym pojemniku wszystkich wymiennych nośników oraz dokumentów papierowych zawierających informacje szczególnie chronione w formie zwykłego tekstu;

- aby każda osoba wchodząca do obszarów zabezpieczonych, nieposiadająca stałego upoważnienia, nie była pozostawiona bez nadzoru upoważnionego pracownika obiektów głównego urzędu certyfikacji, centralnego punktu kontaktowego i zarządzającego zaufaną listą;
- prowadzenie dziennika dostępu i jego okresową kontrolę;
- dwa poziomy stopniowego zwiększania bezpieczeństwa, np. na poziomie granicy obiektu, budynku i pomieszczenia operacyjnego;
- wprowadzenia dwóch mechanizmów kontroli (zaufanych użytkowników) zabezpieczających przed nieuprawnionym dostępem fizycznym do modułu kryptograficznego HSM i danych aktywacyjnych.

192) Jeżeli urządzenia znajdujące się w obiekcie mają być pozostawione bez nadzoru, należy przeprowadzić kontrolę bezpieczeństwa. W ramach takiej kontroli należy sprawdzić co najmniej:

- czy stan urządzeń jest odpowiedni dla aktualnego trybu pracy;
- w przypadku elementów składowych działających w trybie off-line – czy wszystkie urządzenia są wyłączone;
- czy wszystkie bezpieczne pojemniki (koperty zabezpieczone przed naruszeniem, sejf itp.) zostały odpowiednio zabezpieczone;
- czy systemy bezpieczeństwa fizycznego (np. zamki w drzwiach, pokrywy przewodów wentylacyjnych, elektryczność) działają prawidłowo;
- czy obszar jest zabezpieczony przed nieuprawnionym dostępem.

193) Przed składowaniem należy dezaktywować wymienne moduły kryptograficzne. Gdy takie moduły nie są używane, muszą zostać umieszczone w bezpiecznym miejscu wraz z danymi aktywacyjnymi umożliwiającymi dostęp do tych modułów lub ich aktywację. Dane aktywacyjne muszą zostać zapisane w pamięci albo zarejestrowane i przechowywane w sposób odpowiadający poziomowi bezpieczeństwa, jaki zapewniono w przypadku modułu kryptograficznego. Dane te nie mogą być przechowywane razem z modułem kryptograficznym, aby uniknąć sytuacji, w której tylko jedna osoba ma dostęp do klucza prywatnego.

194) Bezpośrednią odpowiedzialność za przeprowadzenie takich kontroli ponosi osoba lub grupa osób, którym powierzono zaufane role. W przypadku gdy odpowiedzialność spoczywa na grupie osób, należy prowadzić dziennik, w którym wskazano tożsamość osoby przeprowadzającej każdą kontrolę. Jeżeli obiekt nie jest obsługiwany w sposób ciągły, ostatnia osoba, która opuszcza obiekt, musi złożyć parafę na liście wyjść z podaniem daty i godziny oraz potwierdzić obecność i uruchomienie wszystkich niezbędnych mechanizmów ochrony fizycznej.

5.1.2.2. Organ ds. rejestracji / organ autoryzujący

195) Zastosowanie mają te same przepisy sekcji 5.1.2.1.

5.1.3. Zasilanie i klimatyzacja

196) Zabezpieczone obiekty, w których znajdują się elementy składowe modelu zaufania C-ITS (główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą, organ ds. rejestracji i organ autoryzujący) muszą posiadać niezawodne zasilanie zapewniające bezawaryjne lub prawie bezawaryjne działanie. Instalacje podstawowe i zapasowe są wymagane w przypadku zewnętrznej awarii zasilania oraz w celu zapewnienia płynnego wyłączenia urządzeń modelu zaufania C-ITS w razie braku zasilania. Infrastruktura modelu zaufania C-ITS musi być wyposażona w instalacje ogrzewania/wentylacji/klimatyzacji zapewniające utrzymanie temperatury i wilgotności względnej tworzących ją urządzeń podczas ich działania. Oświadczenie dotyczące praktyk w zakresie certyfikacji dla elementu składowego modelu zaufania C-ITS będzie zawierać szczegółowy opis planu i procesów zapewniających wdrożenie takich wymogów.

5.1.4. Narażenie na działanie wody

197) Zabezpieczone obiekty, w których znajdują się elementy składowe modelu zaufania C-ITS (główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą, organ ds. rejestracji i organ autoryzujący) powinny być chronione w sposób ograniczający do minimum narażenie na działanie wody. Z tego powodu należy unikać prowadzenia przewodów z wodą i ściekami. Oświadczenie dotyczące praktyk w zakresie certyfikacji dla elementu składowego modelu zaufania C-ITS będzie zawierać szczegółowy opis planu i procesów zapewniających wdrożenie takich wymogów.

5.1.5. Ochrona przeciwpożarowa

198) Aby zapobiec niszczącemu narażeniu na działanie płomieni lub dymu, zabezpieczone obiekty, w których znajdują się elementy składowe modelu zaufania C-ITS (główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą, organ ds. rejestracji i organ autoryzujący) muszą być zbudowane i wyposażone w odpowiedni sposób; należy również wdrożyć procedury pozwalające podjąć skuteczne działania w przypadku zagrożenia pożarowego. Nośniki danych powinny być zabezpieczone przed ogniem w odpowiednich pojemnikach.

199) Elementy składowe modelu zaufania C-ITS muszą zapewniać ochronę nośników fizycznych zawierających kopie zapasowe krytycznych danych systemowych lub wszelkich innych informacji szczególnie chronionych przed zagrożeniami środowiskowymi oraz nieuprawnionym dostępem do takich nośników lub ich nieuprawnionym wykorzystaniem lub udostępnieniem. Oświadczenie dotyczące praktyk w zakresie certyfikacji dla elementu składowego modelu zaufania C-ITS będzie zawierać szczegółowy opis planu i procesów zapewniających wdrożenie takich wymogów.

5.1.6. Zarządzanie nośnikami danych

200) Z nośnikami danych wykorzystywanych w elementach składowych modelu zaufania C-ITS (główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą, organ ds. rejestracji i organ autoryzujący) należy obchodzić się w bezpieczny sposób, aby zapobiec ich zniszczeniu i kradzieży oraz nieuprawnionemu dostępowi do tych nośników. Procedury zarządzania

nośnikami danych są wdrażane, aby zapewnić ochronę przed dezaktualizacją i zniszczeniem nośników w okresie, w którym należy przechowywać rekordy.

201) Dane wrażliwe muszą być zabezpieczone przed dostępem w wyniku ponownego użycia przechowywanych obiektów (np. usuniętych plików), przez co takie dane mogą stać się dostępne dla nieupoważnionych użytkowników.

202) Należy prowadzić wykaz wszystkich zasobów informacyjnych oraz ustanowić wymogi dotyczące ochrony tych zasobów na podstawie analizy ryzyka. Oświadczenie dotyczące praktyk w zakresie certyfikacji dla elementu składowego modelu zaufania C-ITS będzie zawierać szczegółowy opis planu i procesów zapewniających wdrożenie takich wymogów.

5.1.7. Usuwanie odpadów

203) Elementy składowe modelu zaufania C-ITS (główny urząd certyfikacji, centralny punkt kontaktowy, zarządzający zaufaną listą, organ ds. rejestracji i organ autoryzujący) muszą wdrożyć procedury bezpiecznego i nieodwracalnego unieszkodliwiania odpadów (papieru, nośników danych lub wszelkich innych odpadów), aby zapobiec nieuprawnionemu dostępowi do odpadów zawierających informacje poufne/prywatne oraz ich nieuprawnionemu wykorzystaniu lub ujawnieniu. Wszystkie nośniki wykorzystywane do przechowywania informacji szczególnie chronionych, takie jak: klucze, dane aktywacyjne lub pliki, muszą zostać zniszczone przed ich oddaniem do unieszkodliwienia. Oświadczenie dotyczące praktyk w zakresie certyfikacji dla elementu składowego modelu zaufania C-ITS będzie zawierać szczegółowy opis planu i procesów zapewniających wdrożenie takich wymogów.

5.1.8. Kopie zapasowe poza obiektem

5.1.8.1. Główny urząd certyfikacji, centralny punkt kontaktowy i zarządzający zaufaną listą

204) Pełne kopie zapasowe elementów składowych głównego urzędu certyfikacji, centralnego punktu kontaktowego i zarządzającego zaufaną listą, wystarczające do przywrócenia gotowości do pracy po awarii systemu, są tworzone w trybie offline po uruchomieniu głównego urzędu certyfikacji, centralnego punktu kontaktowego i zarządzającego zaufaną listą, a także każdorazowo po wygenerowaniu nowej pary kluczy. Regularnie sporządzane są kopie zapasowe podstawowych informacji handlowych (pary kluczy i lista unieważnionych certyfikatów) i oprogramowania. Zapewniona zostaje odpowiednia infrastruktura zapasowa w celu zapewnienia możliwości odzyskania wszystkich podstawowych informacji handlowych i oprogramowania po wystąpieniu klęski żywiołowej lub awarii nośników. Ustalenia dotyczące kopii zapasowych poszczególnych systemów są regularnie sprawdzane, aby zapewnić ich zgodność z wymogami planu ciągłości działania. Co najmniej jedna pełna kopia zapasowa jest przechowywana poza obiektem (przywrócenie gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej). Kopia zapasowa jest przechowywana w miejscu, w którym kontrole fizyczne i kontrole proceduralne odpowiadają poziomowi kontroli działającego systemu infrastruktury klucza publicznego.

205) Dane kopii zapasowej podlegają tym samym wymogom dostępu co dane operacyjne. Dane kopii zapasowej są szyfrowane i przechowywane poza obiektem. W przypadku całkowitej utraty danych informacje niezbędne do

ponownego uruchomienia głównego urzędu certyfikacji, centralnego punktu kontaktowego oraz zarządzającego zaufaną listą muszą zostać w całości odzyskane z danych kopii zapasowej.

206) W przypadku materiałów dotyczących klucza prywatnego głównego urzędu certyfikacji, centralnego punktu kontaktowego oraz zarządzającego zaufaną listą kopia zapasowa nie może zostać utworzona z wykorzystaniem standardowych mechanizmów tworzenia kopii zapasowych, tylko przy użyciu funkcji kopii zapasowej w module kryptograficznym.

5.1.8.2. Organ ds. rejestracji / organ autoryzujący

207) Do niniejszej sekcji mają zastosowanie procesy opisane w sekcji 5.1.8.1.

5.2. Kontrole proceduralne

W niniejszej sekcji opisano wymogi dotyczące funkcji i obowiązków personelu oraz jego identyfikacji.

5.2.1. Zaufane role

208) Pracowników, wykonawców i konsultantów którym powierzono zaufane role, uznaje się za „zaufane osoby". Osoby, które chcą zostać uznane za zaufane osoby pod kątem uzyskaniu zaufanego stanowiska, muszą spełniać wymogi kontroli bezpieczeństwa określone w niniejszej polityce certyfikacji.

209) Zaufane osoby mają dostęp do operacji uwierzytelniania lub operacji kryptograficznych, lub kontrolują te operacje, które mogą mieć istotny wpływ na:

- potwierdzenie informacji zawartych we wnioskach o wydanie certyfikatu;
- przyjęcie, odrzucenie lub innego rodzaju przetwarzanie wniosków o wydanie certyfikatu, wniosków o unieważnienie certyfikatu lub wniosków o przedłużenie certyfikatu;
- wydawanie lub unieważnienie certyfikatów, w tym na personel posiadający dostęp do ograniczonych części repozytorium, lub na przetwarzanie informacji na temat abonentów lub ich wniosków.

210) Zaufane role obejmują między innymi:

- obsługę klientów;
- administrację systemu;
- wskazane kwestie techniczne;
- kadrę zarządzającą odpowiedzialną za wiarygodność infrastruktury.

211) Urząd certyfikacji przedstawia jasne opisy wszystkich zaufanych ról w swoim oświadczeniu dotyczącym praktyk w zakresie certyfikacji.

5.2.2. Liczba osób wymaganych do realizacji zadania

212) W ramach elementów składowych modelu zaufania C-ITS ustanawiane są, utrzymywane i wprowadzane w życie rygorystyczne procedury kontroli, aby zapewnić podział obowiązków według zaufanych ról oraz aby wiele zaufanych osób miało obowiązek wykonywania szczególnie istotnych zadań. Elementy składowe modelu zaufania (zarządzający zaufaną listą, centralny punkt

kontaktowy, główny urząd certyfikacji, organ ds. rejestracji i organ autoryzujący) powinny być zgodne z [4] oraz z wymogami określonymi w poniższych punktach.

213) Wprowadzono procedury w zakresie polityki i kontroli zapewniające podział zadań na podstawie obowiązków służbowych. Najbardziej istotne zadania, takie jak dostęp do sprzętu kryptograficznego (HSM) urzędu certyfikacji i materiałów dotyczących powiązanych z nim kluczy oraz zarządzanie tym modułem, muszą wymagać upoważnienia ze strony wielu zaufanych osób.

214) Takie wewnętrzne procedury kontroli muszą być zaprojektowane w taki sposób, aby co najmniej dwie zaufane osoby musiały mieć dostęp fizyczny lub logiczny do tego urządzenia. Ograniczenia dostępu do sprzętu kryptograficznego urzędu certyfikacji muszą być ściśle egzekwowane przez wiele zaufanych osób przez cały czas pracy tego sprzętu, od odbioru nowego sprzętu po jego końcowe zniszczenie logiczne lub fizyczne. Po uruchomieniu modułu za pomocą kluczy operacyjnych stosowane są dalsze kontrole dostępu w celu utrzymania podziału kontroli nad dostępem zarówno fizycznym, jak i logicznym, do danego urządzenia.

5.2.3. Identyfikacja i uwierzytelnianie każdej roli

215) Wszystkie osoby, którym przyznano rolę, jak opisano w ramach tej polityki certyfikacji, są identyfikowane i uwierzytelniane w celu zagwarantowania, aby rola ta umożliwiała im wykonywanie obowiązków w zakresie infrastruktury klucza publicznego.

216) Elementy modelu zaufania C-ITS weryfikują i potwierdzają tożsamość i upoważnienie wszystkich pracowników, którzy chcą zostać zaufanymi osobami, zanim takie osoby:

- otrzymają urządzenia dostępowe i dostęp do wymaganych obiektów;
- otrzymają elektroniczne dane uwierzytelniające umożliwiające dostęp do systemów urzędu certyfikacji i wykonywanie określonych funkcji w tych systemach.

217) Oświadczenie dotyczące praktyk w zakresie certyfikacji opisuje mechanizmy stosowane do identyfikacji i uwierzytelniania poszczególnych osób.

5.2.4. Role wymagające podziału obowiązków

218) Role wymagające podziału obowiązków obejmują (między innymi):

- przyjmowanie, odrzucanie i uchylanie wniosków oraz innego rodzaju rozpatrywanie wniosków o wydanie certyfikatu urzędu certyfikacji;
- generowanie, wydawanie i niszczenie certyfikatu urzędu certyfikacji.

219) Podział obowiązków może być wykonywany z wykorzystaniem urządzeń lub procedur infrastruktury klucza publicznego, lub obu tych elementów. Żadnej osobie nie można przypisać więcej niż jednej tożsamości, chyba że zostały one zatwierdzone przez główny urząd certyfikacji.

220) Część głównego urzędu certyfikacji i urząd certyfikacji, które zajmują się zarządzaniem w zakresie generowania i unieważniania certyfikatów, są niezależne od innych organizacji w zakresie podejmowanych przez nie decyzji dotyczących tworzenia, świadczenia, utrzymywania i zawieszania usług

zgodnie z mającymi zastosowanie politykami certyfikacji. W szczególności kadra zarządzająca wyższego szczebla, kadra kierownicza wyższego szczebla i pracownicy pełniący zaufane role nie mogą podlegać żadnym naciskom komercyjnym, finansowym ani innego rodzaju naciskom, które mogłyby negatywnie wpłynąć na zaufanie do świadczonych przez takie osoby usług.

221) Organ ds. rejestracji i organ autoryzujący, które obsługują ruchome stacje C-ITS, są odrębnymi jednostkami operacyjnymi, posiadającymi oddzielne zespoły ds. infrastruktury informatycznej i zarządzania systemami informatycznymi. Zgodnie z ogólnym rozporządzeniem o ochronie danych organ ds. rejestracji i organ autoryzujący nie wymieniają się żadnymi danymi osobowymi, z wyjątkiem danych wymienianych w celu autoryzacji wniosków o bilety autoryzacyjne. Organy te przekazują dane związane z zatwierdzaniem wniosków o bilet autoryzacyjny wyłącznie za pomocą protokołu walidacji autoryzacji z [1] wykorzystaniem specjalnego bezpiecznego interfejsu. Dopuszcza się stosowanie innych protokołów, pod warunkiem że stosuje się [1].

222) Rejestry przechowywane przez organ ds. rejestracji i organ autoryzujący mogą być wykorzystywane wyłącznie w celu anulowania nieprawidłowo zachowujących się danych uwierzytelniających rejestrację w oparciu o bilety autoryzacyjne w przejętych złośliwych komunikatach CAM/DENM. Po stwierdzeniu, że komunikat CAM/DENM jest złośliwy, organ autoryzujący sprawdzi klucz weryfikacji biletu autoryzacyjnego w prowadzonych przez siebie rejestrach wydanych biletów autoryzacyjnych i złoży do organu ds. rejestracji wniosek o unieważnienie zawierający podpis zaszyfrowany według klucza prywatnego danych uwierzytelniających rejestrację, który został wykorzystany przy wydawaniu biletu autoryzacyjnego. Wszystkie rejestry muszą być odpowiednio chronione przed dostępem osób nieupoważnionych i nie mogą być udostępniane innym jednostkom ani organom.

Uwaga: W czasie sporządzania niniejszej wersji polityki certyfikacji nie zdefiniowano konstrukcji funkcji o nieodpowiednim zachowaniu. Planuje się ewentualne zaprojektowanie funkcji o nieodpowiednim zachowaniu w ramach przyszłych przeglądów polityki.

5.3. Nadzorowanie personelu

5.3.1. Wymogi w zakresie kwalifikacji, doświadczenia i poświadczeń

223) W ramach elementów modelu zaufania C-ITS zatrudnia się wystarczającą liczbę pracowników posiadających wiedzę fachową, doświadczenie i kwalifikacje niezbędne do wykonywania funkcji w zakresie wykonywanej pracy i świadczenia oferowanych usług. Personel infrastruktury klucza publicznego spełnia te wymogi dzięki formalnym szkoleniom i danym uwierzytelniającym, faktycznemu doświadczeniu lub połączeniu obu warunków. Zaufane role i obowiązki, określone w oświadczeniu dotyczącym praktyk w zakresie certyfikacji, są udokumentowane w opisach stanowisk pracy i wyraźnie określone. Konieczne jest sporządzenie opisu stanowisk pracy podwykonawców personelu infrastruktury klucza publicznego, aby zapewnić rozdzielenie obowiązków i uprawnień, a newralgiczność stanowiska określa się na podstawie obowiązków i poziomów dostępu, sprawdzania przeszłości oraz szkolenia i świadomości pracowników.

5.3.2. Procedury sprawdzania przeszłości

224) W ramach elementów modelu zaufania C-ITS przeprowadza się sprawdzanie przeszłości pracowników, którzy zamierzają zostać zaufanymi osobami. W przypadku pracowników zajmujących zaufane stanowiska sprawdzanie przeszłości musi odbywać się przynajmniej raz na pięć lat.

225) Czynniki wykryte w ramach sprawdzania przeszłości, które można uznać za podstawę do odrzucenia kandydatów ubiegających się o zaufane stanowiska lub do podjęcia działania przeciwko zaufanej osobie, obejmują (między innymi):

- podanie nieprawdziwych informacji przez kandydata lub zaufaną osobę;
- wysoce niekorzystne lub niewiarygodne referencje zawodowe;
- niektóre wyroki skazujące;
- przesłanki świadczące o braku odpowiedzialności finansowej.

226) Sprawozdania zawierające takie informacje są oceniane przez personel ds. zasobów ludzkich, który podejmuje odpowiednie działania w zależności od rodzaju, skali i częstotliwości zachowania wykrytego w toku sprawozdania przeszłości. Takie działanie może obejmować środki obejmujące nawet anulowanie ofert zatrudnienia przedstawionych kandydatom na zaufane stanowiska lub rozwiązanie stosunku pracy z zaufanymi osobami. Wykorzystanie jako podstawy takiego działania informacji ujawnionych w toku sprawdzania przeszłości podlega obowiązującym przepisom.

227) Sprawdzanie przeszłości osób, które chcą zostać zaufaną osobą, obejmuje między innymi:

- potwierdzenie poprzedniego zatrudnienia;
- kontrolę referencji zawodowych obejmującą zatrudnienie przez okres co najmniej pięciu lat;
- uzyskanie potwierdzenia najwyższego lub najodpowiedniejszego uzyskanego stopnia wykształcenia;
- przeszukanie rejestrów karnych.

5.3.3. Wymogi szkoleniowe

228) W ramach elementów modelu zaufania C-ITS pracownicy przechodzą wymagane szkolenia umożliwiające im pełnienie swoich obowiązków związanych z działalnością urzędu certyfikacji w sposób kompetentny i zadowalający.

229) Programy szkolenia podlegają okresowemu przeglądowi, a określone w nich szkolenia dotyczą kwestii istotnych z punktu widzenia funkcji pełnionych przez pracowników.

230) Programy szkolenia uwzględniają kwestie istotne z punktu widzenia konkretnego środowiska uczestnika szkolenia, w tym:

- zasady i mechanizmy bezpieczeństwa elementów modelu zaufania C-ITS;
- używane wersje sprzętu i oprogramowania;

- wszystkie obowiązki, które dana osoba ma wykonywać, oraz wewnętrzne i zewnętrzne procesy i sekwencje sprawozdawczości;
- procesy biznesowe i przepływy pracy w infrastrukturze klucza publicznego;
- zgłaszanie incydentów i przypadków naruszenia bezpieczeństwa oraz postępowanie w przypadku ich wystąpienia;
- procedury przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej oraz procedury ciągłości działania;
- dostateczną wiedzę informatyczną.

5.3.4. Częstotliwość i wymogi powtarzania szkoleń

231) Osoby, którym powierzono zaufane role, są zobowiązane do ustawicznego utrwalania wiedzy zdobytej w ramach szkolenia, przy korzystaniu ze środowiska szkoleniowego. Szkolenie musi być powtarzane zawsze, gdy uznaje się, że zachodzi taka potrzeba, i co najmniej raz na dwa lata.

232) Podmioty stanowiące elementy modelu zaufania C-ITS zapewniają swoim pracownikom szkolenie przypominające i dostarczają im aktualne informacje w takim zakresie i tak często, jak jest to konieczne do zapewnienia, aby pracownicy utrzymali wymagany poziom biegłości umożliwiający im wykonywanie swoich obowiązków zawodowych w sposób kompetentny i zadowalający.

233) W stosownych przypadkach osoby pełniące zaufane role muszą wiedzieć o zmianach w funkcjonowaniu infrastruktury klucza publicznego. Każdej istotnej zmianie dotyczącej operacji towarzyszy plan szkolenia (w zakresie świadomości), którego realizacja jest dokumentowana.

5.3.5. Częstotliwość i kolejność rotacji stanowisk

234) Częstotliwość i kolejność rotacji stanowisk nie jest określona, tylko ma być prowadzona tak, aby zapewnione zostały umiejętności techniczne, doświadczenie i prawa dostępu. Administratorzy elementów modelu zaufania C-ITS zapewniają, aby zmiany personelu nie miały wpływu na bezpieczeństwo systemu.

5.3.6. Sankcje z tytułu nieuprawnionych działań

235) Każdy z elementów modelu zaufania C-ITS musi opracować formalny proces dyscyplinarny, aby zapewnić odpowiednie karanie działań nieuprawnionych. W poważnych przypadkach należy cofnąć przypisaną rolę i związane z nią przywileje.

5.3.7. Wymogi dotyczące niezależnego wykonawcy

236) Elementy modelu zaufania C-ITS mogą umożliwiać niezależnym wykonawcom lub konsultantom uzyskanie statusu zaufanych osób tylko w takim zakresie, w jakim jest to niezbędne do utrzymywania wyraźnie określonego stosunku outsourcingu, oraz pod warunkiem, że jednostka ufa wykonawcom lub konsultantom w takim samym stopniu co pracownikom, a wykonawcy i konsultanci spełniają wymogi mające zastosowanie do pracowników.

237) W przeciwnym razie niezależni wykonawcy i konsultanci mają dostęp do zabezpieczonych obiektów infrastruktury klucza publicznego C-ITS wyłącznie w towarzystwie i pod bezpośrednim nadzorem zaufanych osób.

5.3.8. Dokumentacja przekazana personelowi

238) Podmioty stanowiące elementy modelu zaufania C-ITS zapewniają swoim pracownikom wymagane szkolenia i dostęp do dokumentacji, których potrzebują, aby wypełniać swoje obowiązki w sposób kompetentny i zadowalający.

5.4. Procedury rejestracji kontroli

239) W niniejszej sekcji określono wymogi dotyczące rodzajów zdarzeń, które mają być rejestrowane, oraz zarządzania dziennikami kontroli.

5.4.1. Rodzaje zdarzeń rejestrowanych i zgłaszanych przez każdy urząd certyfikacji

240) Przedstawiciel urzędu certyfikacji dokonuje regularnego przeglądu rejestrów, zdarzeń i procedur urzędu certyfikacji.

241) Elementy modelu zaufania C-ITS rejestrują następujące rodzaje zdarzeń audytowych (w stosownych przypadkach):

- uzyskanie fizycznego dostępu do obiektu – wejście osób fizycznych do obiektów będzie rejestrowane przez przechowywanie wniosków o dostęp za pomocą kart elektronicznych. Każdorazowo po utworzeniu rekordu zostanie utworzone zdarzenie;
- zarządzanie zaufanymi rolami – rejestracji będą podlegać wszelkie zmiany w definicji poszczególnych ról i przypisanym im poziomie dostępu, w tym zmiana atrybutów ról. Każdorazowo po utworzeniu rekordu zostanie utworzone zdarzenie;
- dostęp logiczny – zdarzenie zostanie wygenerowane, gdy jednostka (np. program) ma dostęp do obszarów wrażliwych (tj. sieci i serwerów);
- zarządzanie kopiami zapasowymi – zdarzenie jest tworzone każdorazowo po udanym albo nieudanym procesie tworzenia kopii zapasowej;
- zarządzanie rejestrami – rejestry będą przechowywane. Zdarzenie zostaje utworzone, jeżeli rozmiar rejestru przekracza określony rozmiar;
- dane z procesu uwierzytelnienia w odniesieniu do abonentów i elementów modelu zaufania C-ITS – zdarzenia zostaną wygenerowane dla każdego wniosku o uwierzytelnienie ze strony abonentów i elementów modelu zaufania C-ITS;
- przyjęcie i odrzucenie wniosków o wydanie świadectwa, w tym utworzenie i przedłużenie certyfikatu – zdarzenie będzie generowane okresowo wraz z listą zatwierdzonych i odrzuconych wniosków o wydanie certyfikatu w ciągu poprzednich siedmiu dni;
- rejestracja producenta – zdarzenie zostanie utworzone w momencie rejestracji producenta;
- rejestracja stacji C-ITS – zdarzenie zostanie utworzone w momencie rejestracji stacji C-ITS;

- zarządzanie HSM – zdarzenie zostanie utworzone w momencie rejestracji naruszenia bezpieczeństwa HSM;
- zarządzanie systemami informatycznymi i siecią, które odnoszą się do systemów infrastruktury klucza publicznego – zdarzenie zostanie utworzone w momencie wyłączenia lub ponownego uruchomienia serwera infrastruktury klucza publicznego;
- zarządzanie bezpieczeństwem (udane i nieudane próby uzyskania dostępu do systemu infrastruktury klucza publicznego, realizowane działania infrastruktury klucza publicznego i systemu bezpieczeństwa, zmiany profilu bezpieczeństwa, awarie systemu, awarie sprzętu komputerowego oraz inne nieprawidłowości, działania zapory sieciowej i routera; wejścia do obiektów infrastruktury klucza publicznego i opuszczanie takich obiektów);
- dane dotyczące zdarzenia będą przechowywane co najmniej przez pięć lat, chyba że zastosowanie mają dodatkowe przepisy krajowe.

242) Zgodnie z ogólnym rozporządzeniem o ochronie danych dzienniki kontroli nie mogą umożliwiać dostępu do danych osobowych dotyczących pojazdów prywatnych, w których znajduje się stacja C-ITS.

243) W miarę możliwości dzienniki kontroli dotyczące bezpieczeństwa są gromadzone automatycznie. Jeżeli nie jest to możliwe, stosuje się dziennik pokładowy, formularz papierowy lub inny mechanizm fizyczny. Wszystkie dzienniki kontroli dotyczące bezpieczeństwa, zarówno w formie elektronicznej i nieelektronicznej, są przechowywane i udostępniane podczas audytów zgodności.

244) Każde zdarzenie związane z cyklem życia certyfikatu jest zarejestrowane w taki sposób, że można go przypisać osobie, która je przeprowadziła. Wszystkie dane związane z tożsamością osobistą są szyfrowane i chronione przed dostępem osób nieupoważnionych.

245) Każdy rekord audytu zawiera przynajmniej następujące elementy (rejestrowane automatycznie lub ręcznie w odniesieniu do każdego zdarzenia podlegającego audytowi):

- rodzaj zdarzenia (zgodnie z listą powyżej);
- zaufaną datę i godzinę wystąpienia zdarzenia;
- rezultat zdarzenia – w stosownych przypadkach powodzenie albo niepowodzenie;
- w stosownych przypadkach tożsamość jednostki lub operatora, który spowodował zdarzenie;
- tożsamość jednostki, której dane wydarzenie dotyczy.

5.4.2. Częstotliwość przetwarzania dziennika

246) Dzienniki kontroli podlegają przeglądowi w odpowiedzi na ostrzeżenia wysyłane na podstawie nieprawidłowości i incydentów zachodzących w systemach urzędu certyfikacji, a także corocznemu okresowemu przeglądowi.

247) Przetwarzanie dziennika kontroli polega na przeglądzie dzienników kontroli i udokumentowaniu powodu wszystkich istotnych zdarzeń w podsumowaniu dzienników kontroli. Przeglądy dziennika kontroli obejmują weryfikację, czy nie miała miejsca żadna nieuprawniona ingerencja w dziennik, kontrolę wszystkich wpisów do dziennika oraz analizę wszelkich ostrzeżeń lub nieprawidłowości zawartych w dziennikach. Działania podejmowane na podstawie przeglądów dzienników kontroli są dokumentowane.

248) Dziennik kontroli jest archiwizowany co najmniej raz w tygodniu. Administrator archiwizuje go ręcznie, jeżeli wolna przestrzeń przeznaczona na dziennik kontroli jest niewystarczająca wobec przewidywanej ilości danych dziennika kontroli generowanych w danym tygodniu.

5.4.3. Okres przechowywania dziennika kontroli

249) Zapisy dziennika kontroli dotyczące cyklu życia certyfikatu są przechowywane przez co najmniej pięć lat po wygaśnięciu danego certyfikatu.

5.4.4. Ochrona dziennika kontroli

250) Integralność i poufność dziennika kontroli gwarantuje się dzięki mechanizmowi kontroli dostępu w oparciu o podział na role. Dostęp do wewnętrznych dzienników kontroli mają wyłącznie administratorzy, natomiast dostęp do dzienników kontroli związanych z cyklem życia certyfikatu mogą uzyskać również użytkownicy posiadający odpowiednią autoryzację za pośrednictwem strony internetowej z logowaniem użytkownika. Dostęp udzielany jest w ramach uwierzytelnienia przez kilku użytkowników (przynajmniej dwóch) i co najmniej na dwóch poziomach. Należy zapewnić techniczne zabezpieczenia tak, aby użytkownicy nie mieli dostępu do ich własnych rejestrów.

251) Wszystkie wpisy w rejestrze są podpisywane z użyciem materiału klucza z HSM.

252) Rejestry zdarzeń zawierające informacje, które mogą prowadzić do identyfikacji osób, np. informacje o prywatnym pojeździe, są szyfrowane w taki sposób, aby jedynie upoważnione osoby mogły je odczytać.

253) Rejestry zdarzeń są tworzone w taki sposób, aby nie mogły być łatwo usunięte ani zniszczone (z wyjątkiem transferu do nośników długoterminowego przechowywania danych) w okresie, w którym należy je przechowywać.

254) Rejestry zdarzeń są chronione w sposób umożliwiający ich odczytanie przez okres ich przechowywania.

5.4.5. Procedury tworzenia kopii zapasowych dzienników kontroli

255) Kopie zapasowe dzienników kontroli i podsumowań audytów są tworzone za pomocą mechanizmów kopii zapasowych przedsiębiorstwa, pod kontrolą upoważnionych zaufanych ról, niezależnie od źródłowego generowania ich elementów składowych. Kopie zapasowe dzienników kontroli są chronione na takim samym poziomie zaufania, jaki ma zastosowanie do pierwotnych rejestrów.

5.4.6. System zbierania danych z audytu (wewnętrzny lub zewnętrzny)

256) Urządzenia elementów modelu zaufania C-ITS aktywują procesy audytu w momencie uruchomienia systemu i wyłączają je jedynie w momencie

zamknięcia systemu. Jeżeli procesy audytu nie są dostępne, element modelu zaufania C-ITS zawiesza działanie.

257) Na koniec każdego okresu operacyjnego i przy tworzeniu nowych kluczy dla certyfikatów zbiorowy status urządzeń powinien zostać zgłoszony kierownikowi ds. operacyjnych i organowi zarządzającemu operacjami w danym elemencie infrastruktury klucza publicznego.

5.4.7. Powiadamianie jednostki odpowiedzialnej za zdarzenie

258) W przypadku gdy zdarzenie zostaje zarejestrowane przez system zbierania danych z audytu, taki system zapewnia, aby dane zdarzenie było powiązane z zaufaną rolą.

5.4.8. Ocena luk w zabezpieczeniach

259) Rola związana z odpowiedzialnością za przeprowadzenie audytu i role związane z odpowiedzialnością za działanie systemu infrastruktury klucza publicznego w ramach elementów modelu zaufania C-ITS mają na celu wyjaśnianie wszystkich istotnych zdarzeń w podsumowaniu ścieżki audytu. W ramach takich przeglądów najpierw sprawdza się, czy ścieżka nie została zmieniona przez niepowołane osoby, czy nie ma braku ciągłości danych audytowych lub czy nie doszło do innego rodzaju utraty takich danych, a następnie wszystkie wpisy w ścieżce zostają pobieżnie zbadane, przy czym wszelkie ostrzeżenia lub nieprawidłowości w ścieżkach zostają szczegółowo przeanalizowane. Działania podjęte w wyniku tych przeglądów są dokumentowane.

260) Elementy modelu zaufania C-ITS:

- wdrażają kontrole organizacyjne lub techniczne w zakresie wykrywania i zapobiegania w ramach kontroli elementów modelu zaufania C-ITS, aby ochronić systemy infrastruktury klucza publicznego przed wirusami i złośliwym oprogramowaniem;
- dokumentują i śledzą proces korygowania luk w zabezpieczeniach, który obejmuje identyfikację, przegląd, reagowanie i usuwanie luk w zabezpieczeniach;
- podlegają skanowaniu pod kątem luk w zabezpieczeniach lub przeprowadzają takie skanowanie:
  - po wprowadzeniu wszelkich zmian w systemie lub sieci, które to zmiany elementy modelu zaufania C-ITS uznają za istotne dla elementów składowych infrastruktury klucza publicznego; oraz
  - co najmniej raz w miesiącu, w odniesieniu do publicznych i prywatnych adresów IP zidentyfikowanych przez urząd certyfikacji, centralny punkt kontaktowy jako systemy infrastruktury klucza publicznego;
- poddaje systemy infrastruktury klucza publicznego badaniu wniknięcia co najmniej raz do roku oraz po aktualizacjach lub modyfikacjach infrastruktury lub aplikacji, które to aktualizacje lub modyfikacje zostają uznane przez elementy modelu zaufania C-ITS za istotne dla elementów składowych infrastruktury klucza publicznego urzędu certyfikacji;
- w przypadku systemów online – dokumentują dowody wskazujące, że każdorazowo skanowanie pod kątem luk w zabezpieczeniach i badanie wniknięcia były przeprowadzane przez osobę lub jednostkę (lub wspólnie), które wykazują umiejętności, narzędzia, biegłość, kodeks etyczny i niezależność niezbędne do przeprowadzenia wiarygodnego badania pod kątem luk w zabezpieczeniach lub badania wniknięcia;
- śledzą i eliminują luki w zabezpieczeniach zgodnie z polityką w zakresie cyberbezpieczeństwa w przedsiębiorstwach oraz z metodyką ograniczania ryzyka.

5.5. Archiwizacja zapisów

5.5.1. Rodzaje archiwizowanych zapisów

261) Elementy modelu zaufania C-ITS muszą archiwizować rekordy, które są wystarczająco szczegółowe do ustalenia ważności podpisu i prawidłowego funkcjonowania infrastruktury klucza publicznego. Archiwizuje się przynajmniej następujące rekordy zdarzeń dotyczących infrastruktury klucza publicznego (w stosownych przypadkach):

- rejestr dostępu do fizycznego obiektu elementów modelu zaufania C-ITS (co najmniej jeden rok);
- rejestr zarządzania zaufanymi rolami w zakresie elementów modelu zaufania C-ITS (co najmniej 10 lat);
- rejestr dostępu do systemu informatycznego dotyczący elementów modelu zaufania C-ITS (co najmniej pięć lat);

- rejestr tworzenia, użytkowania i niszczenia kluczy w przypadku urzędu certyfikacji (co najmniej pięć lat) (a nie w przypadku zarządzającego zaufaną listą i centralnego punktu kontaktowego);
- rejestr tworzenia, użytkowania i niszczenia certyfikatów (co najmniej dwa lata);
- rejestr wniosków organu ds. polityki certyfikacji C-ITS (co najmniej dwa lata);
- rejestr zarządzania danymi aktywacyjnymi dotyczący elementów modelu zaufania C-ITS (co najmniej pięć lat);
- rejestr systemów informatycznych i sieci dotyczący elementów modelu zaufania C-ITS (co najmniej pięć lat);
- dokumentację infrastruktury klucza publicznego w zakresie elementów modelu zaufania C-ITS (co najmniej pięć lat);
- incydent związany z bezpieczeństwem i sprawozdanie z audytu dotyczące elementów modelu zaufania C-ITS (co najmniej 10 lat);
- urządzenia systemu, oprogramowanie i konfigurację (co najmniej pięć lat).

262) Elementy modelu zaufania C-ITS zachowują następujące dokumenty dotyczące wniosków o wydanie certyfikatu i ich weryfikacji – oraz wszystkie certyfikaty zarządzającego zaufaną listą, głównego urzędu certyfikacji i urzędu certyfikacji oraz listę unieważnionych certyfikatów – przez okres co najmniej siedmiu lat po wygaśnięciu ważności każdego certyfikatu wydanego na podstawie tych dokumentów:

- dokumentację z audytu infrastruktury klucza publicznego prowadzoną przez elementy modelu zaufania C-ITS;
- dokumenty w ramach oświadczenia dotyczącego praktyk w zakresie certyfikacji przechowywane przez elementy modelu zaufania C-ITS;
- umowę między organem ds. polityki certyfikacji C-ITS a innymi jednostkami przechowywaną przez elementy modelu zaufania C-ITS;
- certyfikaty (lub inne informacje o unieważnieniu) przechowywane przez urząd certyfikacji i zarządzającego zaufaną listą;
- rekordy wniosków o wydanie certyfikatu w systemie głównego urzędu certyfikacji (nie dotyczy zarządzającego zaufaną listą);
- inne dane lub wnioski wystarczające do weryfikacji treści archiwalnych;
- wszystkie prace związane z elementami modelu zaufania C-ITS i audytorami zgodności lub przez nie wykonane.

263) Urząd certyfikacji zachowuje wszystkie dokumenty dotyczące wniosków o wydanie certyfikatu i ich weryfikacji – oraz wszystkie certyfikaty i informacje o ich unieważnieniu – przez okres co najmniej siedmiu lat po wygaśnięciu ważności każdego certyfikatu wydanego na podstawie tych dokumentów.

5.5.2. Okres przechowywania archiwum

264) Nie naruszając przepisów wymagających dłuższego okresu archiwizacji, elementy modelu zaufania C-ITS przechowują całą dokumentację przez co najmniej pięć lat po wygaśnięciu odpowiedniego certyfikatu.

5.5.3. Ochrona archiwum

265) Elementy modelu zaufania C-ITS przechowują archiwum rejestrów w bezpiecznym, chronionym miejscu przechowywania oddzielonym od sprzętu urzędu certyfikacji, przy czym fizyczne i proceduralne kontrole bezpieczeństwa są przynajmniej równoważne z kontrolami infrastruktury klucza publicznego.

266) Archiwum chroni się przed nieuprawnionym przeglądaniem, modyfikacją, usuwaniem lub inną ingerencją poprzez przechowywanie w zaufanym systemie.

267) Nośniki, na których przechowuje się dane archiwalne i aplikacje wymagane do ich przetwarzania, są utrzymywane w celu zapewnienia dostępu do nich przez okres wskazany w polityce certyfikacji.

5.5.4. Archiwum systemu i jego przechowywanie

268) Elementy składowe modelu zaufania C-ITS stopniowo tworzą codziennie kopie zapasowe archiwów systemowych takich informacji, a co tydzień tworzą pełne kopie zapasowe. Kopie dokumentów w formie papierowej przechowuje się w zabezpieczonym obiekcie poza zakładem.

5.5.5. Wymogi dotyczące oznaczania czasu zapisów

269) Elementy modelu zaufania C-ITS zarządzające bazą danych o unieważnieniach zapewniają, aby rejestry zawierały informacje na temat czasu i daty utworzenia rejestrów dotyczących unieważnień. Integralność takich informacji będzie wdrażana za pomocą rozwiązań kryptograficznych.

5.5.6. System zbierania zapisów archiwalnych (wewnętrzny lub zewnętrzny)

270) System zbierania zapisów archiwalnych jest systemem wewnętrznym.

5.5.7. Procedury uzyskiwania dostępu do informacji archiwalnych i ich weryfikacji

271) Wszystkie elementy modelu zaufania C-ITS umożliwiają dostęp do archiwum jedynie upoważnionym osobom zaufanym. W oświadczeniu dotyczącym praktyk w zakresie certyfikacji główne urzędy certyfikacji i pozostałe urzędy certyfikacji opisują procedury tworzenia, weryfikacji, pakowania, przekazywania i przechowywania danych archiwalnych.

272) Sprzęt głównego urzędu certyfikacji i urzędów certyfikacji weryfikuje integralność informacji zanim zostaną przywrócone.

5.6. Zmiana klucza dla elementów modelu zaufania C-ITS

273) Następujące elementy modelu zaufania C-ITS mają szczególne wymogi dotyczące zmiany ich klucza: certyfikaty zarządzającego zaufaną listą, głównego urzędu certyfikacji oraz organu ds. rejestracji / organu autoryzującego.

5.6.1. Zarządzający zaufaną listą

274) Zarządzający zaufaną listą usuwa swój klucz prywatny po wygaśnięciu odpowiedniego certyfikatu. Generuje nową parę kluczy i odpowiedni certyfikat zarządzającego zaufaną listą zanim dezaktywuje aktualny ważny klucz prywatny. Zarządzający zadba o to, aby nowy certyfikat (łączący) został wpisany na europejską zaufaną listę certyfikatów w czasie umożliwiającym rozesłanie go do wszystkich stacji C-ITS, zanim zacznie obowiązywać. Certyfikat łączący i nowy autonomiczny certyfikat są przekazywane do centralnego punktu kontaktowego.

5.6.2. Główny urząd certyfikacji

275) Główny urząd certyfikacji dezaktywuje i usuwa aktualny klucz prywatny (w tym klucze zapasowe), tak aby nie wydawał certyfikatu organu ds. rejestracji / organu autoryzującego z okresem ważności wykraczającym poza ważność certyfikatu głównego urzędu certyfikacji.

276) Główny urząd certyfikacji generuje nową parę kluczy oraz odpowiadający im certyfikat głównego urzędu certyfikacji i certyfikat łączący przed dezaktywacją aktualnego klucza prywatnego (w tym kluczy zapasowych) i przesyła go do zarządzającego zaufaną listą w celu wprowadzenia go na europejskiej zaufanej liście certyfikatów. Okres ważności nowego certyfikatu głównego urzędu certyfikacji rozpoczyna się od planowanej dezaktywacji aktualnego klucza prywatnego. Główny urząd certyfikacji zadba o to, aby nowy certyfikat został wpisany na europejską zaufaną listę certyfikatów w czasie umożliwiającym jego rozesłanie do wszystkich stacji C-ITS, zanim zacznie obowiązywać.

277) Główny urząd certyfikacji uruchamia nowy klucz prywatny, gdy jego odpowiedni certyfikat staje się ważny.

5.6.3. Certyfikat organu ds. rejestracji / organu autoryzującego

278) Organ ds. rejestracji / organ autoryzujący dezaktywuje aktualny klucz prywatny, tak aby nie mógł on wydawać danych uwierzytelniających rejestrację / biletów autoryzacyjnych z okresem ważności wykraczającym poza ważność certyfikatu organu ds. rejestracji / organu autoryzującego.

279) Organ ds. rejestracji / organ autoryzujący generuje nową parę kluczy i wnioskuje o odpowiedni certyfikat organu ds. rejestracji / organu autoryzującego przed dezaktywacją aktualnego klucza prywatnego. Okres ważności nowego certyfikatu organu ds. rejestracji / organu autoryzującego rozpoczyna się od planowanej dezaktywacji aktualnego klucza prywatnego. Organ ds. rejestracji / organ autoryzujący zadba o to, aby nowy certyfikat został opublikowany w czasie umożliwiającym jego rozesłanie do wszystkich stacji C-ITS, zanim zacznie obowiązywać.

280) Organ ds. rejestracji / organ autoryzujący aktywuje nowy klucz prywatny, gdy jego odpowiedni certyfikat staje się ważny.

5.6.4. Audytor

Brak przepisów.

5.7. Naruszenie ochrony i przywrócenie gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej

5.7.1. Postępowanie w przypadku incydentu i naruszenia ochrony

281) Elementy modelu zaufania C-ITS na bieżąco monitorują swoje urządzenia, aby wykryć potencjalne próby włamania lub inne formy naruszenia. W takim przypadku przeprowadzają one dochodzenie w celu określenia charakteru i stopnia szkody.

282) Jeżeli pracownicy odpowiedzialni za zarządzanie głównym urzędem certyfikacji lub zarządzający zaufaną listą wykryją potencjalne próby włamania lub inną formę naruszenia, przeprowadzają dochodzenie w celu określenia charakteru i stopnia szkody. W przypadku naruszenia klucza prywatnego certyfikat głównego urzędu certyfikacji zostaje unieważniony. Eksperci ds. bezpieczeństwa IT organu ds. polityki certyfikacji C-ITS oceniają zakres potencjalnych szkód w celu ustalenia, czy infrastruktura klucza publicznego musi zostać przebudowana, czy tylko niektóre certyfikaty muszą zostać unieważnione lub czy infrastruktura klucza publicznego została naruszona. Ponadto organ ds. polityki certyfikacji C-ITS określa, które usługi mają być utrzymane (informacje o unieważnieniu i statusie certyfikatu) oraz w jaki sposób, zgodnie z planem ciągłości działania organu ds. polityki certyfikacji C-ITS.

283) Oświadczenie dotyczące praktyk w zakresie certyfikacji obejmuje incydent, naruszenie i ciągłość działania, które mogą również opierać się na innych zasobach przedsiębiorstwa i planach wdrożenia.

284) Jeżeli pracownicy odpowiedzialni za zarządzanie organem ds. rejestracji / organem autoryzującym / centralnym punktem kontaktowym wykryją potencjalne próby włamania lub inną formę naruszenia, przeprowadzają dochodzenie w celu określenia charakteru i stopnia szkody. Pracownicy odpowiedzialni za zarządzanie urzędem certyfikacji lub jednostką centralnego punktu kontaktowego oceniają zakres potencjalnych szkód w celu ustalenia, czy element infrastruktury klucza publicznego musi zostać przebudowany, czy tylko niektóre certyfikaty muszą zostać unieważnione lub czy element infrastruktury klucza publicznego został naruszony. Ponadto podporządkowany urząd certyfikacji określa, które usługi mają być utrzymane, i w jaki sposób – zgodnie z planem ciągłości działania podporządkowanego urzędu certyfikacji. W przypadku naruszenia elementu infrastruktury klucza publicznego, urząd certyfikacji ostrzega swój własny główny urząd certyfikacji i zarządzającego zaufaną listą za pośrednictwem centralnego punktu kontaktowego.

285) Oświadczenie dotyczące praktyk w zakresie certyfikacji głównego urzędu certyfikacji lub zarządzającego zaufaną listą lub inne istotne dokumenty w przypadku centralnego punktu kontaktowego obejmują incydent, naruszenie i ciągłość działania, które mogą również opierać się na innych zasobach przedsiębiorstwa i planach wdrożenia.

286) Główny urząd certyfikacji i urząd certyfikacji ostrzegają każdego przedstawiciela państwa członkowskiego i główny urząd certyfikacji, z którymi zawarły porozumienie w ramach C-ITS, oraz podają dokładne informacje na temat konsekwencji incydentu, aby umożliwić im uruchomienie własnego planu zarządzania incydentami.

5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania lub danych

287) W przypadku wykrycia sytuacji nadzwyczajnej, która uniemożliwia właściwe działanie elementu modelu zaufania C-ITS, element ten zawiesza swoją działalność i bada, czy doszło do naruszenia klucza prywatnego (z wyjątkiem centralnego punktu kontaktowego). Należy jak najszybciej wymienić uszkodzony sprzęt komputerowy oraz stosować procedury opisane w sekcjach 5.7.3 i 5.7.4.

288) Główny urząd certyfikacji informuje się o uszkodzeniu zasobów obliczeniowych, oprogramowania lub danych w ciągu 24 godzin w przypadku najwyższych poziomów zagrożenia. Wszystkie pozostałe zdarzenia muszą zostać zawarte w sprawozdaniu okresowym głównego urzędu certyfikacji, organów ds. rejestracji i organów autoryzujących.

5.7.3. Procedury w przypadku ujawnienia klucza prywatnego jednostki

289) Jeżeli klucz prywatny głównego urzędu certyfikacji zostaje naruszony, utracony, zniszczony lub podejrzewa się, że został naruszony, główny urząd certyfikacji:

- zawiesza swoje działanie;
- rozpoczyna realizację planu przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej oraz planu migracji;
- unieważnia certyfikat głównego urzędu certyfikacji;
- bada „kluczową kwestię", która doprowadziła do naruszenia i powiadamia organ ds. polityki certyfikacji C-ITS, który unieważni certyfikat głównego urzędu certyfikacji za pośrednictwem zarządzającego zaufaną listą (zob. sekcja 7);
- ostrzega wszystkich abonentów, z którymi zawarł umowę.

290) Jeżeli klucz organu ds. rejestracji / organu autoryzującego zostaje naruszony, utracony, zniszczony lub podejrzewa się, że został naruszony organ ds. rejestracji / organ autoryzujący:

- zawiesza swoje działanie;
- unieważnia swój własny certyfikat;
- bada „kluczową kwestię" i powiadamia główny urząd certyfikacji;
- ostrzega abonentów, z którymi zawarł umowę.

291) Jeżeli dane uwierzytelniające rejestrację lub bilet autoryzacyjny stacji C-ITS zostały naruszone, utracone, zniszczone lub podejrzewa się, że zostały naruszone, organ ds. rejestracji / organ autoryzujący, do którego przypisana jest stacja C-ITS:

- unieważnia dane uwierzytelniające rejestrację danego ITS;
- bada „kluczową kwestię" i powiadamia główny urząd certyfikacji;
- ostrzega abonentów, z którymi zawarł umowę.

292) W przypadku gdy którykolwiek z algorytmów lub powiązane z nimi parametry stosowane przez główny urząd certyfikacji, urząd certyfikacji lub stacje C-ITS są niewystarczające, jeżeli chodzi o pozostałe zamierzone wykorzystanie,

organ ds. polityki certyfikacji C-ITS (z zaleceniem ekspertów kryptograficznych) informuje o tym jednostkę głównego urzędu certyfikacji, z którym zawarł umowę i wprowadza zmiany w stosowanych algorytmach. (Szczegółowe informacje można znaleźć w sekcji 6 oraz oświadczeniach dotyczących praktyk w zakresie certyfikacji głównego urzędu certyfikacji i podporządkowanego urzędu certyfikacji).

5.7.4. Zapewnienie ciągłości działania po wystąpieniu katastrofy

293) Elementy modelu zaufania C-ITS obsługujące bezpieczne obiekty dla operacji prowadzonych przez urząd certyfikacji opracowują, badają, utrzymują i wdrażają plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej mający na celu łagodzenie skutków każdej klęski żywiołowej lub katastrofy spowodowanej przez człowieka. Takie plany dotyczą przywracania usług systemów informatycznych oraz kluczowych funkcji biznesowych.

294) Po wystąpieniu zdarzenia o określonym poziomie ryzyka, zagrożony urząd certyfikacji musi zostać poddany audytowi przeprowadzanemu przez akredytowanego audytora infrastruktury klucza publicznego (zob. sekcja 8).

295) W przypadku, gdy zagrożony urząd certyfikacji nie jest w stanie dłużej pracować (np. w następstwie poważnego incydentu), należy sporządzić plan migracji w celu przeniesienia jego funkcji do innego głównego urzędu certyfikacji. Na potrzeby wsparcia planu migracji dostępny jest przynajmniej główny urząd certyfikacji UE. Zagrożony urząd certyfikacji przestaje pełnić swoje funkcje.

296) Główne urzędy certyfikacji uwzględniają plan przywrócenia gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej oraz plan migracji w oświadczeniu dotyczącym praktyk w zakresie certyfikacji.

5.8. Zakończenie i przekazanie działalności

5.8.1. Zarządzający zaufaną listą

297) Zarządzający zaufaną listą nie kończy swojej działalności, ale jednostka nim zarządzająca może przejąć inną jednostkę.

298) W przypadku zmiany jednostki zarządzającej:

- zwraca się ona do organu ds. polityki certyfikacji C-ITS z wnioskiem o zatwierdzenie zmiany kierownictwa zarządzającego zaufaną listą ze starego podmiotu na nowy podmiot;
- organ ds. polityki certyfikacji C-ITS zatwierdza zmianę kierownictwa zarządzającego zaufaną listą;
- wszystkie dzienniki kontroli i zarchiwizowane zapisy są przekazywane nowej jednostce przez starą jednostkę zarządzającą.

5.8.2. Główny urząd certyfikacji

299) Główny urząd certyfikacji nie kończy/rozpoczyna swojej działalności bez ustanowienia planu migracji (określonego w odpowiednim oświadczeniu dotyczącym praktyk w zakresie certyfikacji), który gwarantuje ciągłą działalność dla wszystkich abonentów.

300) W przypadku zakończenia świadczenia usługi przez główny urząd certyfikacji, urząd:

- powiadamia organ ds. polityki certyfikacji C-ITS;
- powiadamia zarządzającego zaufaną listą o tym, że może usunąć certyfikat głównego urzędu certyfikacji z europejskiej zaufanej listy certyfikatów;
- odwołuje odpowiedni główny urząd certyfikacji poprzez wydanie listy unieważnionych certyfikatów, która zawiera jego certyfikat;
- ostrzega główne urzędy certyfikacji, z którymi zawarł umowę o przedłużenie certyfikatów organu ds. rejestracji / organu autoryzującego;
- niszczy klucz prywatny głównego urzędu certyfikacji;
- przekazuje stronie ufającej informacje o ostatnim statusie unieważnienia (lista unieważnionych certyfikatów podpisana przez główny urząd certyfikacji), wskazując wyraźnie, że są to najnowsze informacje dotyczące unieważnienia;
- archiwizuje wszystkie dzienniki kontroli i inne zapisy przed rozwiązaniem infrastruktury klucza publicznego;
- przekazuje zarchiwizowane zapisy właściwemu organowi.

1) Zarządzający zaufaną listą usuwa odpowiednie certyfikaty głównego urzędu certyfikacji z europejskiej zaufanej listy certyfikatów.

5.8.3. Organ ds. rejestracji / organ autoryzujący

302) W przypadku zakończenia świadczenia usługi przez organ ds. rejestracji / organ autoryzujący jednostkę organu ds. rejestracji / organu autoryzującego przekazuje powiadomienie przed rozwiązaniem umowy. Organ ds. rejestracji lub organ autoryzujący nie kończy/rozpoczyna swojej działalności bez ustanowienia planu migracji (określonego w odpowiednim oświadczeniu dotyczącym praktyk w zakresie certyfikacji), który gwarantuje ciągłą działalność dla wszystkich abonentów. Organ ds. rejestracji / organ autoryzujący wykonuje następujące czynności:

- powiadamia główny urząd certyfikacji listem poleconym;
- niszczy klucz prywatny urzędu certyfikacji;
- przekazuje swoją bazę danych jednostce wyznaczonej przez główny urząd certyfikacji;
- zaprzestaje wydawania certyfikatów;
- w trakcie przekazywania swojej bazy danych i do czasu, gdy baza danych będzie w pełni operacyjna u nowej jednostki, zachowuje możliwość zatwierdzania wniosków składanych przez właściwy organ ds. ochrony prywatności;
- w przypadku, gdy doszło do naruszenia podporządkowanego urzędu certyfikacji, główny urząd certyfikacji unieważnia podporządkowany urząd certyfikacji i publikuje nową listę unieważnionych certyfikatów

wraz z listą unieważnionych certyfikatów podporządkowanych urzędów certyfikacji;

- archiwizuje wszystkie dzienniki kontroli i inne zapisy przed rozwiązaniem infrastruktury klucza publicznego;
- przekazuje zarchiwizowane zapisy jednostce wskazanej przez główny urząd certyfikacji.

303) W przypadku zakończenia świadczenia usług przez urząd certyfikacji urząd odpowiada za prowadzenie wszystkich stosownych zapisów dotyczących potrzeb elementów urzędu certyfikacji i infrastruktury klucza publicznego.

6. KONTROLA BEZPIECZEŃSTWA TECHNICZNEGO

6.1. Generowanie pary kluczy i jej instalacja

6.1.1. Zarządzający zaufaną listą, główny urząd certyfikacji, organ ds. rejestracji, organ autoryzujący

304) Proces generowania pary kluczy musi spełniać następujące wymagania:

- każdy uczestnik jest w stanie wygenerować własną parę kluczy zgodnie z sekcjami 6.1.4 i 6.1.5;
- proces uzyskiwania kluczy szyfrowania symetrycznego oraz klucza MAC dla wniosków o wydanie certyfikatu (ECIES) przeprowadza się zgodnie z [1] i [5];
- w procesie generowania kluczy używa się algorytmów i długości kluczy opisanych w sekcjach 6.1.4.1 i 6.1.4.2;
- proces generowania pary kluczy podlega wymogom „bezpiecznego przechowywania kluczy prywatnych” (zob. sekcja 6.1.5);
- główne urzędy certyfikacji i ich abonenci (podporządkowane urzędy certyfikacji) zapewniają zachowanie integralności i autentyczności ich kluczy publicznych oraz wszelkich związanych z nimi parametrów w trakcie dystrybucji do zarejestrowanych jednostek podporządkowanych urzędów certyfikacji.

6.1.2. Jednostka końcowa – ruchoma stacja C-ITS

305) Każda ruchoma stacja C-ITS generuje własne pary kluczy zgodnie z sekcjami 6.1.4 i 6.1.5.

306) proces uzyskiwania kluczy szyfrowania symetrycznego oraz klucza MAC dla wniosków o wydanie certyfikatu (ECIES) przeprowadza się zgodnie z [1] i [5];

307) w procesie generowania kluczy używa się algorytmów i długości kluczy opisanych w sekcjach 6.1.4.1 i 6.1.4.2;

308) procesy generowania pary kluczy podlegają wymogom „bezpiecznego przechowywania kluczy prywatnych” (zob. sekcja 6.1.5);

6.1.3. Jednostka końcowa – stała stacja C-ITS

309) Każda stała stacja C-ITS generuje własne pary kluczy zgodnie z sekcjami 6.1.4 i 6.1.5.

310) w procesach generowania kluczy używa się algorytmów i długości kluczy opisanych w sekcjach 6.1.4.1 i 6.1.4.2;

311) procesy generowania pary kluczy podlegają wymogom „bezpiecznego przechowywania kluczy prywatnych” (zob. sekcja 6.1.5);

6.1.4. Wymogi kryptograficzne

312) Wszyscy uczestnicy infrastruktury klucza publicznego spełniają wymogi kryptograficzne określone w poniższych punktach w odniesieniu do algorytmu podpisu, długości klucza, generatora liczb losowych i certyfikatów łączących.

6.1.4.1. *Długość algorytmu i klucza – algorytmy podpisu*

313) Wszyscy uczestnicy infrastruktury klucza publicznego (zarządzający zaufaną listą, główny urząd certyfikacji, organ ds. rejestracji, organ autoryzujący i stacje C-ITS) mogą generować pary kluczy i korzystać z klucza prywatnego w celu podpisywania operacji przy pomocy wybranych algorytmów najpóźniej dwa lata po wejściu w życie niniejszego rozporządzenia zgodnie z tabelą 4.

314) Wszyscy uczestnicy infrastruktury klucza publicznego, którzy muszą sprawdzić poprawność europejskiej zaufanej listy certyfikatów, certyfikatów lub podpisanych komunikatów zgodnie z ich rolą określoną w sekcji 1.3.6, obsługują odpowiednie algorytmy wymienione w tabeli 5 na potrzeby weryfikacji. W szczególności stacje C-ITS muszą mieć możliwość sprawdzenia poprawności europejskiej zaufanej listy certyfikatów.

	Zarządzający zaufaną listą	główny CA	EA	AA	Stacja C-ITS
ECDSA_nistP256_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	-	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	-	-
X oznacza obowiązkową obsługę					

Tabela 4: Generowanie par kluczy i wykorzystanie klucza prywatnego do operacji związanych z podpisaniem

	Zarządzający zaufaną listą	główny CA	EA	AA	Stacja C-ITS
ECDSA_nistP256_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP256r1_with_SHA 256	X	X	X	X	X
ECDSA_brainpoolP384r1_with_SHA 384	X	X	X	X	X
X oznacza obowiązkową obsługę					

Tabela 5: Przegląd weryfikacji

315) Jeżeli organ ds. polityki certyfikacji C-ITS podejmie taką decyzję na podstawie nowo stwierdzonych niedociągnięć kryptograficznych, wszystkie stacje C-ITS będą mogły jak najszybciej przejść na jeden z dwóch algorytmów (ECDSA_nistP256_with_SHA 256 lub ECDSA_brainpoolP256_with_SHA 256). Faktycznie stosowane algorytmy określa się w oświadczeniu dotyczącym praktyk w zakresie certyfikacji sporządzonym przez urząd certyfikacji, które wydaje certyfikat dla odpowiedniego klucza publicznego zgodnie z niniejszą polityką certyfikacji.

6.1.4.2. *Długość algorytmu i klucza – algorytmy szyfrujące do celów rejestracji i autoryzacji*

316) Wszyscy uczestnicy infrastruktury klucza publicznego (organ ds. rejestracji, organ autoryzujący i stacje C-ITS) są w stanie korzystać z kluczy publicznych do szyfrowania wniosków/odpowiedzi dotyczących zapisu i uwierzytelniania przy pomocy wybranych algorytmów najpóźniej dwa lata po wejściu w życie niniejszego rozporządzenia zgodnie z tabelą 6. Faktycznie stosowane algorytmy określa się w oświadczeniu dotyczącym praktyk w zakresie certyfikacji sporządzonym przez urząd certyfikacji, które wydaje certyfikat dla odpowiedniego klucza publicznego zgodnie z niniejszą polityką certyfikacji.

317) Algorytmy wymienione w tabeli 6 wskazują długość klucza i długość algorytmu haszującego i są wdrażane zgodnie z [5].

	Zarządzający zaufaną listą	główny CA	EA	AA	Stacja C-ITS
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES128_CCM	-	-	X	X	X
X oznacza obowiązkową obsługę					

Tabela 6: Korzystanie z kluczy publicznych do szyfrowania wniosków/odpowiedzi dotyczących zapisu i autoryzacji

318) Wszyscy uczestnicy infrastruktury klucza publicznego (organ ds. rejestracji, organ autoryzujący i stacje C-ITS) mogą generować pary kluczy i korzystać z klucza prywatnego do odszyfrowywania wniosków/odpowiedzi dotyczących zapisu i uwierzytelniania przy pomocy wybranych algorytmów najpóźniej dwa lata po wejściu w życie niniejszego rozporządzenia zgodnie z tabelą 7.

	Zarządzający zaufaną listą	główny CA	EA	AA	Stacja C-ITS
ECIES_nistP256_with_AES 128_CCM	-	-	X	X	X
ECIES_brainpoolP256r1_with_AES128_CCM	-	-	X	X	X
X oznacza obowiązkową obsługę					

Tabela 7: Generowanie par kluczy i korzystanie z klucza prywatnego do odszyfrowywania wniosków/odpowiedzi dotyczących rejestracji i autoryzacji

6.1.4.3. *Zręczność kryptograficzna*

319) Wymogi dotyczące długości kluczy i algorytmów muszą być z czasem zmieniane w celu utrzymania odpowiedniego poziomu bezpieczeństwa. Organ ds. polityki certyfikacji C-ITS monitoruje potrzebę wprowadzenia takich zmian w świetle rzeczywistych słabych punktów podatnych na zagrożenia i najnowocześniejszej kryptografii. Opracowuje, zatwierdza i publikuje zaktualizowaną politykę certyfikacji, jeżeli zdecyduje, że należy zaktualizować algorytmy kryptograficzne. Jeżeli w zaktualizowanej wersji polityki certyfikacji zasygnalizowano zmianę algorytmu lub długości klucza, organ ds. polityki certyfikacji C-ITS przyjmie strategię migracyjną obejmującą okresy przejściowe, w których konieczne jest obsługiwanie starych algorytmów i długości klucza.

320) Aby umożliwić i ułatwić przekazywanie nowych algorytmów lub długości kluczy, zaleca się, aby wszyscy uczestnicy infrastruktury klucza publicznego wdrożyli sprzęt lub oprogramowanie będące w stanie zmienić długości kluczy i algorytmy.

321) Zmiany certyfikatów głównych i certyfikatów zarządzającego zaufaną listą są obsługiwane i wykorzystywane przy pomocy certyfikatów łączących (zob. sekcja 4.6), które stosuje się do objęcia okresu przejściowego między starymi i nowymi certyfikatami głównymi („migracja modelu zaufania”).

6.1.5. Bezpieczne przechowywanie kluczy prywatnych

W niniejszej sekcji opisano wymogi dotyczące bezpiecznego przechowywania i generowania par kluczy oraz liczb losowych dla właściwych urzędów certyfikacji i jednostek końcowych. Wymogi te są określone dla modułów kryptograficznych i są opisane w poniższych podsekcjach.

6.1.5.1. *Poziom głównego urzędu certyfikacji, podporządkowanego urzędu certyfikacji i zarządzającego zaufaną listą*

322) Moduł kryptograficzny wykorzystuje się do następujących czynności:

- generowania, stosowania i przechowywania kluczy prywatnych oraz zarządzania tymi kluczami;
- generowania i stosowania liczb losowych (ocena funkcji generowania liczb losowych stanowi część oceny bezpieczeństwa i certyfikacji);
- tworzenie kopii zapasowych kluczy prywatnych zgodnie z sekcją 6.1.6;
- niszczenie kluczy prywatnych.

Moduł kryptograficzny poświadcza się jednym z następujących profili zabezpieczeń (PP) o poziomie zaufania EAF-4 lub wyższym:

- profile zabezpieczeń w przypadku modułów zabezpieczeń sprzętu:
  - CEN EN 419 221-2: profile zabezpieczeń w przypadku modułów kryptograficznych dostawcy usług zaufania – część 2: moduł kryptograficzny dla operacji podpisywania CSP wraz z kopią zapasową;
  - CEN EN 419 221-4: profile zabezpieczeń w przypadku modułów kryptograficznych dostawcy usług zaufania – część 4: moduł kryptograficzny dla operacji podpisywania CSP bez kopii zapasowej;
  - CEN EN 419 221-5: profile zabezpieczeń w przypadku modułów kryptograficznych dostawcy usług zaufania – część 5: moduł kryptograficzny na potrzeby usług zaufania;
- profile zabezpieczeń w przypadku kart elektronicznych:
  - CEN EN 419 211-2: profile zabezpieczeń w przypadku bezpiecznego urządzenia do składania podpisu – część 2: urządzenie z generowaniem kluczy;
  - CEN EN 419 211-3: profile zabezpieczeń w przypadku bezpiecznego urządzenia do składania podpisu – część 3: urządzenie z importem kluczy.

Ręczny dostęp do modułu kryptograficznego wymaga uwierzytelnienia dwóch czynników przez administratora. Ponadto wymaga to udziału dwóch upoważnionych osób.

Wdrożenie modułu kryptograficznego gwarantuje, że klucze nie są dostępne poza modułem kryptograficznym. Moduł kryptograficzny obejmuje mechanizm kontroli dostępu zapobiegający nieupoważnionemu wykorzystaniu kluczy prywatnych.

6.1.5.2. *Jednostka końcowa*

323) Moduł kryptograficzny dla jednostek końcowych wykorzystuje się do następujących czynności:

- generowania, stosowania i przechowywania kluczy prywatnych oraz zarządzania tymi kluczami;
- generowania i stosowania liczb losowych (ocena funkcji generowania liczb losowych stanowi część oceny bezpieczeństwa i certyfikacji);
- bezpiecznego usunięcia klucza prywatnego.

324) Moduł kryptograficzny jest chroniony przed nieupoważnionym usunięciem, zastąpieniem i modyfikacją. Wszystkie profile zabezpieczenia i powiązane dokumenty mające zastosowanie do certyfikacji bezpieczeństwa modułu kryptograficznego podlegają ocenie, walidacji i certyfikacji zgodnie z ISO 15408, z zastosowaniem umowy o wzajemnym uznawaniu dotyczącej certyfikatów oceny bezpieczeństwa technologii informacyjnych zawartej przez grupę wyższych urzędników ds. bezpieczeństwa systemów informatycznych (SOG-IS) lub równoważnego europejskiego systemu certyfikacji w odpowiednich europejskich ramach cyberbezpieczeństwa.

325) Ze względu na znaczenie utrzymania możliwie najwyższego poziomu bezpieczeństwa certyfikaty bezpieczeństwa dla modułu kryptograficznego wydaje się w ramach systemu wspólnych kryteriów certyfikacji (ISO 15408) przez organ oceny zgodności uznany przez komitet zarządzający w ramach umowy SOG-IS lub przez organ oceny zgodności akredytowany przez krajowy organ certyfikacji cyberbezpieczeństwa państwa członkowskiego. Taki organ oceny zgodności zapewnia co najmniej warunki oceny bezpieczeństwa równoważne z warunkami przewidzianymi w umowie o wzajemnym uznawaniu SOG-IS.

Uwaga: należy zapewnić ochronę łącza między modułem kryptograficznym a stacją C-ITS.

6.1.6. Kopie zapasowe kluczy prywatnych

326) Generowanie, przechowywanie i wykorzystywanie kopii zapasowych kluczy prywatnych musi być zgodne z wymogami co najmniej poziomu bezpieczeństwa wymaganego w przypadku kluczy pierwotnych.

327) Kopie zapasowe kluczy prywatnych są wykonywane przez główne urzędy certyfikacji, organy ds. rejestracji i organy autoryzujące.

328) Kopie zapasowe kluczy prywatnych nie są wykonywane dla danych uwierzytelniających rejestrację i biletów autoryzacyjnych.

6.1.7. Niszczenie kluczy prywatnych

329) Główne urzędy certyfikacji, organy ds. rejestracji i organy autoryzujące oraz ruchome i stałe stacje C-ITS niszczą swój klucz prywatny i wszelkie powiązane kopie zapasowe, jeżeli utworzono i z powodzeniem zainstalowano nową parę kluczy i odpowiadający im certyfikat, a czas nakładania się (jeżeli dotyczy – tylko urząd certyfikacji) minął. Klucz prywatny zostaje zniszczony przy użyciu mechanizmu znajdującego się w module kryptograficznym używanym do przechowywania kluczy lub zostaje zniszczony zgodnie z opisem w odpowiednim profilu zabezpieczeń, o którym mowa w sekcji 6.1.5.2.

6.2. Dane aktywacyjne

330) Dane aktywacyjne odnoszą się do czynników potwierdzających autentyczność wymaganych do obsługi modułów kryptograficznych w celu uniemożliwienia nieuprawnionego dostępu. Użycie danych aktywacyjnych urządzenia kryptograficznego urzędu certyfikacji wymaga podjęcia działań przez dwie upoważnione osoby.

6.3. Zabezpieczenia komputerowe

331) Zabezpieczenia komputerowe urzędu certyfikacji są zaprojektowane zgodnie z wysokim poziomem zabezpieczenia przez spełnienie wymogów normy ISO/IEC 27002.

6.4. Techniczne kontrole cyklu życia

332) Kontrole techniczne urzędu certyfikacji obejmują cały cykl życia urzędu certyfikacji. W szczególności obejmuje to wymogi określone w sekcji 6.1.4.3 („zręczność kryptograficzna").

6.5. Zabezpieczenia sieci

333) Sieci urzędów certyfikacji (głównego urzędu certyfikacji, organu ds. rejestracji i organu autoryzującego) są zabezpieczone przed atakami zgodnie z wymogami i wytycznymi dotyczącymi wdrażania normy ISO/IEC 27001 i ISO/IEC 27002.

334) Dostępność sieci urzędu certyfikacji projektuje się w świetle szacowanego ruchu.

7. PROFILE CERTYFIKATÓW, CRL I CTL

7.1. Profil certyfikatu

335) Profile certyfikatów zdefiniowane w [5] stosuje się w odniesieniu do zarządzających zaufaną listą, certyfikatów głównych, certyfikatów organów ds. rejestracji, certyfikatów organów autoryzujących, biletów autoryzacyjnych i danych uwierzytelniających rejestrację. Rządowe organy ds. rejestracji na szczeblu krajowym mogą korzystać z innych profili certyfikatów w odniesieniu do danych uwierzytelniających rejestrację.

336) W certyfikatach głównego urzędu certyfikacji, organu ds. rejestracji i organu autoryzującego określono zezwolenia, w odniesieniu do których urzędy certyfikacji (główne urzędy certyfikacji, organ ds. rejestracji i organ autoryzujący) mogą wydawać certyfikaty.

337) Na podstawie [5]:

- każdy główny urząd certyfikacji stosuje własny prywatny klucz podpisu do wydawania listy unieważnionych certyfikatów;
- zarządzający zaufaną listą stosuje własny prywatny klucz podpisu do wydawania europejskiej zaufanej listy certyfikatów.

7.2. Ważność certyfikatu

338) Wszystkie profile certyfikatów C-ITS obejmują datę wydania i wygaśnięcia, która stanowi okres ważności certyfikatu. Na każdym poziomie infrastruktury klucza publicznego certyfikaty sporządza się w odpowiednim czasie przed ich wygaśnięciem.

339) Okres ważności certyfikatów urzędu certyfikacji i danych uwierzytelniających rejestrację obejmuje okres nakładania się. Certyfikaty zarządzającego zaufaną listą i głównego urzędu certyfikacji wydaje się i umieszcza na europejskiej zaufanej liście certyfikatów na maksymalnie trzy miesiące i co najmniej jeden miesiąc przed rozpoczęciem ich ważności w oparciu o czas rozpoczęcia ważności określony w certyfikacie. Ta faza wystawiania wstępnych

certyfikatów jest wymagana do bezpiecznego rozsyłania certyfikatów do wszystkich powiązanych stron ufających zgodnie z sekcją 2.2. Dzięki temu od początku okresu nakładania się wszystkie strony ufające są już w stanie zweryfikować komunikaty wydawane na podstawie nowego certyfikatu.

340) Na początku okresu nakładania się, odpowiednie strony ufające wystawiają, rozsyłają i instalują kolejne certyfikaty urzędu certyfikacji, danych uwierzytelniających rejestrację i biletów autoryzacyjnych (w stosownych przypadkach). W okresie nakładania się aktualny certyfikat wykorzystuje się wyłącznie do weryfikacji.

341) W związku z tym, że okresy ważności wymienione w tabeli 8 nie mogą przekraczać okresu ważności nadrzędnego certyfikatu, obowiązują następujące ograniczenia:

- maximumvalidity(Root CA) = privatekeyusage(Root CA) + maximumvalidity(EA,AA);
- maximumvalidity(EA) = privatekeyusage(EA) + maximumvalidity(EC);
- maximumvalidity(AA) = privatekeyusage(AA) + preloadingperiod(AT).

342) Okres ważności certyfikatów łączących (głównego urzędu certyfikacji i zarządzającego zaufaną listą) rozpoczyna się w momencie zastosowania odpowiedniego klucza prywatnego i kończy w maksymalnym okresie ważności ustanowionym przez główny urząd certyfikacji lub zarządzającego zaufaną listą.

343) W tabeli 8 przedstawiono maksymalny okres ważności certyfikatów urzędu certyfikacji C-ITS (informacje na temat okresów ważności biletów autoryzacyjnych można znaleźć w sekcji 7.2.1).

Jednostka	**Maksymalny okres stosowania klucza prywatnego**	**Maksymalny okres ważności**
Główny CA	3 lata	8 lat
EA	2 lata	5 lat
AA	4 lata	5 lat
EC	3 lata	3 lata
Zarządzający zaufaną listą	3 lata	4 lata

Tabela 8: Okresy ważności certyfikatów w modelu zaufania C-ITS

7.2.1. Certyfikaty z zastosowaniem pseudonimu

344) W tym kontekście pseudonimy wykorzystywane są przez bilety autoryzacyjne. W związku z tym sekcja ta dotyczy raczej biletów autoryzacyjnych niż pseudonimów.

345) Wymogi określone w niniejszej sekcji mają zastosowanie wyłącznie do biletów autoryzacyjnych ruchomych stacji C-ITS wysyłających komunikaty CAM i DENM, w przypadku których występuje ryzyko związane z prywatnością lokalizacji. Nie stosuje żadnych szczególnych wymogów dotyczących certyfikatów biletów autoryzacyjnych w odniesieniu do biletów

autoryzacyjnych stałych i ruchomych stacji C-ITS wykorzystywanych do specjalnych funkcji, w których prywatność lokalizacji nie ma zastosowania (np. w przypadku oznaczonych pojazdów uprzywilejowanych i pojazdów organów ścigania).

346) Stosuje się następujące definicje:

- „okres ważności biletów autoryzacyjnych” – okres ważności biletu autoryzacyjnego, tj. okres między datą uruchomienia a datą wygaśnięcia biletu autoryzacyjnego;
- „okres wystawiania wstępnych certyfikatów dla biletów autoryzacyjnych” – dzięki wstępnemu wystawiania certyfikatów stacje C-ITS mogą uzyskać bilety autoryzacyjne przed rozpoczęciem okresu ważności. Okres wystawiania wstępnych certyfikatów jest maksymalnym dopuszczalnym okresem od złożenia wniosku w sprawie biletów autoryzacyjnych do końca okresu ważności dowolnego biletu autoryzacyjnego będącego przedmiotem wniosku;
- „okres stosowania biletów autoryzacyjnych” – okres, w którym bilet autoryzacyjny jest skutecznie wykorzystywany do podpisywania komunikatów CAM/DENM;
- „maksymalna liczba równoległych biletów autoryzacyjnych” – liczba biletów autoryzacyjnych, z których może wybierać stacja C-ITS w dowolnym momencie podczas podpisywania komunikatu CAM/DENM, tj. liczba różnych biletów autoryzacyjnych wydanych jednej stacji C-ITS i ważnych w tym samym czasie.

347) Zastosowanie mają następujące wymogi:

- okres wystawiania wstępnych certyfikatów dla biletów autoryzacyjnych nie przekracza trzech miesięcy;
- okres ważności biletów autoryzacyjnych nie przekracza jednego tygodnia;
- maksymalna liczba równoległych biletów autoryzacyjnych nie przekracza 100 na stację C-ITS;
- okres stosowania biletów autoryzacyjnych zależy od strategii zmiany biletu autoryzacyjnego i czasu pracy pojazdu, ale jest ograniczony przez maksymalną liczbę równoległych biletów autoryzacyjnych i okres ważności. W szczególności, średni okres stosowania w przypadku jednej stacji C-ITS to co najmniej czas pracy pojazdu w jednym okresie ważności, podzielony przez maksymalną liczbę równoległych biletów autoryzacyjnych.

7.2.2. Bilety autoryzacyjne dla stałych stacji C-ITS

348) Zastosowanie mają definicje określone w sekcji 7.2.1 i następujące wymogi:

- okres wystawiania wstępnych certyfikatów dla biletów autoryzacyjnych nie przekracza trzech miesięcy;
- maksymalna liczba równoległych biletów autoryzacyjnych nie przekracza dwóch na stację C-ITS.

7.3. Unieważnianie certyfikatów

7.3.1. Unieważnianie certyfikatów urzędu certyfikacji, organu ds. rejestracji i organu autoryzującego

Certyfikaty głównego urzędu certyfikacji, organu ds. rejestracji i organu autoryzującego mogą zostać unieważnione. Unieważnione certyfikaty głównych urzędów certyfikacji, organów ds. rejestracji i organów autoryzujących publikuje się na liście unieważnionych certyfikatów możliwie jak najszybciej i bez zbędnej zwłoki. Ta lista unieważnionych certyfikatów jest podpisywana przez odpowiadający jej główny urząd certyfikacji i korzysta z profilu opisanego w sekcji 7.4. W przypadku unieważniania certyfikatów głównego urzędu certyfikacji, odpowiedni główny urząd certyfikacji publikuje listę unieważnionych certyfikatów zawierającą jego własny certyfikat. Ponadto w przypadkach naruszenia bezpieczeństwa zastosowanie ma sekcja 5.7.3. Ponadto zarządzający zaufaną listą usuwa unieważnione główne urzędy certyfikacji z zaufanej listy i publikuje nową zaufaną listę. Wygasłe certyfikaty usuwa się z odpowiedniej listy unieważnionych certyfikatów i zaufanej listy.

349) Certyfikaty unieważnia się, w przypadku gdy:

- główne urzędy certyfikacji mają powody, by przypuszczać lub poważnie podejrzewać, że doszło do naruszenia odpowiedniego klucza prywatnego;
- główne urzędy certyfikacji powiadomiono o zakończeniu umowy z abonentem;
- informacje (takie jak nazwisko i związek między urzędem certyfikacji a podmiotem) w certyfikacie są nieprawidłowe lub uległy zmianie;
- ma miejsce incydent związany z bezpieczeństwem, który ma wpływ na właściciela certyfikatu;
- audyt (zob. sekcja 8) prowadzi do negatywnego wyniku.

350) Abonent niezwłocznie powiadamia urząd certyfikacji o znanym lub podejrzewanym naruszeniu jego klucza prywatnego. Należy zapewnić, że tylko uwierzytelnione wnioski skutkują unieważnionymi certyfikatami.

7.3.2. Unieważnianie danych uwierzytelniających rejestrację

351) Proces unieważniania danych uwierzytelniających rejestrację może zostać wszczęty przez abonenta stacji C-ITS (przepływ 34) i jest wdrażany za pomocą wewnętrznej czarnej listy w bazie danych o unieważnianiu, ze znacznikiem czasu wygenerowanym i utrzymywanym przez każdy organ ds. rejestracji. Czarna lista nie jest nigdy publikowana i musi być traktowana jako poufna i stosowana wyłącznie przez odpowiedni organ ds. rejestracji w celu weryfikacji ważności odpowiednich danych uwierzytelniających rejestrację w kontekście wniosków o wydanie biletów autoryzacyjnych i nowych danych uwierzytelniających dotyczących rejestracji.

7.3.3. Unieważnianie biletów autoryzacyjnych

352) Z uwagi na fakt, że bilety autoryzacyjne nie są unieważniane przez odpowiednie główne urzędy certyfikacji, mają one krótki okres użytkowania i nie można ich wydawać zbyt długo przed tym, jak staną się ważne.

Dopuszczalne wartości parametrów cyklu życia certyfikatu określono w sekcji 7.2.

7.4. Lista unieważnionych certyfikatów

353) Format i treść listy unieważnionych certyfikatów wydawanej przez główne urzędy certyfikacji są takie, jak określono w [1].

7.5. Europejska zaufana lista certyfikatów

354Format i treść europejskiej zaufanej listy certyfikatów wydawanej przez zarządzającego zaufaną listą są takie, jak określono w [1].

8. AUDYT ZGODNOŚCI I INNE OCENY

8.1. Tematy objęte audytem i podstawa audytu

355) Celem audytu zgodności jest sprawdzenie, czy zarządzający zaufaną listą, główne urzędy certyfikacji, organy ds. rejestracji i organy autoryzujące działają zgodnie z polityką certyfikacji. W celu przeprowadzenia audytu swoich oświadczeń dotyczących praktyk w zakresie certyfikacji zarządzający zaufaną listą, główne urzędy certyfikacji, organy ds. rejestracji i organy autoryzujące wybierają niezależnego i akredytowanego audytora infrastruktury klucza publicznego. Audyt jest powiązany z oceną zgodnie z normą ISO/IEC 27001 i ISO/IEC 27002.

356) Audyt zgodności jest zlecany przez główny urząd certyfikacji (przepływ 13) w odniesieniu do samego urzędu, a w przypadku podporządkowanego urzędu certyfikacji przez podległy mu organ ds. rejestracji / organ autoryzujący.

357) Audyt zgodności dla zarządzającego zaufaną listą jest zlecany przez organ ds. polityki certyfikacji C-ITS (przepływ 38).

358) Akredytowany audytor infrastruktury klucza publicznego przeprowadza, na wniosek, audyt zgodności na jednym z następujących poziomów:

1) zgodność oświadczeń dotyczących praktyk w zakresie certyfikacji zarządzającego zaufaną listą, głównego urzędu certyfikacji, organów ds. rejestracji lub organów autoryzujących z tą polityką certyfikacji;

2) zgodność zamierzonych praktyk zarządzającego zaufaną listą, głównego urzędu certyfikacji, organu ds. rejestracji lub organu autoryzującego z jego oświadczeniem dotyczącym praktyk w zakresie certyfikacji przed rozpoczęciem pracy;

3) zgodność praktyk i działalności operacyjnej zarządzającego zaufaną listą, głównego urzędu certyfikacji, organu ds. rejestracji lub organu autoryzującego z jego oświadczeniem dotyczącym praktyk w zakresie certyfikacji podczas pracy.

359) Audyt obejmuje wszystkie wymogi tej polityki certyfikacji, jakie muszą zostać spełnione przez zarządzającego zaufaną listą, główne urzędy certyfikacji, organy ds. rejestracji i organy autoryzujące, które mają zostać poddane audytowi. Obejmuje on również funkcjonowanie urzędu certyfikacji w infrastrukturze klucza publicznego C-ITS, w tym wszystkie procesy wymienione w jego oświadczeniu dotyczącym praktyk w zakresie certyfikacji, obiekty i odpowiedzialne osoby.

360) W stosownych przypadkach akredytowany audytor infrastruktury klucza publicznego przekazuje szczegółowe sprawozdanie z audytu głównemu urzędowi certyfikacji (przepływ 36), organowi ds. rejestracji, organowi autoryzującemu lub organowi ds. polityki certyfikacji C-ITS (przepływ 16 i 40).

8.2. Częstotliwość audytów

361) Główny urząd certyfikacji, zarządzający zaufaną listą, organ ds. rejestracji, organ autoryzujący zlecają przeprowadzenie własnego audytu zgodności niezależnemu i akredytowanemu audytorowi infrastruktury klucza publicznego w następujących przypadkach:

- przy pierwszym uruchomieniu (poziomy zgodności 1 i 2);
- przy każdej zmianie polityki certyfikacji. Organ ds. polityki certyfikacji C-ITS określa treść zmiany wprowadzonej do polityki certyfikacji oraz harmonogram uruchomienia i odpowiednio określa potrzeby w zakresie audytów (w tym niezbędny poziom zgodności);
- przy każdej zmianie jego oświadczenia dotyczącego praktyk w zakresie certyfikacji (poziomy zgodności 1, 2 i 3). Ponieważ jednostki zarządzające głównych urzędów certyfikacji, zarządzających zaufaną listą, organów ds. rejestracji / organów autoryzujących decydują o tym, jakie zmiany we wdrażaniu są zgodne z aktualizacją ich oświadczeń dotyczących praktyk w zakresie certyfikacji, przed wdrożeniem tych zmian dokonują one audytu zgodności. W przypadku niewielkich zmian w oświadczeniu dotyczącym praktyk w zakresie certyfikacji (np. zmian o charakterze redakcyjnym) jednostka zarządzająca może przesłać organowi ds. polityki certyfikacji C-ITS należycie uzasadniony wniosek o zgodę na przeprowadzenie audytów zgodności na poziomie 1, 2 lub 3;
- regularnie, co najmniej co trzy lata podczas jego działania (zgodność na poziomie 3).

8.3. Tożsamość/kwalifikacje audytora

362) Urząd certyfikacji, który ma zostać poddany audytowi wybiera niezależne i akredytowane przedsiębiorstwo/organizację („organ kontrolny”) lub akredytowanych audytorów infrastruktury klucza publicznego do przeprowadzenia audytu zgodnie z tą polityką certyfikacji. Organ kontrolny jest akredytowany i certyfikowany przez członka europejskiej instytucji akredytacyjnej[1].

8.4. Powiązania audytora z audytowaną jednostką

363) Akredytowany audytor infrastruktury klucza publicznego jest niezależny od jednostki objętej audytem.

8.5. Działania podjęte w wyniku uchybienia

364) W przypadku gdy audytor wykaże w swoim sprawozdaniu, że zarządzający zaufaną listą nie spełnia wymogów, organ ds. polityki certyfikacji C-ITS zleca

[1] Lista członków europejskiej instytucji akredytacyjnej znajduje się na stronie: http://www.european-accreditation.org/ea-members

zarządzającemu zaufaną listą podjęcie natychmiastowych działań zapobiegawczych/naprawczych.

365) W przypadku gdy główny urząd certyfikacji, który według sprawozdania z audytu nie spełnia wymogów, złoży nowy wniosek, organ ds. polityki certyfikacji C-ITS odrzuca ten wniosek i wysyła odpowiednią odmowę do głównego urzędu certyfikacji (przepływ 4). W takich przypadkach główny urząd certyfikacji zostaje zawieszony. Musi podjąć działania naprawcze, ponownie zlecić audyt i złożyć nowy wniosek o zatwierdzenie przez organ ds. polityki certyfikacji C-ITS. Główny urząd certyfikacji nie może wystawiać certyfikatów w trakcie zawieszenia.

366) W przypadku regularnego audytu głównego urzędu certyfikacji lub wprowadzenia zmiany do oświadczenia dotyczącego praktyk w zakresie certyfikacji głównego urzędu certyfikacji, a także w zależności od charakteru niezgodności opisanej w sprawozdaniu z audytu, organ ds. polityki certyfikacji C-ITS może podjąć decyzję o unieważnieniu głównego urzędu certyfikacji i przekazać tę decyzję zarządzającemu zaufaną listą (przepływ 2), powodując usunięcie certyfikatu głównego urzędu certyfikacji z europejskiej zaufanej listy certyfikatów oraz wprowadzenie głównego urzędu certyfikacji na listę unieważnionych certyfikatów. Organ ds. polityki certyfikacji C-ITS wysyła odpowiednią odmowę do głównego urzędu certyfikacji (przepływ 4). Główny urząd certyfikacji musi podjąć działania naprawcze, ponownie zlecić pełny audyt (poziom 1-3) i złożyć nowy wniosek o zatwierdzenie przez organ ds. polityki certyfikacji C-ITS. Alternatywnie organ ds. polityki certyfikacji C-ITS może podjąć decyzję o nieunieważnianiu głównego urzędu certyfikacji oraz o przedłużeniu mu okresu, w którym podejmie działania naprawcze, ponownie zleci audyt i ponownie przedstawi organowi ds. polityki certyfikacji C-ITS sprawozdanie z audytu. W takim przypadku główny urząd certyfikacji musi zawiesić działalność i nie może wydawać certyfikatów ani list unieważnionych certyfikatów.

367) W przypadku audytu organu ds. rejestracji / organu autoryzującego główny urząd certyfikacji podejmuje decyzję o przyjęciu lub odrzuceniu sprawozdania. W zależności od wyniku audytu główny urząd certyfikacji podejmuje decyzję o unieważnieniu certyfikatu organu ds. rejestracji / organu autoryzującego zgodnie z przepisami określonymi w oświadczeniu dotyczącym praktyk w zakresie certyfikacji głównego urzędu certyfikacji. Główny urząd certyfikacji przez cały czas zapewnia, aby organ ds. rejestracji / organ autoryzujący przestrzegał tej polityki certyfikacji.

8.6. Ogłoszenie wyników

368) Główny urząd certyfikacji i zarządzający zaufaną listą przesyła organowi ds. polityki certyfikacji C-ITS sprawozdanie z audytu (przepływ 16). Główny urząd certyfikacji i zarządzający zaufaną listą przechowują wszystkie zlecone przez siebie sprawozdania z audytu. Organ ds. polityki certyfikacji C-ITS wysyła do głównego urzędu certyfikacji i zarządzającego zaufaną listą odpowiednie wiadomość zatwierdzenie lub odmowę (przepływ 4).

369) Główny urząd certyfikacji wysyła certyfikat zgodności do odpowiedniego organu ds. rejestracji / organu autoryzującego.

9. POZOSTAŁE PRZEPISY

9.1. Opłaty

370) Jedna z zasad wdrażania unijnego modelu zaufania C-ITS jest taka, że główne urzędy certyfikacji wspólnie w całości pokrywają regularne stałe koszty działalności organu ds. polityki certyfikacji C-ITS i głównych podmiotów (zarządzającego zaufaną listą i centralnego punktu kontaktowego) związane z działaniami określonymi w tej polityce certyfikacji.

371) Główne urzędy certyfikacji (w tym główny urząd certyfikacji UE) są uprawnione do pobierania opłat od swoich podporządkowanych urzędów certyfikacji.

372) W całym okresie prowadzenia działalności każdy uczestnik modelu zaufania C-ITS ma dostęp do co najmniej jednego głównego urzędu certyfikacji, organu ds. rejestracji i organu autoryzacyjnego na zasadach niedyskryminacyjnych.

373) Każdy główny urząd certyfikacji ma prawo przenieść opłaty na rzecz organu ds. polityki certyfikacji C-ITS i centralnych podmiotów (zarządzającego zaufaną listą i centralnego punktu kontaktowego) na zarejestrowanych uczestników modelu zaufania C-ITS, w tym zarejestrowane i zatwierdzone stacje C-ITS.

9.2. Odpowiedzialność finansowa

374) Wstępne ustanowienie głównego urzędu certyfikacji obejmuje okres co najmniej trzech lat działalności, aby mógł zostać członkiem unijnego modelu zaufania C-ITS. Oświadczenie dotyczące praktyk w zakresie certyfikacji operatora głównego urzędu certyfikacji zawiera również szczegółowe przepisy dotyczące unieważnienia lub zamknięcia głównego urzędu certyfikacji.

375) Każdy główny urząd certyfikacji musi wykazać rentowność finansową podmiotu prawnego, który wdraża ją od co najmniej trzech lat. Ten plan rentowności finansowej stanowi część pierwotnego zestawu dokumentów do rejestracji oraz musi być aktualizowany co trzy lata i zgłaszany organowi ds. polityki certyfikacji C-ITS.

376) Każdy główny urząd certyfikacji musi co roku zgłosić strukturę opłat stosowanych w odniesieniu do organów ds. rejestracji / organów autoryzujących oraz zarejestrowanych i zatwierdzonych stacji C-ITS kierownikowi ds. operacyjnych i organowi ds. polityki certyfikacji C-ITS w celu wykazania swojej stabilności finansowej.

377) Wszystkie jednostki finansowe i prawne głównego urzędu certyfikacji, organu ds. rejestracji, organu autoryzującego oraz podmiotów centralnych (centralnego punktu kontaktowego i zarządzającego zaufaną listą) modelu zaufania C-ITS muszą objąć swoje obowiązki operacyjne odpowiednimi poziomami ubezpieczeń, aby zrekompensować błędy operacyjne i wyrównanie finansowe swoich obowiązków w przypadku awarii jednego z elementów technicznych.

9.3. Poufność informacji biznesowych

378) Poniższe dokumenty muszą pozostać poufne i prywatne:

- dokumentacja dotycząca wniosków głównego urzędu certyfikacji, organu ds. rejestracji i organu autoryzującego, niezależnie od tego, czy wniosek został zatwierdzony, czy odrzucony;
- sprawozdania z audytu głównego urzędu certyfikacji, organu ds. rejestracji, organu autoryzującego i zarządzającego zaufaną listą;
- plany przywracania gotowości do pracy po wystąpieniu sytuacji nadzwyczajnej, głównych urzędów certyfikacji, organów ds. rejestracji, organów autoryzujących, centralnych punktów kontaktowych i zarządzającego zaufaną listą;
- klucze prywatne elementów modelu zaufania C-ITS (stacji C-ITS, zarządzającego zaufaną listą, organu ds. rejestracji, organu autoryzującego, głównego urzędu certyfikacji);
- wszelkie inne informacje określone jako poufne przez organ ds. polityki certyfikacji C-ITS, główne urzędy certyfikacji, organ ds. rejestracji, organ autoryzujący, zarządzającego zaufaną listą i centralny punkt kontaktowy.

9.4. Plan ochrony prywatności

379) Główne urzędy certyfikacji oraz organy ds. rejestracji / organy autoryzujące określają w swoich oświadczeniach dotyczących praktyk w zakresie certyfikacji plan i wymogi dotyczące przetwarzania danych osobowych i prywatności na podstawie ogólnego rozporządzenia o ochronie danych i innych mających zastosowanie ram prawnych (np. krajowych).

10. ODNIESIENIA

W niniejszym załączniku zastosowano następujące odniesienia:

[1] ETSI TS 102 941 V1.2.1, Intelligent transport systems (ITS) – security, trust and privacy management [Inteligentne systemy transportowe (ITS) – zarządzanie bezpieczeństwem, zaufaniem i prywatnością]

[2] ETSI TS 102 940 V1.3.1, Intelligent transport systems (ITS) – security, ITS communications security architecture and security management [Inteligentne systemy transportowe (ITS) – bezpieczeństwo, systemy bezpieczeństwa łączności inteligentnych systemów transportowych oraz zarządzanie bezpieczeństwem]

[3] Certificate policy and certification practices framework [Polityka certyfikacji i ramy praktyk certyfikacji] (RFC 3647, 1999).

[4] ETSI TS 102 042 V2.4.1 Policy requirements for certification authorities issuing public key certificates [Wymogi dotyczące polityki wobec organów certyfikujących wydających certyfikaty klucza publicznego]

[5] ETSI TS 103 097 V1.3.1, Intelligent transport systems (ITS) – security, security header and certificate formats [Inteligentne systemy transportowe (ITS) – formaty bezpieczeństwa, nagłówka bezpieczeństwa i certyfikatów]

[6] Calder, A. (2006). Information security based on ISO 27001/ISO 1779: a management guide [Bezpieczeństwo informacji w oparciu o normę ISO 27001/ISO 1779: przewodnik zarządzania]. Van Haren Publishing.

[7] ISO, I., & Std, I. E. C. (2011). ISO 27005 (2011) – Information technology, security techniques, information security risk management [Technologia informacyjna, techniki bezpieczeństwa, zarządzanie ryzykiem w zakresie bezpieczeństwa informacji]. ISO.