**MINISTERSTWO TRANSPORTU**
**I BUDOWNICTWA**

# Polityka Organu Państwa Członkowskiego - Polska

**Warszawa, 5 stycznia 2006 r.**

## Zgłoszone uwagi

| | **Imię i nazwisko** | **Organizacja** | **Data** | **Podpis** |
|---|---|---|---|---|
| Uwagi zgłoszone przez Komisję Europejską | James Bishop | Komisja Europejska | 24.11.2005 | |
| Uwagi zgłoszone przez Komisję Europejską | James Bishop | Komisja Europejska | 20.12.2005 | |

## Historia zmian

| Wersja dokumentu | Data wydania | Opis |
|---|---|---|
| 01.01 | 20/10/2005 | Wersja początkowa |
| 01.02 | 01/12/2005 | Wersja zmodyfikowana zgodnie z uwagami zgłoszonymi przez P. James'a Bishop'a oraz Ministerstwo Transportu i Budownictwa |
| 01.03 | 05/01/2006 | Wersja zmodyfikowana na podstawie uwag P. James'a Bishop'a zawartych w Załączniku 1 „Review Findings" do dokumentu: G07-TRVA/JB/jb/(2005)D32853, z dnia 20 grudnia 2005 r. Uwzględniono wszystkie uwagi zgłoszone w w/w dokumencie. |

Zestawienie spełnienia wymagań:

| **Polityka ERCA wer.2.0** | **Polityka PL.-MSA** | **Uwagi** |
|---|---|---|
| §5.3.1 | §1.2, §1.4 | |
| §5.3.2 | §6.2.1, §6.2.3, §6.2.4, §6.4 | |
| §5.3.3 | §6.2.1, §9.3.1 | |
| §5.3.4 | §6.2.2 | |
| §5.3.5 | §6.2.1 | |
| §5.3.6 | §6.4 | |
| §5.3.7 | §6.4 | |
| §5.3.8 | §6.4 | |
| §5.3.9 | §6.4 | |
| §5.3.10 | §6.4 | |
| §5.3.11 | §6.2.7 | |
| §5.3.12 | §5.1.1, §7.1, §7.2 | |
| §5.3.13 | §3.1.3, §5.1.8.3, §6.2.1, §6.2.3, §7.1, §7.2 | |
| §5.3.14 | §3.1.6, §5.1.8.3, §6.2.3, §7.2.3 | |
| §5.3.15 | §6.2.4 | |
| §5.3.16 | §5.1.8.3, §6.4, §7.2.3 | |
| §5.3.17 | §6.2.5, §7.2.4 | |
| §5.3.18 | §6.3 | |
| §5.3.19<br>§5.3.20 | Nie dotyczy | Brak w Polsce producentów czujników ruchu;<br>Jeśli w przyszłości PL-MSA zawrze umowę z producentami czujników ruchu Polityka PL-MSA zostanie uaktualniona i ponownie przedłożona ERCA do akceptacji. |
| §5.3.21 | §3.1.4, §6.3 | |
| §5.3.22 | Nie dotyczy | Brak w Polsce producentów tachografów;<br>Jeśli w przyszłości PL-MSA zawrze umowę z producentami tachografów Polityka PL-MSA zostanie uaktualniona i ponownie przedłożona ERCA do akceptacji. |
| §5.3.23 | §3.4.1, §6.3 | |
| §5.3.24 | §6.3 | |
| §5.3.25 | Nie dotyczy | Ma zastosowanie wyłącznie dla kart (§6.2.1 ) z uwagi na brak w Polsce producentów tachografów. |
| §5.3.26 | §6.1, §6.2.1 | |
| §5.3.27 | §6.2 | |
| §5.3.28 | §6.2.3 | |
| §5.3.29 | §8.1.1 | |
| §5.3.30 | §6.2.3, §8.4 | |
| §5.3.31 | §8.6, §8.8 | |
| §5.3.32 | §8.3 | |
| §5.3.33 | §8.3 | |
| §5.3.34 | Nie dotyczy | Brak w Polsce producentów tachografów. |
| §5.3.35 | §5.1.2, §5.1.8.5 | |
| §5.3.36 | §6.2.6 | |

| Polityka ERCA wer.2.0 | Polityka PL.-MSA | Uwagi |
|---|---|---|
| §5.3.37 | §6.2.1, §6.2.4, §9.6 | |
| §5.3.38 | §9.1, §9.2 | |
| §5.3.39 | §9.3.1, §9.3.2, §9.3.3, §9.3.4 | |
| §5.3.40 | §9.5.1, §9.5.3 | |
| §5.3.41 | §10 | |
| §5.3.42 | §12 | |
| §5.3.43 | §11, §11.2 | |
| §5.3.44 | §11.1 | |
| §5.3.45 | §11.5 | |
| §5.3.46 | §11.4, §11.5 | |

# 1 Wprowadzenie

Niniejszy dokument zawiera krajową politykę bezpieczeństwa dla systemu tachografów cyfrowych w Polsce, zwaną dalej w skrócie „Polityką PL-MSA". Polityka PL-MSA będzie regulować funkcjonowanie systemu tachografów cyfrowych (STC) w Polsce.

Dokument opisuje wymagania dotyczące w szczególności zarządzania kluczami, certyfikatami i urządzeniami, które wchodzą w skład STC.

Polityka PL-MSA jest zgodna z następującymi aktami prawnymi:

- Rozporządzeniem Rady (EWG) nr 3821/85 …… ……[1]
- Rozporządzeniem Rady (WE) nr 2135/98 (http://europa.eu.int/eur-lex/pri/en/oj/dat/1998/l_274/l_27419981009en00010021.pdf) ……..[2]
- Rozporządzeniem Komisji (WE) nr 1360/2002 (http://europa.eu.int/eur-lex/pri/en/oj/dat/2002/l_207/l_20720020805en00010252.pdf) ……..[3]
- dokumentem „Guideline and Template National CA policy"(http://www.urba2000.com/chrono/public/ts-NCA-POLICY%20Guideline%20v1.pdf)……..[4]
- dokumentem „Common Security Guideline" (http://www.urba2000.com/chrono/public/CommonSecurityGuideline10.pdf)..... ..[5]
- dokumentem „The Digital Tachograph European Root Policy v.2.0" (http://dtc.jrc.it/ERCAdocs/SPI04131.pdf) …….....[6]
- Ustawą z dnia 28 lipca 2005 r. o systemie tachografów cyfrowych (Dz.U. 2005, nr 180, poz. 1494)…….....[7]
- Wspólnymi kryteriami. ISO/IEC 15408 (1999): „Technologie informacyjne. Techniki bezpieczeństwa — Kryteria oceny bezpieczeństwa informacji" (części 1–3)"……..... .[CC]
- CEN Workshop Agreement 14167-2: Cryptographic Module for CSP Signing Operations – Protection Profile (MCSO-PP)……...…..[CEN]
- FIPS PUB 140-2 (25 maja 2001 r.): „Security Requirements for Cryptographic Modules". Information Technology Laboratory, National Institute of Standards and Technology (NIST)……....[FIPS]

## 1.1 Cel

Zadaniem STC jest wdrożenie ogólnoeuropejskiego planu zwiększenia efektywności kontroli nad czasem jazdy oraz odpoczynku kierowców ciężarówek i autobusów w celu poprawy bezpieczeństwa ruchu drogowego i warunków pracy.
Środkiem do realizacji tego celu będzie zastąpienie dotychczasowego systemu opartego na papierowych dyskach przez cyfrowe urządzenia rejestrujące. Urządzenia te wymagają od kierowców, organów kontrolnych itp. uwierzytelnienia za pomocą karty elektronicznej i certyfikatu podpisanego elektronicznie. W systemie będą wykorzystywane 4 typy kart elektronicznych: karta kierowcy, karta warsztatowa, karta przedsiębiorstwa i karta kontrolna.

## 1.2 Instytucje odpowiedzialne

**PL-MSA**

Instytucją odpowiedzialną za wdrożenie aktów [1], [2] i [3] w Polsce będzie Ministerstwo Transportu i Budownictwa, zwane dalej, zgodnie z terminologią międzynarodową, PL-MSA. Oficjalne dane kontaktowe są następujące:

Ministerstwo Transportu i Budownictwa

ul. Chałubińskiego 4/6, 00-928 Warszawa
Polska

Telefon: (+48-22) 630-10-00

Faks: (+48-22) 630-11-16
http:// www.mtib.gov.pl

**PL-MSCA**

Podmiotem wyznaczonym zgodnie z Ustawą z dnia 29 lipca 2005 r. o systemie tachografów cyfrowych (Dz.U. nr 180, poz. 1494) jako Centrum Certyfikacji w Polsce (zwanym dalej PL-MSCA), będzie:
Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)
ul. Karczunkowska 30, 02-871 Warszawa
Polska
Telefon: (+48-22) 332-91-00
Faks: (+48-22) 332-91-99

**PL-CIA**

Podmiotem wyznaczonym zgodnie z Ustawą z dnia 29 lipca 2005 r. o systemie tachografów cyfrowych (Dz.U. nr 180, poz. 1494) jako Podmiot Wydający Karty w Polsce (zwanym dalej PL-CIA), będzie:
Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)
ul. Karczunkowska 30, 02-871 Warszawa
Polska
Telefon: (+48-22) 332-91-00
Faks: (+48-22) 332-91-99

**PL-CP**

Centrum Personalizacji w Polsce (zwanym dalej PL-CP) będzie:
Polska Wytwórnia Papierów Wartościowych S.A. (PWPW)
ul. Karczunkowska 30, 02-871 Warszawa
Polska
Telefon: (+48-22) 332-91-00
Faks: (+48-22) 332-91-99

PL-MSCA lub PL-CP mogą zlecić części swoich procesów podwykonawcom. Korzystanie z usług podwykonawców nie zwalnia w żadnym stopniu z odpowiedzialności PL-MSCA oraz PL-CP za realizację zadań im powierzonych.

## 1.3 Zatwierdzenie

Polityka PL-MSA została zatwierdzona przez:
Digital Tachagraph Root Certification Authority
Traceability and Vulnerability Assessment Unit
European Commission
Joint Research Centre, Ispra Establishment (TP.360)
Via E. Fermi, 1
I-21020 Ispra (VA)
w dniu 8 lutego 2006 r.

Dostępność i dane kontaktowe
**Dostępność publiczna:**
Po zatwierdzeniu, Polityka PL-MSA będzie publicznie dostępna pod adresem:
http://www.mtib.gov.pl
**Pytania dotyczące niniejszej Polityki PL-MSA należy kierować do:**

Ministerstwo Transportu i Budownictwa
Departament Dróg i Transportu Drogowego

ul. Chałubińskiego 4/6, 00-928 Warszawa
Polska

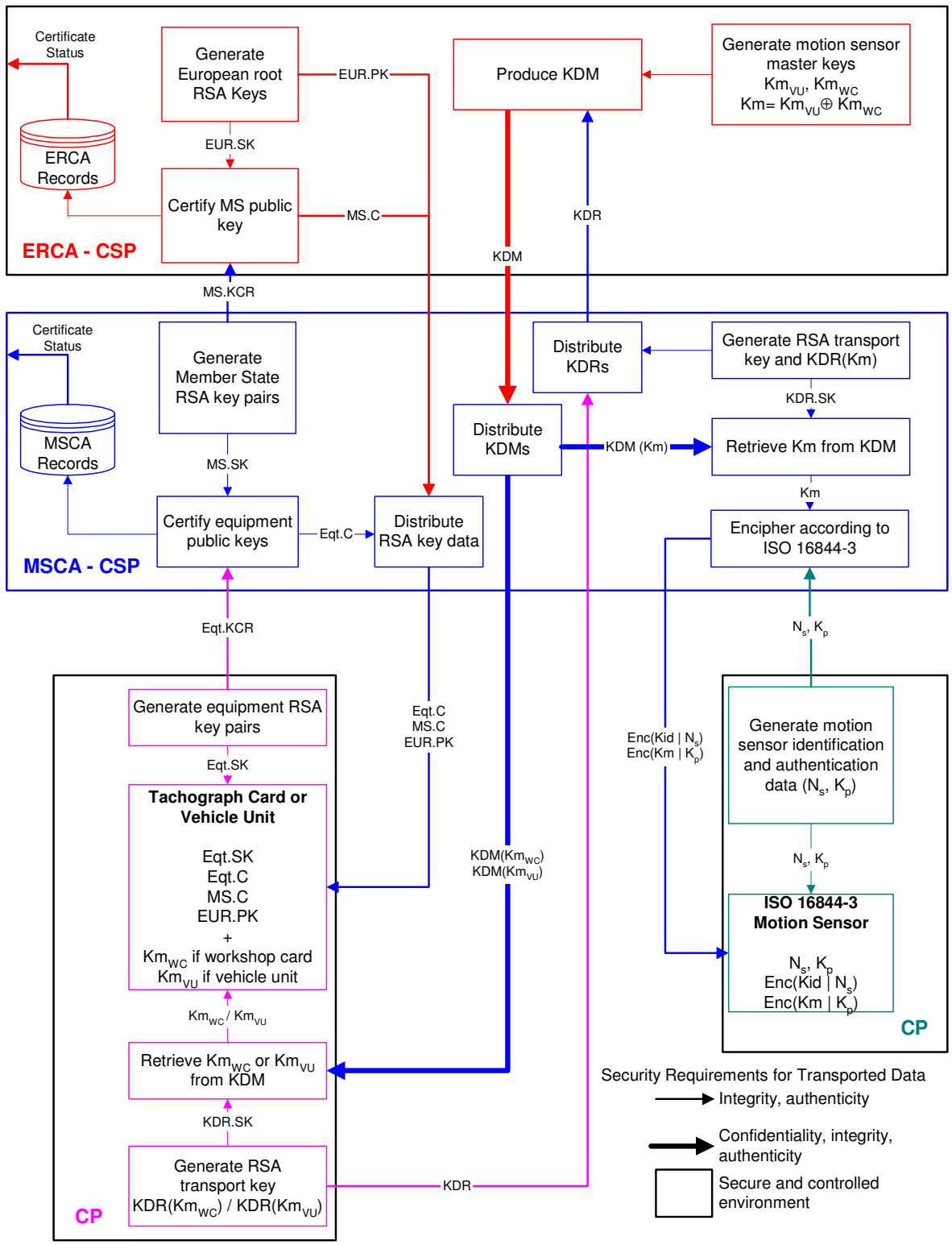
Telefon: (+48-22) 630-12-51 lub 630 12 53

Faks: (+48-22) 630-12-72

**Dane kontaktowe dotyczące niniejszej Polityki PL-MSA:**
Nazwa niniejszego dokumentu: Polityka Organu Państwa Członkowskiego – Polska dla Systemu Tachografów Cyfrowych.
Identyfikator niniejszego dokumentu:
PLMSAPolicy_Polish.pdf — wersja polska
PLMSAPolicy_English.pdf — wersja angielska

# 2 Zakres obowiązywania

Polityka PL-MSA dotyczy wyłącznie STC w Polsce.
Usługi szyfrowania i wydawania certyfikatów świadczone przez PL-MSCA są przeznaczone tylko dla STC.
Karty wydawane przez PL-CP są przeznaczone wyłącznie do użytku w STC.




Na powyższym rysunku została przedstawiona infrastruktura logiczna STC. Obszar obowiązywania Polityki PL-MSA jest zaznaczony liniami pogrubionymi.

# 3 Postanowienia ogólne

## 3.1 Zobowiązania

Niniejszy podrozdział zawiera postanowienia dotyczące zobowiązań następujących podmiotów w zakresie Polityki PL-MSA:

- PL-MSA;
- PL-CIA;
- PL-MSCA;
- PL-CP;
- Użytkownicy STC - posiadacze kart.

### 3.1.1 Zobowiązania PL-MSA

Instytucja PL-MSA jest zobowiązana do:

- Aktualizowania Polityki PL-MSA;
- Wyznaczenia podmiotów PL-MSCA, PL-CIA i PL-CP;
- Kontroli wyznaczonych podmiotów PL-MSCA, PL-CIA i PL-CP;
- Zatwierdzania Deklaracji Praktyk (PS) dla PL-MSCA i PL-CP;
- Informowania wyznaczonych podmiotów o Polityce PL-MSA;
- Przedstawiania Polityki PL-MSA do zatwierdzenia przez ERCA.

### 3.1.2 Zobowiązania PL-CIA

Podmiot wyznaczony jako PL-CIA jest zobowiązany do:

- Przestrzegania Polityki PL-MSA;
- Publikowania PL-CP PS zgodnych z Polityką PL-MSA;
- Zapewnienia, by poprawne informacje z wniosków aplikacyjnych były przekazywane do PL-CP;
- Informowania użytkowników STC o zawartych w Polityce PL-MSA wymaganiach dotyczących korzystania z STC;
- Utrzymywania wystarczających zasobów organizacyjnych i finansowych, aby spełniać wymagania przedstawione w Polityce PL-MSA.

### 3.1.3 Zobowiązania PL-MSCA

Podmiot wyznaczony jako PL-MSCA jest zobowiązany do:

- Przestrzegania Polityki PL-MSA;
- Publikowania PL-MSCA PS zgodnych z Polityką PL-MSA;
- Utrzymywania wystarczających zasobów organizacyjnych i finansowych, aby spełniać wymagania przedstawione w Polityce PL-MSA, zwłaszcza w odniesieniu do odszkodowań;

- Zapewnienia wdrożenie wszystkich wymagań ciążących na PL-MSCA, które są wyszczególnione w Polityce PL-MSA.

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 PS i Polityką PL-MSA.

### 3.1.4 Zobowiązania PL-CP

Podmiot wyznaczony jako PL-CP jest zobowiązany do:

- Przestrzegania Polityki PL-MSA;
- Utrzymywania wystarczających zasobów organizacyjnych i finansowych, aby spełniać wymagania przedstawione w Polityce PL-MSA, zwłaszcza w odniesieniu do odszkodowań.

PL-CP zapewni wdrożenie wszystkich ciążących na nim wymagań, które są wyszczególnione w Polityce PL-MSA.
PL-CP ponosi pełną odpowiedzialność za realizacje wymagań opisanych w Polityce PL-MSA, nawet, jeśli funkcje PL-CP są realizowane przez podwykonawców.

### 3.1.5 Zobowiązania posiadaczy kart

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

## 3.2 Odpowiedzialność

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 użytkowników STC, jedynie wobec PL-MSA i PL-CIA.
Wszelką odpowiedzialność wobec użytkowników STC ponoszą PL-MSA/PL-CIA.

Certyfikaty wydane przez PL-MSCA lub ERCA są przeznaczone wyłącznie do użytku w STC. Inne certyfikaty znajdujące się na kartach stanowią naruszenie Polityki PL-MSA, w związku z czym PL-MSA, PL-CIA, PL-MSCA i PL-CP nie ponoszą żadnej odpowiedzialności za użytkowanie urządzeń z nieautoryzowanymi certyfikatami.

**Odpowiedzialność PL-MSA i PL-CIA wobec użytkowników STC**

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.

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

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

## 3.3 Interpretacja i wykonanie zobowiązań prawnych

### 3.3.1 Obowiązujące ustawodawstwo

Wszelkie kontrowersje wynikłe w czasie wdrażania Polityki PL-MSA będą interpretowane zgodnie z prawem polskim.

## 3.4 Poufność

W celu zapewnienia poufności i ochrony osób prywatnych, przetwarzanie danych osobowych i przenoszenie takich danych są ograniczone zgodnie z Dyrektywą 95/46/EC oraz obowiązującą polską Ustawą o ochronie danych osobowych, Dz.U. 2002, nr 101, poz. 926, wraz z późniejszymi zmianami (**http://www.giodo.gov.pl/data/filemanager_pl/473.doc**)

### 3.4.1 Informacje, które należy traktować jako poufne

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.
Należy zachować poufność wszystkich prywatnych kluczy RSA, kluczy kryptograficznych wykorzystywanych w ramach PL-MSCA/PL-CP zgodnie z niniejszą Polityką PL-MSA.
Logi i dzienniki kontroli nie mogą być udostępniane jako całość chyba, że prawo tego wymaga.

### 3.4.2 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.

# 4 Deklaracja Praktyk (PS)

PL-MSCA i PL-CP muszą mieć instrukcje dokumentujące ich czynności i procedury wykorzystywane do spełnienia wszystkich wymagań określonych w Polityce PL-MSA, zwane Deklaracją Praktyk (PS). PS musi zostać zatwierdzona przez PL-MSA.
W szczególności:

- PS będzie określać zobowiązania wszystkich podmiotów zewnętrznych wspomagających PL-MSCA i PL-CP w wykonywaniu usług, włącznie ze stosownymi politykami i procedurami;
- Zawartość PS zostanie udostępniona PL-MSA, użytkownikom STC i zainteresowanym stronom (np. organom kontrolnym), chociaż PL-MSCA/PL-CP nie są generalnie zobowiązane do udostępniania wszystkich szczegółów swojej działalności publicznie oraz użytkownikom STC;
- Kierownictwo PL-MSCA/PL-CP ponosi odpowiedzialność za to, by PS była właściwie wdrażana;
- PL-MSCA/PL-CP musi zdefiniować proces przeglądu PS;
- PL-MSCA/PL-CP będzie z odpowiednim wyprzedzeniem informować o zmianach,

które zamierza wprowadzić w PS, a także, po zatwierdzeniu tych zmian przez PL-MSA, natychmiast udostępniać zmodyfikowaną wersję PS.

# 5 Zarządzanie urządzeniami STC

Jako urządzenia STC definiuje się:

- Karty elektroniczne;
- Tachografy cyfrowe (VU);
- Czujniki ruchu.

Urządzenia są obsługiwane lub zarządzane przez:

- PL-MSA;
- PL-CIA;
- PL-MSCA;
- PL-CP;
- Producentów VU;
- Producentów czujników ruchu.

**PL-MSA realizuje następujące funkcje:**

- Nadzór nad jakością procesów STC w Polsce;
- Zatwierdzanie PS;
- Monitorowanie bezpieczeństwa PL-MSCA. PL-MSA wdroży odpowiedni system monitorowania zapewniający poprawność procesu generowania certyfikatów przez PL-MSCA i bezpiecznego udostępniania kluczy kryptograficznych zgodnie z wymaganiami aktów [2], [3].

**PL-CIA realizuje następujące funkcje:**

- Rejestrowanie 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, by wydawanie nowych, wznowionych i wymienionych kart było dokonane tylko w przypadku spełnienia warunków określonych w [2], [3] przy zachowaniu obowiązujących terminów;
- Wymienianie informacji z innymi Państwami Członkowskimi;
- Przechowywanie danych dotyczących zarejestrowanych kart oraz udostępnianie informacji o ich statusie.

**PL-CP realizuje następujące funkcje:**

- Przesyłanie wniosków o certyfikaty do PL-MSCA;
- Umieszczanie klucza i certyfikatu na karcie;
- Personalizacja karty
    a) Nanoszenie danych wnioskodawcy na kartę;
    b) Kontrola formatu i kompletności danych.
- Generowanie kodu PIN dla karty warsztatowej;
- Przygotowanie spersonalizowanych kart do wysłania do wnioskodawcy;
- Anulowanie kart, które nie zostały odebrane przez wnioskodawcę;
- Anulowanie unieważnionych kart.

**PL-MSCA wykonuje następujące funkcje:**

- Generowanie kluczy PL-MSCA dla Polski i zarządzanie interfejsem obsługującym proces certyfikacji kluczy PL-MSCA przez ERCA;

## 5.1 Karty

### 5.1.1 Kontrola jakości — funkcja PL-MSCA/PL-CP

PL-MSCA/PL-CP musi zapewnić, że tylko karty posiadające świadectwo homologacji typu będą personalizowane i wydawane do użytku zgodnie z [3].

### 5.1.2 Wniosek 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 o wydanie karty kierowcy, przedsiębiorstwa, warsztatowej lub kontrolnej oraz prawidłową identyfikację osoby prawnej, w imieniu, której wniosek jest składany.
PL-CIA informuje wnioskodawcę o warunkach dotyczących używania karty. Informacje te będą dostępne po polsku, a w razie potrzeby również po angielsku.
Wnioskodawca, składając wniosek o wydanie karty i potwierdzając jej otrzymanie, akceptuje obowiązujące warunki.

#### *5.1.2.1 Umowy*

Składając wniosek o wydanie karty i potwierdzając jej otrzymanie, wnioskodawca zawiera z PL-CIA umowę z następującymi zobowiązaniami:

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

#### *5.1.2.2 Warunki zatwierdzenia przez PL-CIA dotyczące karty kierowcy*

Karty kierowcy będą wydawane osobom mającym miejsce stałego pobytu w Polsce.
PL-CIA podejmie należyte starania, aby sprawdzić, czy wnioskodawca nie posiada innej ważnej karty kierowcy wydanej w Polsce lub 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) i podlega przepisom rozporządzenia (EWG) 3820/85.

### 5.1.3 Okresy ważności kart

Karty kierowcy są ważne przez maksymalnie **pięć** lat, przy czym okres ten nie może być dłuższy niż okres ważności prawa jazdy.
Karty warsztatowe są ważne przez maksymalnie **jeden** rok.
Karty przedsiębiorstwa są ważne przez maksymalnie **pięć** lat, przy czym okres ten nie może być dłuższy niż okres ważności licencji lub zaświadczenia potwierdzającego zgłoszenie przez przedsiębiorcę prowadzenia przewozów drogowych jako działalności pomocniczej

w stosunku do jego podstawowej działalności.
Karty kontrolne są ważne przez maksymalnie **pięć** lat.

### 5.1.4 Wznawianie kart przez PL-CIA

#### *5.1.4.1 Upływ terminu ważności karty*

PL-CIA wyda nową 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 ważności karty.
Procedura w przypadku wniosku o wznowienie karty jest taka sama jak w przypadku wniosku o wydanie nowej karty.

#### *5.1.4.2 Zmiana danych osobowych i administracyjnych*

Zmiana nazwiska kierowcy lub technika, zmiana miejsca pracy technika lub zmiana innych danych istotnych dla identyfikacji posiadacza karty uzasadniają potrzebę wymiany karty, w celu uaktualnienia danych, na podstawie formularza wniosku o wznowienie karty, jeśli poprzednia karta była wydana w Polsce.

### 5.1.5 Zmiana karty przez PL-CIA

#### *5.1.5.1 Zmiana kraju zamieszkania*

Posiadacz karty, wydanej przez inne Państwo Członkowskie UE może złożyć wniosek o nową kartę kierowcy lub zażądać wymiany karty, o ile udowodni, że stale zamieszkuje w Polsce przez co najmniej 185 dni w roku.
Po zaakceptowaniu wniosku o zmianę karty, poprzednia karta zostaje zwrócona PL-CIA. PL-CIA przekazuje tę kartę odpowiedniemu organowi w innym Państwie Członkowskim, który wydał kartę.

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

#### *5.1.6.1 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 otrzymać 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 zgłoszenia kradzieży.
Numer skradzionej karty jest wpisywany na tzw. „czarną listę” dostępną dla upoważnionych organów w innych Państwach Członkowskich.

#### *5.1.6.2 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 w innych Państwach Członkowskich.

#### *5.1.6.3 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 wymagania, PL-CIA wydaje kartę zastępczą z nowymi kluczami i certyfikatem w ciągu 5 dni roboczych od daty otrzymania wypełnionego wniosku.
Karta zastępcza zachowuje okres ważności karty oryginalnej. Jeśli do końca okresu ważności karty zastępczej zostało mniej niż 2 miesiące, PL-CIA wznowi kartę.

### 5.1.7 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.

### 5.1.8 Personalizacja kart

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

#### *5.1.8.1 Personalizacja wizualna*

Karty są personalizowane wizualnie zgodnie z Aneksem do Rozporządzenia 1B [3], a w szczególności:

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

#### *5.1.8.2 Wprowadzanie danych o wniskodawcy*

Dane na karcie powinny być rozmieszczone zgodnie ze strukturą określoną w Rozporządzeniu 1360/2002, Aneks 1B, dodatek 2 [3], reguły TCS_403, TCS_408, TCS_413 i TCS_418, w zależności od typu karty.

#### *5.1.8.3 Zapisywanie kluczy na karcie*

Klucz prywatny musi być zapisywany na karcie w środowisku, 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.

#### *5.1.8.4 Zapisywanie certyfikatu na karcie*

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

#### *5.1.8.5 Kontrola jakości*

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

#### *5.1.8.6 Unieważnienie i zniszczenie niewysłanych kart*

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

#### *5.1.8.7 Unieważnienie i zniszczenie zwróconych kart*

Wszystkie karty, które zostały zwrócone PL-CIA, z wyjatkiem kart, które zostały wydane przez inne państwo członkowskie są niszczone, a PL-CIA prowadzi dokładny 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.

### 5.1.9 Rejestracja kart i przechowywanie danych przez PL-CP i PL-CIA

PL-CP jest zobowiązany rejestrować typy i numery kart wydawane poszczególnym wnioskodawcom. Dane te będą przesyłane z PL-CP do rejestru PL-CIA. PL-CIA będzie również prowadzić aktualny rejestr statusów kart.
PL-CIA prowadzi ewidencję kart wydanych, wznowionych, wymienionych, skradzionych, utraconych i uszkodzonych przez okres co najmniej równy okresowi ich ważności administracyjnej.

### 5.1.10 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. W nocy karty mogą być przechowywane wyłącznie w bezpiecznym środowisku. Wdrożone zostaną formalne procedury dla sytuacji wyjątkowych, w tym zakłóceń w procesie produkcyjnym, niedostarczenia karty wnioskodawcy, jej utraty lub uszkodzenia.
- Spersonalizowane karty były przesyłane do odpowiedniego miejsca, skąd zostaną dostarczone lub wysłane wnioskodawcy;
- Spersonalizowane karty muszą być zawsze oddzielone od niespersonalizowanych.

### 5.1.11 Kody uwierzytelnienia (PIN)

PL-CP jest zobowiązany do wygenerowania osobistego numeru identyfikacyjnego (PIN) do każdej karty warsztatowej.

#### *5.1.11.1 Generowanie kodów PIN*

Kody PIN są co najmniej 4-cyfrowe (Aneks 1B, Dodatek 10: Cele bezpieczeństwa dla VU 4.1.2 [3]), generowane w bezpiecznym systemie i przesyłane w bezpieczny sposób do wnioskodawców kart warsztatowych.

#### *5.1.11.2 Dystrybucja kodów PIN*

Kody PIN i karty warsztatowe nie mogą być wysyłane w tej samej kopercie. PL-CP będzie wysyłać pocztą kody PIN technikom warsztatowym.
Karty warsztatowe będą wysyłane wnioskodawcom kart warsztatowych pocztą.

### 5.1.12 Dezaktywacja karty

W przypadku zwrotu karty do PL-CIA, informacja o tym zostanie przekazana – w razie potrzeby – CIA w innym Państwie Członkowskim.
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.

# 6 Zarządzanie kluczami: klucz publiczny ERCA, klucze PL-MSCA, klucze czujników ruchu i klucze transportowe

Postanowienia dotyczące zarządzania następującymi kluczami:

- Klucz publiczny ERCA;
- Klucze PL-MSCA;
- Klucze czujników ruchu;
- Klucze transportowe (służącymi do transportu między ERCA i PL-MSCA).

**Klucz publiczny ERCA** jest używany do weryfikacji kluczy publicznych 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 czujników ruchu** to klucze symetryczne, które są zapisywane na karcie warsztatowej i w VU. PL-MSCA otrzymuje klucze czujników ruchu od ERCA, przechowuje je i przekazuje producentom.
**Klucze transportowe** służą do zapewnienia bezpieczeństwa wymiany informacji między ERCA i PL-MSCA.
Jeśli PL-MSCA potrzebuje innych kluczy kryptograficznych oprócz powyższych, nie będą one traktowane jako część STC i nie podlegają Polityce PL-MSA.

## 6.1 Klucz publiczny ERCA

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

## 6.2 Klucze PL-MSCA

Para kluczy Państwa Członkowskiego składa się z klucza publicznego (MS.PK) i prywatnego (MS.SK).
W Polsce kluczami Państwa Członkowskiego są klucze PL-MSCA, którymi są podpisywane wszystkie certyfikaty urządzeń.
Klucze publiczne PL-MSCA muszą zostać certyfikowane przez ERCA, ale są generowane zawsze przez PL-MSCA.
Klucze PL-MSCA nie mogą być używane do żadnych innych celów niż podpisywanie certyfikatów do urządzeń i generowania KCR (Key Certification Request).

### 6.2.1 Generowanie kluczy PL-MSCA

Para kluczy PL-MSCA jest generowana w urządzeniu HSM (Hardware Security Module), które:

- Spełnia wymagania określone w standardzie FIPS 140-2 (lub 140-1) na poziomie 3 lub wyższym [FIPS];
- Spełnia wymagania określone w dokumencie CEN Workshop Agreement 14167-2 [CEN];
- Jest systemem z certyfikatem kategorii EAL 4 lub wyższej zgodnie z normą ISO 15408 [CC], E3 lub wyższej według kryteriów ITSEC lub spełnia równoważne kryteria bezpieczeństwa. Jest to docelowy poziom zabezpieczenia lub profil ochrony, który spełnia wymagania niniejszego dokumentu oparty na analizie ryzyka oraz zabezpieczeniach fizycznych i innych zabezpieczeniach nietechnicznych.

Urządzenie do generowania kluczy powinno być urządzeniem wolnostojącym. Opis wymogów urządzenia powinien być zawarty w PL-MSCA PS. Generowanie kluczy PL-MSCA musi odbywać się w środowisku o dużym poziomie bezpieczeństwa fizycznego.
Proces generowania kluczy PL-MSCA powinien odbywać się w obecności co najmniej dwóch osób przy czym przynajmniej jedna z nich musi pełnić rolę CAA lub PA (patrz 9.3.1).
Klucze muszą być generowane z użyciem algorytmu RSA , a długość klucza n = 1024 bity.
PL-MSCA musi mieć co najmniej 2 i nie więcej niż 6 kluczy Pl-MSCA jednocześnie, aby zapewnić właściwy poziom ciągłości działania procesu certyfikacji (proces certyfikacji kluczy PL-MSCA zabiera dużo czasu).

### 6.2.2 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 bezterminowo.
Certyfikaty wydawane przez ERCA mają ważność 7 lat.

### 6.2.3 Przechowywanie kluczy prywatnych PL-MSCA

Klucze prywatne PL-MSCA są przechowywane i eksploatowane wewnątrz bezpiecznego urządzenia, które:

- Spełnia wymagania określone w standardzie FIPS 140-2 (lub 140-1) na poziomie 3 lub wyższym [FIPS];
- Spełnia wymagania określone w dokumencie CEN Workshop Agreement 14167-2 [CEN];
- Jest systemem z certyfikatem kategorii EAL 4 lub wyższej zgodnie z normą ISO 15408 [CC], E3 lub wyższej według kryteriów ITSEC lub spełnia równoważne kryteria bezpieczeństwa. Jest to docelowy poziom zabezpieczenia lub profil ochrony, który spełnia wymagania niniejszego dokumentu oparty na analizie ryzyka oraz zabezpieczeniach fizycznych i innych zabezpieczeniach nietechnicznych.

Dostęp do prywatnych kluczy PL-MSCA wymaga jednoczesnej obecności co najmniej dwóch osób. W żadnym wypadku pojedyncza osoba nie może mieć dostępu do tych kluczy.

### 6.2.4 Kopia zapasowa klucza prywatnego PL-MSCA

Kopie zapasowe kluczy prywatnych PL-MSCA można wykonywać przy użyciu procedury backupowania wymagającej obecności przynajmniej dwóch osób. Procedura jest opisana w

PL-MSCA PS.

### 6.2.5 Deponowanie klucza prywatnego PL-MSCA

Klucze prywatne PL-MSCA nie mogą być deponowane.

### 6.2.6 Naruszenie bezpieczeństwa kluczy PL-MSCA

Musi istnieć pisemna instrukcja, zawarta w PL-MSCA PS, określająca środki, które powinny być zastosowane przez osoby odpowiedzialne za bezpieczeństwo w PL-MSCA, gdy klucze prywatne PL-MSCA zostaną ujawnione lub przypuszcza się, że mogły zostać przechwycone.
W takim przypadku PL-MSCA musi bezzwłocznie poinformować PL-MSA, ERCA i wszystkie MSCA Państw Członkowskich.

### 6.2.7 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.

## 6.3 Klucze czujników ruchu

ERCA będzie wydawać klucze czujników ruchu Km, $Km_{VU}$ i $Km_{WC}$ na wniosek PL-MSCA, zgodnie z zapotrzebowaniem (Aneks 1B, dod. 11; 3.1.3 do Rozporządzenia [3].
PL-MSCA przekazuje klucz warsztatowy $Km_{WC}$ do PL-CP w celu zapisania go na kartach warsztatowych.
PL-CP zapewni, aby na wszystkich wydawanych kartach warsztatowych był zapisany klucz warsztatowy $Km_{WC}$ (Aneks 1B, dod. 11; 3.1.3 do Rozporządzenia [3]).
PL-MSCA i PL-CP chroni przechowywane klucze czujników ruchu z zastosowaniem skutecznych logicznych i fizycznych zabezpieczeń. Klucze są przechowywane i eksploatowane wewnątrz modułu HSM (Hardware Security Module), który:

- Spełnia wymagania określone w standardzie FIPS 140-2 (lub 140-1) na poziomie 3 lub wyższym [FIPS];
- Jest systemem z certyfikatem kategorii EAL 4 lub wyższej zgodnie z normą ISO 15408 [CC], E3 lub wyższej według kryteriów ITSEC lub spełnia równoważne kryteria bezpieczeństwa. Jest to docelowy poziom zabezpieczenia lub profil ochrony, który spełnia wymagania niniejszego dokumentu oparty na analizie ryzyka oraz zabezpieczeniach fizycznych i innych zabezpieczeniach nietechnicznych.

## 6.4 Transport kluczy

Dla bezpiecznej komunikacji pomiędzy ERCA a PL-MSCA muszą być wygenerowane klucze RSA w urządzeniu, które:

- Spełnia wymagania określone w standardzie FIPS 140-2 (lub 140-1) na poziomie 3 lub wyższym [FIPS];
- Jest systemem z certyfikatem kategorii EAL 4 lub wyższej zgodnie z normą ISO 15408 [CC], E3 lub wyższej według kryteriów ITSEC lub spełnia równoważne kryteria bezpieczeństwa. Jest to docelowy poziom zabezpieczenia lub profil ochrony,

który spełnia wymagania niniejszego dokumentu zgodnie z analizą ryzyka oraz zabezpieczenia fizyczne i inne zabezpieczenia nietechniczne.

Do transportu kluczy między PL-MSCA a ERCA muszą być zawsze wykorzystywane środki, media, nośniki i protokoły określone przez Politykę ERCA. Jeśli do transportu kluczy są wykorzystywane nośniki fizyczne, PL-MSA wyznacza upoważnioną osobę do przenoszenia nośnika.
PL-MSCA wnioskuje o certyfikację klucza przy użyciu protokołu KCR określonego w Polityce ERCA, Aneks A.
PL-MSCA akceptuje klucz publiczny ERCA w formacie opisanym w Polityce ERCA, Aneks B.
Identyfikator KID i moduł kluczy przesłanych do ERCA w celu certyfikacji i dystrybucji kluczy czujników ruchu muszą być unikalne w ramach domeny PL-MSCA.
PL-MSCA wnioskuje o klucz czujnika ruchu do ERCA przy użyciu protokołu KDR określonego w Polityce ERCA, Aneks D.

# 7 Klucze urządzenia (asymetryczne)

Klucze urządzenia to asymetryczne klucze wygenerowane przez producenta urządzenia, PL-MSCA lub PL-CP i certyfikowane przez PL-MSCA dla następujących urządzeń:

- Kart,
- VU.

Zasady te nie dotyczą symetrycznych kluczy czujnika ruchu.

## 7.1 Aspekty ogólne dotyczące PL-CP/PL-MSCA

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.

## 7.2 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 bezpiecznym urządzeniu, które:

- Spełnia wymagania określone w standardzie FIPS 140-2 (lub 140-1) na poziomie 3 lub wyższym [FIPS];
- Spełnia wymagania określone w dokumencie CEN Workshop Agreement 14167-2 [CEN];
- Jest systemem z certyfikatem kategorii EAL 4 lub wyższej zgodnie z normą ISO

15408 [CC], E3 lub wyższej według kryteriów ITSEC lub spełnia równoważne kryteria bezpieczeństwa. Jest to docelowy poziom zabezpieczenia lub profil ochrony, który spełnia wymagania niniejszego dokumentu oparty na analizie ryzyka oraz zabezpieczeniach fizycznych i innych zabezpieczeniach nietechnicznych

Klucze są generowane przy użyciu algorytmu RSA o długości klucza $n$ = 1024 bity. (Aneks 1B, [3]).

Sposób przechowywania i generowania prywatnych kluczy musi gwarantować, że klucze prywatne nigdy nie pojawią się jawnie poza systemem, który je wygenerował. Ponadto klucze prywatne powinny być zniszczone od razu po wprowadzeniu ich do urządzeń.

Podmiot generujący klucze musi, stosując odpowiednie środki, zapewnić unikalność klucza publicznego we własnej domenie (należy w tym celu zapewnić, by system generowania kluczy działał w sposób losowy, w związku z czym prawdopodobieństwo wygenerowania identycznych kluczy byłoby bliskie zeru).

### 7.2.1 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.

### 7.2.2 Ważność klucza urządzenia

#### *7.2.2.1 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.

### 7.2.3 Ochrona i przechowywanie kluczy prywatnych karty

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 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.

### 7.2.4 Deponowanie i archiwizacja kluczy prywatnych urządzenia

Kluczy prywatnych urządzenia nie można deponować ani archiwizować.

### 7.2.5 Archiwizacja klucza publicznego urządzenia

Wszystkie certyfikowane klucze publiczne są archiwizowane przez PL-MSCA, lub przez PL-CIA.

### 7.2.6 Wycofanie z użytku kluczy urządzenia

Po zakończeniu korzystania z karty klucz publiczny jest zarchiwizowany, a klucz prywatny jest:

- Niszczony w taki sposób, aby nie można go było odtworzyć;

- Zachowany w taki sposób, aby nie można było z niego ponownie korzystać.

# 8 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.

## 8.1 Wprowadzanie danych

### 8.1.1 Karty

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.

## 8.2 Certyfikaty kart

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

## 8.3 Okres ważności certyfikatu urządzenia

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

- Okres ważności certyfikatów karty kierowcy nie może być dłuższy niż **5** lat;
- Okres ważności certyfikatów karty warsztatowej nie może być dłuższy niż **1** rok;
- Okres ważności certyfikatów karty kontrolnej nie może być dłuższy niż 5 lat;
- Okres ważności certyfikatów karty przedsiębiorstwa nie może być dłuższy niż **5** lat;

## 8.4 Wystawianie certyfikatu urządzenia

Wystawianie certyfikatów przez PL-MSCA odbywa się w sposób pozwalający na utrzymanie ich autentyczności i integralności. Zawartość certyfikatu jest określona w [3], Aneks1B, Dodatek 11.
Sposób przekazywania danych pomiędzy PL-MSCA i PL-CP w celu generowania certyfikatów musi zapewniać zachowanie oryginalności tych danych o ile nie będzie przekazywany klucz prywatny RSA do PL-MSCA do sprawdzenia jego zgodności z odpowiadającym mu kluczem publicznym.

## 8.5 Wznawianie i aktualizacja certyfikatu urządzenia

Patrz rozdział dotyczący zarządzania urządzeniami. Ponieważ okres ważności certyfikatów i kart jest taki sam, są one omawiane łącznie.

## 8.6 Rozpowszechnianie informacji i certyfikatów urządzenia

PL-CIA zapewnia w miarę potrzeb dostępność informacji o certyfikatach dla posiadaczy kart

i odpowiednich podmiotów.

## 8.7 Użytkowanie certyfikatu urządzenia

Certyfikaty systemu tachografów cyfrowych są przeznaczone do użytku wyłącznie w tym systemie.

## 8.8 Anulowanie certyfikatu urządzenia

Mimo iż Polityka PL-MSA nie określa żadnych zasad dotyczących anulowania 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.

# 9 Zarządzanie bezpieczeństwem informacji PL-MSCA i PL-CP

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

## 9.1 Zarządzanie bezpieczeństwem informacji PL-MSCA i PL-CP

PL-MSCA/PL-CP stosuje adekwatne i zgodne z powszechnie przyjętymi standardami procedury administracji i zarządzania bezpieczeństwem informacji.
PL-MSCA/PL-CP ponosi odpowiedzialność za wszystkie aspekty świadczenia usług certyfikacji kart, nawet jeśli część tych funkcji zleca podwykonawcom. PL-MSCA/PL-CP wyraźnie określa zakres odpowiedzialności stron trzecich i podejmuje należyte starania, aby strony trzecie były zobowiązane do wdrożenia wszelkich mechanizmów kontroli wymaganych przez PL-MSCA/PL-CP. PL-MSCA/PL-CP jest zobowiązany do ujawnienia odpowiednich PS wszystkim zainteresowanym.
PL-MSCA/PL-CP przez cały czas utrzymuje infrastrukturę bezpieczeństwa informacji niezbędną do zarządzania bezpieczeństwem w PL-MSCA/PL-CP. Wszelkie zmiany wpływające na poziom bezpieczeństwa są zatwierdzane przez PL-MSA.
PL-MSCA/PL-CP powinny posiadać system zarządzania bezpieczeństwem równoważny normie ISO-17799. Formalna certyfikacja tego systemu nie jest wymagana.

## 9.2 Zarządzanie zasobami PL-MSCA/PL-CP i ich klasyfikacja

PL-MSCA/PL-CP zapewnia odpowiedni poziom ochrony swoich zasobów i informacji.
W szczególności:

- PL-MSCA/PL-CP przeprowadza ocenę ryzyka w celu oszacowania elementów ryzyka i określenia niezbędnych wymagań w zakresie bezpieczeństwa i procedur operacyjnych;
- PL-MSCA/PL-CP prowadzi rejestr zasobów informacji i klasyfikuje je na potrzeby wymagań w zakresie ochrony zgodnie z analizą ryzyka.

## 9.3 Mechanizmy zabezpieczeń związane z personelem PL-MSCA/CP

### 9.3.1 Zaufane role

PL-MSCA i PL-CP, realizując Politykę PL-MSA, powinny rozróżniać trzy role opisane poniżej. Dopuszczalny jest inny podział obowiązków, pod warunkiem, że ochrona przed atakiem od wewnątrz jest przynajmniej równie silna jak w zalecanym poniżej modelu oraz, że role są opisane w PL-MSCA/PL-CP PS.
Aby nikt, działając w pojedynkę, nie mógł samodzielnie obejść zabezpieczeń, zadania w systemach PL-MSCA/PL-CP muszą być wykonywane przez wiele osób. Każde konto w systemach ma ograniczone możliwości, właściwe dla roli posiadacza konta.
Role są następujące:

- Administrator Centrum Certyfikacji lub Administrator Personalizacji (CAA/PA),
- Administrator Systemu (SA),
- Kierownik ds. Bezpieczeństwa Systemów Informacyjnych (ISSO).

Rola CAA/PA obejmuje następujące zadania:

- Generowanie kluczy PL-MSCA;
- Nadzór nad generowaniem certyfikatów;
- Funkcje administracyjne związane z utrzymaniem bazy danych PL-MSCA/PL-CP oraz pomoc przy dochodzeniach w sprawie naruszeń.

Rola SA obejmuje następujące zadania:

- Początkowa konfiguracja systemu, włącznie z bezpiecznym uruchomieniem i wyłączeniem systemu;
- Początkowe tworzenie wszystkich nowych kont;
- Ustawienie początkowej konfiguracji sieci;
- Utworzenie nośnika awaryjnego restartu systemu umożliwiającego odzyskanie sprawności operacyjnej po poważnej awarii systemu;
- Tworzenie kopii zapasowych systemu, aktualizacja i odtwarzanie oprogramowania, w tym bezpieczne przechowywanie i dystrybucja kopii zapasowych do lokalizacji poza siedzibą przedsiębiorstwa.

Rola ISSO obejmuje następujące zadania:

- Przypisywanie uprawnień bezpieczeństwa i praw dostępu CAA/PA;
- Archiwizowanie wymaganych danych systemowych;
- Przeglądanie dziennika kontroli w celu przestrzegania polityki bezpieczeństwa systemu przez CAA/PA; dziennik kontroli jest przeglądany przynajmniej raz na tydzień;
- Osobiste przeprowadzanie lub nadzorowanie corocznej inwentaryzacji danych PL-MSCA/PL-CP;
- Uczestnictwo w generowaniu kluczy PL-MSCA.

ISSO, który mimo, że nie jest bezpośrednio zaangażowany w wystawianie certyfikatów, pełni funkcję kontrolną, badając dane systemowe i dzienniki kontroli w celu sprawdzenia, czy inne osoby działają w ramach swoich kompetencji.

### 9.3.2 Podział ról

W przypadku PL-MSCA/PL-CP każdą z trzech opisanych powyżej ról powinny pełnić inne osoby, a do każdego zadania powinna być przypisana przynajmniej jedna osoba.

### 9.3.3 Wymagania dotyczące wykształcenia, kwalifikacji, doświadczenia i prawa dostępu do informacji niejawnych

Znaczenie krytyczne ma stanowisko CAA/PA, do którego należą zadania związane z tworzeniem certyfikatów oraz zarządzaniem certyfikatami i informacjami o kluczach. Osoba przyjmująca rolę CAA/PA powinna odznaczać się niekwestionowaną lojalnością i wiarygodnością, a także wykazywać się sumiennością i odpowiedzialnością w kwestiach bezpieczeństwa w wykonywaniu swoich codziennych obowiązków.
Wszyscy pracownicy PL-MSCA/PL-CP zajmujący newralgiczne stanowiska, w tym przynajmniej role CAA/PA i ISSO:

- Nie mogą mieć przydzielanych innych obowiązków, które byłyby sprzeczne z ich obowiązkami i odpowiedzialnością jako CAA/PA i ISSO;
- Posiadają nienaganną opinię z poprzednich miejsc pracy, w których pełnili podobne role;
- Są odpowiednio przeszkoleni;
- Są niekarani.

### 9.3.4 Wymagania dotyczące szkoleń

Personel powinien być przeszkolony odpowiednio do swojej roli i stanowiska.

## 9.4 Mechanizmy zabezpieczeń systemu PL-MSCA i PL-CP

PL-MSCA/PL-CP zapewnia 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 jest minimalizowany przez raportowanie incydentów i procedury interwencyjne.

## 9.5 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.

### 9.5.1 Typy rejestrowanych zdarzeń

Funkcje audytu bezpieczeństwa związane z systemem/komputerami PL-MSCA/PL-CP rejestrują, na potrzeby audytu, przynajmniej następujące informacje:

- Tworzenie kont (z uprawnieniami lub bez);
- Żądania transakcji włącznie z zapisem konta żądającego, typu żądania, wskazaniem, czy transakcja została zrealizowana czy nie oraz ewentualną przyczyną niezrealizowania transakcji;
- Instalacja nowego oprogramowania lub aktualizacji oprogramowania;
- Data i godzina oraz inne informacje opisowe o tworzeniu kopii zapasowych;
- Zamknięcia i restarty systemu;
- Data i godzina wszystkich modernizacji sprzętu.

### 9.5.2 Czas przechowywania dziennika kontroli

Dziennik kontroli jest przechowywany przynajmniej przez 7 lat.

### 9.5.3 Ochrona dziennika kontroli

Integralność dzienników kontroli musi być odpowiednio chroniona.
Dzienniki kontroli są weryfikowane i konsolidowane przynajmniej raz na miesiąc. Przy takiej weryfikacji i konsolidacji powinny być obecne przynajmniej dwie osoby pełniące role SA lub ISSO.

### 9.5.4 Procedury tworzenia kopii zapasowej dziennika kontroli

Dwie kopie skonsolidowanego dziennika są przechowywane w osobnych, zabezpieczonych lokalizacjach fizycznych.
Dziennik kontroli jest przechowywany w sposób umożliwiający analizę w trakcie jego czasu przechowywania.
Dziennik kontroli jest chroniony przed dostępem bez uprawnień.

## 9.6 Planowanie ciągłości PL-MSCA/PL-CP

PL-MSCA/PL-CP musi mieć plan ciągłości operacyjnej. Plan ten musi w szczególności obejmować następujące zdarzenia:

- Przechwycenie kluczy;
- Katastrofalna utrata danych wskutek np. kradzieży, pożaru, awarii sprzętu lub oprogramowania;
- Awarie systemowe innych rodzajów.

### 9.6.1 Przechwycenie kluczy PL-MSCA

Postępowanie w przypadku przechwycenia kluczy PL-MSCA musi być zgodne z Polityką ERCA.

## 9.7 Fizyczne mechanizmy zabezpieczeń PL-MSCA i PL-CP

W celu kontroli dostępu do sprzętu i oprogramowania PL-MSCA lub PL-CP wdrażane są fizyczne mechanizmy zabezpieczeń. Obejmują one stacje robocze i inne elementy infrastruktury sprzętowej personalizacji i PL-MSCA oraz kartę lub moduł dowolnego zewnętrznego urządzenia szyfrującego.
Klucze PL-MSCA do podpisywania certyfikatów są fizycznie i logicznie chronione w sposób opisany w PS.
W ośrodku PL-MSCA/PL-CP 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.

### 9.7.1 Dostęp fizyczny

Dostęp do pomieszczeń PL-MSCA/PL-CP mają wyłącznie osoby pełniące jedną z powyżej opisanych ról. Dostęp jest kontrolowany przez zastosowanie listy kontroli dostępu do pomieszczenia z ich systemami.

# 10 Rozwiązanie PL-MSCA lub PL-CP

## 10.1 Ostateczne rozwiązanie — zobowiązania PL-MSA

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.

## 10.2 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 dawnego podmiotu.

PL-MSA zapewnia przeniesienie obowiązków i zasobów w sposób uporządkowany.
Poprzedni PL-MSCA przenosi wszystkie klucze PL-MSCA do nowego MSCA w sposób ustalony przez PL-MSA.
Poprzedni PL-MSCA niszczy wszystkie kopie kluczy, które nie zostały przeniesione.

# 11 Audyt

PL-MSA jest zobowiązany do przeprowadzania audytów PL-MSCA i PL-CP.

## 11.1 Częstotliwość audytu zgodności

PL-MSCA/PL-CP działający w ramach Polityki PL-MSA jest przynajmniej raz na 12 miesięcy poddawany audytowi sprawdzającemu zgodność jego działania z Polityką PL-MSA.

## 11.2 Zakres audytu

Audyt obejmuje PL-MSCA/PL-CP PS w zakresie ustalonym przez ERCA Policy [6], §5.3.
Audyt obejmuje przestrzeganie Polityki PL-MSA przez PL-MSCA/PL-CP.
Audyt uwzględnia również działania ewentualnych podwykonawców.

## 11.3 Podmiot prowadzący audyt

PL-MSA może skonsultować zatwierdzenie PL-MSCA/PL-CP PS z zewnętrzną instytucją certyfikującą lub akredytacyjną, aby wdrożenie było bardziej wiarygodne dla zainteresowanych stron.

## 11.4 Działania podejmowane w przypadku nieprawidłowości

Jeśli w wyniku audytu zostaną wykryte nieprawidłowości, PL-MSA podejmuje odpowiednie działania w zależności od elementów ryzyka i ich istotności. Raporty z audytów wysyłane do ERCA powinny zawierać opis działań naprawczych i harmonogram ich wdrożenia.

## 11.5 Przesyłanie wyników

Wyniki audytów stanu bezpieczeństwa (w jęz. angielskim) są przesyłane do ERCA.

# 12 Procedury zmian Polityki PL-MSA

## 12.1 Elementy, które można zmieniać bez powiadomienia

Bez powiadomienia można w Polityce PL-MSA i wprowadzać wyłącznie następujące zmiany:

- Poprawki redaktorskie lub drukarskie;
- Zmiany danych kontaktowych.

## 12.2 Zmiany wymagające powiadomienia

### 12.2.1 Okres wyprzedzenia

Każdy element w Polityce PL-MSA można zmienić, powiadamiając o tym z wyprzedzeniem **90** dni.
O zmianach elementów, które w opinii instytucji odpowiedzialnej za Politykę PL-MSA **nie będą** miały istotnego wpływu na znaczącą liczbę użytkowników lub podmiotów korzystających z Polityki PL-MSA , można powiadamiać z wyprzedzeniem **30** dni.

### 12.2.2 Okres zgłaszania uwag

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

### 12.2.3 Powiadamiane podmioty

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

- ERCA;
- PL-MSCA, PL-CIA i PL-CP.

### 12.2.4 Okres poprzedzający wejście zmian w życie

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

## 12.3 Zmiany wymagające zatwierdzenia nowej Polityki PL-MSA

Jeśli PL-MSA uzna, że zmiana Polityki PL-MSA ma istotny wpływ na znaczną liczbę użytkowników STC, PL-MSA przesyła zmienioną Politykę PL-MSA do zatwierdzenia przez ERCA.

# 13 Definicje i skróty

## 13.1 Definicje

**Polityka MSA**: zbiór reguł, które określają zakres stosowania kluczy, certyfikatów i urządzeń dla danej grupy użytkowników stosowania ujednoliconych wymagań w zakresie bezpieczeństwa.
**Karta**: karta wyposażona w procesor.
**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 STC stosuje się następujące urządzenia: karty, VU i czujniki ruchu.
**Producent/producent urządzeń**: producenci VU lub czujników ruchu.
**Klucz czujnika ruchu**: klucz symetryczny używany w czujniku ruchu i VU, który umożliwia wzajemną autentykację tych urządzeń.
**Deklaracja Praktyk**: deklaracja, że w procesach STC przestrzegane są wymogi bezpieczeństwa określone w polityce. Deklaracja Praktyk 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.
**Klucze RSA**: Algorytm szyfrowania wykorzystywany w przypadku kluczy asymetrycznych w STC.
**Typy kart**: cztery typy kart wykorzystywanych w STC: karta kierowcy, karta przedsiębiorstwa, karta warsztatowa, karta kontrolna.

## 13.2 Lista skrótów

| | |
|---|---|
| CA | Certification Authority (Centrum Certyfikacji) |
| CAA/PA | Certification Authority Administrator/ Personalization Administrator (Administrator Centrum Certyfikacji lub Administrator Personalizacji) |
| CAS | Certification Authority System (Centrum Certyfikacji) |
| CIA | Card Issuing Authority (Podmiot Wydający Karty) |
| CC | Common Criteria (Wspólne Kryteria Bezpieczeństwa) |
| CP | Card Personalisation Centre (Centrum Personalizacji Kart) |
| CPS | Certification Practice Statement (Deklaracja Praktyk ) |
| DTS | Digital Tachograph System (System Tachografów Cyfrowych) |
| ERCA | European Root Certification Authority (Główne Europejskie Centrum Certyfikacji) |
| ISSO | Information System Security Officer (Kierownik ds. Bezpieczeństwa Systemów Informacyjnych) |
| ITSEC | Information Technology Security Evaluation Criteria (Kryteria oceny bezpieczeństwa technologii informatycznej) |
| KG | Key Generation (Generowanie kluczy) |
| MS | Member State (Państwo Członkowskie) |
| MSA | Member State Authority (Instytucja Wdrażająca STC w Państwie Członkowskim) |
| MSCA | Member State Certification Authority (Centrum Certyfikacji Państwa Członkowskiego) |
| PIN | Personal Identification Number (osobisty numer identyfikacyjny) |
| 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 Policy | Polish Member State Authority Policy (Polityka MSA) |
| RSA | Konkretny algorytm klucza publicznego |
| SA | System Administrator (Administrator Systemu) |
| PS | Practice Statement (Deklaracja Praktyk) |
| VU | Vehicle Unit (tachograf cyfrowy) |