MINISTERSTWO INFRASTRUKTURY

Polityka Organu Państwa Członkowskiego - Polska

Warszawa, 14 marca 2019 – ver. 01.02

Inteligentny Tachograf

Zatwierdzenie dokumentu

	Imię i nazwisko	Organizacja	Data	Podpis

Historia zmian

Wersja dokumentu	Data wydania	Opis
01.00	18/01/2019	Wersja początkowa
01.01	09/03/2019	Wersja zaktualizowana zgodnie z uwagami zgłoszonymi przez Pana Michel Chiaramello w dokumencie „Review of the Poland policy for the smart tachograph V1.0”, ref. Ares(2019)1520724 z dnia 6 marca 2019 r. Uwzględniono wszystkie uwagi zgłoszone w wyżej wymienionym dokumencie.
01.02	14/03/2019	Wersja zaktualizowana zgodnie z uwagami zgłoszonymi przez Pana Michel Chiaramello w dokumencie „Review of the Poland policy for the smart tachograph V1.01”, ref. Ares(2019)1688796 z dnia 14 marca 2019 r. Uwzględniono wszystkie uwagi zgłoszone w wyżej wymienionym dokumencie.

Spis treści

1. Wprowadzenie

Niniejszy dokument zawiera krajową politykę bezpieczeństwa dla systemu Inteligentnego Tachografu w Polsce, zwaną dalej w skrócie „Polityką PL-MSA". Polityka PL-MSA reguluje funkcjonowanie systemu Inteligentnego Tachografu w Polsce.

Celem systemu Inteligentnego Tachografu jest poprawa bezpieczeństwa transportu drogowego poprzez bardziej kompleksową kontrolę czasu pracy kierowców i zwiększenie możliwości kontroli. Można będzie to osiągnąć poprzez zastąpienie kart pierwszej generacji kartami drugiej generacji. Nowe karty są kompatybilne wstecz z poprzednią generacją kart. Dotyczy to kart używanych przez kierowców, warsztaty, firmy i organy kontrolne.

Dokument zawiera wymagania dotyczące w szczególności bezpiecznego zarządzania kluczami, certyfikatami oraz powiązanymi urządzeniami, które wchodzą w skład systemu Inteligentnego Tachografu.

1.1 Informacje

System Tachografów Cyfrowych drugiej generacji, zwany Inteligentnym Tachografem, został wprowadzony Rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 165/2014 [1].

Załącznik IC do Rozporządzenia Wykonawczego Komisji (UE) 2016/799 [2] określa wymagania techniczne dotyczące budowy, testowania, instalacji, obsługi i naprawy inteligentnych tachografów i ich komponentów.

Dodatek 11 (Wspólne mechanizmy zabezpieczenia) Załącznika 1C określa mechanizmy bezpieczeństwa zapewniające:

- Wzajemne uwierzytelnianie po między różnymi komponentami systemu tachografu.
- Poufność, integralność, autentyczność i/lub niezaprzeczalność danych przesyłanych po między różnymi komponentami systemu tachografu lub pobieranych na zewnętrzne nośniki pamięci.

Część B Dodatku 11 opisuje, w jaki sposób systemy kryptograficzne klucza publicznego oparte na krzywych eliptycznych i symetryczne systemy kryptograficzne oparte o AES są wykorzystywane do realizacji systemu tachografu drugiej generacji.

Infrastruktura klucza publicznego (PKI) została zaprojektowana do obsługi systemów kryptograficznych z kluczem publicznym, podczas gdy symetryczne systemy kryptograficzne opierają się na kluczach głównych, które muszą zostać dostarczone odpowiednim podmiotom. Utworzona została infrastruktura składająca się z trzech warstw. Na poziomie europejskim Główne Europejskie Centrum Certyfikacji (ERCA) jest odpowiedzialne za generowanie i zarządzanie głównymi parami kluczy publicznych i prywatnych z odpowiednimi certyfikatami oraz symetrycznymi kluczami głównymi. ERCA wydaje certyfikaty Urzędom Certyfikacji Państw Członkowskich (MSCA) i dystrybuuje symetryczne klucze główne do MSCA. Na poziomie krajowym MSCA są odpowiedzialne za wydawanie certyfikatów dla urządzeń w ramach systemu Inteligentnego Tachografu, a także za dystrybucję symetrycznych kluczy głównych i innych danych powstających przy użyciu kluczy głównych, które są zainstalowane w urządzeniach Inteligentnego Tachografu.

Oprócz kluczy produkcyjnych i certyfikatów ERCA wydaje również certyfikaty testowe i

dystrybuuje testowe symetryczne klucze główne do MSCA, które mogą być wykorzystywane do celów testowania interoperacyjności. Korzystając z tych kluczy testowych i certyfikatów, MSCA mogą podpisywać i rozpowszechniać certyfikaty, klucze symetryczne i zaszyfrowane dane dla czujników ruchu instalowanych w Inteligentnym Tachografie do celów testowania interoperacyjności.

Niniejszy dokument definiuje Politykę Certyfikacji (CP) dla PKI na poziomie MSCA w Polsce. Dokument ten określa zasady na poziomie MSCA dotyczące generowania kluczy, zarządzania kluczami i podpisywania certyfikatów dla systemu Inteligentnego Tachografu. Podmiot wskazany jako PL-MSCA musi spełniać wymagania określone w polityce certyfikacji ERCA (CP) [6].

Polityka PL-MSA dotyczy wyłącznie Systemu Inteligentnego Tachografu w Polsce.

Dokument polityki PL-MSA jest zgodny ze strukturą polityki certyfikacji CP opisaną w dokumencie RFC 3647 [4]. Do dokumentu polityki PL-MSA została dodana treść polityki dotyczącej infrastruktury kluczy symetrycznych zachowując układ wskazany w RFC 3647.

Sposób, w jaki podmiot PL-MSCA spełnia wymagania z niniejszej polityki jest opisany w dokumencie Deklaracji Praktyk PL-MSCA (CPS).

W tym dokumencie słowa kluczowe „wymagane”, „powinny”, „nie powinny”, „powinny”, „nie powinny”, „zalecane”, „mogą” i „opcjonalne” należy interpretować zgodnie z RFC 2119 [5].

1.2 Nazwa i identyfikacja dokumentu

Ten dokument nosi nazwę Polityka Certyfikacji Organu Państwa Członkowskiego - Polska. Ta polityka certyfikacji nie posiada identyfikatora obiektu ASN.1. Taki identyfikator nie jest potrzebny, ponieważ certyfikaty używane w systemie Inteligentnego Tachografu nie zawierają odniesienia do tej polityki.

Aktualna wersja dokumentu to 01.02.

Polityka PL-MSA została zatwierdzona przez:

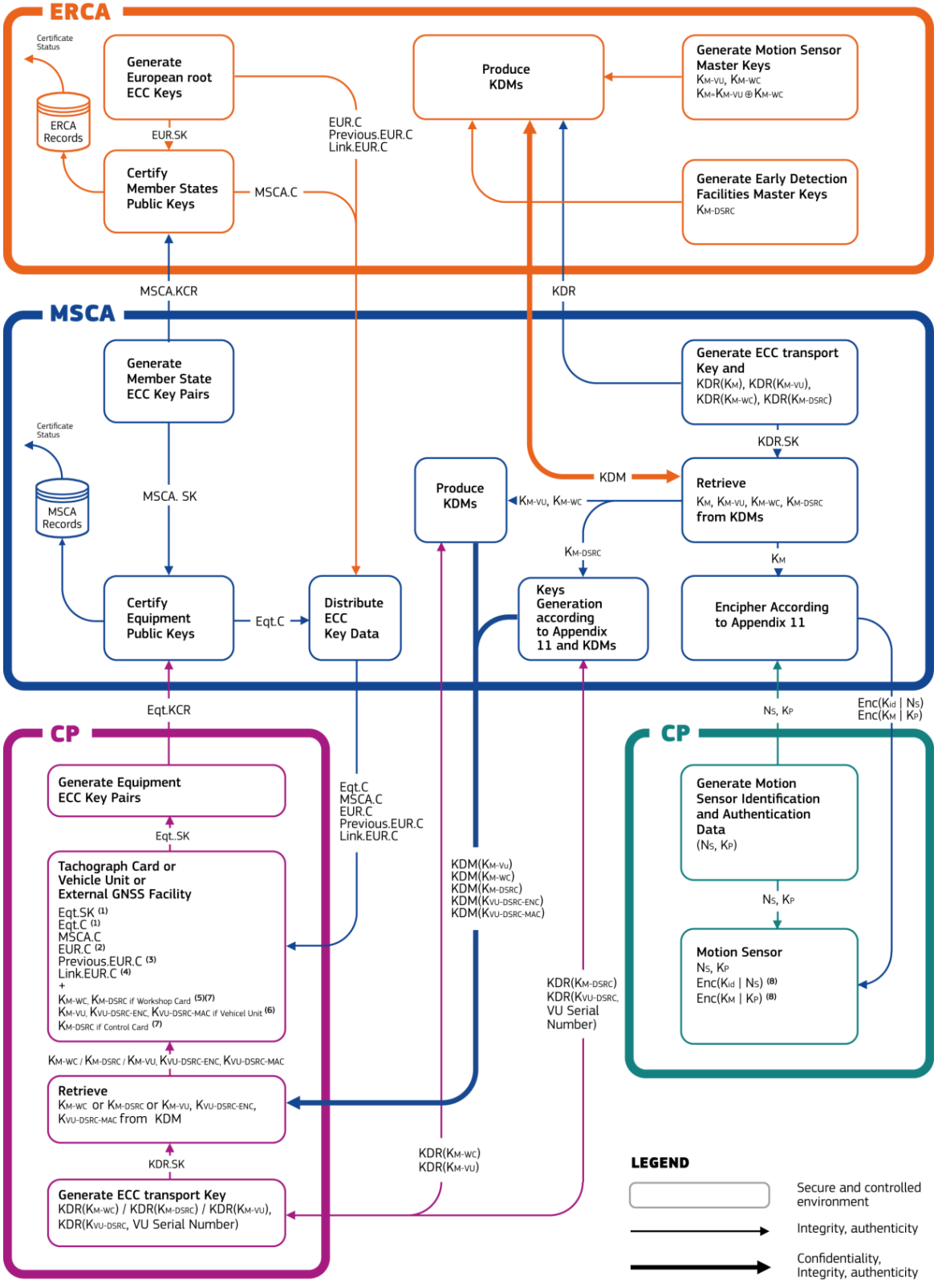
Head of the Cyber and Digital Citizens’ Security Unit E3
Directorate E - Space, Security and Migration
DG JRC - Joint Research Centre (TP 361)
European Commission
Via Enrico Fermi, 2749
I-21027 Ispra (VA)

pod nazwą *Member State Authority Policy - Poland ver. 01.02* pod numerem
D Ares(2019)1715946 - 15/03/2019.

Po zatwierdzeniu Polityka PL-MSA będzie publicznie dostępna pod adresem:
https://www.gov.pl/infrastruktura/polityka-organu-panstwa-czlonkowskiego-polska

1.3 Uczestnicy

Podmioty realizujące zadania w ramach infrastruktury klucza publicznego (PKI) oraz infrastruktury klucza symetrycznego w systemie Inteligentnego Tachografu zostały przedstawione i opisane na Rysunek 1.



NOTES

1. For VUs and Tachograph Cards there are two certificates and relative keys, one for the mutual authentication (MA) and one for signing (Sign).
2. The EUR certificate used to generate the MSCA.C certificate.
3. The EUR certificate whose validity directly precedes the validity period of the EUR certificate of note 2 if existing.
4. The Link certificate linking the EUR certificates of note 2 and 3, if existing.
5. All $K_{M\text{-}WC}$ keys associated to $K_{M\text{-}VU}$ keys currently in circulation have to be inserted.
6. The $K_{M\text{-}VU}$ key associated to the EUR certificate of note 2.
7. All $K_{M\text{-}DSRC}$ keys currently in circulation have to be inserted.
8. NS and KP have to be encrypted according to all K_M keys currently in circulation.

Rysunek 1 Podmioty realizujące zadania w ramach infrastruktury klucza publicznego (PKI) oraz infrastruktury klucza symetrycznego w systemie Inteligentnego Tachografu

Na Rysunek 1 przedstawiono również przepływy danych po między uczestnikami, w szczególności ERCA, MSCA i podmiotami realizującymi personalizację komponentów (CP). Więcej informacji na temat kluczy symetrycznych i asymetrycznych wymienionych w tej sekcji znajduje się w Dodatku 11, w części B.

1.3.1 Urzędy certyfikacji

Centrum Certyfikacji Państwa Członkowskiego w Polsce (PL-MSCA) działa jako urząd podrzędny (sub-CA) względem ERCA. PL-MSCA podpisuje certyfikaty klucza publicznego dla urządzeń. W tym celu realizuje usługę rejestracji, usługę generowania certyfikatów i usługę rozpowszechniania.

PL-MSCA odbiera wnioski o wydanie certyfikatów od podmiotów realizujących personalizację urządzeń i rozsyła wydane certyfikaty do nich. Istnieje jeden typ pary kluczy PL-MSCA i odpowiedni certyfikat PL-MSCA do wydawania certyfikatów dla kart zwany parą kluczy PL-MSCA_Card. PL-MSCA może zażądać od ERCA wymienionego typu certyfikatu PL-MSCA, zgodnie ze swoimi obowiązkami dotyczącymi wydawania urządzeń. Urząd PL-MSCA odpowiedzialny za wydawanie certyfikatów kart do tachografów jest określany w tym dokumencie jako PL-MSCA_Card.

Urząd PL-MSCA w zależności od swoich obowiązków jest również podmiotem, który może wnioskować o wydanie symetrycznych kluczy głównych do ERCA. PL-MSCA dystrybuuje $K_{M\text{-}WC}$ i K_{DSRC} do podmiotów personalizujących karty. PL-MSCA może również na żądanie producenta czujników ruchu użyć klucza głównego czujnika ruchu (K_M) do szyfrowania kluczy parowania czujnika ruchu (K_P) oraz wyprowadzić klucz identyfikacyjny czujnika ruchu (K_{ID}) z K_M, który następnie wykorzystuje do szyfrowania numerów seryjnych czujników ruchu.

1.3.2 Organy rejestracyjne

Organem rejestracyjnym dla PL-MSCA jest PL-CIA. PL-CIA wykonuje następujące funkcje:

- Rejestrowanie, zatwierdzanie i przetwarzanie wniosków związanych z wydawaniem, wznawianiem i wymianą zgubionych, skradzionych i uszkodzonych kart dla kierowców, przedsiębiorstw, warsztatów i organów kontrolnych;
- Wydawanie kart. PL-CIA zapewni, że wydawanie nowych, wznowionych oraz wymienianych kart jest przeprowadzane zgodnie z polityką PL-MSA i przy zachowaniu obowiązujących terminów;
- Wymienianie informacji z innymi Państwami Członkowskimi;
- Przechowywanie danych dotyczących zarejestrowanych kart oraz udostępnianie informacji o ich statusie.

1.3.3 Subskrybenci

Jedynymi subskrybentami usługi certyfikacji kluczy publicznych świadczonej przez PL-MSCA są podmioty personalizujące urządzenia. Podmioty te są odpowiedzialne za personalizację:

- Czujników ruchu (MoS);
- Karty do tachografów (TC). Istnieją cztery różne rodzaje kart do tachografów: karty kierowcy, karty firmowe, karty warsztatowe i karty kontrolne.

Wymienione wyżej urządzenia zawierają klucze kryptograficzne, a karty do tachografów zawierają również certyfikaty, jak niżej:

- Czujniki ruchu (MoS) zawierają klucz parowania K_p, zaszyfrowany klucz parowania i zaszyfrowany numer seryjny czujnika.

- Karty kierowcy i karty warsztatowe posiadają dwie pary kluczy oraz odpowiednie certyfikaty wydane przez PL-MSCA_Card, to jest:
  - parę kluczy i certyfikat do wzajemnego uwierzytelniania o nazwie Card_MA;
  - parę kluczy i certyfikat do podpisania, o nazwie Card_Sign.

  Karty warsztatowe zawierają również K_{M-WC} i K_{DSRC}.
- Karty firmowe i kontrolne posiadają parę kluczy i odpowiedni certyfikat wydany przez PL-MSCA_Card w celu wzajemnego uwierzytelnienia.

  Karty kontrolne zawierają również K_{DSRC}.

Podmioty personalizujące urządzenia są odpowiedzialne za zapewnienie, iż wydawane urządzenia są wyposażone w odpowiednie klucze i certyfikaty:

- Producent czujników ruchu (MoS)
  - generuje numer seryjny czujnika ruchu (MoS);
  - generuje klucz parowania K_P wymagany do sparowania czujnika ruchu (MoS) z tachografem (VU);
  - wysyła do PL-MSCA wnioski o zaszyfrowanie klucza parowania za pomocą klucza głównego czujnika ruchu K_M i zaszyfrowania numeru seryjnego czujnika ruchu (MoS) za pomocą klucza identyfikacyjnego K_{ID};
  - umieszcza numer seryjny i klucz parowania w czujniku ruchu (MoS) w formie zwykłej i zaszyfrowanej.
- Podmiot personalizujący karty (PL-CP) dla kart kierowcy i warsztatowych
  - generuje dwie pary kluczy na karcie do wzajemnego uwierzytelnienia i podpisywania;
  - realizuje proces składania wniosku o certyfikat poprzez urząd PL-MSCA_Card;
  - realizuje wniosek o klucze K_{M-WC} i K_{DSRC} (tylko dla kart warsztatowych);
  - umieszcza na karcie klucze i certyfikaty do wzajemnego uwierzytelniania i podpisywania, parowania MoS-VU i deszyfrowania komunikacji DSRC oraz weryfikacji autentyczności danych (tylko karty warsztatowych).
- Podmiot personalizujący karty (PL-CP) dla kart firmowych i kontrolnych
  - generuje parę kluczy na karcie dla wzajemnego uwierzytelnienia;
  - realizuje proces składania wniosku o certyfikat poprzez urząd PL-MSCA_Card;
  - realizuje wniosek o klucz K_{DSRC} (tylko dla kart kontrolnych);
  - umieszcza na karcie klucze i certyfikaty do wzajemnego uwierzytelniania i deszyfrowania komunikacji DSRC oraz weryfikacji autentyczności danych (tylko kraty kontrolne).

1.3.4 Strony ufające

Stronami polegającymi na usłudze certyfikacji kluczy publicznych PL-MSCA są przede wszystkim organy krajowe, których zadaniem jest egzekwowanie zasad i przepisów dotyczących czasu prowadzenia pojazdu oraz okresów odpoczynku. Wskazane instytucje wykorzystują certyfikaty PL-MSCA do walidacji autentyczności certyfikatów urządzeń, które z kolei służą do walidacji autentyczności danych pobranych z tachografów (VU) i kart kierowców.

Inne strony ufające to kierowcy, firmy i serwisy urządzeń.

1.4 Wykorzystanie kluczy i certyfikatów

Organ PL-MSA i podmioty realizujące zadania w ramach infrastruktury klucza publicznego PKI (zob. Rozdział 1.3) powinny uznawać certyfikaty klucza publicznego ERCA, pod warunkiem, że są one publikowane przez ERCA.

PL-MSCA powinno używać kluczy prywatnych państwa członkowskiego tylko do:

- Podpisywania certyfikatów dla urządzeń, zgodnie z Załącznikiem IC Dodatek 11 [2].
- Podpisywania żądań o podpisanie certyfikatu (patrz sekcja 4.1.1).

PL-MSCA powinno używać symetrycznych kluczy głównych wyłącznie do szyfrowania danych związanych z czujnikiem ruchu jak to określono w Dodatku 11 do Załącznika IC [2].

PL-MSCA powinno przekazywać symetryczne klucze główne, klucze wyprowadzone z tych kluczy głównych lub dane zaszyfrowane za pomocą tych kluczy głównych do podmiotów personalizujących urządzenia za pomocą odpowiednio zabezpieczonych środków, wyłącznie w celu, do którego przeznaczone są te klucze i dane jak określono w Dodatku 11 do Załącznika 1C 11 [2].

Certyfikaty PL-MSCA_Card powinny być wykorzystywane do weryfikacji certyfikatów wydanych przez PL-MSCA_Card.

Certyfikaty Card_MA powinny być wykorzystywane do wzajemnego uwierzytelniania i uzgadniania klucza sesji między kartą do tachografu, a tachografem (VU).

Certyfikaty Card_Sign powinny być wykorzystywane do weryfikacji autentyczności i integralności danych pobieranych z karty. Klucz prywatny Card_Sign może być używany wyłącznie do podpisywania danych pobranych z karty.

Klucz K_M powinien być wykorzystywany przez PL-MSCA do szyfrowania kluczy parowania czujników ruchu – K_P oraz do wyprowadzenia klucza identyfikacyjnego czujnika ruchu – K_{ID}. Klucz K_{ID} powinien być wykorzystywany przez PL-MSCA do szyfrowania numerów seryjnych czujników ruchu.

Klucz $K_{M\text{-}WC}$ powinien być dostarczany do podmiotów personalizujących urządzenia celem instalowania go w kartach warsztatowych.

Klucz K_{DSRC} powinien być używany przez karty kontrolne i warsztatowe do wyprowadzania specyficznych dla tachografu (VU) kluczy DSRC wymaganych do odszyfrowania, weryfikacji autentyczności oraz integralności komunikacji DSRC realizowanej przez VU.

Karty, klucze i certyfikaty wydane przez PL-MSCA lub PL-CP są przeznaczone wyłącznie do użytku w systemie Inteligentnego Tachografu.

1.5 Administrowanie polityką

1.5.1 Organ krajowy (PL-MSA)

Organem odpowiedzialnym za tę politykę w Polsce będzie Ministerstwo Infrastruktury, zwane dalej, zgodnie z terminologią międzynarodową, „PL-MSA” (PL-Member State Authority). Oficjalne dane kontaktowe są następujące:

Ministerstwo Infrastruktury
ul. Chałubińskiego 4/6,
00-928 Warszawa
Poland
Telefon: (+48-22) 630-10-00
https://www.gov.pl/infrastruktura

Po zatwierdzeniu Polityka PL-MSA będzie publicznie dostępna pod adresem

https://www.gov.pl/infrastruktura/polityka-organu-panstwa-czlonkowskiego-polska

Pytania dotyczące tej polityki PL-MSA należy kierować do:
Ministerstwo Infrastruktury
Departament Transportu Drogowego
ul. Chałubińskiego 4/6,
00-928 Warszawa
Polska
Telefon: (+48-22) 630-12-51
Faks: (+48-22) 630-12-02
e-mail: anna.kowalczyk@mi.gov.pl

Organ będący PL-MSA powinien:

- Ustanowić, udokumentować i zarządzać Polityką PL-MSA zgodnie ze wszystkimi obowiązującymi wymaganiami Polityki Certyfikacji ERCA [6];
- Wyznaczyć podmiot, która wdraża tę politykę na poziomie krajowym (PL-MSCA) i realizuje usługi certyfikacji kluczy oraz usługi dystrybucji kluczy do podmiotów personalizujących urządzenia;
- Upewnić się, że wyznaczony podmiot PL-MSCA posiada zasoby wymagane do działania zgodnie z tą polityką;
- Wyznaczyć podmiot wydający karty (PL-CIA);
- Wyznaczyć podmiot personalizujący karty (PL-CP);
- Ustalić, czy dokument Deklaracji Praktyk (CPS) PL-MSCA jest zgodny z tą polityką;
- Audytować wyznaczone podmioty: PL-MSCA, PL-CIA i PL-CP;
- W razie potrzeby audytować inne podmioty personalizujące urządzenia oraz innych dostawców zewnętrznych usług;
- Zatwierdzać Deklarację Praktyk (CPS) PL-MSCA, Deklarację Praktyk (PS) podmiotów personalizujących urządzenia i Deklarację Praktyk (PS) innych dostawców zewnętrznych usług, o ile to jest konieczne;
- Informować wyznaczone podmioty o Polityce PL-MSA;
- Przekazywać Politykę PL-MSA do zatwierdzenia przez ERCA;
- Monitorować bezpieczeństwo PL-MSCA. PL-MSA wdroży odpowiedni system monitorowania i kontroli, zapewniający poprawność procesu generowania certyfikatów przez PL-MSCA i bezpiecznego udostępniania kluczy kryptograficznych zgodnie z wymaganiami Polityki PL-MSA;
- Nadzorować jakość procesów w ramach Inteligentnego tachografu w Polsce;
- Obsługiwać skargi od podmiotów personalizujących urządzenia oraz dostawców zewnętrznych usług dotyczące usług świadczonych przez PL-MSCA.

1.5.2 Centrum Certyfikacji Państwa Członkowskiego (PL-MSCA)

Podmiotem wyznaczonym zgodnie z Ustawą z dnia 5 lipca 2018 r. o tachografach (Dz.U. 2018 poz. 1480) jako Centrum Certyfikacji w Polsce (zwanym „PL-MSCA”), jest:

Polska Wytwórnia Papierów Wartościowych S.A. (PWPW S.A.)
ul. Karczunkowska 30,
02-871 Warszawa
Polska

Telefon: (+48-22) 332-92-90
Faks: (+48-22) 332-92-98
e-mail: tachograf@pwpw.pl
http://info-car.pl/infocar/tachograf

Podmiot wyznaczony jako PL-MSCA powinien:

- Przestrzegać Polityki PL-MSA;
- Przygotować i opublikować PL-MSCA CPS zgodny z Polityką PL-MSA;
- Utrzymywać wystarczające zasoby organizacyjne i finansowe, aby funkcjonować zgodnie z wymaganiami określonymi w Polityce PL-MSA, zwłaszcza w odniesieniu do ponoszenia ryzyka odpowiedzialności odszkodowawczej;
- Sprawdzać i zapewniać, że jest w stanie spełniać wymagania Common Criteria określone w normie ISO / IEC 15408 [8] w odniesieniu do zakresu realizowanych zadań i świadczonych usług;
- Zapewnić wdrożenie wszystkich wymagań ciążących na PL-MSCA, które są wyszczególnione w Polityce PL-MSA.
- Przeprowadzić testy funkcjonalne, aby udowodnić zgodność z Polityką PL-MSA;
- Prowadzić dzienniki swoich działań, aby wykazać zgodność z niniejszą polityką i udostępnić te zapisy PL-MSA na żądanie.

Właścicielem dokumentu deklaracji praktyk - PL-MSCA CPS jest PL-MSCA. PL-MSCA CPS będzie traktowany jako informacja zastrzeżona. PL-MSCA udostępni zawartość dokumentu deklaracji praktyk dla PL-MSA, PL-CIA oraz podmiotom personalizującym urządzenia w zakresie niezbędnych informacji. PL-MSCA CPS będzie zarządzany, weryfikowany oraz modyfikowany zgodnie z procedurami obsługi i kontroli dokumentów.

PL-MSCA ponosi odpowiedzialność za zgodność z procedurami opisanymi w Polityce PL-MSA, nawet jeśli funkcje PL-MSCA są realizowane przez podwykonawców. PL-MSCA ponosi odpowiedzialność za zapewnienie, by wszyscy podwykonawcy świadczyli usługi zgodnie z PL-MSCA CPS i Polityką PL-MSA.

1.5.3 Podmiot wydający karty (PL-CIA)

Podmiotem wyznaczonym zgodnie z Ustawą z dnia 5 lipca 2018 r. o tachografach (Dz.U. 2018 poz. 1480) [8] jako Podmiot Wydający Karty w Polsce (zwanym „PL-CIA”), jest:

Polska Wytwórnia Papierów Wartościowych S.A. (PWPW S.A.)
ul. Karczunkowska 30,
02-871 Warszawa
Polska
Telefon: (+48-22) 332-92-90
Faks:(+48-22) 332-92-98
e-mail: tachograf@pwpw.pl
http://info-car.pl/infocar/tachograf

Podmiot wyznaczony jako PL-CIA powinien:

- Przestrzegać Polityki PL-MSA;
- Zapewnić, aby PL-CP otrzymywała poprawne i właściwe informacje o użytkownikach wynikające z procesu obsługi wniosków (o karty);

- Informować użytkowników o zawartych w Polityce PL-MSA wymaganiach dotyczących korzystania z Inteligentnego Tachografu (lub Tachografu Cyfrowego, jeśli to konieczne);
- Utrzymywać wystarczające zasoby organizacyjne i finansowe, aby funkcjonować zgodnie z wymaganiami określonymi w Polityce PL-MSA.

PL-CIA może zlecić wykonanie części swoich procesów podwykonawcom. Korzystanie z podwykonawców w żaden sposób nie zmniejsza ogólnej odpowiedzialności PL-CIA za te procesy.

1.5.4 Centrum personalizacji kart (PL-CP)

Centrum Personalizacji Kart w Polsce (zwanym jako „PL-CP") jest:

Polska Wytwórnia Papierów Wartościowych S.A. (PWPW S.A.)
ul. Karczunkowska 30,
02-871 Warszawa
Polska
Telefon: (+48-22) 332-92-90
Faks: (+48-22) 332-92-98
e-mail: tachograf@pwpw.pl
http://info-car.pl/infocar/tachograf

Podmiot wyznaczony jako PL-CP musi:

- Przestrzegać Polityki PL-MSA;
- Przygotować dokument Deklaracji Praktyk (PS), w którym opisany jest przynajmniej sposób wdrożenia Polityki PL-MSA, Polityki ERCA i mających zastosowanie właściwych przepisów prawnych;
- Utrzymywać wystarczające zasoby organizacyjne i finansowe, aby funkcjonować zgodnie z wymaganiami określonymi w Polityce PL-MSA, zwłaszcza w odniesieniu do ponoszenia ryzyka odpowiedzialności odszkodowawczej;
- Sprawdzać i zapewniać, że jest w stanie spełniać wymagania Common Criteria określone w normie ISO / IEC 15408 [8] dotyczących personalizacji kart do Inteligentnych Tachografów;
- Sprawdzać i zapewniać, że jest w stanie spełniać wymagania Common Criteria Protection Profile (Digital Tachograph - Tachograph Card) [10] dotyczące personalizacji kart do Inteligentnych Tachografów.

PL-CP zapewni wdrożenie wszystkich ciążących na nim wymagań, które są wyszczególnione w Polityce PL-MSA.

PL-CP ponosi odpowiedzialność za zgodność z wymaganiami opisanymi w Polityce PL-MSA, nawet jeśli funkcje PL-CP są realizowane przez podwykonawców. PL-CP może zlecić wykonanie części swoich procesów podwykonawcom. Korzystanie z podwykonawców w żaden sposób nie zmniejsza ogólnej odpowiedzialności PL-CP za te procesy.

1.5.5 Inne podmioty personalizujące urządzenia

Producentem czujników ruchu (MoS) w Polsce jest:

BOGART Sp. z o.o.
ul. Nowa Wieś Mała 40,
11-040 Dobre Miasto
Polska

Telefon: (+48-89) 615-17-17
Faks: (+48-89) 615-17-18
e-mail: bogart@bogart.pro
http://www.bogart.pro

Producenci czujników ruchu (MoS) zobowiązani są w szczególności do:

- Przestrzegania odpowiednich dla nich wymagań - tj. [1], [2], [6], [7], [8] oraz wszystkich innych przepisów i rozporządzeń mających znaczenie w tym obszarze, w szczególności niniejszej polityki PL-MSA zgodnie z ich najlepszą wiedzą i zgodnie z aktualnymi osiągnięciami technologicznymi w tym zakresie,
    - zapewnienia, że zintegrowane klucze i certyfikaty lub te, które mają zostać zintegrowane z produkowanym przez nich urządzeniami, mogą być wykorzystywane wyłącznie do celów zgodnych z zakresem określonym w: [1], [2], [6], [7], [8],
    - zapewnienia poufności prywatnych i tajnych kluczy podczas całego procesu produkcji, a także przez cały okres świadczenia usług;
- Sprawdzania i zapewniania, że są w stanie spełniać wymagania Common Criteria określone w normie ISO / IEC 15408 [8] dotyczących procesu produkcji czujników ruchu (MoS);
- Sprawdzania i zapewniania, że są w stanie spełniać wymagania Common Criteria Protection Profile (Digital Tachograph - Motion Sensor) [11] dotyczące procesu produkcji czujników ruchu (MoS);
- Informowania PL-MSA o wszystkich zewnętrznych dostawcach usług, którym powierzono odpowiedzialność za produkcję i personalizację urządzeń, a także zobowiązać ich do stosowania odpowiednich wymagań. Dopóki producent nie przekaże swoich zadań osobie trzeciej, jego prawa i obowiązki pozostają nienaruszone;
- Przygotowania dokumentu Deklaracji Praktyk PS, w którym co najmniej wyjaśniono metody realizacji Polityki PL-MSA, Polityki ERCA i mających zastosowanie właściwych przepisów prawnych;
- Natychmiastowego informowania PL-MSA lub jednej z jej upoważnionych agencji o wszystkich przypadkach naruszenia bezpieczeństwa produkcji, personalizacji i użytkowania urządzeń oraz kluczy i certyfikatów z nimi zintegrowanych;
- Umożliwienia PL-MSA lub jednej z jej upoważnionych agencji przeprowadzenia praktycznej oceny realizowanych przez nich obowiązków.

1.5.6 Posiadacze kart i użytkownicy czujników ruchu

PL-CIA będzie wymagać od posiadacza karty do tachografu lub instytucji go reprezentującej wywiązywania się ze zobowiązań wynikających z warunków korzystania z kart.

Organizacje lub użytkownicy czujników ruchu (MoS) powinni wypełniać zobowiązania wynikające z warunków użytkowania tych urządzeń.

1.6 Definicje i skróty

1.6.1 Definicje

Nazwa	Definicja
Polityka MSA	Zbiór reguł, które określają zakres stosowania kluczy, certyfikatów i urządzeń dla danej grupy użytkowników i / lub typów aplikacji ze wspólnymi wymaganiami dotyczącymi bezpieczeństwa.
Karta	Karta wyposażona w procesor, w Polityce PL-MSA termin równoznaczny z „Karta IC" i „Karta inteligentna".
Posiadacz karty	Osoba lub instytucja, która jest posiadaczem lub użytkownikiem karty. Posiadaczami kart mogą być kierowcy, przedsiębiorstwa transportowe, warsztaty i technicy warsztatów, organy kontrolne lub ich funkcjonariusze.
Certyfikat	W kontekście ogólnym certyfikat to struktura komunikatu zawierająca wiążący podpis wystawcy, który potwierdza, że informacje zawarte w certyfikacie są prawdziwe oraz że posiadacz certyfikowanego klucza publicznego może udowodnić posiadanie odpowiedniego klucza prywatnego.
Centrum Certyfikacji	Organizacja, w której wystawiane są certyfikaty przez podpisanie danych użytkownika kluczem prywatnym, którym podpisuje się Centrum Certyfikacji
Urządzenie	W systemie Inteligentnego Tachografu stosuje się następujące urządzenia: karty, tachografy (VU), zewnętrzne urządzenia GNSS (EGF), czujniki ruchu (MoS).
Producent/ Producent Urządzeń	Producenci urządzeń stosownych w systemie Inteligentnego Tachografu.
Klucz czujnika ruchu	Klucz symetryczny używany w czujniku ruchu i tachografie (VU), który umożliwia wzajemną autentykację tych urządzeń
Deklaracja Praktyk/ Deklaracja Praktyk Certyfikacyjnych	Deklaracja dotycząca praktyk bezpieczeństwa stosowanych w procesach Inteligentnego Tachografu. Deklaracja Praktyk (PS / CPS) jest porównywalna ze standardowym dokumentem CPS PKI.
Klucz prywatny	Prywatna część asymetrycznej pary kluczy wykorzystywana przez techniki szyfrowania kluczem publicznym. Klucz prywatny służy zazwyczaj do podpisywania certyfikatów cyfrowych lub odszyfrowywania wiadomości
Klucz publiczny	Publiczna część asymetrycznej pary kluczy wykorzystywana przez techniki szyfrowania kluczem publicznym. Klucz publiczny służy zazwyczaj do weryfikowania podpisów cyfrowych lub szyfrowania wiadomości dla posiadacza klucza prywatnego.
Klucz AES	Symetryczny klucz odpowiedni do szyfrowania / deszyfrowania informacji zgodnie z algorytmem AES.
Klucz ECC	Para asymetrycznych kluczy odpowiednich do szyfrowania / deszyfrowania informacji zgodnie z algorytmem ECC.
Typy kart	Cztery rodzaje kart do tachografów są używane w systemie Inteligentnego Tachografu: karta kierowcy, karta firmowa, karta warsztatowa, karta kontrolna.

Tabela 1 Lista definicji

1.6.2 Skróty

Skrót	Definicja
AES	Advanced Encryption Standard (Zaawansowany Standard Szyfrowania)
CA	Certification Authority (Centrum Certyfikacji)
CAA/PA	Certification Authority Administrator/ Personalization Administrator (Administrator Centrum Certyfikacji lub Administrator Personalizacji)
CAS	Certification Authority System (System Centrum Certyfikacji)
CIA	Card Issuing Authority (Podmiot Wydający Karty)
CC	Common Criteria (Wspólne Kryteria Bezpieczeństwa)
CP	Component Personaliser, Card Personalisation Centre (Podmiot Personalizujący Urządzenia, Centrum Personalizacji Kart)
CP	Certificate Policy (Polityka Certyfikacji)
CPS	Certification Practice Statement (Deklaracja Praktyk Certyfikacyjnych)
CSR	Certificate Signing Request (Wniosek o podpisanie certyfikatu)
DSRC	Dedicated Short Range Communications (Dedykowana Komunikacja Krótkiego Zasięgu)
EA	European Authority (Organ/Urząd Europejski)
EC	Elliptic Curve (Krzywa Eliptyczna)
EC	European Commission (Komisja Europejska)
ECC	Elliptic Curve Cryptography, an encryption algorithm based on elliptic curves (Kryptografia Krzywych Eliptycznych, algorytm szyfrowania oparty na krzywych eliptycznych)
EF	Elementary File. File stored on the tachograph card (Podstawowy plik. Plik przechowywany na karcie do tachografów)
EGF	External GNSS Facility (Zewnętrzne urządzenie GNSS)
ERCA	European Root Certification Authority (Główne Europejskie Centrum Certyfikacji)
EU	European Union (Unia Europejska)
EUR.PK	ERCA Public Key (Klucz publiczny ERCA)
EUR.SK	ERCA Secret Key (Klucz prywatny ERCA)
GNSS	Global Navigation Satellite System (Globalny System Nawigacji Satelitarnej)
HSM	Hardware Security Module (Sprzętowy moduł bezpieczeństwa)

ISSO	Information System Security Officer / Inspector of IT Security (Kierownik ds. Bezpieczeństwa Systemów Informacyjnych)
ITSEC	Information Technology Security Evaluation Criteria (Kryteria oceny bezpieczeństwa technologii informatycznej)
JRC	Joint Research Centre (Wspólne Centrum Badawcze)
KDM	Key Distribution Message (Komunikat dystrybucji klucza)
KDR	Key Distribution Request (Wniosek o dystrybucję/wydanie klucza)
KG	Key Generation (Generacja Klucza)
$\mathbf{K_{DSRC}}$	DSRC Master Key (Klucz główny DSRC)
$\mathbf{K_{ID}}$	Motion Sensor Identification Key (Klucz czujnika ruchu – identyfikacyjny)
$\mathbf{K_{M}}$	Motion Sensor Master Key (Klucz główny czujnika ruchu)
$\mathbf{K_{M\text{-}VU}}$	Motion Sensor Master Key (Vehicle Unit part) (Klucz główny czujnika ruchu – część VU)
$\mathbf{K_{M\text{-}WC}}$	Motion Sensor Master Key (Workshop Card part) (Klucz główny czujnika ruchu – część WC)
$\mathbf{K_{P}}$	Motion Sensor Pairing Key (Klucza parowania czujnika ruchu)
MA	Mutual Authentication (Wzajemna Autentykacja)
MoS	Motion Sensor (Czujnik ruchu)
MS	Member State (Państwo Członkowskie)
MSA	Member State Authority (Instytucja Wdrażająca system Inteligentnego Tachografu w Państwie Członkowskim)
MSCA	Member State Certification Authority (Centrum Certyfikacji Państwa Członkowskiego)
MSCA.PK	MSCA Public Key (Klucz publiczny MSCA)
MSCA.SK	MSCA Secret Key (Klucz Prywatny MSCA)
NCP	Normalised Certificate Policy (Znormalizowana polityka certyfikacji)
PIN	Personal Identification Number (Osobisty numer identyfikacyjny)
PK	Public Key (Klucz publicznny)
PKI	Public Key Infrastructure (Infrastruktura Klucza Publicznego)
PL-CIA	Polish Card Issuing Authority (Polski Podmiot Wydający Karty)
PL-CP	Polish Card Personalisation Centre (Polskie Centrum Personalizacji Kart)

PL-MSCA	Polish Member State Certification Authority (Polskie Centrum Certyfikacji)
PL-MSA	Polish Member State Authority (Organ Polskiego Państwa Członkowskiego)
PL-MSA Policy	Polish Member State Authority Policy (Polityka Organu Polskiego Państwa Członkowskiego)
PS	Practice Statement (Deklaracja Praktyk)
RFC	Request for Comment (Zbiór technicznych oraz organizacyjnych dokumentów mających formę memorandum związanych z Internetem oraz sieciami komputerowymi)
SA	System Administrator (Administrator Systemu)
SK	Secret Key (Klucz prywatny)
TC	Tachograph Card (Driver Card, Company Card, Workshop Card, Control Card) Karta do Tachografu (Karta Kierowcy, Karta Firmowa, Karta Warsztatowa, Karta Kontrolna)
VU	Vehicle Unit (Smart Tachograph) (Tachograf / Inteligentny Tachograf)
WC	Workshop Card (Karta Warsztatowa)

Tabela 2 Lista skrótów

Inne definicje można znaleźć w dokumentach, do których odwołuje się niniejsza polityka PL-MSA - zobacz w sekcji Bibliografia na końcu tego dokumentu.

2. Obowiązki w zakresie publikacji i przechowywania

2.1 Przechowywanie

PL-MSA odpowiada za publiczną stronę internetową https://www.gov.pl/infrastruktura/ , która będzie repozytorium dokumentów PL-MSA.

PL-MSCA odpowiada za publiczną stronę internetową https://www.info-car.pl/infocar/tachograf/ , która będzie repozytorium dokumentów PL-MSCA.

Certyfikaty podpisane przez PL-MSCA są przechowywane w niezależnej bazie danych. PL-MSCA odpowiada za przechowywanie w repozytorium wszystkich wydanych certyfikatów dla urządzeń. To repozytorium nie będzie publicznie dostępne.

2.2 Publikacja informacji dotyczących certyfikacji

PL-MSA opublikuje niniejszy dokument (Polityka certyfikacji Organu Państwa Członkowskiego) na swojej stronie internetowej.

Dokumenty Deklaracji Praktyk Certyfikacyjnych (CPS) PL-MSCA, PL-CP oraz Deklaracje Praktyk (PS) podmiotów personalizujących urządzenia lub innych zewnętrznych dostawców usług nie będą dostępne publicznie, ale będą przekazywane na żądanie odpowiednim stronom.

2.3 Częstotliwość publikacji

Informacje dotyczące zmian w tej polityce będą publikowane zgodnie z harmonogramem określonym w procedurach zmiany określonych w sekcji 9.11 niniejszego dokumentu.

Informacje dotyczące zmian w Polityce PL-MSA i CPS PL-MSCA będą publikowane zgodnie z harmonogramami określonymi w procedurach zmiany określonych odpowiednio w Polityce PL-MSA i CPS PL-MSCA.

Zmiany w PL-MSCA CPS i PL-CP PS oraz PS podmiotów personalizujących urządzenia lub innych zewnętrznych dostawców usług nie będą jawne, ale będą przekazywane wyłącznie odpowiednim stronom.

Zasady dystrybucji dotyczące zmian w polityce PL-MSA i CPS PL-MSCA zostaną określone w odpowiednich dokumentach.

2.4 Uprawnienia dostępu do repozytoriów

Wszystkie informacje dostępne za pośrednictwem stron internetowych wymienionych w pkt 2.1 są tylko w trybie do odczytu.

Każdy z podmiotów (PL-MSA, PL-MSCA, podmioty personalizujące urządzenia) wyznacza personel uprawniony do modyfikowania treści dokumentu lub modyfikowania dostępu do odpowiedniego dokumentu.

Wszystkie informacje publikowane na stronie internetowej PL-MSA będą dostępne za pośrednictwem bezpiecznego połączenia internetowego.

3. Identyfikacja i uwierzytelnianie

3.1 Nazewnictwo

3.1.1 Typy nazw

3.1.1.1 Podmiot i wystawca certyfikatu

Identyfikator urzędu certyfikacji (ang. *Certification Authority Reference, CAR*) i identyfikator posiadacza certyfikatu (ang. *Certificate Holder Reference, CHR*) identyfikują wystawcę i podmiot certyfikatu. Powinny być one tworzone w sposób, jak to zostało opisane w Załączniku 1C, Dodatek 11, CSM_136 i Dodatek 1 [2]:

Urząd	**Identyfikator**	**Struktura**
ERCA	Certification Authority Key Identifier (KID) (*Identyfikator Klucza Urzędu Certyfikacji*)	Nation numeric (‘FD’) (*numer kraju*) Nation alpha (EC) (*kod kraju*) Key serial number (numer seryjny klucza) Additional info (*dodatkowe informacje*) CA identifier (‘01’) (*identyfikator CA*)
PL-MSCA	Certification Authority Key Identifier (KID) (*Identyfikator Klucza Urzędu Certyfikacji*)	Nation numeric (*numer kraju*) Nation alpha (*kod kraju*) Key serial number (*numer seryjny klucza*) Additional info (*dodatkowe informacje*) CA identifier (*identyfikator CA*)

Tabela 3 Identyfikatory podmiotów i wystawców certyfikatów

3.1.1.2 Wniosek o dystrybucję klucza i Komunikat dystrybucji klucza

Wnioski o dystrybucję klucza (KDR) i komunikaty dystrybucji klucza (KDM) są identyfikowane przez identyfikator klucza dla publicznego efemerycznego klucza generowanego przez PL-MSCA, patrz sekcja 4.2.1 Polityki certyfikacji ERCA [6]. Wartość identyfikatora klucza jest określana zgodnie z sekcją 3.1.1.1 z następującymi modyfikacjami:

- NationNumeric: (‘28’)
- NationAlpha: (PL)
- keySerialNumber: unikalny dla PL-MSCA
- additionalInfo: ‘4B 52’ (“KR”, dla wniosku o klucz)
- CA identifier: ‘01’.

3.2 Początkowa weryfikacja tożsamości

3.2.1 Metoda weryfikacji, czy podmiot posiada klucz prywatny

PL-MSCA składając wniosek o podpisanie certyfikatu (ang. *Certificate Signing Request, CSR*) musi udowodnić, że posiada odpowiedni klucz prywatny za pomocą podpisu wewnętrznego, jak to zostało określone w sekcji 4.1.1 w polityce certyfikacji ERCA [6]. Wnioski o podpisanie certyfikatu (CSR) mogą również posiadać podpis zewnętrzny potwierdzający autentyczność wiadomości. Podpis zewnętrzny powinien być utworzony poprzez certyfikowany klucz prywatny wskazany w CSR.

3.2.2 Uwierzytelnianie tożsamości organizacji

PL-MSCA określa procedurę rejestracji subskrybenta i uwierzytelnienia jego tożsamości w dokumencie CPS PL-MSCA.

3.2.3 Uwierzytelnianie tożsamości osób

PL-MSCA określa procedurę uwierzytelniania tożsamości osób. Procedura ta jest dostępna w

dokumencie PL-MSCA CPS.

3.2.4 Weryfikacja urzędów certyfikacji

PL-MSCA określa procedurę weryfikacji urzędów certyfikacji w dokumencie CPS PL-MSCA.

3.2.5 Kryteria współdziałania

PL-MSCA nie będzie polegać na żadnym zewnętrznym urzędzie certyfikacji w zakresie usług podpisywania certyfikatów oraz dystrybucji klucza dostarczanych w ramach systemu Inteligentnego Tachografu.

Jeżeli PL-MSCA musi polegać na zewnętrznej infrastrukturze PKI dla jakiejkolwiek innej usługi lub funkcji, to przed złożeniem wniosku o usługi certyfikacyjne w charakterze podmiotu, powinno przejrzeć i zatwierdzić dokumenty polityki (CP) i / lub deklaracji praktyk certyfikacyjnych (CPS) zewnętrznego dostawcy usług certyfikacyjnych.

3.3 Identyfikacja i uwierzytelnianie dla wniosków o odnowienie klucza

Procedury identyfikacji i uwierzytelniania dla wniosków o odnowienie klucza są takie same, jak opisane w sekcji 3.2.

3.4 Identyfikacja i uwierzytelnianie dla wniosków o unieważnienie

Jeśli jest dozwolone unieważnianie certyfikatów dla urządzeń, PL-MSCA powinno opisać w swoim dokumencie deklaracji praktyk certyfikacyjnych CPS, w jaki sposób będą weryfikowane wnioski o unieważnienie certyfikatów dla urządzeń.

4. Wymagania eksploatacyjne dotyczące cyklu życia certyfikatów, kluczy głównych oraz urządzeń

Formaty wiadomości, mechanizmy kryptograficzne i procedury dotyczące wnioskowania oraz dystrybucji certyfikatów PL-MSCA, a także symetrycznych kluczy głównych między ERCA i MSCA (PL-MSCA) są szczegółowo opisane w sekcjach 4.1 i 4.2 Polityki certyfikacyjnej ERCA [6].

W dokumencie deklaracji praktyk certyfikacyjnych PL-MSCA są szczegółowo opisane formaty komunikatów, mechanizmy kryptograficzne oraz procedury dotyczące wnioskowania i dystrybucji certyfikatów dla urządzeń oraz kluczy symetrycznych dla kart, a także procedury dotyczące wnioskowania i dystrybucji zaszyfrowanych danych dla czujników ruchu, które są wykorzystywane w komunikacji po między PL-MSCA i podmiotami personalizującymi urządzenia.

4.1 Wnioskowanie o certyfikat klucza publicznego MSCA i jego wydawanie

4.1.1 Wniosek o podpisanie certyfikatu

Wniosek o podpisanie certyfikatu (ang. *Certificate Signing Request, CSR*) może być złożony tylko przez PL-MSCA wskazane przez PL-MSA w niniejszej polityce. Organ europejski akceptuje decyzje PL-MSA.

CSR powinien mieć format TLV (ang. *Tag-Lenght-Value*, Tag-Długość-Wartość). Tabela 4 przedstawia zawartość (wszystkie tagi) CSR. Dla długości stosuje się zasady kodowania DER określone w [19]. Wartości są określone w pozostałej części tej sekcji.

Obiekt danych	**Wymagalność**	**Tag**
Authentication (*Autentykacja*)	o	‘67’
ECC (CV) Certificate (*Certyfikat ECC (CV)*)	w	‘7F 21’
Certificate Body (*Certyfikat*)	w	‘7F 4E’
Certificate Profile Identifier (*Identyfikator profilu certyfikatu*)	w	‘5F 29’
Certification Authority Reference (*Referencja do Urzędu Certyfikacji*)	w	‘42’
Certificate Holder Authorisation (*Identyfikacja właściciela certyfikatu*)	w	‘5F 4C’
Public Key (*Klucz publiczny*)	w	‘7F 49’
Standardised Domain Parameters OID (*Standardowe parametry domeny OID*)	w	‘06’
Public Point (*Punkt Publiczny*)	w	‘86’

Certificate Holder Reference (*Referencja do właściciela certyfikatu*)	w	‘5F 20’
Certificate Effective Date (*Data początku ważności certyfikatu*)	w	‘5F 25’
Certificate Expiry Date (*Data końca ważności certyfikatu*)	w	‘5F 24’
Inner Signature (*Podpis wewnętrzny*)	w	‘5F 37’
Certification Authority Reference of Outer Signature Signatory (*Referencja do wystawcy certyfikatu dla podpisu zewnętrznego*)	o	‘42’
Outer Signature (*Podpis zewnętrzny*)	o	‘5F 37’

Tabela 4 Format wniosku o podpisanie certyfikatu

w: wymagany
o: opcjonalny

Obiekt danych **Authentication** powinien być obecny tylko w przypadku, gdy obecny jest obiekt danych Outer Signature.

Wersja profilu jest identyfikowana przez **Certificate Profile Identifier**. Wersja 1, określona w sekcji 7.1, powinna być oznaczona wartością ‘00’.

Obiekt danych **Certification Authority Reference** powinien być wykorzystany do poinformowania ERCA o kluczu prywatnym ERCA, którego PL-MSCA spodziewa się, iż będzie użyty do podpisania certyfikatu. Wartości Certification Authority Reference określono w sekcji 3.1. Identyfikator klucza głównego ERCA wykorzystywanego do podpisywania certyfikatów jest zawsze dostępny na stronie internetowej ERCA.

Obiekt danych **Certificate Holder Authorisation** służy do identyfikacji typu certyfikatu. Składa się z sześciu najbardziej znaczących bajtów identyfikatora aplikacji do tachografów (‘FF 53 4D 52 44 54’), połączonych z rodzajem urządzenia, dla którego przeznaczony jest certyfikat (Załącznik 1C, Dodatek 11, CSM_141). W przypadku certyfikatów PL-MSCA typ urządzenia należy ustawić na „0E” (14 dziesiętnie).

Obiekt danych **Public Key** zawiera dwa obiekty danych:

- Obiekt danych **Domain Parameters** odwołuje się do standardowych parametrów domeny, które mają być używane z kluczem publicznym w certyfikacie. Zawiera jeden z identyfikatorów obiektów wyszczególnionych w Tabeli 1 w Dodatku 11, Załączniku 1C.
- Obiekt danych **Public Point** zawiera punkt publiczny. Punkty publiczne krzywej eliptycznej są konwertowane na ciągi oktetów określone w [20]. Należy użyć nieskompresowanego formatu kodowania (Załącznik 1C, Dodatek 11, CSM_143).

Obiekt danych **Certificate Holder Reference** jest wykorzystywany do identyfikacji klucza publicznego zawartego w żądaniu oraz w wynikowym certyfikacie. Obiekt danych Certificate Holder Reference powinien być unikalny. Ten obiekt danych może być używany do budowania referencji do tego klucza publicznego w certyfikatach dla urządzeń (Załącznik 1C, Dodatek 11,

CSM_144). Informacje na temat wartości Certificate Holder Reference znajdują się w sekcji 3.1.

Obiekt danych **Certificate Effective Date** wskazuje datę i godzinę rozpoczęcia okresu ważności certyfikatu. Obiekt danych **Certificate Expiration Date** wskazuje datę końcową i czas okresu ważności. Oba elementy danych będą typu danych `TimeReal`, określonego w Dodatku 1. Należy pamiętać, że okres ważności określony przez te dwa elementy danych wynosi 7 lat i 1 miesiąc dla certyfikatów MSCA_Card.

Obiekt danych **Certificate Body** powinien być podpisany przez podpis wewnętrzny (**Inner Signature**), który musi być możliwy do zweryfikowania za pomocą klucza publicznego zawartego w żądaniu certyfikatu. Podpis powinien być złożony dla pola Certificate Body (w tym tag '7F 4E' i jego długość). Algorytmem podpisu będzie ECDSA, jak określono w [14], przy użyciu algorytmu haszującego powiązanego z rozmiarem klucza publicznego w CSR, jak określono w Załączniku 1C, Dodatku 11, CSM_50. Podpis powinien być złożony w formacie plain, jak określono w [20].

Obiekt danych **Certification Authority Reference of Outer Signature Signatory** wskazuje na PL-MSCA i odpowiedni klucz, przy użyciu którego powstał zewnętrzny podpis. Występuje tylko w przypadku, gdy obecny jest podpis zewnętrzny. Możliwe wartości określono sekcji 3.1.

Obiekt danych **Outer Signature** nie występuje, jeżeli PL-MSCA ubiega się o swój pierwszy certyfikat. Outer Signature jest wymagany, jeśli PL-MSCA ubiega się o kolejny certyfikat. W takim przypadku Certificate Signing Request zostanie dodatkowo podpisany zewnętrznym podpisem przez MSCA, przy użyciu (jednego z) aktualnych ważnych kluczy prywatnych PL-MSCA. Zewnętrzny podpis uwierzytelnia wniosek. W przypadku, gdy PL-MSCA wnioskuje o certyfikat MSCA_Card, zewnętrzny podpis należy złożyć przy użyciu klucza prywatnego powiązanego z certyfikatem tego samego typu.

Outer Signature powinien być złożony dla pola ECC (CV) Certificate (w tym tag '7F 21' i jego długość) oraz dla pola Certification Authority Reference of Outer Signature Signatory (w tym tag '42' i jego długość). Algorytmem podpisu będzie ECDSA, jak określono w [14], przy użyciu algorytmu haszującego powiązanego z rozmiarem klucza PL-MSCA używanego do podpisywania, jak określono w Załączniku 1C, Dodatku 11, CSM_50. Podpis powinien być złożony w formacie plain, jak określono w [20].

PL-MSCA oblicza i przechowuje skrót dla całego CSR, stosując algorytm haszujący powiązany z rozmiarem klucza organu podpisującego, jak to określono w Załączniku 1C, Dodatku 11, CSM_50. Skrót będzie używany przez ERCA do weryfikacji autentyczności CSR.

4.1.2 Certyfikaty

Format certyfikatów klucza publicznego PL-MSCA jest zaprezentowany w sekcji 7.1.

4.1.3 Wymiana wniosków i odpowiedzi

Do przenoszenia wniosków o podpisanie certyfikatu oraz podpisanych certyfikatów należy używać nośników CD-R. Płyta CD-R powinna mieć średnicę 12 cm i powinna być nagrana w trybie pojedynczej sesji (format ISO 9660: 1988).

PL-MSCA zapisuje od jednej do trzech kopii każdego wniosku o podpisanie certyfikatu na nośniku transportowym, który będzie dostarczony do ERCA. Kopie powinny być w formacie

szesnastkowym ASCII (plik .txt), Base64 (plik .pem) lub binarnym (plik .bin).

Do każdego wniosku o podpisanie certyfikatu oraz podpisanego certyfikatu dołączona jest papierowa kopia danych, sformatowana zgodnie z szablonem zdefiniowanym w ERCA CPS [7]. Osobna papierowa kopia danych będzie przechowywana odpowiednio przez ERCA lub PL-MSCA.

4.1.4 Przyjęcie certyfikatu

Po otrzymaniu certyfikatu na w siedzibie PL-MSCA, tenże podmiot sprawdza, czy:

- media transportowe są czytelne; tj. nie są uszkodzone lub zniszczone;
- format certyfikatu jest zgodny z Tabela 8 w sekcji 7.1;
- wszystkie wartości pól certyfikatu odpowiadają wartościom wymaganym w CSR;
- podpis certyfikatu można zweryfikować przy użyciu publicznego klucza głównego ERCA wskazanego w polu CAR.

Jeśli którykolwiek z tych testów nie powiedzie się, PL-MSCA powinno przerwać proces i skontaktować się z ERCA. Odrzucenie certyfikatu jest realizowane zgodnie z procedurą unieważniania certyfikatu (patrz sekcja 4.1.9).

4.1.5 Użycie pary kluczy i certyfikatu

PL-MSCA powinno używać otrzymane pary kluczy i odpowiedniego dla ich certyfikaty zgodnie zapisami z sekcji 6.2.

4.1.6 Odnowienie certyfikatu

Odnowienie certyfikatu, tj. przedłużenie okresu ważności istniejącego certyfikatu, jest niedozwolone.

4.1.7 Ponowne wydanie certyfikatu

Ponowne wydanie certyfikatu oznacza podpisanie nowego certyfikatu PL-MSCA, który zastąpi istniejący certyfikat. Ponowny wydanie certyfikatu powinno mieć miejsce:

- gdy PL-MSCA zbliża się do końca okresu użytkowania (jednego ze) swoich kluczy prywatnych. W takim przypadku ponowne wydanie certyfikatu należy przeprowadzić w odpowiednim czasie, aby zapewnić, że PL-MSCA może kontynuować działanie po zakończeniu okresu użytkowania poprzedniego certyfikatu;
- po unieważnieniu certyfikatu.

Procedury wnioskowania o certyfikat, przetwarzania wniosku, wydawania certyfikatu, akceptacji i publikacji są takie same jak dla początkowej pary kluczy.

Para kluczy PL-MSCA może być regularnie zmieniana. Nie ma żadnych ograniczeń co do liczby certyfikatów PL-MSCA, które zostaną podpisane przy użyciu certyfikatów PL-MSCA. PL-MSCA może zażądać wielu certyfikatów PL-MSCA tego samego typu z nakładającymi się okresami ważności, jeśli jest to uzasadnione jego działalnością.

4.1.8 Modyfikacja Certyfikatu

Modyfikacja certyfikatu nie jest dozwolona.

4.1.9 Zawieszenie i unieważnienie certyfikatu

4.1.9.1 Okoliczności unieważnienia certyfikatu

Certyfikaty PL-MSCA zostaną unieważnione w następujących okolicznościach:

- odrzucenie podczas przyjęcia nowo wystawionego certyfikatu (sekcja 4.1.4);

- kompromitacja lub podejrzenie kompromitacji klucza prywatnego PL-MSCA;
- utrata klucza prywatnego PL-MSCA;
- zakończenie działania PL-MSCA;
- brak spełnienia przez PL-MSA lub PL-MSCA zobowiązań wynikających z rozporządzenia i polityki certyfikacji ERCA [6].

4.1.9.2 Kto może wnioskować o unieważnienie

Organ europejski jest upoważniony do wnioskowania o unieważnienie certyfikatu PL-MSCA.

PL-MSA jest upoważnione do wnioskowania o unieważnienie certyfikatów wydanych dla PL-MSCA wskazanych w Polityce PL-MSA.

PL-MSCA jest upoważnione do wnioskowania o unieważnienie certyfikatów wydanych dla siebie.

4.1.9.3 Procedura wnioskowania o unieważnienie

Procedura wnioskowania o unieważnienie certyfikatu została opisana w dokumencie deklaracji praktyk ERCA CPS [7].

4.1.9.4 Specjalne wymagania dotyczące sytuacji kompromitacji klucza

Wymagania dotyczące sytuacji kompromitacji klucza zostały opisane w rozdziale 4.5.2.6.

4.1.9.5 Zawieszenie certyfikatu

Zawieszenie certyfikatu nie jest dozwolone.

4.1.10 Koniec subskrypcji certyfikatów

Korzystanie z usług podpisywania certyfikatów przez ERCA kończy się, gdy PL-MSA podejmie decyzję o rozwiązaniu PL-MSA. Taka zmiana jest zgłaszana ERCA przez PL-MSA jako zmiana w polityce PL-MSA.

W przypadku zakończenia subskrypcji decyzja o złożeniu wniosku o unieważnienie certyfikatów dla wszystkich ważnych certyfikatów PL-MSCA lub zgoda na wygaśnięcie wszystkich certyfikatów PL-MSCA spoczywa na PL-MSA.

4.2 Wnioskowanie o klucze główne oraz ich wydawanie

4.2.1 Wniosek o wydanie klucza

Wniosek o wydanie klucza (ang. *Key distribution requests, KDR*) może być złożony tylko przez PL-MSCA wskazane przez PL-MSA w niniejszej polityce. Organ europejski akceptuje decyzje PL-MSA.

KDR powinien mieć format TLV (ang. *Tag-Lenght-Value*, Tag-Długość-Wartość). Tabela 5 przedstawia zawartość (wszystkie tagi) KDR. Dla długości stosuje się zasady kodowania DER określone w [19]. Wartości są określone w pozostałej części tej sekcji.

Obiekt danych	**Wymagalność**	**Tag**
Key Distribution Request (*Wniosek o wydanie klucza*)	w	‘A1’
Request Profile Identifier (*Identyfikator profilu wniosku*)	w	‘5F 29’
Message Recipient Authorisation	w	‘83’

(*Identyfikacja odbiorcy wiadomości*)		
Key Identifier (*Identyfikator klucza*)	w	'84'
Public Key (for ECDH key agreement) (*Klucz publiczny (dotyczy uzgodnienia kluczy ECDH)*)	w	'7F 49'
Standardised Domain Parameters OID (*Standardowe Parametry domeny OID*)	w	'06'
Public Point (*Punkt Publiczny*)	w	'86'

Tabela 5 Format wniosku o wydanie klucza

w: wymagany
o: opcjonalny

Wersja profilu jest identyfikowana przez **Request Profile Identifier**. Wersja 1, określona w Tabela 5, powinna być oznaczona wartością '00'.

Obiekt danych **Message Recipient Authorisation** powinien być używany do identyfikacji żądanego klucza symetrycznego. Składa się z konkatenacji

- sześć najbardziej znaczących bajtów identyfikatora aplikacji do tachografów ('FF 53 4D 52 44 54'),
- typ żądanego klucza (opis zamieszczono poniżej, 1 bajt),
- numer wersji żądanego klucza głównego (1 bajt).

W celu wskazania rodzaju żądanego klucza należy używać następujących wartości:

- '07': KM, klucz główny czujnika ruchu
- '27': KM-WC, klucz główny czujnika ruchu – część WC
- '67': KM-VU, klucz główny czujnika ruchu – część VU
- '09': KDSRC, klucz główny DSRC

Obiekt danych **Key Identifier** jest unikalnym 8-bajtowym ciągiem oktetów identyfikującym klucz publiczny, który jest umieszczony w KDR i stosowany w wymianie kluczy ECDH, szczegóły w rozdziale 4.2.3 Polityki ERCA [6]. Jego wartość określa się zgodnie z opisem w rozdziale 3.1.1.2. Ponieważ PL-MSCA może użyć innej pary kluczy efemerycznych dla każdego wniosku o wydanie klucza, może wykorzystywać identyfikator klucza do określenia efemerycznego klucza prywatnego, który będzie używany do deszyfrowania danego komunikatu dystrybucji klucza, jak tylko dotrze on do PL-MSCA. Z tego powodu ERCA kopiuje identyfikator klucza w komunikacie o dystrybucji klucza, patrz Tabela 6.

Obiekt danych **Public Key** zawiera dwa obiekty danych:

- Obiekt danych **Public Point** zawiera publiczny punkt efemerycznej pary kluczy PL-MSCA, który zostanie użyty do uzgodnienia klucza. PL-MSCA konwertuje punkt publiczny na ciąg oktetów określony w [20], używając nieskompresowanego formatu kodowania.
- Obiekt danych **Domain Parameters** zawiera identyfikator obiektu zestawu standardowych parametrów domeny, które mogą być używane w połączeniu z obiektem danych Public Point. Więcej informacji można znaleźć w sekcji 4.2.3 Polityki ERCA [6].

PL-MSCA oblicza i przechowuje skrót dla całego KDR, stosując algorytm haszujący powiązany z rozmiarem klucza, o który wnioskuje, jak to określono w Załączniku 1C, Dodatku 11, CSM_50. Skrót będzie używany przez ERCA do weryfikacji autentyczności KDR.

4.2.2 Wiadomość dystrybucji klucza

Wiadomość dystrybucji klucza (ang. *Key distribution message, KDM*) jest tworzona przez ERCA, zgodnie z formatem zaprezentowanym w Tabela 6. Dla długości stosuje się zasady kodowania DER określone w [19]. Wartości są określone w pozostałej części tej sekcji.

Obiekt danych	**Wymagalność**	**Tag**
Key Distribution	w	‘A1’
Request Profile Identifier (*Identyfikator profilu wniosku*)	w	‘5F 29’
Message Recipient Authorisation (*Identyfikacja odbiorcy wiadomości*)	w	‘83’
Key Identifier of the MSCA ephemeral key pair for ECDH key agreement (*Identyfikator klucza efemerycznej pary kluczy MSCA do uzgodnienia kluczy ECDH*)	w	‘84’
Public Point of the ERCA for ECDH key agreement (*Punkt publiczny ERCA do uzgodnienia kluczy ECDH*)	w	‘86’
Encrypted symmetric key (*Zaszyfrowany klucz symetryczny*)	w	‘87’
MAC	w	‘88’

Tabela 6 Wiadomość dystrybucji klucza

w: wymagany
o: opcjonalny

Wersja profilu jest identyfikowana przez **Request Profile Identifier**. Wersja 1, określona w Tabela 6, powinna być oznaczona wartością ‘00’.

Obiekt danych **Message Recipient Authorisation** musi być identyczny z obiektem danych Message Recipient Authorisation w KDR z PL-MSCA (sekcja 4.2.1).

Obiekt danych **Public Point** będzie zawierał punkt publiczny efemerycznej pary kluczy ERCA używanej do uzgodnienia klucza (punkt 4.2.3 Polityki ERCA [6]). Obiekt danych Public Point jest konwertowany na ciąg oktetów określony w [20], przy użyciu nieskompresowanego formatu kodowania.

Obiekt danych **Encrypted symmetric key** powinien zawierać dane wyjściowe kroku numer 4 w sekcji 4.2.3 Polityki ERCA [6].

Obiekt danych **MAC** zawiera dane wyjściowe kroku numer 5 w sekcji 4.2.3 Polityki ERCA [6].

Po pomyślnym wygenerowaniu wiadomości dystrybucji klucza, efemeryczny klucz prywatny używany do uzgodnienia klucza, klucz szyfrowania K_{ENC} i klucz K_{MAC} są bezpiecznie niszczone w HSM.

Wiadomość o dystrybucji klucza jest przekazywana do PL-MSCA, które wygenerowało KDR.

4.2.3 Wymiana wniosków i odpowiedzi

Do przenoszenia wniosków o wydanie klucza oraz wiadomości dystrybucji klucza należy używać nośników CD-R. Płyta CD-R powinna mieć średnicę 12 cm i powinna być nagrana w trybie pojedynczej sesji (format ISO 9660: 1988).

PL-MSCA zapisuje od jednej do trzech kopii każdego wniosku o wydanie klucza na nośniku transportowym, który będzie dostarczony do ERCA. Kopie powinny być w formacie szesnastkowym ASCII (plik .txt), Base64 (plik .pem) lub binarnym (plik .bin).

Do każdego wniosku o wydanie klucza oraz wiadomości dystrybucji klucza dołączona jest papierowa kopia danych, sformatowana zgodnie z szablonem zdefiniowanym w ERCA CPS [7]. Osobna papierowa kopia danych będzie przechowywana odpowiednio przez ERCA lub PL-MSCA.

4.2.4 Przyjęcie klucza

Po otrzymaniu wiadomości dystrybucji klucza w siedzibie PL-MSCA, tenże podmiot sprawdza, czy:

- media transportowe są czytelne; tj. nie są uszkodzone lub zniszczone;
- format certyfikatu jest zgodny z Tabela 6;
- wiadomość jest oryginalna. PL-MSCA powinien to zweryfikować kontaktując się z ERCA tak jak to zostało opisane w dokumencie ERCA CPS [7] oraz sprawdzając, czy MAC w odebranym KDM jest zgodny z MAC w KDM wysłanym przez ERCA;
- typ klucza głównego i wersja w komunikacie odpowiadają żądanemu typowi i wersji klucza;
- punkt publiczny określony we wiadomości znajduje się na krzywej określonej we wniosku o wydanie klucza wysłanym przez PL-MSCA do ERCA.

Jeśli którykolwiek z tych testów nie powiedzie się, PL-MSCA powinno przerwać proces i skontaktować się z ERCA.

Jeśli wszystkie testy zakończą się powodzeniem, PL-MSCA powinno:

- wykorzystać algorytm ECKA-DH, aby uzyskać wspólny punkt (K_x, K_y), jak opisano w kroku 3 w punkcie 4.2.3 Polityki ERCA [6], używając efemerycznego klucza prywatnego PL-MSCA wskazanego przez identyfikator klucza w komunikacie oraz efemerycznego klucza publicznego ERCA. PL-MSCA powinno sprawdzić, czy wspólny punkt nie jest punktem nieskończoności. Jeśli tak, PL-MSCA przerywa proces i kontaktuje się z ERCA. W innym przypadku PL-MSCA tworzy wspólną ukrytą wartość K, konwertując K_x na ciąg oktetów określony w [20] (*Conversion between Field Elements and Octet Strings*);
- uzyskać klucze K_{ENC} i K_{MAC} zgodnie z opisem w kroku 4 w sekcji 4.2.3 Polityki ERCA [6];
- zweryfikować MAC za pomocą zaszyfrowanego klucza symetrycznego, jak opisano w kroku 5 w sekcji 4.2.3 Polityki ERCA [6]. Jeśli weryfikacja się nie powiedzie, PL-MSCA powinno przerywać proces i skontaktować się z ERCA;
- odszyfrować klucz symetryczny zgodnie z opisem w kroku 4 w sekcji 4.2.3 Polityki ERCA [6]. PL-MSCA powinno sprawdzić, czy dopełnienie odszyfrowanego klucza jest

poprawne. Jeśli weryfikacja nie powiedzie się, PL-MSCA powinno przerwać proces i skontaktować się z ERCA.

Wszystkie operacje wykonywane przy użyciu: efemerycznego klucza prywatnego, wspólnej ukrytej wartości K oraz kluczy pochodnych K_{ENC} i K_{MAC} powinny odbywać się w HSM spełniającym wymagania podane w sekcji 6.2. Po pomyślnym odzyskaniu klucza głównego lub po przerwaniu przetwarzania wiadomości dystrybucji klucza i gdy nie w rozpoczęto odnawiania KDM (rozdział 4.2.6) PL-MSCA bezpiecznie niszczy w HSM: swój efemeryczny klucz prywatny używany do uzgodnienia klucza, klucz szyfrowania K_{ENC} i klucz K_{MAC}.

4.2.5 Użycie klucza głównego

PL-MSCA powinno używać otrzymany klucz główny zgodnie zapisami z sekcji 6.2.

4.2.6 Odnowienie KDM

Odnowienie KDM oznacza wydanie kopii istniejącego KDM do PL-MSCA bez zmiany efemerycznego klucza publicznego lub jakichkolwiek innych informacji w KDM.

Odnowienie KDM może nastąpić tylko wtedy, gdy oryginalne media transportowe odebrane w PL-MSCA są uszkodzone lub zniszczone. Uszkodzenie lub zniszczenie środków transportu jest incydentem bezpieczeństwa, który należy zgłosić do PL-MSA i ERCA. Po zaraportowaniu incydentu bezpieczeństwa PL-MSCA może wysłać żądanie odnowienia KDM do ERCA, odnosząc się do pierwotnego wniosku o wydanie klucza. Procedura ta jest opisana w ERCA CPS [7] oraz w PL-MSCA CPS.

Uwaga - w przypadku, gdy PL-MSCA musi wysłać żądanie ponownego wydania klucza głównego, który został już pomyślnie przekazany do PL-MSCA, powinno wygenerować nowy wniosek o wydanie klucza, używając nowo wygenerowanej pary kluczy efemerycznych. Taki wniosek może skutkować wszczęciem przez ERCA dochodzenia w sprawie możliwości kompromitacji klucza.

4.2.7 Powiadomienie o kompromitacji klucza symetrycznego

Wymagania dotyczące zdarzenia kompromitacji klucza zostały opisane w rozdziale 4.5.3.6.

4.2.8 Koniec subskrypcji klucza

Korzystanie z usług dystrybucji kluczy przez ERCA kończy się, gdy PL-MSA podejmie decyzję o rozwiązaniu PL-MSA. Taka zmiana jest zgłaszana ERCA przez PL-MSA jako zmiana w polityce PL-MSA.

W przypadku zakończenia subskrypcji PL-MSCA powinno bezpiecznie zniszczyć wszystkie kopie każdego symetrycznego klucza głównego, które posiada.

4.3 Zarządzanie urządzeniami

Zgodnie z Polityką PL-MSA jako urządzenia w ramach systemu Inteligentnego Tachografu definiuje się:

- Karty do tachografów zwane dalej ”kartami”;
- Czujniki ruchu (MoS).

Sprzęt jest obsługiwany lub zarządzany przez:

- PL-MSA;
- PL-CIA;

- PL-MSCA;
- PL-CP;
- Producentów czujników ruchu.

4.4 Karty

4.4.1 Kontrola jakości

PL-CP zapewni, że tylko karty posiadające świadectwo homologacji typu zgodnie z [2], będą wykorzystane w procesie personalizacji i wydawania do użytkowania.

4.4.2 Wnioskowanie o wydanie karty

Wnioskodawca chcący otrzymać kartę, dostarcza wniosek do PL-CIA w formacie określonym przez PL-MSA. Wniosek wraz z odpowiednimi załącznikami powinien zawierać dane pozwalające na prawidłową identyfikację wnioskodawcy.

PL-CIA informuje wnioskodawcę o warunkach dotyczących używania karty. Informacje te będą dostępne po polsku, a w razie potrzeby również po angielsku.

Wnioskodawca, poprzez złożenie wniosku o kartę i akceptację sposobu jej dostarczenia, zgadza się na obowiązujące warunki, określone w szczególności w [1], [2], [6] i [7].

4.4.2.1 Umowy

Wnioskodawca, poprzez złożenie wniosku o kartę i akceptację sposobu jej dostarczenia zawiera z PL-CIA umowę, z następującymi zobowiązaniami:

- Wnioskodawca zgadza się na warunki stosowania i użytkowania karty, określone w [1], [2], [6] i [7];
- Wnioskodawca zgadza się i oświadcza, że:
    a. Od chwili otrzymania karty i przez cały okres jej eksploatacji nie będzie udostępniać karty ani zezwalać na korzystanie z niej w sposób niedozwolony;
    b. Wszystkie informacje podane PL-CIA przez wnioskodawcę według stanu obowiązującego w chwili złożenia wniosku, są prawdziwe.

4.4.2.2 Warunki zatwierdzenia przez PL-CIA specyficzne dla wydawanej karty kierowcy

Karty kierowcy będą wydawane osobom podlegającym przepisom rozporządzenia (WE) nr 561/2006 [18] i mającym miejsce zamieszkania na terytorium Polski.

PL-CIA podejmie należyte starania, aby sprawdzić, czy wnioskodawca nie posiada innej ważnej karty kierowcy wydanej w Polsce lub w innym Państwie Członkowskim.

PL-CIA podejmie należyte starania, aby sprawdzić, czy wnioskodawca składający wniosek o wydanie karty kierowcy posiada ważne prawo jazdy odpowiedniej kategorii (B lub wyższej).

4.4.3 Okres ważności kart

Karty kierowcy będą ważne przez maksymalnie pięć lat od daty rozpoczęcia ważności.

Karty warsztatowe będą ważne przez maksymalnie jeden rok od daty rozpoczęcia ważności.

Karty przedsiębiorstwa są ważne przez maksymalnie pięć lat od daty rozpoczęcia ważności.

Karty kontrolne są ważne przez maksymalnie dwa lata od daty rozpoczęcia ważności.

Karty tymczasowe, nieodnawialne, są ważne nie dłużej niż 185 dni od daty rozpoczęcia ważności.

4.4.4 Wznawianie kart przez PL-CIA

4.4.4.1 Upływ terminu ważności karty

PL-CIA wznowi kartę przed upływem ważności karty bieżącej pod warunkiem, że wniosek o wznowienie karty zostanie złożony przynajmniej 15 dni przed upływem daty ważności karty bieżącej.

PL-CIA wdroży procedury przypominania posiadaczom kart o zbliżającym się upływie terminu ważności karty.

Procedura w przypadku składania wniosku o wznowienie karty jest taka sama jak w przypadku wniosku o wydanie nowej karty.

4.4.4.2 Uaktualnienie danych osobowych i administracyjnych

Zmiana danych istotnych dla identyfikacji posiadacza karty uzasadnia konieczność wymiany istniejącej karty w celu modyfikacji danych administracyjnych. PL-CIA powinno przestrzegać procedur dotyczących odnowienia, jeżeli poprzednia karta została wydana w Polsce.

4.4.5 Zamiana karty przez PL-CIA

4.4.5.1 Zmiana kraju zamieszkania

Posiadacz karty wydanej przez inne państwo członkowskie, który zmienia kraj zamieszkania na terytorium Unii Europejskiej, może złożyć wniosek o nową kartę kierowcy lub zażądać zamiany karty w Polsce, o ile udowodni, że zamieszkuje w Polsce przez co najmniej 185 dni w roku.

Jeśli aktualna karta została wydana przez inne państwo członkowskie Unii Europejskiej, to posiadacz karty powinien przedstawić dowód, iż zamieszkuje w Polsce, aby jego wniosek o wymianę karty został zaakceptowany.

Wnioskodawca o zamianę karty, zwraca poprzednią kartę PL-CIA. PL-CIA przekazuje tę kartę odpowiedniemu organowi w innym państwie członkowskim, który wydał kartę.

Procedura zamiany karty w związku ze zmianą kraju zamieszkania jest taka sama jak w przypadku wniosku o pierwsze wydanie karty.

4.4.6 Wymiana utraconych, skradzionych, uszkodzonych lub wadliwie działających kart przez PL-CIA

4.4.6.1 Wymiana skradzionych kart

Jeśli karta została skradziona, posiadacz karty powinien zgłosić kradzież organowi kontrolnemu upoważnionemu do wykonywania kontroli transportu drogowego lub w najbliższej jednostce Policji i uzyskać potwierdzenie zgłoszenia.

Kradzież karty musi również zostać zgłoszona PL-CIA. PL-CIA rejestruje zgłoszenie o skradzionej karcie.

Składając do PL-CIA wniosek o wymianę skradzionej karty, posiadacz karty załącza do wniosku kopię zaświadczenia potwierdzającego zgłoszenie kradzieży.

Numer skradzionej karty jest wpisywany na tzw. „czarną listę” dostępną dla upoważnionych organów we wszystkich państwach członkowskich.

4.4.6.2 Wymiana utraconej karty

Utratę karty należy zgłosić do PL-CIA. PL-CIA rejestruje zgłoszenie o utracie karty.

Posiadacz utraconej karty składa w PL-CIA wniosek o wymianę karty.

Numer utraconej karty jest wpisywany na tzw. „czarną listę" dostępną dla upoważnionych organów we wszystkich państwach członkowskich.

4.4.6.3 Wymiana uszkodzonej lub wadliwie działającej karty

Karty uszkodzone i wadliwie działające należy dostarczyć do PL-CIA. Jeśli uszkodzona lub wadliwie działająca karta zostanie zwrócona do PL-CIA, jej numer jest wpisywany na tzw. „czarną listę", natomiast karta jest unieważniana wizualnie i elektronicznie, a następnie niszczona.

Jeśli karta została utracona, skradziona, uszkodzona lub działa wadliwie, posiadacz karty powinien złożyć wniosek o jej wymianę w ciągu 7 dni kalendarzowych.

Jeśli posiadacz karty spełni powyższe wymaganie, a wniosek zostanie uznany za wypełniony poprawnie i zaakceptowany, PL-CIA wyda kartę zastępczą z nowymi kluczami i certyfikatem w ciągu 8 dni roboczych (Rozporządzenie [1]) od daty otrzymania wniosku.

Karta zastępcza zachowuje okres ważności karty oryginalnej. Jeśli do końca okresu ważności karty zastępczej zostało mniej niż 2 miesiące, PL-CIA wznowi kartę.

Jeśli karta warsztatowa została utracona, skradziona, uszkodzona lub działa wadliwie, PL-CIA wyda kartę zastępczą z nowymi kluczami i certyfikatem w ciągu 5 dni roboczych (Rozporządzenie [1]) od otrzymania wypełnionego wniosku.

4.4.7 Rejestrowanie przyjętych wniosków

PL-CIA rejestruje wszystkie wnioski w bazie danych i wykorzystuje te informacje jako dane wejściowe dla podsystemów generowania certyfikatów i personalizacji kart.

4.4.8 Personalizacja kart

PL-CP personalizuje karty zarówno wizualnie, jak i elektronicznie.

4.4.8.1 Personalizacja wizualna

Karty są personalizowane wizualnie zgodnie z Rozporządzeniem [2] (wymagania 227 - 237), a w szczególności:

- Na karcie kierowcy musi być umieszczone zdjęcie wnioskodawcy;
- Na karcie warsztatowej może być umieszczone zdjęcie technika warsztatu;
- Na karcie kontrolnej może być umieszczone zdjęcie kontrolera;
- Na karcie przedsiębiorstwa zdjęcie nie jest wymagane.

4.4.8.2 Wprowadzanie danych o wnioskodawcy

Dane na karcie powinny być rozmieszczone zgodnie ze strukturą określoną w Rozporządzeniu [2] w Aneksie 1 C, w Załączniku nr 2, Rozdział 4 "TACHOGRAPH CARD STRUCTURE" - reguły TCS_140 - TCS_179, w zależności od rodzaju karty.

4.4.8.3 Zapisywanie kluczy na karcie

Klucz prywatny musi być zapisywany na karcie bez opuszczania środowiska, w którym został wygenerowany. Środowisko to musi być tak zabezpieczone, aby nikt nie mógł w jakikolwiek sposób dokonać niemonitorowanych czynności dotyczących kluczy prywatnych. W miarę możliwości klucze powinny być generowane na karcie lub wewnątrz HSM.

4.4.8.4 Zapisywanie certyfikatu na karcie

Certyfikat karty jest zapisywany na karcie przed jej wysłaniem do wnioskodawcy.

4.4.8.5 Kontrola jakości

Przyjęta zostanie udokumentowana procedura weryfikacji, czy informacje wizualne na wydawanej karcie i informacje elektroniczne są zgodne z danymi wejściowymi. Procedury powinny zostać opisane w PS dla PL-CP.

4.4.8.6 Unieważnienie i niszczenie niewysłanych kart

Wszystkie karty, które zostały uszkodzone podczas personalizacji (bądź z innych powodów nie zostały do prawidłowo wyprodukowane i nie zostały wysłane) są niszczone. PL-CIA prowadzi szczegółowy rejestr zniszczonych kart.

4.4.8.7 Unieważnienie i niszczenie zwróconych kart

Wszystkie karty, które zostały zwrócone PL-CIA, z wyjątkiem kart, które zostały wydane przez inne państwo członkowskie, są niszczone. PL-CIA prowadzi szczegółowy rejestr zniszczonych kart.

W przypadku zwrotu do PL-CIA karty wydanej w innym państwie członkowskim, karta ta zostanie zwrócona organowi w innym państwie członkowskim, który wydał kartę.

4.4.9 Rejestracja kart i przechowywanie danych przez PL-CP i PL-CIA

PL-CP jest odpowiedzialne za prowadzenie rejestru wydawanych poszczególnym wnioskodawcom rodzajów kart i ich numerów.

Niezbędne dane z wniosków o karty, przesyłane z PL-CIA do PL-CP celem personalizacji kart, po przedmiotowej operacji są następnie usuwane z zasobów PL-CP.

PL-CIA będzie również prowadzić aktualny rejestr statusów kart.

PL-CIA prowadzi ewidencję kart wydanych, wznowionych, zamienionych i wymienionych, skradzionych, utraconych i uszkodzonych przez okres co najmniej równy okresowi ich ważności administracyjnej.

4.4.10 Wysyłanie karty wnioskodawcy

PL-CIA jest zobowiązany do wysyłania kart wnioskodawcom. PL-CIA zapewni, by:

- Personalizacja była tak zorganizowana, aby maksymalnie skrócić czas, przez który spersonalizowana karta musi być przechowywana w bezpiecznym miejscu przed dostarczeniem wnioskodawcy. Poza godzinami pracy karty mogą być przechowywane wyłącznie w bezpiecznym środowisku. Wdrożone zostaną formalne procedury dla sytuacji wyjątkowych, w tym zakłóceń w procesie produkcyjnym, nieudanego dostarczenia karty wnioskodawcy, jej utraty lub uszkodzenia.
- Spersonalizowane karty były przesyłane do odpowiedniego miejsca, skąd zostaną dostarczone lub wysłane wnioskodawcy.

The PL-CP zawsze przechowuje oddzielnie karty spersonalizowane i karty niespersonalizowane.

4.4.11 Kody uwierzytelnienia (PIN)

PL-CP odpowiada za wytwarzanie osobistego numeru identyfikacyjnego (PIN) do każdej karty warsztatowej.

4.4.11.1 Generowanie kodów PIN

Kody PIN są generowane w bezpiecznym systemie i bezpiecznie przesyłane do wnioskodawców kart warsztatowych. Ich długość nie przekracza 8 bajtów. W przypadku używania kodów PIN krótszych niż 8 bajtów, prawa strona kodu powinna być uzupełniona o "FF" do pełnych 8 bajtów (Rozporządzenie [2] Aneks 1 C, Dodatek 1, Rozdział 2, punkt 238).

4.4.11.2 Dystrybucja kodów PIN

Kody PIN i karty warsztatowe nie mogą być wysyłane w tej samej kopercie.

PL-CP będzie wysyłać kody PIN technikom warsztatu pocztą za potwierdzeniem odbioru.

Karty warsztatowe będą wysyłane wnioskodawcom kart warsztatowych pocztą za potwierdzeniem odbioru.

4.4.12 Dezaktywacja karty

W przypadku zwrotu karty do PL-CIA, informacja o tym zostanie przekazana do CIA w innych państwach członkowskich – w razie potrzeby i na zasadach „do wiadomości".

W przypadku zwrotu do PL-CIA karty wydanej w innym państwie członkowskim, karta ta zostanie zwrócona organowi w innym państwie członkowskim, który wydał kartę wraz z odpowiednią informacją o powodach zwrotu karty.

4.5 Zarządzanie kluczami

Ten rozdział zawiera postanowienia dotyczące zarządzania kluczami wymienionymi poniżej:

- Europejski klucz główny (klucz publiczny ERCA - EUR.PK);
- Klucze państwa członkowskiego, tj. para kluczy podpisujących państwa członkowskiego (MS.SK, MS.PK);
- Symetryczne klucze główne to jest: klucz główny czujnika ruchu (K_M), klucz główny czujnika ruchu – część WC (K_{M-WC}) i klucz główny DSRC (K_{DSRC}).
- Klucze transportowe.

Klucz publiczny ERCA jest używany do weryfikacji certyfikatów PL-MSCA. Klucz prywatny ERCA nie jest omawiany w niniejszym dokumencie, ponieważ nigdy nie opuszcza ERCA.

Klucze PL-MSCA są kluczami służącymi do podpisywania certyfikatów urządzeń.

Klucze symetryczne są umieszczane na karcie warsztatowej i w tachografie. PL-MSCA odbiera klucze symetryczne z ERCA, przechowuje je i dystrybuuje do PL-CP. Poza tym klucze symetryczne są używane do szyfrowania informacji umieszczonych w czujniku ruchu.

Klucze transportowe służą do zapewnienia bezpieczeństwa wymiany informacji po między ERCA i PL-MSCA oraz po między PL-MSCA i producentami czujników ruchu.

Jeśli PL-MSCA potrzebuje innych kluczy kryptograficznych oprócz powyższych, nie będą one traktowane jako część systemu Inteligentnego Tachografu i nie podlegają Polityce PL-MSA.

4.5.1 Klucz publiczny ERCA

PL-CP oraz PL-MSCA zawsze przechowują klucz publiczny ERCA (EUR.PK) w sposób gwarantujący utrzymanie jego integralności i dostępności w każdej chwili. PL-CP zapewnia, by certyfikat klucza EUR.PK był zapisywany na wszystkich kartach.

4.5.2 Klucze PL-MSCA

Klucze państwa członkowskiego (klucze PL-MSCA) służą do podpisywania certyfikatów wydawanych dla urządzeń drugiej generacji. Na potrzeby obsługi tych urządzeń PL-MSCA posiada następujący typ pary kluczy oraz powiązanych certyfikatów:

- MSCA_Card - służy do podpisywania certyfikatów dla kart do tachografów.

Klucze publiczne PL-MSCA są zawsze generowane przez PL-MSCA i muszą być certyfikowane przez ERCA.

Klucze państwa członkowskiego nie mogą być wykorzystywane do żadnych innych celów niż podpisywanie certyfikatów urządzeń do tachografów oraz generowanie wniosków o podpisanie certyfikatu (CSR).

4.5.2.1 Generowanie kluczy PL-MSCA

Para kluczy PL-MSCA powinna być wygenerowana i używana w godnym zaufania dedykowanym urządzeniu HSM (Hardware Security Module), które:

- posiada certyfikat EAL 4 lub wyższy zgodnie ze wymaganiami Common Criteria określonymi w normie ISO / IEC 15408 [8] dla odpowiedniego profilu ochrony (Protection Profile); lub
- spełnia wymagania określone w ISO / IEC 19790 [10] poziom 3; lub
- spełnia wymagania określone w FIPS PUB 140-2 poziom 3 [13]; lub
- zapewnia równoważny poziom bezpieczeństwa zgodnie z równoważnymi krajowymi lub międzynarodowymi kryteriami oceny bezpieczeństwa IT.

Obecnie użytkowane urządzenie i wymagania, które ono spełnia zostaną określone w PL-MSCA CPS.

Generowanie pary kluczy państwa członkowskiego powinno odbywać się w fizycznie zabezpieczonym środowisku. Generowanie pary kluczy PL-MSCA wymaga aktywnego udziału co najmniej dwóch oddzielnych osób pełniących zaufane role.

Klucze do pierwszej generacji systemu cyfrowego tachografu muszą być generowane przy użyciu algorytmu RSA, a długość klucza powinna wynosić 1024 bity.

Klucze do drugiej generacji systemu tachografu cyfrowego (Inteligentnego Tachografu) muszą być generowane przy użyciu algorytmu opartego na krzywych eliptycznych (ECC), a długość klucza powinna wynosić 256 bitów lub 384 bity lub 512/521 bitów.

PL-MSCA powinno posiadać jednocześnie odpowiednią liczbę par kluczy PL-MSCA, z odpowiednimi certyfikatami podpisów elektronicznych, aby zapewnić odpowiedni poziom ciągłości działania procesu certyfikacji, przy założeniu, że proces certyfikacji kluczy dla państwa członkowskiego realizowany przez ERCA nie jest wykonywany natychmiast.

4.5.2.2 Okres ważności kluczy PL-MSCA

Okres ważności klucza prywatnego PL-MSCA nie może być dłuższy niż 2 lata od daty wydania jego certyfikatu przez ERCA. Po upływie tego okresu klucz nie możne być używany.

Odpowiedni klucz publiczny jest ważny w okresie ważności odpowiedniego certyfikatu.

Certyfikaty wydawane przez ERCA są ważne:

- MSCA_Card - 7 lat i 1 miesiąc.

4.5.2.3 Przechowywanie kluczy prywatnych PL-MSCA

Para kluczy PL-MSCA powinna być osadzona i obsługiwana wewnątrz specjalnego urządzenia odpornego na manipulacje - HSM (Hardware Security Module), które:

- posiada certyfikat EAL 4 lub wyższy zgodnie ze wymaganiami Common Criteria określonymi w normie ISO / IEC 15408 [8] dla odpowiedniego profilu ochrony (Protection Profile); lub
- spełnia wymagania określone w ISO / IEC 19790 [10] poziom 3; lub
- spełnia wymagania określone w FIPS PUB 140-2 poziom 3 [13]; lub
- zapewnia równoważny poziom bezpieczeństwa zgodnie z równoważnymi krajowymi lub międzynarodowymi kryteriami oceny bezpieczeństwa IT.

4.5.2.4 Kopia zapasowa kluczy prywatnych PL-MSCA

Kopie zapasowe kluczy prywatnych PL-MSCA można wykonać przy użyciu procedury archiwizacji, która wymaga obecności co najmniej dwóch osób pełniących zaufane role w

środowisku o wysokim poziomie bezpieczeństwa fizycznego. Zastosowana procedura archiwizacji powinna być podana w PL-MSCA CPS.

Wszelkie kopie kluczy prywatnych PL-MSCA podlegają takiemu samemu poziomowi zabezpieczeń, jak klucze używane.

Klucze prywatne PL-MSCA mogą być importowane lub eksportowane tylko do celów tworzenia kopii zapasowych lub odzyskiwania.

4.5.2.5 Deponowanie klucza prywatnego PL-MSCA

Klucze prywatne PL-MSCA nie mogą być deponowane.

4.5.2.6 Kompromitacja kluczy PL-MSCA

Powinna istnieć pisemna instrukcja zawarta w PL-MSCA CPS, która określa środki, które mają być podjęte przez osoby odpowiedzialne za bezpieczeństwo w PL-MSCA, gdy klucze prywatne PL-MSCA zostaną ujawnione lub w inny sposób uznane lub podejrzane o to, że zostały skompromitowane.

W takim przypadku PL-MSCA musi niezwłocznie, w ciągu nie więcej niż 8 godzin od wykrycia, poinformować PL-MSA i ERCA, zainicjować niezbędne śledztwo i wdrożyć działania wskazane przez PL-MSA. Wyniki dochodzenia powinny być przekazane do ERCA.

Jeśli klucz jest skompromitowany lub nie można tego wykluczyć, wszystkie klucze prywatne oraz ich kopie powinny zostać zniszczone w taki sposób, aby nie można było ich odzyskać.

Jeśli to możliwe, do zniszczenia kluczy prywatnych należy użyć dedykowanej funkcji urządzenia HSM.

4.5.2.7 Wycofanie z użytku kluczy PL-MSCA

PL-MSCA wdroży procesy gwarantujące ciągłą dostępność ważnych, certyfikowanych przez ERCA pary kluczy PL-MSCA.

Po zakończeniu korzystania z kluczy PL-MSCA, jego klucz publiczny zostanie zarchiwizowany, a klucz prywatny będzie zniszczony w taki sposób, aby nie można go było odtworzyć.

Jeśli to możliwe, do zniszczenia kluczy prywatnych należy użyć dedykowanej funkcji urządzenia HSM.

4.5.3 Symetryczne klucze główne

W ramach systemu Inteligentnego Tachografu są wykorzystywane symetryczne klucze główne, które służą do parowania tachografów (VU) i czujników ruchu (MoS), wzajemnego uwierzytelniania między VU i MoS, a także do szyfrowania komunikacji między VU i MoS.

PL-MSCA:

- przekazuje w bezpieczny sposób klucz $K_{M\text{-}WC}$ do PL-CP, aby był on instalowany na kartach warsztatowych,
- przekazuje w bezpieczny sposób klucz K_{DSRC} do PL-CP, aby był on instalowany na kartach warsztatowych i kontrolnych,
- używa klucza głównego czujnika ruchu (K_M) do szyfrowania kluczy parowania czujnika ruchu (K_P) na wniosek producentów czujników ruchu,
- wyprowadza klucz identyfikacyjny czujnika ruchu (K_{ID}) z K_M, który następnie wykorzystuje do szyfrowania numerów seryjnych czujników ruchu na wniosek producentów czujników ruchu.

PL-CP:

- zapewnia, że klucz warsztatowy $K_{M\text{-}WC}$ jest umieszczony na wszystkich wydanych kartach warsztatowych (Załącznik IC, Dodatek 11, Rozdział 9, Punkt 9.2

do Rozporządzenia [2]),

- zapewnia, że klucz warsztatowy K_{DSRC} jest umieszczony na wszystkich wydanych kartach warsztatowych i kontrolnych (Załącznik IC, Dodatek 11, Rozdział 9, Punkt 9.2 do Rozporządzenia [2]).

Symetryczne klucze główne nie mogą być używane do innych celów niż wymienione w tym dokumencie polityki PL-MSA.

4.5.3.1 Generacja symetrycznych kluczy głównych

Symetryczne klucze główne są zawsze generowane i dystrybuowane przez ERCA. PL-MSCA w razie potrzeby wnioskuje o symetryczne klucze główne K_M, K_{M-WC} do ERCA (Rozporządzenie [6], Rozporządzenie [2]).

Klucze do pierwszej generacji systemu tachografów cyfrowych muszą być generowane przy użyciu algorytmu TDES, a efektywna długość klucza powinna wynosić 112 bitów (całkowita długość 128 bitów).

Klucze do drugiej generacji systemu tachografu cyfrowego muszą być generowane przy użyciu algorytmu AES, a długość klucza powinna wynosić 128 bitów lub 192 bity lub 256 bitów.

PL-MCSA powinno posiadać jednocześnie odpowiednią liczbę symetrycznych kluczy głównych tak, aby zapewnić odpowiedni poziom ciągłości usług, które realizuje w odniesieniu do okresu ważności kluczy.

4.5.3.2 Okres ważności symetrycznych kluczy głównych

Okres ważności symetrycznych kluczy głównych nie może być dłuższy niż 17 lat od daty wydania przez ERCA. Po tym okresie klucz prywatny nie może być używany.

4.5.3.3 Przechowywanie symetrycznych kluczy głównych

PL-MSCA i PL-CP chronią symetryczne klucze główne z zastosowaniem skutecznych logicznych i fizycznych zabezpieczeń.

Klucze powinny być osadzone i obsługiwane wewnątrz specjalnego urządzenia odpornego na manipulacje - HSM (Hardware Security Module), które:

- posiada certyfikat EAL 4 lub wyższy zgodnie ze wymaganiami Common Criteria określonymi w normie ISO / IEC 15408 [8] dla odpowiedniego profilu ochrony (Protection Profile); lub
- spełnia wymagania określone w ISO / IEC 19790 [10] poziom 3; lub
- spełnia wymagania określone w FIPS PUB 140-2 poziom 3 [13]; lub
- zapewnia równoważny poziom bezpieczeństwa zgodnie z równoważnymi krajowymi lub międzynarodowymi kryteriami oceny bezpieczeństwa IT.

4.5.3.4 Kopia zapasowa symetrycznych kluczy głównych

Kopie zapasowe symetrycznych kluczy głównych można wykonać przy użyciu procedury archiwizacji, która wymaga obecności co najmniej dwóch osób pełniących zaufane role w środowisku o wysokim poziomie bezpieczeństwa fizycznego. Zastosowana procedura archiwizacji powinna być podana w PL-MSCA CPS.

Wszelkie kopie symetrycznych kluczy głównych podlegają temu samemu poziomowi zabezpieczeń, jak klucze używane.

Eksport kluczy K_{M-WC} i K_{DSRC} (K_VUDSRC_ENC, K_VUDSRC_MAC - klucze VU specyficzne dla DSR) jest dozwolony tylko w postaci zaszyfrowanej w odpowiedzi na wniosek o wydanie klucza wysłany przez PL-CP do PL-MSCA.

Oprócz wyżej wymienionych przypadków symetryczne klucze główne mogą być importowane lub eksportowane tylko do celów tworzenia kopii zapasowych lub odzyskiwania.

Procedura eksportu w obu wyżej wymienionych kluczy wymaga obecności co najmniej dwóch osób pełniących zaufane role.

4.5.3.5 Deponowanie symetrycznych kluczy głównych

Symetryczne klucze główne nie mogą być deponowane.

4.5.3.6 Kompromitacja symetrycznych kluczy głównych

Powinna istnieć pisemna instrukcja, zawarta w PL-MSCA CPS, która określa środki, które mają być podjęte przez osoby odpowiedzialne za bezpieczeństwo w PL-MSCA, gdy symetryczne klucze główne zostaną ujawnione lub w inny sposób uznane lub podejrzane o to, że zostały skompromitowane.

W takim przypadku PL-MSCA musi niezwłocznie, w ciągu nie więcej niż 8 godzin od wykrycia, poinformować PL-MSA i ERCA, zainicjować niezbędne śledztwo i wdrożyć działania wskazane przez PL-MSA. Wyniki dochodzenia powinny być przekazane do ERCA.

Jeśli klucz jest skompromitowany lub nie można tego wykluczyć, wszystkie symetryczne klucze główne oraz ich kopie powinny zostać zniszczone w taki sposób, aby nie można było ich odzyskać.

Jeśli to możliwe, do zniszczenia symetrycznych kluczy głównych należy użyć dedykowanej funkcji urządzenia HSM.

4.5.3.7 Wycofanie z użytku symetrycznych kluczy głównych

PL-MSCA wdroży procesy gwarantujące ciągłą dostępność ważnych symetrycznych kluczy głównych wydanych przez ERCA.

Po zakończeniu korzystania z symetrycznych kluczy głównych powinny być one zniszczone w taki sposób, aby nie można ich było odtworzyć.

Jeśli to możliwe, do zniszczenia symetrycznych kluczy głównych należy użyć dedykowanej funkcji urządzenia HSM.

4.5.4 Klucze transportowe

Aby zapewnić bezpieczną komunikację między ERCA i PL-MSCA, powinien być używany zintegrowany schemat szyfrowania eliptycznego (ang. *Elliptic Curve Integrated Encryption Scheme, ECIES*) (rozdział 4.2.3 Polityki ERCA [6]).

Do transportu kluczy między PL-MSCA a ERCA muszą być zawsze wykorzystywane środki, nośniki i protokoły zdefiniowane w Polityce ERCA [6]. Jeśli do transportu kluczy są wykorzystywane nośniki fizyczne, PL-MSA wyznacza upoważnioną osobę do przewozu nośników.

W przypadku certyfikacji klucza PL-MSCA stosuje CSR określony w Polityce ERCA [6].

PL-MSCA akceptuje klucz publiczny ERCA w formacie dystrybucyjnym opisanym w polityce ERCA [6].

PL-MSCA powinno wnioskować o symetryczny klucz główny od ERCA przy użyciu KDR określonego w polityce ERCA [6]. PL-MSCA otrzymuje symetryczny klucz główny w KDM zgodnie z Polityką ERCA [6].

Aby zapewnić bezpieczną komunikację między PL-MSCA i PL-CP lub podmiotami

personalizującymi urządzenia, poziom zastosowanych zabezpieczeń kryptograficznych powinien być adekwatny do transportowanych kluczy oraz zaszyfrowanych danych. Algorytmy używane w tych przypadkach są opisane w PL-MSCA CPS i odpowiedniej deklaracji praktyk - PS.

4.5.4.1 Generowanie kluczy transportowych

Klucze transportowe PL-MSCA będą generowane i używane w godnym zaufania dedykowanym urządzeniu HSM (Hardware Security Module), które:

- posiada certyfikat EAL 4 lub wyższy zgodnie ze wymaganiami Common Criteria określonymi w normie ISO / IEC 15408 [8] dla odpowiedniego profilu ochrony (Protection Profile); lub
- spełnia wymagania określone w ISO / IEC 19790 [10] poziom 3; lub
- spełnia wymagania określone w FIPS PUB 140-2 poziom 3 [13]; lub
- zapewnia równoważny poziom bezpieczeństwa zgodnie z równoważnymi krajowymi lub międzynarodowymi kryteriami oceny bezpieczeństwa IT.

Obecnie użytkowane urządzenie i wymagania, które ono spełnia zostaną określone w PL-MSCA CPS.

4.5.4.2 Okres ważności kluczy transportowych

Okres ważności kluczy transportowych powinien odpowiadać wymaganiom zadania wykonywanego przy ich użyciu. Po tym okresie klucze transportowe nie mogą być używane.

4.5.4.3 Przechowywanie kluczy transportowych

PL-MSCA chroni klucze transportowe z zastosowaniem skutecznych logicznych i fizycznych zabezpieczeń. Klucze powinny być osadzone i obsługiwane wewnątrz specjalnego urządzenia odpornego na manipulacje - HSM (Hardware Security Module), które:

- posiada certyfikat EAL 4 lub wyższy zgodnie ze wymaganiami Common Criteria określonymi w normie ISO / IEC 15408 [8] dla odpowiedniego profilu ochrony (Protection Profile); lub
- spełnia wymagania określone w ISO / IEC 19790 [10] poziom 3; lub
- spełnia wymagania określone w FIPS PUB 140-2 poziom 3 [13]; lub
- zapewnia równoważny poziom bezpieczeństwa zgodnie z równoważnymi krajowymi lub międzynarodowymi kryteriami oceny bezpieczeństwa IT.

4.5.4.4 Kopia zapasowa kluczy transportowych

Kopie zapasowe kluczy transportowych można wykonać przy użyciu procedury archiwizacji, która wymaga obecności co najmniej dwóch osób pełniących zaufane role w środowisku o wysokim poziomie bezpieczeństwa fizycznego. Zastosowana procedura archiwizacji powinna być podana w PL-MSCA CPS.

Wszelkie kopie kluczy transportowych podlegają temu samemu poziomowi zabezpieczeń, jak klucze używane.

4.5.4.5 Deponowanie kluczy transportowych

Klucze transportowe nie mogą być deponowane.

4.5.4.6 Kompromitacja kluczy transportowych

Powinna istnieć pisemna instrukcja, zawarta w PL-MSCA CPS, która określa środki, które mają być podjęte przez osoby odpowiedzialne za bezpieczeństwo w PL-MSCA, gdy klucze transportowe zostaną ujawnione lub w inny sposób uznane lub podejrzane o to, że zostały skompromitowane.

W takim przypadku PL-MSCA musi niezwłocznie, w ciągu nie więcej niż 8 godzin od wykrycia, poinformować PL-MSA i ERCA, zainicjować niezbędne śledztwo i wdrożyć działania wskazane

przez PL-MSA. Wyniki dochodzenia powinny być przekazane do ERCA.

Jeśli klucz jest skompromitowany lub nie można tego wykluczyć, wszystkie klucze transportowe oraz ich kopie powinny zostać zniszczone w taki sposób, aby nie można było ich odzyskać.

Jeśli to możliwe, do zniszczenia kluczy transportowych należy użyć dedykowanej funkcji urządzenia HSM.

4.5.4.7 Wycofanie z użytku kluczy transportowych

Po zakończeniu korzystania z kluczy transportowych powinny być one zniszczone w taki sposób, aby nie można odtworzyć ich kluczy prywatnych.

Jeśli to możliwe, do zniszczenia kluczy transportowych należy użyć dedykowanej funkcji urządzenia HSM.

4.5.5 Klucze urządzeń

Klucze urządzeń to symetryczne lub asymetryczne klucze generowane lub uzyskiwane z innych kluczy przez producenta urządzenia lub PL-MSCA lub PL-CP. Klucze asymetryczne są certyfikowane przez PL-MSCA. Poniższa tabela przedstawia urządzenia i typy przechowywanych na nich kluczy.

Urządzenie / Klucz	**Symetryczny**	**Asymetryczny**
Karta do tachografu (karta kierowcy)	---	Card_MA, Card_Sign
Karta do tachografu (karta firmowa)	---	Card_MA
Karta do tachografu (karta kontrolna)	K_{DSRC}	Card_MA
Karta do tachografu (karta warsztatowa)	K_{M-WC}, K_{DSRC}	Card_MA, Card_Sign
Czujnik ruchu (MoS)	K_P	---

Tabela 7 Klucze urządzeń

Aby zachować kompatybilność wsteczną, klucze wymagane dla urządzeń pierwszej generacji są również przechowywane w urządzeniach drugiej generacji.

4.5.5.1 Aspekty ogólne

Inicjowanie kart, ładowanie kluczy i personalizacja odbywają się w fizycznie zabezpieczonym i kontrolowanym środowisku. Wstęp do tego obszaru jest ściśle regulowany, kontrolowany na poziomie personalnym, a obsługa systemu wymaga obecności przynajmniej dwóch osób. Jest prowadzony dziennik wejść i czynności wykonywanych w tych systemach.

Żadne poufne informacje zawarte w systemach generowania kluczy nie mogą ich opuścić w sposób naruszający Politykę PL-MSA.

Żadne poufne informacje zawarte w systemach personalizacji kart nie mogą ich opuścić w sposób naruszający Politykę PL-MSA.

Dziennik systemu personalizacji zawiera odniesienie do wniosku z zamówieniem wraz z listą odpowiednich certyfikatów i numerów urządzeń. Dzienniki są dostępne na żądanie PL-MSA.

4.5.5.2 Generowanie kluczy urządzeń

Klucze są generowane przez producenta urządzenia, PL-MSCA lub PL-CP. Podmiot generujący klucze musi zadbać o bezpieczeństwo sposobu generowania kluczy i utrzymanie poufności klucza prywatnego urządzenia.

Generowanie kluczy odbywa się w urządzeniu (karcie) lub w godnym zaufania dedykowanym urządzeniu HSM (Hardware Security Module), które:

- posiada certyfikat EAL 4 lub wyższy zgodnie ze wymaganiami Common Criteria określonymi w normie ISO / IEC 15408 [8] dla odpowiedniego profilu ochrony (Protection Profile); lub
- spełnia wymagania określone w ISO / IEC 19790 [10] poziom 3; lub
- spełnia wymagania określone w FIPS PUB 140-2 poziom 3 [13]; lub
- zapewnia równoważny poziom bezpieczeństwa zgodnie z równoważnymi krajowymi lub międzynarodowymi kryteriami oceny bezpieczeństwa IT.

Jeżeli generowanie kluczy prywatnych lub symetrycznych jest realizowane w urządzeniu, to działalność ta powinna być objęta certyfikacją bezpieczeństwa urządzeń zapewniając, iż stosowane są publicznie określone oraz odpowiednie algorytmy generowania kluczy kryptograficznych. Typ urządzeń wykorzystywanych do generowania kluczy prywatnych lub symetrycznych powinien być podany w odpowiednich dokumentach - CPS lub PS.

Klucze symetryczne są generowane przy użyciu algorytmu AES, a klucze asymetryczne są generowane przy użyciu algorytmu ECC zgodnie z Polityką certyfikacji ERCA [6].

Procedura generowania i przechowywania klucza prywatnego powinna uniemożliwiać jego ujawnienie poza systemem, który go utworzył. Ponadto klucz prywatny należy usunąć z systemu natychmiast po zainstalowaniu go w urządzeniu.

Obowiązkiem podmiotu generującego klucze jest podjęcie odpowiednich działań w celu zapewnienia, że klucz publiczny jest unikalny we własnej domenie, zanim nastąpi powiązanie go z certyfikatem. Należy w tym celu zapewnić by system generowania kluczy działał w sposób losowy z natury, w związku z czym prawdopodobieństwo wygenerowania identycznych kluczy jest nieznaczne.

4.5.5.3 Wsadowe generowanie kluczy

Generowanie kluczy kryptograficznych może być wykonywane wsadowo lub bezpośrednio w odpowiedzi na żądanie certyfikatu.

Przetwarzanie wsadowe musi być wykonywane w wydzielonym urządzeniu. Integralność kluczy musi być chroniona do momentu wydania certyfikatu.

4.5.5.4 Ważność klucza urządzenia

4.5.5.4.1 Klucze na kartach

Użytkowanie klucza prywatnego urządzenia w połączeniu z certyfikatami wydanymi zgodnie z Polityką PL-MSA nie powinno nigdy wykraczać poza datę ważności certyfikatu.

4.5.5.5 Ochrona i przechowywanie kluczy prywatnych na karcie

PL-CP i PL-CIA zapewniają, aby klucz prywatny karty był chroniony przez kartę, która została dostarczona wnioskodawcy zgodnie z procedurami określonymi w Polityce PL-MSA.

Kopie klucza prywatnego nie mogą być przechowywane gdziekolwiek indziej poza kartą, chyba że jest to wymagane podczas generowania klucza i personalizacji urządzenia.

W żadnym przypadku klucz prywatny karty nie może zostać ujawniony ani być przechowywany

poza kartą.

4.5.5.6 Deponowanie i archiwizacja kluczy prywatnych urządzenia

Kluczy prywatnych urządzenia nie można deponować ani archiwizować.

4.5.5.7 Archiwizacja klucza publicznego urządzenia

Wszystkie certyfikowane klucze publiczne są archiwizowane przez PL-MSCA na czas określony w CPS PL-MSCA.

4.5.5.8 Wycofanie z użytku kluczy urządzenia

Po zakończeniu korzystania z karty klucz publiczny jest archiwizowany, a klucz prywatny jest niszczony w taki sposób, aby nie można było go odzyskać.

4.6 Zarządzanie certyfikatami urządzeń

W tym rozdziale opisano cykl życia certyfikatu, który obejmuje funkcję rejestracji, wystawienie certyfikatu, dystrybucję, użytkowanie, anulowanie (jeśli ma zastosowanie) oraz wycofanie z użytku.

PL-MSCA CPS i PL-CP PS powinny opisać pełne procedury składania wniosków o certyfikaty dla urządzeń.

4.6.1 Karty

4.6.1.1 Wprowadzanie danych

Posiadacze kart nie składają wniosków o certyfikaty. Certyfikaty są wystawiane na podstawie informacji zawartych we wniosku o wydanie karty.

PL-CP zapewnia, aby dane wejściowe zawierały informacje sprawiające, że identyfikator posiadacza karty (CHR, Certificate Holder Reference) jest unikalny. Podmiot PL-MSCA weryfikuje unikalność każdego identyfikatora CHR w swojej domenie.

4.6.1.2 Certyfikaty dla kart

Certyfikaty kart kierowcy, warsztatowych, kontrolnych i przedsiębiorstwa są wystawiane dopiero po zatwierdzeniu przez PL-CIA wniosku o wydanie karty.

4.6.1.3 Okres ważności certyfikatów dla kart

Karta kierowcy będzie zawierać certyfikaty z następującymi okresami ważności:

- certyfikat Card_Ma – 5 lat,
- certyfikat Card_Sign – 5 lat + 1 miesiąc.

Karta warsztatowa będzie zawierać certyfikaty z następującymi okresami ważności:

- certyfikat Card_Ma – 1 rok,
- certyfikat Card_Sign – 1 rok + 1 miesiąc.

Karta firmowa będzie zawierać certyfikaty z następującymi okresami ważności:

- certyfikat Card_Ma – 5 lat.

Karta kontrolna będzie zawierać certyfikaty z następującymi okresami ważności:

- certyfikat Card_Ma – 2 lata.

Data wejścia w życie certyfikatów Card_Ma i Card_Sign musi być równa początkowi ważności samej karty do tachografów, zakodowanej w pliku przechowywanym na kracie EF_Identification.

Okres ważności certyfikatów nie może być dłuższy niż okres ważności urządzenia.

Data wejścia w życie pary certyfikatów Card_Ma i Card_Sign odpowiedniej karty kierowcy lub karty warsztatowej musi być taka sama.

Aby zachować kompatybilność wsteczną na kartach drugiej generacji, przechowywane są certyfikaty wymagane dla kart pierwszej generacji.

4.6.1.4 Wystawianie certyfikatów dla kart

Wystawianie certyfikatów przez PL-MSCA odbywa się w sposób zapewniający zachowanie ich autentyczności i integralności. Treść certyfikatu jest zdefiniowana w polityce certyfikacji ERCA [6] i Rozporządzeniu [2] (Załącznik 1C, Dodatek 11 i 1).

PL-MSCA i PL-CP powinny weryfikować pochodzenie i integralność wniosków o certyfikat. Mechanizmy weryfikacji pochodzenia i kontroli integralności nie mogą opierać się na procedurach, które spowodowałyby ujawnienie kluczy prywatnych.

4.6.1.5 Wznawianie i aktualizacja certyfikatu karty

Zostało opisane w rozdziale dotyczącym zarządzania urządzeniami. Ponieważ okres ważności certyfikatów i kart jest taki sam, są one omawiane łącznie.

4.6.1.6 Rozpowszechnianie informacji o certyfikatach karty

PL-CIA zapewni, że informacje o certyfikatach zostaną udostępnione w razie potrzeby posiadaczowi karty i odpowiednim podmiotom.

4.6.1.7 Użytkowanie certyfikatu karty

Certyfikaty z kart są przeznaczone wyłącznie do użytku w systemie Inteligentnego Tachografu.

4.6.1.8 Unieważnienie certyfikatu karty

Mimo iż Polityka PL-MSA nie określa żadnych zasad dotyczących unieważniania certyfikatów kart, to PL-CIA rejestruje szczegóły dotyczące kart, które zostały utracone, zgłoszone jako skradzione, zniszczone lub z innych przyczyn nie są już w użytku. Informacje z tego rejestru będą udostępniane odpowiednim podmiotom i innym Państwom Członkowskim na żądanie.

5. Zarządzanie bezpieczeństwem informacji

W niniejszym rozdziale opisano wymagania dotyczące zabezpieczenia informacji nakładane przez Politykę PL-MSA.

5.1 Kontrola bezpieczeństwa fizycznego

Usługi generowania kluczy i certyfikatów powinny być umieszczane w bezpiecznej strefie, chronionej określonym obwodem bezpieczeństwa wyposażonym w odpowiednie bariery bezpieczeństwa i kontrolę wejścia, aby zapobiegać nieautoryzowanemu dostępowi, uszkodzeniom oraz zakłóceniom.

Nośniki pamięci używane do przechowywania informacji poufnych, takich jak dyski twarde, karty inteligentne i HSM, są chronione przed nieuprawnionym lub niezamierzonym użyciem, dostępem, ujawnieniem lub uszkodzeniem przez ludzi lub inne zagrożenia (np. ogień, woda).

W celu uniknięcia nieuprawnionego użycia, dostępu lub ujawnienia poufnych danych należy wdrożyć procedury usuwania odpadów.

Powinna zostać wdrożona procedura tworzenia kopii zapasowych poza lokalizacją podstawową dla krytycznych danych PL-MSCA.

5.1.1 Klasyfikacja i zarządzanie zasobami PL-MSCA oraz podmiotów personalizujących urządzenia

PL-MSCA i podmioty personalizujące urządzenia zapewnią odpowiedni poziom ochrony swoich zasobów i informacji. W szczególności:

- PL-MSCA i podmioty personalizujące urządzenia przeprowadzają ocenę ryzyka w celu oszacowania elementów ryzyka i określenia niezbędnych wymagań w zakresie bezpieczeństwa i procedur operacyjnych;
- PL-MSCA i podmioty personalizujące urządzenia prowadzą rejestr zasobów informacji i klasyfikują je na potrzeby wymagań w zakresie ochrony zgodnie z analizą ryzyka.

5.1.2 Mechanizmy zabezpieczeń systemu PL-MSCA oraz podmiotów personalizujących urządzenia

PL-MSCA oraz podmioty personalizujące urządzenia zapewnią bezpieczeństwo systemów i prawidłową ich eksploatację przy jak najmniejszym ryzyku awarii. W szczególności:

- Integralność systemów i informacji jest chroniona przed wirusami oraz szkodliwymi i nieautoryzowanymi programami;
- Zakres szkód wyrządzanych przez incydenty i wadliwe działanie są minimalizowane przez raportowanie incydentów i procedury interwencyjne.

5.1.3 Fizyczne mechanizmy zabezpieczeń PL-MSCA oraz podmiotów personalizujących urządzenia

W celu kontroli dostępu do sprzętu i oprogramowania PL-MSCA lub podmiotów personalizujących urządzenia wdrażane są fizyczne mechanizmy zabezpieczeń. Obejmują one stacje robocze i inne elementy PL-MSCA oraz infrastrukturę sprzętową personalizacji, karty lub moduły dowolnego zewnętrznego urządzenia szyfrującego.

Klucze PL-MSCA do podpisywania certyfikatów są fizycznie i logicznie chronione w sposób opisany w deklaracji praktyk - PS.

W ośrodku PL-MSCA/podmiotu personalizującego urządzenia jest również miejsce na przechowywanie kopii zapasowych i nośników dystrybucyjnych w sposób zapobiegający

utracie przechowywanych informacji, manipulowaniu nimi lub ich wykorzystaniu bez zezwolenia. Kopie zapasowe są przechowywane zarówno na potrzeby odtwarzania danych, jak i archiwizacji ważnych informacji.

5.1.3.1 Dostęp fizyczny

Dostęp do pomieszczeń PL-MSCA oraz podmiotów personalizujących urządzenia mają wyłącznie osoby pełniące jedną z ról opisanych w rozdziale 5.3. Dostęp jest kontrolowany przez zastosowanie listy kontroli dostępu do pomieszczenia z ich systemami.

5.2 Kontrole proceduralne

Aby zapewnić bezpieczeństwo operacji, należy wdrożyć kontrole proceduralne. Rozdzielenie obowiązków będzie wymuszone poprzez wdrożenie kontroli wieloosobowej dla krytycznych zadań.

Dostęp do systemów PL-MSCA oraz podmiotów personalizujących urządzenia jest ograniczony do osób, które są poprawnie zautoryzowane i na zasadzie niezbędnej wiedzy. W szczególności obowiązują następujące środki kontroli dostępu:

- Poufne dane[1] są chronione, aby zabezpieczyć ich integralność i poufność podczas przechowywania;
- Poufne dane są chronione, aby zabezpieczyć ich integralność i poufność w przypadku przesyłania ich przez niezabezpieczone sieci;
- Poufne dane do usunięcia są trwale niszczone, np. przez wielokrotne nadpisywanie losowymi danymi;
- Systemy PL-MSCA i podmiotów personalizujących urządzenia zapewniają efektywne zarządzanie użytkownikami oraz zarządzanie dostępem;
- Systemy PL-MSCA i podmiotów personalizujących urządzenia zapewniają, że dostęp do informacji oraz funkcji systemu jest ograniczony do upoważnionego personelu, a także zapewnia wystarczającą kontrolę bezpieczeństwa komputerowego w celu zapewnienia rozdzielenia zaufanych ról. W szczególności stosowanie programów narzędziowych systemu powinno być ograniczone i ściśle kontrolowane. Dostęp będzie ograniczony, zezwalając jedynie na dostęp do zasobów niezbędnych do wykonywania roli przypisanej użytkownikowi;
- Personel PL-MSCA oraz personel podmiotów personalizujących urządzenia jest identyfikowany i uwierzytelniany przed użyciem systemów;
- Personel PL-MSCA oraz personel podmiotów personalizujących urządzenia jest odpowiedzialny za swoje działania, które są rejestrowane w dziennikach zdarzeń, jak opisano w sekcji 5.4.

PL-MSCA i podmioty personalizujące urządzenia ustanowią system zarządzania bezpieczeństwem informacji (ISMS) w oparciu o ocenę ryzyka dla wszystkich realizowalnych operacji. PL-MSCA i podmioty personalizujące urządzenia zapewnią, że zasady ISMS będą dotyczyć szkolenia personelu, uprawnień i ról. Implementacje ISMS w PL-MSCA oraz w podmiotach personalizujących urządzenia powinny być zgodne z wymaganiami opisanymi w ISO / IEC 27001 [14].

PL-MSCA oraz podmioty personalizujące urządzenia ponoszą odpowiedzialność za wszystkie aspekty świadczenia usług certyfikacji klucza, nawet jeśli część tych funkcji zlecają podwykonawcom. PL-MSCA oraz podmioty personalizujące urządzenia wyraźnie określają zakres

[1] Dane, które należy uznać za poufne, określono w sekcji **Błąd! Nie można odnaleźć źródła odwołania.**.

odpowiedzialności stron trzecich i podejmują należyte starania, aby strony trzecie były zobowiązane do wdrożenia wszelkich mechanizmów kontroli wymaganych przez PL-MSCA oraz podmioty personalizujące urządzenia. PL-MSCA oraz podmioty personalizujące urządzenia są zobowiązane do ujawnienia odpowiednich deklaracji praktyk (PS) wszystkim zainteresowanym.

PL-MSCA oraz podmioty personalizujące urządzenia przez cały czas utrzymują infrastrukturę bezpieczeństwa informacji niezbędną do zarządzania bezpieczeństwem. Wszelkie zmiany wpływające na poziom bezpieczeństwa są zatwierdzane przez PL-MSA.

5.3 Kontrola personelu

PL-MSCA oraz podmioty personalizujące urządzenia realizując Politykę PL-MSA, powinni rozróżniać trzy osobne role, jak opisano poniżej. Zaufane role, od których zależy bezpieczeństwo operacji, powinny być jasno określone i szczegółowo opisane w odpowiednim PL-MSCA CPS lub deklaracjach praktyk (PS) podmiotów personalizujących urządzenia. Te role i związane z nimi obowiązki powinny być udokumentowane w opisach stanowisk. Wskazane opisy stanowisk pracy powinny być określone z punktu widzenia rozdzielenia obowiązków i niezbędnych przywilejów. Żadna osoba nie może być upoważniona do jednoczesnego wykonywania więcej niż jednej z zaufanych ról.

Aby upewnić się, że jedna osoba działająca samodzielnie nie może obejść zabezpieczeń, obowiązki w systemach PL-MSCA oraz podmiotów personalizujących urządzenia muszą być wykonywane przez wiele ról i osób. Każde konto w systemach ma ograniczone możliwości, właściwe dla roli posiadacza konta.

Role są następujące:

- Administrator Centrum Certyfikacji lub Administrator Personalizacji;
- Administrator Systemu;
- Kierownik ds. Bezpieczeństwa Systemów Informacyjnych.

Dla PL-MSCA oraz podmiotów personalizujących urządzenia różne osoby wypełniają każdą z trzech ról opisanych powyżej i co najmniej jedna osoba musi zostać wskazana do wykonania jednego zadania.

Cały personel zaangażowany w PL-MSCA oraz w podmiotach personalizujących urządzenia musi być odpowiednio przeszkolony, posiadać specjalistyczną wiedzę, doświadczenie, a także kwalifikacje niezbędne do realizacji oferowanych usług i odpowiednie do stanowiska pracy.

Szkolenie personelu powinno być prowadzone zgodnie z planem szkolenia opisanym w PL-MSCA CPS oraz w deklaracji praktyk (PS) podmiotów personalizujących urządzenia.

Zatrudnianie personelu do pełnienia zaufanych ról będzie realizowane zgodnie z procesem rekrutacji i selekcji ustalonym w PL-MSCA CPS oraz w deklaracji praktyk (PS) podmiotów personalizujących urządzenia.

5.4 Procedury audytu bezpieczeństwa

Opisane w tym podrozdziale procedury audytu bezpieczeństwa dotyczą wszystkich komputerów i komponentów systemowych, które są związane z procesami wydawania urządzeń, certyfikatów i kluczy

Wszystkie znaczące zdarzenia związane z bezpieczeństwem w oprogramowaniu PL-MSCA oraz podmiotów personalizujących urządzenia powinny być automatycznie oznaczane czasem i rejestrowane w plikach dziennika systemu. Obejmują one co najmniej następujące zdarzenia:

- Pomyślne i nieudane próby tworzenia, aktualizowania, usuwania lub pobierania informacji o stanie kont pracowników PL-MSCA oraz podmiotów personalizujących urządzenia lub ustawiania lub cofania przywilejów kont;
- Pomyślne i nieudane próby ustawienia lub zmiany metody uwierzytelniania (np. hasła, biometrycznego, certyfikatu kryptograficznego) powiązanego z kontem osobistym;
- Pomyślne i nieudane próby zalogowania się i wylogowania z konta;
- Pomyślne i nieudane próby zmiany konfiguracji oprogramowania;
- Uruchomienia i zatrzymania oprogramowania;
- Aktualizacje oprogramowania;
- Uruchomienie i wyłączenie systemu;
- Pomyślne i nieudane próby dodania lub usunięcia podmiotu z rejestru subskrybentów, którym obecnie PL-MSCA świadczy usługi certyfikacji klucza lub zmiany jakichkolwiek danych dla któregokolwiek z subskrybentów lub pobrania informacji z rejestru;
- Pomyślne i nieudane próby przetworzenia wniosku o podpisanie certyfikatu lub wniosku o wydanie klucza;
- Udane i nieudane próby podpisania certyfikatu;
- Udane i nieudane interakcje z bazą danych zawierającą dane o (statusie) wydanych certyfikatów, w tym próby połączenia i operacje odczytu, zapisu i aktualizacji lub usuwania;
- Pomyślne i nieudane próby połączenia do lub odłączenia od HSM;
- Pomyślne i nieudane próby uwierzytelnienia użytkownika na HSM;
- Pomyślne i nieudane próby wygenerowania lub zniszczenia pary kluczy lub klucza symetrycznego wewnątrz HSM;
- Pomyślne i nieudane próby importowania lub eksportowania klucza do lub z HSM;
- Pomyślne i nieudane próby zmiany stanu cyklu życia dowolnej pary kluczy lub klucza symetrycznego;
- Pomyślne i nieudane próby użycia klucza prywatnego lub klucza symetrycznego wewnątrz HSM w dowolnym celu.

Aby móc badać zdarzenia związane z bezpieczeństwem dziennik systemowy zawiera, w miarę możliwości, informacje umożliwiające identyfikację osoby lub konta, które wykonało zadania systemowe.

Integralność dzienników zdarzeń systemowych powinna być zachowana i chroniona przed nieuprawnionym dostępem, modyfikacją, usunięciem lub zniszczeniem. Dzienniki zdarzeń systemowych powinny być archiwizowane i przechowywane zgodnie z procedurami opisanymi w odpowiednim CPS.

5.5 Archiwizacja dzienników zdarzeń

Lista zdarzeń, które będą archiwizowane, zostanie opisana w procedurach wewnętrznych i będzie zgodna z odpowiednimi zasadami i przepisami. PL-MSCA wdraża odpowiednie procedury archiwizacji rekordów. Powinny istnieć procedury zapewniające integralność, autentyczność i poufność zapisów.

Dla wszystkich zarchiwizowanych informacji okresy przechowywania będą nieskończone.

Należy podjąć środki w celu zapewnienia, że zarchiwizowane dziennki zdarzeń są przechowywane w taki sposób, że ich utrata jest praktycznie wykluczona.

Zdarzenia wymienione w sekcji [5.4] będą okresowo sprawdzane pod kątem integralności. Kontrole te odbywają się co najmniej raz w roku. Poza tym dzienniki kontroli są konsolidowane co najmniej raz w roku.

Dwie kopie skonsolidowanego dziennika są sporządzane i przechowywane w osobnych, zabezpieczonych lokalizacjach fizycznych. Dziennik kontroli jest przechowywany w sposób umożliwiający analizę w trakcie jego czasu przechowywania.

5.6 Zmiana klucza

PL-MSCA generuje nowe pary kluczy PL-MSCA w razie potrzeby. Po wygenerowaniu przez PL-MSCA nowej pary kluczy wysyła wniosek o ponowną certyfikację klucza.

PL-MSCA zapewnia, że klucze zastępcze są generowane w kontrolowanych okolicznościach i zgodnie z procedurami określonymi w polityce certyfikacji ERCA [6].

5.7 Kompromitacja i przywracanie działania po awarii

PL-MSCA definiuje procedury postepowania na wypadek incydentów bezpieczeństwa i kompromitacji w podręczniku Procedury obsługi incydentów bezpieczeństwa, który jest wydawany administratorom i audytorom.

PL-MSCA i PL-CP utrzymują plan ciągłości działania (ang. *Business Continuity Plan, BCP*), w którym wyszczególniają, w jaki sposób będą zarządać swoimi usługami w przypadku incydentu, który wpływa na standardowe operacje. Po wykryciu incydentu operacje zostają zawieszone do czasu ustalenia poziomu kompromitacji. Ponadto PL-MSCA i PL-CP powinny założyć, iż postęp technologiczny sprawia, że ich systemy informatyczne staną się przestarzałe z upływem czasu i w związku z tym powinny określić procedury zarządzania procesem starzenia sprzętu i oprogramowania.

Procedury tworzenia kopii zapasowych i odzyskiwania dotyczące wszystkich istotnych danych zostaną opisane w Planie tworzenia kopii zapasowych i odzyskiwania danych (ang. *Back-up and Recovery Plan*).

Następujące zdarzenia są uważane za poważne awarie:

a) kompromitacja lub kradzież klucza prywatnego i / lub klucza głównego;

b) utrata klucza prywatnego i / lub klucza głównego / i / lub innych chronionych danych;

c) awaria sprzętu IT.

PL-MSCA CPS i PL-CP PS opisują odpowiednie mechanizmy przywrócenia działania po awarii oraz określają wszystkie środki i działania podejmowane w celu zapobiegania poważnym awariom w przyszłości. Mechanizmy odzyskiwania po awarii nie zależą od czasów reakcji ERCA.

W przypadku kompromitacji lub kradzieży klucza prywatnego PL-MSCA i / lub symetrycznego klucza głównego, PL-MSCA niezwłocznie informuje PL-MSA i ERCA. PL-MSA podejmie odpowiednie działania w stosownym czasie.

Nie ma możliwości odzyskania kluczy PL-MSCA lub symetrycznych kluczy głównych po ich utracie. W związku z tym należy zapobiegać ich utratom poprzez posiadanie wielu kopii zapasowych kluczy głównych i symetrycznych kluczy głównych, poddawanych okresowym kontrolom.

Ochronę przed awariami sprzętu IT zapewnia redundancja, tj. dostępność nadmiarowych urządzeń IT.

5.8 Zakończenie działalności CA lub RA

W przypadku zakończenia działalności PL-MSCA przez wyznaczoną organizację, PL-MSA powiadomi o tym Urząd Europejski i ERCA oraz opcjonalnie poinformuje Urząd Europejski i ERCA o nowo mianowanym PL-MSCA.

PL-MSA powinien zapewnić, że przynajmniej jeden podmiot PL-MSCA działa w jego jurysdykcji przez cały czas.

5.8.1 Ostateczne rozwiązanie PL-MSCA lub PL-CP

Rozwiązanie PL-MSCA lub PL-CP następuje, gdy wszystkie usługi związane z podmiotem logicznym zostają trwale zakończone. PL-MSA zapewnia wówczas wykonanie zadań określonych poniżej:

- Poinformowanie wszystkich użytkowników i podmiotów, z którymi PL-MSCA i PL-CP miały zawarte umowy lub inną formę relacji;
- Publiczne udostępnienie informacji o rozwiązaniu z wyprzedzeniem przynajmniej 6-miesięcznym;
- PL-MSCA i PL-CP utrzymują i zapewniają ciągły dostęp do danych archiwalnych, przekazując je PL-MSA.

5.8.2 Przeniesienie odpowiedzialności PL-MSCA lub PL-CP

Przeniesienie odpowiedzialności PL-MSCA lub PL-CP następuje, gdy PL-MSA zadecyduje o wyborze nowego MSCA lub CP, zamiast dotychczasowego podmiotu.

PL-MSA zapewnia przeniesienie obowiązków i zasobów w sposób uporządkowany.

Poprzedni PL-MSCA przenosi wszystkie klucze PL-MSCA do nowego PL-MSCA w sposób ustalony przez PL-MSA.

Poprzedni PL-MSCA niszczy wszystkie kopie kluczy, które nie zostały przeniesione.

6. Kontrola zabezpieczeń technicznych

6.1 Generowanie pary kluczy i instalacja klucza symetrycznego

PL-MSCA generuje klucze prywatne zgodnie z Załącznikiem IC Dodatkiem 11 Rozporządzenia [2].

Generowanie par kluczy i instalowanie symetrycznych kluczy głównych powinno odbywać się w środowisku o wysokim poziomie bezpieczeństwa fizycznego przez personel w postaci co najmniej dwóch osób pełniących zaufane role. Ceremonia generowania klucza zostanie udokumentowana.

PL-MSCA powinno dysponować systemem Test PL-MSCA do przeprowadzenia testów interoperacyjności zgodnie z rozporządzeniem. Jeśli istnieje system Test PL-MSCA, to będzie on oddzielnym systemem, który posiada własne klucze prywatne MSCA oraz symetryczne klucze główne. Na rzecz systemu Test PL-MSCA będzie można złożyć wniosek o podpisanie certyfikatów testowych oraz wniosek o wydanie symetrycznych kluczy testowych przy użyciu procesów opisanych w sekcjach 4.1 i 4.2 Polityki certyfikacyjnej ERCA [6]. System Test PL-MSCA powinien także być w stanie podpisywać certyfikaty dla testowych urządzeń, wydawać symetryczne klucze testowe i przekazywać zaszyfrowane dane dla czujników ruchu na wniosek podmiotów personalizujących urządzenia.

6.2 Ochrona kluczy prywatnych i kluczy symetrycznych oraz kontrola zabezpieczeń urządzeń kryptograficznych

PL-MSCA zachowuje poufność, integralność oraz dostępność kluczy prywatnych i symetrycznych kluczy głównych zgodnie z opisem w tej sekcji.

Klucze prywatne są generowane oraz używane, i / lub symetryczne klucze główne są importowane oraz używane w godnym zaufania dedykowanym urządzeniu, które:

- posiada certyfikat EAL 4 lub wyższy zgodnie ze wymaganiami Common Criteria określonymi w normie ISO / IEC 15408 [8] dla odpowiedniego profilu ochrony (Protection Profile); lub
- spełnia wymagania określone w ISO / IEC 19790 [10] poziom 3; lub
- spełnia wymagania określone w FIPS PUB 140-2 poziom 3 [13]; lub
- zapewnia równoważny poziom bezpieczeństwa zgodnie z równoważnymi krajowymi lub międzynarodowymi kryteriami oceny bezpieczeństwa IT.

Najczęstszą implementacją takiego dedykowanego godnego zaufania urządzenia wykorzystywanego w systemie PKI jest sprzętowy moduł bezpieczeństwa (ang. *Hardware Security Module, HSM*). Możliwe są również inne implementacje, wykorzystujące odmienne urządzenia, o ile wybrane urządzenia spełniają jedno z wyżej wymienionych wymagań bezpieczeństwa. Ponadto, oprócz wskazanych wymagań bezpieczeństwa, niniejsza polityka MSA zawiera również inne wymagania funkcjonalne dla HSM używanych w systemach PL-MSCA. W przypadku, gdy zamiast HSM używane jest inne urządzenie, muszą być spełnione wszystkie wskazane wymagania funkcjonalne.

Operacje z użyciem klucza prywatnego i klucza symetrycznego powinny odbywać się wewnątrz urządzenia HSM, w którym przechowywane są klucze.

Klucze prywatne PL-MSCA i symetryczne klucze główne mogą być używane wyłącznie w fizycznie bezpiecznym środowisku przez personel w postaci co najmniej dwóch osób pełniących zaufane role. Wszystkie zdarzenia użycia klucza prywatnego i użycia symetrycznego klucza głównego będą rejestrowane.

Klucze prywatne PL-MSCA i symetryczne klucze główne powinny być archiwizowane, przechowywane i odzyskiwane wyłącznie w fizycznie bezpiecznym środowisku przez personel w postaci co najmniej dwóch osób pełniących zaufane role.

Wszelkie kopie kluczy prywatnych PL-MSCA i symetrycznych kluczy głównych podlegają temu samemu poziomowi kontroli bezpieczeństwa, co używane klucze.

Import i eksport klucza prywatnego odbywa się wyłącznie w celu tworzenia kopii zapasowych i odzyskiwania.

Import i eksport symetrycznego klucza głównego jest dozwolony do celów tworzenia kopii zapasowych i odzyskiwania. Ponadto w przypadku PL-MSCA eksport kluczy $K_{M\text{-}WC}$ i kluczy specyficznych dla tachografu (VU) dla łączności DSRC jest dozwolony tylko w postaci zaszyfrowanej i tylko w odpowiedzi na poprawny wniosek o wydanie klucza od podmiotów personalizujących urządzenia przez personel w postaci co najmniej dwóch osób pełniących zaufane role.

Import i eksport symetrycznego klucza głównego z jakiegokolwiek innego powodu jest zabroniony.

Pod koniec okresu użytkowania klucza prywatnego PL-MSCA podmiot ten niszczy wszystkie kopie klucza w taki sposób, żeby nie można było ich odzyskać (jak to określono w Dodatku 11 do Załącznika IC, Rozporządzenia [2]). Podobnie pod koniec cyklu życia symetrycznego klucza głównego PL-MSCA niszczy wszystkie kopie posiadanego[2] klucza, w taki sposób, żeby nie można ich było odzyskać (jak to określono w Dodatku 11 do Załącznika IC, Rozporządzenia [2]).

Wszystkie klucze prywatne i symetryczne klucze główne należy natychmiast dezaktywować (tak, aby nie można było ich użyć) w sytuacji podejrzenia kompromitacji. PL-MSCA zbada podejrzany incydent kompromitacji. Jeśli kompromitacja zostanie potwierdzona lub nie można jej wykluczyć, klucze zostaną zniszczone. Ponadto wszystkie kopie skompromitowanych kluczy zostaną również zniszczone. Jeśli kompromitację zostanie wykluczona, klucze zostaną ponownie aktywowane.

Niszczenie kluczy prywatnych i symetrycznych kluczy głównych odbywa się za pomocą funkcji HSM do niszczenia kluczy.

6.3 Inne aspekty zarządzania parami kluczy

Certyfikaty kluczy publicznych PL-MSCA, a tym samym klucze publiczne, będą archiwizowane, a ich okres przechowywania będzie nieskończony. Okresy ważności wszystkich certyfikatów PL-MSCA muszą być zgodne z Załącznikiem IC Dodatek 11 Rozporządzenia [2].

Okres użytkowania kluczy prywatnych PL-MSCA wynosi dwa lata. Okres używania klucza prywatnego zaczyna się od daty początku ważności określonej w odpowiednim certyfikacie. PL-MSCA nie będzie używać klucza prywatnego po zakończeniu okresu użytkowania klucza prywatnego.

6.4 Dane niezbędne do uruchomienia systemu

PL-MSCA w swojej deklaracji praktyk certyfikacyjnych (CPS) opisze liczbę osób pełniących zaufane role, które są wymagane do uruchomienia systemu oraz do generowania, używania lub niszczenia klucza prywatnego PL-MSCA lub do importowania lub używania symetrycznego klucza głównego.

[2]Klucze $K_{M\text{-}WC}$ i K_{DSRC} są również przechowywane na kartach do tachografów. Na przykład kopie kluczy znajdujących się na karcie nie zostaną zniszczone do momentu zakończenia użytkowania danej karty.

Generowanie, importowanie, używanie oraz niszczenie kluczy prywatnych PL-MSCA i / lub importowanie, używanie lub niszczenie symetrycznych kluczy głównych przechowywanych w HSM będzie możliwe tylko wtedy, gdy odpowiednia liczba osób pełniących zaufane role określonych dla danego zadania w CPS uwierzytelniła się w HSM. Uwierzytelnianie odbywa się przy użyciu odpowiednich środków (np. haseł, tokenów uwierzytelniających). Czas trwania sesji uwierzytelniania nie może być nieograniczony.

W celu uruchomienia oprogramowania PL-MSCA i systemu, na którym działa to oprogramowanie, uwierzytelnianie użytkownika odbywa się przy użyciu odpowiednich środków (na przykład za pomocą hasła).

6.5 Kontrola zabezpieczeń komputerów

PL-MSCA określa i zatwierdza procedury oraz specyficzne techniczne środki bezpieczeństwa stosowane do zarządzania własnymi systemami komputerowymi. Procedury te gwarantują, że wymagany poziom bezpieczeństwa jest zawsze spełniany. Procedury i techniczne środki bezpieczeństwa zostaną opisane w wewnętrznej dokumentacji PL-MSCA. Systemy komputerowe PL-MSCA powinny być zorganizowane i zarządzane zgodnie z tymi procedurami.

6.6 Kontrola bezpieczeństwa cyklu życia oprogramowania

PL-MSCA powinno przeprowadzić analizę wymagań bezpieczeństwa na etapie projektowania i specyfikacji wymagań, aby zapewnić, że odpowiedni poziom zabezpieczeń jest wbudowany w systemy informatyczne PL-MSCA.

System pre-produkcyjny (testowy, akceptacyjny) powinien być odseparowany do systemu produkcyjnego. Procedury zmian i procedury zarządzania bezpieczeństwem gwarantują utrzymanie wymaganego poziomu zabezpieczeń w systemie produkcyjnym.

Procedury kontroli zmian powinny być udokumentowane i wykorzystywane do wdrażania nowych wydań, modyfikacji i (awaryjnych) poprawek oprogramowania dla dowolnego oprogramowania operacyjnego.

6.7 Kontrola zabezpieczeń sieciowych

PL-MSCA opracuje i wdroży architekturę swojej sieci w taki sposób, że dostęp z Internetu do ich domeny sieci wewnętrznej oraz z domeny sieci wewnętrznej do systemów Centrum Certyfikacji może być skutecznie kontrolowany. W szczególności należy rozważyć całkowite izolowanie systemu CA (tzw. „air-gapping”).

6.8 Znakowanie czasem

Czas i data zdarzenia powinny być umieszczone w każdym wpisie dziennika audytu. W deklaracji praktyk PL-MSCA CPS opisuje, jak czas jest synchronizowany i weryfikowany.

7. Profile certyfikatów, list CRL oraz OCSP

7.1 Profil certyfikatu

Wszystkie certyfikaty mają profil określony w Złączniku 1C, Dodatku 11 oraz Dodatku 1 do Rozporządzenia [2]:

Obiekt danych	**ID pola**	**Tag**	**Długość (bajty)**	**Typ danych ASN.1**
ECC (CV) Certificate (*Certyfikat ECC (CV)*)	C	'7F 21'	zmienna	
Certificate Body (*Certyfikat*)	B	'7F 4E'	zmienna	
Certificate Profile Identifier (*Identyfikator profilu certyfikatu*)	CPI	'5F 29'	'01'	INTEGER (0…255)
Certification Authority Reference (*Referencja do Urzędu Certyfikacji*)	CAR	'42'	'08'	KeyIdentifier
Certificate Holder Authorisation (*Identyfikacja właściciela certyfikatu*)	CHA	'5F 4C'	'07'	Certificate Holder Authorisation
Public Key (*Klucz publiczny*)	PK	'7F 49'	zmienna	
Standardised Domain Parameters OID (*Standardowe parametry domeny OID*)	DP	'06'	zmienna	OBJECT IDENTIFIER
Public Point (*Punkt Publiczny*)	PP	'86'	zmienna	OCTET STRING
Certificate Holder Reference (*Referencja do właściciela certyfikatu*)	CHR	'5F 20'	'08'	KeyIdentifier
Certificate Effective Date (*Data początku ważności certyfikatu*)	CEfD	'5F 25'	'04'	TimeReal
Certificate Expiration Date (*Data końca ważności certyfikatu*)	CExD	'5F 24'	'04'	TimeReal
ECC Certificate Signature (*Podpis certyfikatu ECC*)	S	'5F 37'	zmienna	OCTET STRING

Tabela 8 Profil certyfikatu

Algorytm jest określany przez Standardowe Parametry Domeny OID, jak to określono w Tabeli 1 w Dodatku 11 Załącznika 1C w Rozporządzeniu [2].

Dostępne są następujące warianty:

Nazwa	**Referencja do identyfikatora obiektu**	**Wartość identyfikatora obiektu**
NIST P-256	secp256r1	1.2.840.10045.3.1.7
BrainpoolP256r1	brainpoolP256r1	1.3.36.3.3.2.8.1.1.7
NIST P-384	secp384r1	1.3.132.0.34
Brainpool P384r1	brainpoolP384r1	1.3.36.3.3.2.8.1.1.11
Brainpool P512r1	brainpoolP512r1	1.3.36.3.3.2.8.1.1.13
NIST P-521	secp521r1	1.3.132.0.35

Tabela 9 Dozwolone Standardowe Parametry Domeny OID

7.2 Profil list CRL

Listy CRL nie będą publikowane.

7.3 Profil OCSP

Usługa OCSP nie będzie wykorzystywana.

8. Audyt zgodności i inne weryfikacje

PL-MSA jest odpowiedzialna za zapewnienie, że PL-MSCA, podmioty personalizujące urządzenia oraz inni zewnętrzni dostawcy usług są poddawani audytowi sprawdzającemu, o ile to jest konieczne.

PL-MSCA, podmioty personalizujące urządzenia oraz inni zewnętrzni dostawcy usług ponoszą koszty przeprowadzanego audytu.

PL-MSA może skonsultować zatwierdzenie CPS lub PS przedłożonych przez PL-MSCA, podmioty personalizujące urządzenia oraz innych zewnętrznych dostawców usług z zewnętrzną instytucją certyfikującą lub akredytacyjną, aby wdrożenie było bardziej wiarygodne dla zainteresowanych stron.

8.1 Częstotliwość i okoliczności oceny

Audyt na poziomie krajowym powinien ustalić, czy są spełnione wymagania opisane w Polityce PL-MSA dotyczące organizacji, która ma zostać poddana weryfikacji.

PL-MSA przeprowadza pierwszy audyt w ciągu 12 miesięcy od rozpoczęcia wykonywania działań objętych Polityką PL-MSA. Jeżeli audyt nie wykazuje dowodów niezgodności, to następny audyt zostanie przeprowadzony w ciągu 24 miesięcy. Jeżeli audyt wykryje dowody niezgodności, to w ciągu 12 miesięcy zostanie przeprowadzony audyt uzupełniający w celu sprawdzenia czy niezgodności zostały rozwiązane.

Przed rozpoczęciem wykonywania działań objętych niniejszą Polityką PL-MSA, organ (PL-MSA) przeprowadza ocenę przedoperacyjną, aby potwierdzić, że weryfikowana organizacja jest w stanie działać zgodnie z wymaganiami Polityki PL-MSA.

8.2 Identyfikacja/kwalifikacje audytora

Badanie przeprowadza niezależny audytor.

Każda osoba wybrana lub wskazana do przeprowadzenia audytu zgodności PL-MSCA powinna zostać zatwierdzona przez PL-MSA.

Audytorzy, którzy będą przeprowadzać audyty, powinni być zarejestrowani. Muszą oni spełniać następujące wymagania:

- Cechy etyczne: wiarygodność, obiektywność, poufność w odniesieniu do ich relacji z organizacją, która ma zostać poddana audytowi, a także podczas przetwarzania przez nich informacji i danych organizacji;
- Uczciwa prezentacja - ustalenia, wnioski i raporty z audytu są prawdziwe i precyzyjnie opisują wszystkie działania przeprowadzone podczas audytu;
- Profesjonalne podejście - mają wysoki poziom wiedzy fachowej i kompetencji zawodowych oraz skutecznie wykorzystują swoje doświadczenie zdobyte dzięki dobrej i głęboko zakorzenionej praktyce w technologiach informacyjnych, PKI oraz powiązanych normach technicznych i standardach.

Audytor musi posiadać znaczną najlepiej, gdy potwierdzoną certyfikatami wiedzę w zakresie:

- wykonywania audytów bezpieczeństwa systemów informatycznych;
- PKI i technologii kryptograficznych;
- działania oprogramowania PKI;
- odpowiednich polityk i przepisów Komisji Europejskiej;
- polityki organu państwa członkowskiego w Polsce.

8.3 Związki audytora z podmiotem ocenianym

Audytor musi być niezależny i niezwiązany z organizacją będącą przedmiotem audytu.

8.4 Zakres audytu

Audyt PL-MSA powinien obejmować zgodność z Polityką PL-MSA, z deklaracją praktyk PL-MSCA CPS oraz z powiązanymi procedurami i technikami udokumentowanymi przez organizację, która ma zostać poddana audytowi.

Audyt obejmuje organizacje odgrywające role w całym procesie wydawania urządzeń w kraju. Audyt uwzględnia również działania podwykonawców.

Zakres kontroli zgodności obejmuje wdrożenie technicznych, proceduralnych i personalnych praktyk opisanych w tych dokumentach.

Niektóre z obszarów zainteresowania kontroli to:

- identyfikacja i uwierzytelnianie;
- realizowane funkcje / udostępniane usługi;
- kontrola zabezpieczeń fizycznych, proceduralnych oraz dotyczących personelu;
- kontrola zabezpieczeń technicznych.

Poprzez ocenę dzienników kontroli należy ustalić, czy w systemach bezpieczeństwa organizacji podlegających audytowi występują niedostatecznie zabezpieczone elementy. Określone (możliwe) słabe punkty powinny zostać poprawione. Ewentualnie wykryte słabe punkty powinny zostać rejestrowane i ocenione.

8.5 Działania podejmowane w przypadku nieprawidłowości

Jeżeli audytor wykryje nieprawidłowości, działania naprawcze powinny być podjęte niezwłocznie przez audytowaną organizację. Po wykonaniu działań naprawczych audyt kontrolny odbywa się w ciągu 12 miesięcy.

8.6 Przesyłanie wyników

W przypadku audytu na poziomie krajowym niezależny audytor przekazuje pełne wyniki audytu zgodności organizacji, która została poddana audytowi oraz PL-MSA.

PL-MSA przesyła ERCA raport z audytu obejmujący odpowiednie wyniki audytu. Obejmuje on co najmniej liczbę stwierdzonych odstępstw i charakter każdego odstępstwa.

Raport z audytu powinien zawierać działania naprawcze wraz z harmonogramem wdrożenia niezbędnym do spełnienia wymogów Polityki PL-MSA.

Na żądanie ERCA, PL-MSA przesyła pełne wyniki audytu zgodności do ERCA.

9. Inne kwestie biznesowe oraz prawne

9.1 Opłaty

Nie dotyczy.

9.2 Odpowiedzialność finansowa

Bez zastrzeżeń.

9.3 Poufność informacji biznesowych

9.3.1 Informacje handlowe

Poufność należy zachować przynajmniej w odniesieniu do:

- prywatnych kluczy;
- symetrycznych kluczy głównych;
- logów i dzienników;
- szczegółowych informacji dotyczących zarządzania infrastrukturą klucza publicznego.

Informacje poufne nie mogą być ujawnione, chyba że obowiązujące prawo stanowi inaczej.

9.3.2 Informacje, które nie są traktowane jako poufne

Certyfikaty nie są uznawane za poufne.

Informacje identyfikacyjne lub inne informacje o osobach prywatnych bądź przedsiębiorstwach figurujące na kartach i w certyfikatach nie są uznawane za poufne, o ile nie nakazują tego ustawy lub inne formalne zobowiązania.

9.4 Poufność danych osobowych

Jedyne dane osobowe przetwarzane lub przechowywane w systemie PL-MSCA są to dane przedstawicieli ERCA, PL-MSCA i podmiotów personalizujących urządzenia.

Wszelkie dane o osobach prywatnych bądź przedsiębiorstwach będące w posiadaniu PL-MSCA, PL-CP lub ich podwykonawców, które nie figurują na wydawanych kartach uznaje się za poufne. Nie mogą być one udostępniane bez wcześniejszej zgody osoby, której dotyczą lub (jeśli ma to zastosowanie) pracodawcy lub jej przedstawiciela, chyba, że obowiązujące prawo stanowi inaczej.

W celu zapewnienia poufności i ochrony osób prywatnych, przetwarzanie danych osobowych i przekazywanie takich danych są ograniczone zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 2016/679 [16] i polską Ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych [17].

9.5 Prawa własności intelektualnej

PL-MSCA posiada prawa własności intelektualnej do oprogramowania PL-MSCA.

9.6 Oświadczenia i gwarancje

PL-MSCA będzie działać zgodnie z ERCA CP i PL-MSA CP oraz własnym CPS.

9.7 Ograniczenia odpowiedzialności

Polskie państwo członkowskie nie ponosi odpowiedzialności za jakiekolwiek straty:

- związane z brakiem świadczenia usług z powodu wojny, klęsk żywiołowych lub innych niekontrolowanych sił;

- poniesione w czasie po między zmianą statusu certyfikatu, a następnym zaplanowanym wydaniem informacji o statusie certyfikatu;
- poniesione z powodu nieuprawnionego użycia certyfikatów wydanych przez PL-MSCA oraz wykorzystania certyfikatów poza przewidzianym zastosowaniem określonym w niniejszej Polityce MSA i deklaracji praktyk certyfikacyjnych PL-MSCA CPS;
- spowodowane nieuczciwym lub niedbałym użyciem certyfikatów i / lub informacji o statusie certyfikatu wydanych przez PL-MSCA.

Polskie państwo członkowskie zrzeka się jakiejkolwiek odpowiedzialności za jakiekolwiek kary, odszkodowania lub inne roszczenia lub zobowiązania jakiegokolwiek rodzaju wynikające z czynu niedozwolonego, umowy lub jakiegokolwiek innego powodu w odniesieniu do jakiejkolwiek usługi związanej z wydaniem, wykorzystaniem lub poleganiem na:

- dowolnym certyfikacie wydanym przez PL-MSCA lub powiązaną z nim parą kluczy publiczny/prywatny, używanym przez subskrybenta lub stronę ufającą;
- dowolnym kluczu symetrycznym dystrybuowanym przez PL-MSCA, używanym przez subskrybenta lub stronę ufającą.

Wydawanie certyfikatów i wiadomości dystrybucji klucza przez PL-MSCA nie czyni polskiego państwa członkowskiego, ani PL-MSCA agentem, powiernikiem, kuratorem lub innym przedstawicielem wnioskodawców lub stron ufających, ani innych osób korzystających z systemu zarządzania kluczami Inteligentnego Tachografu.

Subskrybenci i strony ufające nie są uprawnione do roszczeń odszkodowawczych z tytułu strat wynikających z niewłaściwego lub oszukańczego użycia tego systemu zarządzania kluczami.

Ponadto PL-MSCA nie jest pośrednikiem w transakcjach między subskrybentami, a stronami ufającymi. Roszczenia wobec PL-MSCA ograniczają się do wykazania, że działały one w sposób niezgodny z niniejszą Polityką PL-MSA i PL-MSCA CPS.

PL-MSCA i PL-CP ponoszą odpowiedzialność za właściwe wykonywanie swoich zadań także w przypadku, gdy zlecają je w całości lub w części podwykonawcom. Jeśli PL-MSCA lub PL-CP zamierza zlecić swoje zadania innym podmiotom, poinformuje o tym z wyprzedzeniem PL-MSA. Ponadto PL-MSCA lub PL-CP udostępni PL-MSA dodatkowe zasoby niezbędne dla realizacji zobowiązań PL-MSA.

PL-MSCA i PL-CP nie ponoszą odpowiedzialności wobec użytkownika końcowego, jedynie wobec PL-MSA i PL-CIA.

Wszelką odpowiedzialność wobec użytkowników końcowych Inteligentnego Tachografu ponoszą PL-MSA / PL-CIA.

W ramach systemu Inteligentnego Tachografu wykorzystywane będą wyłącznie certyfikaty podpisane przez ERCA lub PL-MSCA. Inne certyfikaty znajdujące się na kartach stanowią naruszenie Polityki PL-MSA, a zatem ani PL-MSA, PL-CIA, PL-MSCA, ani PL-CP nie ponoszą żadnej odpowiedzialności w związku z takim użyciem.

9.7.1 Odpowiedzialność PL-MSA i PL-CIA wobec użytkowników systemu Inteligentnego Tachografu

PL-MSA i PL-CIA ponoszą odpowiedzialność za szkody będące wynikiem niewypełnienia ich zobowiązań tylko wówczas, gdy działały niedbale. Jeśli PL-MSA i PL-CIA działały zgodnie z Polityką PL-MSA lub innym dokumentem regulującym ich postępowanie, to nie można tego uznać za zaniedbanie.

9.7.2 Odpowiedzialność PL-MSCA i PL-CP wobec PL-MSA i PL-CIA

PL-MSCA lub PL-CP ponoszą odpowiedzialność za szkody będące wynikiem niewypełnienia jego zobowiązań tylko wówczas, gdy działały niedbale. Jeśli podmiot działał zgodnie z Polityką PL-MSA lub odpowiednią CPS / PS, to nie można tego uznać za zaniedbanie.

9.8 Odszkodowania

Bez zastrzeżeń.

9.9 Okres obowiązywania i zakończenie obowiązywania

Niniejsza Polityka PL-MSA jest ważna od momentu jej przyjęcia przez ERCA i będzie ważna aż do odwołania.

Ważność niniejszej Polityki PL-MSA kończy się, gdy PL-MSCA przestaje działać[3] lub gdy PL-MSA ogłasza, że niniejsza Polityka nie jest już ważna, na przykład w sytuacji wejścia w życie nowej wersji Polityki.

9.10 Indywidualne powiadomienia i komunikacja z uczestnikami

Oficjalne wiadomości i komunikacja z uczestnikami systemu Inteligentnego Tachografu w Polsce mają formę pisemną i podlegają procedurom rejestracji korespondencji obowiązującej w polskim państwie członkowskim.

9.11 Aktualizacja polityki

Niniejsza polityka jest wydawana pod nadzorem polskiego państwa członkowskiego. PL-MSA, we współpracy z PL-MSCA, może zmienić niniejszą Politykę, jeśli uzna to za konieczne.

Dozwolone jest wprowadzanie poprawek redakcyjnych lub typograficznych do tej polityki bez powiadamiania ERCA i bez zwiększania numeru wersji.

Dozwolone jest zmienianie informacji kontaktowych w sekcji 1.5 z powiadomieniem ERCA, ale bez zmiany numeru wersji dokumentu.

W przypadku wszystkich innych zmian niniejszej Polityki PL-MSA procedura składania propozycji zmian i ich zatwierdzenia jest następująca:

A. PL-MSCA, PL-CIA, PL-CP i producenci czujników ruchu (MoS) z Polski mogą w dowolnym momencie przesyłać propozycje zmiany w Polityce PL-MSA do polskiego organu.

B. Polski organ dystrybuuje wszelkie propozycje zmian Polityki PL-MSA do PL-MSCA, PL-CIA, PL-CP oraz producentów czujników ruchu (MoS) z Polski.

C. Polski organ ustala odpowiedni okres czasu na zgłaszanie uwag. PL-MSCA, PL-CIA, PL-CP i producenci czujników ruchu (MoS) z Polski mogą odnosić się do proponowanych zmiany we wskazanym okresie czasu.

D. Polski organ rozpatruje uwagi i decyduje, które ze zgłoszonych zmian zostaną zaimplementowane.

E. Gdy polski organ postanawia zastosować zmiany w polityce PL-MSA, przesyła nową wersję Polityki PL-MSA do ERCA do zatwierdzenia.

[3] Rozdział 5.8 obejmuje sytuację, w której obowiązki PL-MSCA są przenoszone do innej organizacji.

F. Polski organ powiadamia PL-MSCA, PL-CIA, PL-CP oraz producentów czujników ruchu (MoS) z Polski o decyzji podjętej przez siebie i Urząd Europejski oraz określa odpowiedni okres czasu na wdrożenie zmian.

G. Polski organ publikuje nową wersję Polityki PL-MSA zawierającą wszystkie wprowadzone zmiany oraz zwiększa numeru wersji dokumentu.

9.11.1 Powiadomienia

Każdy element w Polityce PL-MSA można zmienić, powiadamiając o tym z wyprzedzeniem **90** dni.

Zmiany w elementach, które w opinii instytucji odpowiedzialnej za politykę (PL-MSA) nie będą miały istotnego wpływu na znaczącą liczbę użytkowników lub podmiotów korzystających z tej polityki, mogą być wprowadzone z wyprzedzeniem **30** dni.

9.11.2 Okres zgłaszania uwag

Użytkownicy, których dotyczy zmiana, mogą zgłaszać uwagi instytucji zarządzającej Polityką PL-MSA w ciągu **15** dni od pierwszego powiadomienia.

9.11.3 Powiadamianie podmioty

Informacje o zmianach wprowadzanych w Polityce PL-MSA są wysyłane do:

- ERCA;
- PL-MSCA, PL-CIA, PL-CP,
- producentów czujników ruchu.

9.11.4 Okres poprzedzający wejście zmian w życie

Jeśli proponowana zmiana zostanie zmodyfikowana w wyniku zgłaszanych uwag, to o zmodyfikowanej proponowanej zmianie należy powiadomić na co najmniej **30** dni przed ostatecznym wejściem zmiany w życie.

9.12 Procedury rozwiązywania sporów

Wszelkie spory związane z zarządzaniem kluczami i certyfikatami między polskim państwem członkowskim a organizacją lub osobą spoza polskiego państwa członkowskiego będą rozstrzygane przy użyciu odpowiedniego mechanizmu rozstrzygania sporów. Spór zostanie rozstrzygnięty w drodze negocjacji, jeśli to możliwe. Spór nie rozstrzygnięty w drodze negocjacji powinien zostać rozstrzygnięty w drodze arbitrażu przez polski organ lub organ europejski.

9.13 Obowiązujące ustawodawstwo

Regulacje europejskie i polskie przepisy regulują wykonalność, budowę, interpretację i ważność niniejszej polityki PL-MSA.

Wszelkie kontrowersje wynikające z interpretacji Polityki PL-MSA będą interpretowane zgodnie z prawem obowiązującym w Polsce.

9.14 Zgodność z obowiązującym prawem

Niniejsza Polityka PL-MSA jest zgodna z:

- Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 [1],
- Rozporządzenie wykonawcze Komisji (UE) 2016/799 [2],
- Europejską polityką dla certyfikatów głównych i polityką infrastruktury kluczy symetrycznych dla systemu Inteligentnego Tachografu, wersja 1.00 [6].

W przypadku rozbieżności między niniejszą Polityką PL-MSA, a dokumentami wymienionymi powyżej, pierwszeństwo mają te ostatnie.

9.15 Różne postanowienia

Bez zastrzeżeń.

9.16 Inne postanowienia

Bez zastrzeżeń.

10. Bibliografia

1. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 165/2014 z dnia 4 lutego 2014 roku, Dziennik Urzędowy Unii Europejskiej L60
2. Rozporządzenie wykonawcze Komisji (UE) 2016/799 z dnia 18 marca 2016 roku, Dziennik Urzędowy Unii Europejskiej L 139, w tym ref. 3
3. Rozporządzenie wykonawcze Komisji (UE) 2018/502 z dnia 28 lutego 2018 roku, zmieniające rozporządzenie wykonawcze Komisji (UE) 2016/799, Dziennik Urzędowy Unii Europejskiej L 85
4. RFC 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, November 2003
5. RFC 2119, Key words for use in RFCs to Indicate Requirement Levels, March 1997
6. Smart Tachograph European Root Certificate Policy and Symmetric Key Infrastructure Policy version 1.0
7. Smart Tachograph - ERCA Certification Practice Statement, JRC, version 1.0
8. Ustawa z dnia 5 lipca 2018 r. o tachografach (Dziennik Ustaw z 2018 roku poz. 1480, Parlament Rzeczpospolitej Polskiej)
9. Common Criteria. ISO/IEC 15408-1, -2 and -3, Information technology — Security techniques — Evaluation criteria for IT security Parts 1, 2 and 3, third edition, 2008 – 2014
10. Common Criteria Protection Profile, Digital Tachograph – Tachograph Card (TC PP), version 1.0, 9 May 2017
11. Common Criteria Protection Profile, Digital Tachograph – Motion Sensor (MS PP), version 1.0, 9 May 2017
12. ISO/IEC 19790, Information technology — Security techniques — Security requirements for cryptographic modules, second edition, 2012-08-15
13. National Institute of Standards and Technology (NIST), FIPS PUB 140-2, Security requirements for cryptographic modules, May 25, 2001
14. National Institute of Standards and Technology (NIST), FIPS PUB 186-4: Digital Signature Standard (DSS), July 2013
15. ISO/IEC 27001, Information technology — Security techniques — Information security management systems — Requirements. Second edition, 2013-10-01
16. Rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych)
17. Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych (Dziennik Ustaw z 2018 roku poz. 1000, Parlament Rzeczpospolitej Polskiej)
18. Rozporządzenie Parlamentu Europejskiego i Rady (UE) nr 561/2006 z dnia 15 marca 2006 roku, Dziennik Urzędowy Unii Europejskiej L60 L102/1

19. ISO/IEC 8825-1, Information technology - ASN.1 encoding rules: Specification of Basic Encoding Rules (BER), Canonical Encoding Rules (CER) and Distinguished Encoding Rules (DER). Fourth edition, 2008-12-15
20. BSI Technical Guideline TR-03111, Elliptic Curve Cryptography, version 2.00, 2012-06-28

11. Zgodność z polityką certyfikacji ERCA

Wymagania dotyczące polskiej polityki MSA zostały sformułowane w europejskiej polityce dla certyfikatów głównych i polityce infrastruktury kluczy symetrycznych dla systemu Inteligentnego Tachografu [6] w rozdziale 1.5.3.

Poniższa tabela zawiera zestawienie spełnienia wymogów sformułowanych w polityce ERCA przez wymagania zawarte w polityce PL-MSA.

Polityka ERCA wersja 1.0	**Polityka PL-MSA wersja 1.02**	**Uwagi**
Polityka certyfikacji MSA powinna być zgodna z zasadami polityki certyfikacji opisanymi w dokumencie RFC 3647 [4].	§1.1	Dotyczy całego dokumentu.
Polityka certyfikacji MSA powinna opisać role i obowiązki związane z całym procesem wydawania urządzeń w danym kraju, w tym co najmniej role MSCA i podmiotów personalizujących urządzenia. Wszystkie organizacje pełniące jedną lub więcej z tych ról powinny być zidentyfikowane.	§1.3, §1.5	
Polityka certyfikacji MSA powinna wymagać, by przynajmniej te organizacje, które generują lub zarządzają kluczami prywatnymi lub symetrycznymi, były regularnie kontrolowane. Polityka certyfikacji MSA powinna opisywać zakres każdego audytu, w zależności od obowiązków każdej organizacji, np. poprzez wskazanie sekcji polityki certyfikacji MSA szczególnie istotnych dla przeprowadzanego audytu.	§8	
Polityka certyfikacji MSA powinna określać, w jaki sposób MSCA rejestrują podmioty personalizujące urządzenia, którzy mogą wysyłać wnioski o podpisanie certyfikatu i wnioski o wydanie klucza.	§1.5.4, §1.5.6, §3.2.2	Podmioty personalizujące urządzenia (PL-CP) są zdefiniowane w tej polityce.
Polityka certyfikatów MSA obejmuje następujące procesy:		
• Wydawanie kluczy i certyfikatów na kartach do tachografów;	§4.4, §4.5.5, §4.6.1	
• Wydawanie kluczy i certyfikatów dla tachografów;	---	W Polsce nie ma producentów tachografów (VU). Jeśli w dowolnym momencie w przyszłości PL-MSA zawrze umowę o świadczenie usług dla producentów tachografów (VU), polityka PL-MSA zostanie odpowiednio zmodyfikowana i ponownie przedłożona do zatwierdzenia przez ERCA.
• Wydawanie kluczy i certyfikatów dla zewnętrznych urządzeń GNSS;	---	W Polsce nie ma producentów zewnętrznych urządzeń GNSS. Jeśli w dowolnym momencie w przyszłości PL-MSA zawrze umowę o świadczenie usług dla producentów zewnętrznych urządzeń GNSS, polityka PL-MSA zostanie odpowiednio

		zmodyfikowana i ponownie przedłożona do zatwierdzenia przez ERCA.
• Dystrybucja kluczy symetrycznych dla kart i tachografów oraz zaszyfrowanych danych dla czujników ruchu dla podmiotów personalizujących urządzenia;	§4.5.3	W Polsce nie ma producentów tachografów (VU). Dotyczy producentów czujników ruchu. Jeśli w dowolnym momencie w przyszłości PL-MSA zawrze umowę o świadczenie usług dla producentów tachografów (VU), polityka PL-MSA zostanie odpowiednio zmodyfikowana i ponownie przedłożona do zatwierdzenia przez ERCA.
• Zarządzanie kluczami państwa członkowskiego.	§4.5.2	
Polityka certyfikatów MSA powinna wymagać, aby klucze dla urządzeń były generowane, transportowane i umieszczane w urządzeniu w taki sposób, aby zachować ich poufność i integralność. W tym celu MSA powinno:		
• wymagać, aby wszelkie właściwe zalecenia nakazane przez certyfikację bezpieczeństwa urządzeń w Common Criteria były spełnione podczas całego cyklu życia urządzenia;	§1.5.2, §1.5.4, §1.5.5, §4.4.8.3, §4.5.2.1, §4.5.2.3, §4.5.3.3, §4.5.4.1, §4.5.4.3, §4.5.5.2, §4.5.5.5, §6.2	
• wymagać, aby w sytuacji, gdy generowanie klucza prywatnego dla urządzenia nie odbywa się w urządzeniu, generowanie klucza prywatnego odbywało się w HSM, który spełnia wymagania określone w rozdziale 6.2 polityki ERCA [6];	§4.4.8.3, §4.5.2.1, §4.5.4.1, §4.5.5.2	
• wymagać, aby w sytuacji, gdy generowanie klucza symetrycznego dla urządzenia nie odbywa się w urządzeniu, generowanie klucza symetrycznego odbywało się w HSM, który spełnia wymagania określone w rozdziale 6.2 polityki ERCA [6];	§4.5.5.2	
• wymagać, aby instalowanie kluczy prywatnych i kluczy symetrycznych do sprzętu odbywało się w fizycznie zabezpieczonym środowisku;	§4.4.8.3, §4.5.3, §4.5.3.4, §4.5.5.1, §4.5.5.2, §4.5.5.5,	
• wymagać, aby w przypadku, gdy urządzenie jest zdolne do generowania kluczy prywatnych lub symetrycznych, generowanie kluczy powinno być objęte certyfikacją bezpieczeństwa urządzeń, zapewniając stosowanie publicznie określonych i odpowiednich algorytmów generowania kluczy kryptograficznych.	§4.5.5.2	
Polityka certyfikacji MSA powinna wymagać, aby użytkownik każdej karty do tachografu został zidentyfikowany na odpowiednim etapie procesu wydawania karty.	§4.4.2	
Polityka certyfikacji MSA powinna wymagać, aby ERCA zostało bezzwłocznie powiadomione o utracie, kradzieży lub potencjalnej kompromitacji dowolnego	§4.5.2.6, §4.5.3.6, §4.5.4.6, §5.7, §6.2	

klucza prywatnego lub symetrycznego klucza głównego MSCA oraz powinna wskazywać dalsze kroki (dochodzenie) i potencjalne działania MSA.		
Polityka certyfikacji MSA powinna wskazywać odpowiednie mechanizmy odzyskiwania po awarii, zgodnie z wymaganiami w rozdziale 5.7 polityki ERCA [6].	§5.1, §5.7	
Polityka certyfikacji MSA powinna wymagać, aby wszyscy subskrybenci usług MSCA ustanowili system zarządzania bezpieczeństwem informacji (ISMS) w oparciu o ocenę ryzyka dla wszystkich zaangażowanych operacji. Wdrożenie ISMS powinno być zgodne z wymogami opisanymi w ISO 27001 [14].	§5.2	
Polityka certyfikacji MSA powinna wymagać zachowania odpowiednich dzienników operacji dotyczących operacji dla kluczy prywatnych lub symetrycznych.	§5.4	
Polityka certyfikacji MSA powinna obejmować postanowienia dotyczące zakończenia działalności przez MSCA.	§4.1.10, §5.8, §9.10	
Polityka certyfikacji MSA powinna obejmować procedury zmian.	§9.11	
Polityka certyfikacji MSA powinna wymagać, aby MSCA utrzymywał informacje o statusie certyfikatu i udostępniał te informacje stronom mającym prawnie uzasadniony interes.	§1.3.2, §4.4.9, §4.6.1.6, §4.6.1.8,	
Polityka certyfikacji MSA wymaga, aby proces wydawania kart do tachografów zapewniał, że data ważności certyfikatu (certyfikatów) karty była równa początkowi ważności samej karty do tachografów, zakodowanej w pliku przechowywanym na kracie EF_Identification.	§4.6.1.3	
Polityka certyfikacji MSA powinna zabraniać deponowania kluczy, co oznacza, że klucze prywatne MSCA nie powinny być eksportowane do ani przechowywane w żadnym systemie poza systemami odpowiedniego MSCA.	§4.5.2.5, §4.5.3.5, §4.5.4.5, §4.5.5.6	

Tabela 10 Zestawienie spełnienia wymogów sformułowanych w polityce ERCA przez wymagania zawarte w polityce PL-MSA

12. Spis rysunków

13. Spis tabel