Polityka świadczenia usług dla dowodu osobistego z warstwą elektroniczną

Spis treści

Polityka świadczenia usług dla dowodu osobistego z warstwą elektroniczną

1. Wstęp

1.1. Wprowadzenie

Niniejszą Politykę stosuje się do usług certyfikacji w zakresie wydawania certyfikatów dla osób fizycznych i wydawania środka identyfikacji elektronicznej opartego o dowód osobisty z warstwą elektroniczną zgodnie z wymaganiami określonymi w Rozporządzeniu Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE. Polityka stanowi własność intelektualną CPD MSWiA. Polityka określa ogólne zasady stosowane przez MSWiA w trakcie świadczenia usług zaufania w szczególności:

- Wydawania certyfikatów:
    - do identyfikacji i uwierzytelnienia
    - do podpisu osobistego (zaawansowanego podpisu elektronicznego)
    - do potwierdzania obecności
- Zawieszenia, cofnięcia zawieszenia i unieważnienia certyfikatów

Usługi certyfikacji, w zakresie wydawania certyfikatów, zostały zaprojektowane i wdrożone w taki sposób, aby spełnić wymagania nałożone przez krajową Ustawę o dowodach osobistych, Ustawę o usługach zaufania oraz identyfikacji elektronicznej i stosowne rozporządzenia, a także wymagania innych, obowiązujących norm prawnych oraz istniejących standardów międzynarodowych w zakresie tworzenia i funkcjonowania systemów PKI, w szczególności z uwzględnieniem zaleceń zawartych w standardzie ETSI EN 319 411-1 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements” oraz RFC 3647 "Certificate Policy and Certification Practices Framework".

Niniejsza Polityka definiuje także uczestników tego procesu, ich obowiązki odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań certyfikatów.

1.2. Nazwa dokumentu i wersjonowanie

Identyfikator niniejszego dokumentu Polityki.

Nazwa Polityki	**Polityka świadczenia usług dla dowodu osobistego z warstwą elektroniczną.**
Wersja Polityki	1.2
Status wersji	W zatwierdzeniu

Numer referencyjny/OID (ang. Object Identifier)	1.2.616.1.101.5.2.1.1.1.0.1.2
Data publikacji Polityki	6.10.2021 r.
Data wprowadzenia w życie Polityki	7.11.2021 r.
Data wygaśnięcia	Do odwołania

Niniejszy dokument Polityki jest zbiorem polityk i regulaminów stosowanych przez MSWiA przy wydawaniu dowodu osobistego z warstwą elektroniczną. Identyfikator Polityki nie jest umieszczany w treści wystawianych certyfikatów. W wydawanych przez siebie certyfikatach dla dowodów osobistych, MSWiA umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru identyfikatorów polityk certyfikacji określanych w rozdz. 7.1 niniejszego dokumentu. Niniejsza Polityka jest jedynym i głównym dokumentem regulującym wydawanie niekwalifikowanych certyfikatów na potrzeby Elektronicznego Dowodu Osobistego.

1.3. Uczestnicy PKI

W skład systemu PKI obsługiwanego przez MSWiA, realizującego usługi zaufania wchodzą:

- Urzędy certyfikacji (CA), tj. Podmioty wydające certyfikaty;
- Urzędy Gmin;
- Obywatele RP;
- Strony ufające;

Hierarchia PKI dla certyfikatów zawartych w dowodach osobistych z warstwą elektroniczną:

	Parametr	**Wartość**
Level1 - Root CA	Nazwa DN	CN=pl.ID Root CA SERIALNUMBER=2019 C=PL
	Numer seryjny	2e 96 f5 99 0b 4d 0b 93 e0 e6 c1 3c 82 71 cd 4b
	Identyfikator klucza	55 d1 52 32 bc ef ca ec fe 33 b0 18 e7 37 ee e3 b8 2f ab 47
	Odcisk palca [SHA-1]	d0 73 b9 d7 66 a7 37 85 dd 5b a6 7c 32 f2 11 83 a6 0f 13 79
	Odcisk palca [SHA-256]	5a 54 5d c7 80 b8 40 09 00 b2 c1 40 0e 87 1c 43 f0 e0 f3 ad 33 ca 31 c5 08 a9 e9 b1 ab 73 10 95
Level2 - OCSP	Nazwa DN	CN=pl.ID Root CA OCSP SERIALNUMBER=*RRRR (rok wydania)* C=PL

Level2 - Sub CA	Nazwa DN	CN=pl.ID Authentication CA O=MSWiA OU=CPD C=PL SERIALNUMBER=*RRRRMMDD (data wydania)*
Level3 - OCSP	Nazwa DN	CN=pl.ID Authentication CA OCSP O=MSWiA OU=CPD C=PL SERIALNUMBER=*RRRRMMDD (data wydania)*
Level2 - Sub CA	Nazwa DN	CN=pl.ID Authorization CA O=MSWiA OU=CPD C=PL SERIALNUMBER= *RRRRMMDD (data wydania)*
Level3 - OCSP	Nazwa DN	CN=pl.ID Authorization CA OCSP O=MSWiA OU=CPD C=PL SERIALNUMBER=*RRRRMMDD (data wydania)*
Level2 - Sub CA	Nazwa DN	CN=pl.ID Presence CA O=MSWiA OU=CPD C=PL SERIALNUMBER=*RRRRMMDD (data wydania)*
Level3 - OCSP	Nazwa DN	CN=pl.ID Presence CA OCSP O=MSWiA OU=CPD C=PL SERIALNUMBER=*RRRRMMDD (data wydania)*

Aktualna lista zaświadczeń certyfikacyjnych wystawionych z urzędu „pl.ID Root CA” jest dostępna pod adresem:

http://repo.e-dowod.gov.pl/certs/

1.4. Zakres stosowania certyfikatów

W ramach Polityki wystawiane są dla obywateli certyfikaty:

Nazwa typu certyfikatu	Zakres zastosowania
Certyfikat do identyfikacji i uwierzytelnienia	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są osobom prywatnym. Certyfikaty powinny być stosowane do realizacji usługi uwierzytelnienia posiadacza. Certyfikaty mogą być stosowane do uwierzytelnienia klienta w protokole TLS.
Certyfikat dla zaawansowanego podpisu elektronicznego	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są osobom prywatnym. Certyfikaty powinny być stosowane do składania zaawansowanych podpisów elektronicznych, zapewniających integralność oraz niezaprzeczalność podpisywanej informacji. Certyfikaty nie mogą być stosowane do szyfrowania danych lub kluczy kryptograficznych (ogólnie, w operacjach, których celem jest nadanie informacji cech poufności).
Certyfikat do potwierdzania obecności	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty wydawane są osobom prywatnym. Certyfikaty powinny być stosowane do realizacji usługi potwierdzenia obecności posiadacza w "danym miejscu".

MSWiA nie odpowiada za skutki użycia Certyfikatów do innych celów niż opisano w rozdziale 1.4 Polityki. Powyższe ograniczenie odnosi się zarówno do Obywateli, jak i Stron ufających weryfikujących dane zabezpieczone elektronicznie z użyciem dowodu osobistego z warstwą elektroniczną.

1.5. Zarządzanie Polityką

1.5.1.Organizacja odpowiedzialności za administrowanie dokumentem

Centrum Personalizacji Dokumentów MSWiA
ul. Smyczkowa 10
02-678 Warszawa
Polska
REGON: 017232705

1.5.2.Kontakt

Centrum Personalizacji Dokumentów MSWiA
ul. Smyczkowa 10
02-678 Warszawa
Polska
E-mail: [adres email] cc@cpd.mswia.gov.pl
Numer telefonu: 47 72 17 863 – w godzinach 10:00 – 14:00

1.5.3.Podmioty określające aktualność zasad określonych w dokumencie

Za ocenę aktualności i przydatności niniejszej Polityki oraz innych dokumentów dotyczących usług PKI, świadczonych przez CPD MSWiA, a także za zgodność między wymienionymi dokumentami, odpowiada dedykowany zespół w CPD MSWiA. Wszelkie zapytania i uwagi związane z zawartością wymienionych dokumentów powinny być kierowane pod adres podany w punkcie 1.5.2.

1.5.4.Procedura zatwierdzania Polityki

Nowa wersja dokumentu o statusie w zatwierdzeniu staje się obowiązującą Polityką i przyjmuje status aktualny, jeśli w ciągu 10 dni roboczych od daty opublikowania, zespół w CPD MSWiA nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości.

1.6. Słownik

- **Algorytm ECDSA** - (ang. Elliptic Curve Digital Signature Algorithm) - algorytm krzywych eliptycznych używany w procesie cyfrowego podpisu. Określony jest jednoznacznie przez identyfikator obiektu „{joint-iso-itu-t(2) international-organizations(23) set(42) vendor(9) 11 4 1}".
- **Blankiet** - Niespersonalizowany blankiet Dowodu Osobistego wytwarzany i dostarczany przez PWPW do CPD MSWiA. Po spersonalizowaniu Blankiet staje się Dowodem Osobistym.
- **Centrum Certyfikacji CPD MSWiA** - jednostka organizacyjna wystawiająca certyfikaty znajdująca
  się w Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji.
- **Certyfikat klucza publicznego** - certyfikat klucza weryfikującego podpis lub certyfikat klucza szyfrującego.
- **Certyfikat klucza weryfikującego podpis** - elektroniczne zaświadczenie, za pomocą którego klucz weryfikujący podpis jest przyporządkowany do osoby składającej podpis elektroniczny i które umożliwia identyfikację tej osoby.
- **CPD MSWiA** - Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji. Jednostka administracji państwowej odpowiedzialna za personalizację dokumentów takich jak dowód osobisty, paszport i inne.
- **Dowód Osobisty** - Dokument stwierdzający tożsamość i obywatelstwo polskie osoby na terytorium Rzeczypospolitej Polskiej oraz innych państw członkowskich Unii Europejskiej, państw Europejskiego Obszaru Gospodarczego nienależących do Unii Europejskiej oraz państw niebędących stronami umowy o Europejskim Obszarze Gospodarczym, których obywatele mogą korzystać ze swobody przepływu osób na podstawie umów zawartych przez te państwa ze Wspólnotą Europejską i jej państwami członkowskimi oraz na podstawie jednostronnych decyzji innych państw, uznających ten dokument za wystarczający do przekraczania ich granic. Dokument uprawniający także do przekraczania granic państw, o których mowa powyżej. Dokument umożliwiający identyfikację elektronicznej obywatela oraz składanie zaawansowanego podpisu elektronicznego w rozumieniu Rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

- **HSM** (ang. Hardware Security Module) – sprzętowy moduł kryptograficzny stosowany w celu generowania, przechowywania lub używania kluczy kryptograficznych.
- **eIDAS** - Rozporządzenie (UE) nr 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.
- **Klucz** - liczba, symbol lub ciąg liczb lub symboli jednoznacznie wyznaczający przekształcenie kryptograficzne spośród rodziny przekształceń zdefiniowanej przez algorytm kryptograficzny.
- **Klucz podpisujący** - klucz prywatny służący do składania podpisu elektronicznego; klucz podpisujący stanowi dane służące do składania podpisu elektronicznego w rozumieniu Ustawy.
- **Klucz weryfikujący podpis** - klucz publiczny służący do weryfikowania podpisu elektronicznego; klucz weryfikujący podpis stanowi dane służące do weryfikacji podpisu elektronicznego lub dane służące do weryfikacji poświadczenia elektronicznego w rozumieniu Ustawy.
- **Klucze infrastruktury** - klucze kryptograficzne algorytmów kryptograficznych stosowane do:
    - uzgadniania lub dystrybucji kluczy zapewniających poufność danych w protokołach komunikacyjnych,
    - zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń,
    - weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego.

- **Lista CRL** - lista unieważnionych i zawieszonych certyfikatów klucza publicznego wystawionych przez dany podmiot świadczący usługi certyfikacyjne oraz ewentualnie unieważnionych zaświadczeń certyfikacyjnych wystawionych przez ten podmiot. Lista jest poświadczona elektronicznie przez podmiot świadczący usługi certyfikacyjne.
- **MSWiA** - Ministerstwo Spraw Wewnętrznych i Administracji.
- **NIST** (ang. National Institute of Standards and Technology) - amerykańska agencja federalna spełniająca funkcję Narodowego Biura Standaryzacji).
- **OCSP** (ang. Online Certificate Status Protocol) - protokół komunikacyjny oraz serwis on-line zawierający wskazania na aktywne, zawieszone i unieważnione certyfikaty klucza publicznego wystawione przez dany podmiot świadczący usługi certyfikacyjne.
- **PESEL** - Powszechny Elektroniczny System Ewidencji Ludności.
- **PKI** (ang. Public Key Infrastructure) - Infrastruktura Klucza Publicznego, jest to system, na który składają się polityka, procedury i systemy komputerowe niezbędne do świadczenia usług uwierzytelniania, szyfrowania, integralności i niezaprzeczalności za pośrednictwem kryptografii klucza publicznego, klucza prywatnego i certyfikatów elektronicznych.
- **Polityka** - niniejsza Polityka świadczenia usług dla dowodu osobistego z warstwą elektroniczną stanowiąca politykę certyfikacji.
- **SHA** (ang. Secure Hash Algorithms) - rodzina powiązanych ze sobą kryptograficznych funkcji skrótu zaprojektowanych przez NSA (National Security Agency) i publikowanych przez National Institute of Standards and Technology.
- **SPD** - System Personalizacji Dokumentów używany przez CPD MSWiA do personalizacji dowodów osobistych.
- **Strona ufająca** - osoba fizyczna lub prawna, która polega na identyfikacji elektronicznej lub usłudze zaufania.

- **Ścieżka certyfikacji** - uporządkowany ciąg certyfikatów urzędów i certyfikatu obywatela; dane służące do weryfikacji pierwszego certyfikatu są dla weryfikującego „punktem zaufania".
- **RDO** – Rejestr Dowodów Osobistych.
- **TLS** (ang. Transport Layer Security) - jest to protokół, który służy do bezpiecznej wymiany danych za pośrednictwem Internetu.
- **TTP** - W kryptografii zaufana strona trzecia (TTP) to podmiot ułatwiający interakcje między dwiema stronami, które ufają stronie trzeciej; strona trzecia dokonuje przeglądu wszystkich krytycznych komunikatów dotyczących transakcji między stronami, w oparciu o łatwość tworzenia fałszywych treści cyfrowych
- **Usługa zaufania** - oznacza usługę elektroniczną obejmującą: tworzenie, weryfikację i walidację podpisów elektronicznych oraz certyfikatów powiązanych z tymi usługami; Ustawę o dowodach osobistych – Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych wraz z późniejszymi zmianami, zwaną dalej „Ustawą o dowodach".
- **Ustawa o ochronie danych osobowych** – Ustawa z dnia 10 maja 2018 r. o ochronie danych osobowych.
- **Ustawa o usługach zaufania oraz identyfikacji elektronicznej** - Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. (Dz. U. 2016 Poz. 1579) wraz z późniejszymi zmianami, zwaną dalej „Ustawą o usługach zaufania".
- **Uwierzytelnienie** - oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej.
- **X.509** - Standard definiujący konstrukcję certyfikatu klucza publicznego i listy certyfikatów unieważnionych.

Określenia wykorzystywane w niniejszej Polityce, a niezdefiniowane powyżej należy interpretować zgodnie z definicjami zawartymi w Ustawie.

2. Publikowanie i repozytorium

2.1. Repozytorium

1. W ramach swoich obowiązków CPD MSWiA prowadzi repozytorium dostępne dla odbiorców usług certyfikacyjnych.
2. Repozytorium jest dostępne w sieci internetowej za pomocą protokołu OCSP via http oraz stron www. Protokołem OCSP na żądanie Strony ufającej udostępniona będzie informacja o statusie certyfikatu.
3. Repozytorium jest dostępne całą dobę, przez wszystkie dni w roku. Ewentualny czas niedostępności repozytorium nie może każdorazowo przekroczyć *2 godzin*, zaś minimalna dostępność w skali miesiąca to 99% czasu.

2.2. Publikowanie w postaci elektronicznej

Polityki są publikowane elektronicznie w postaci plików w formacie PDF na stronie internetowej MSWiA pod adresem http://e-dowod.gov.pl, oraz na stronie podmiotowej BIP MSWiA pod adresem https://www.gov.pl/web/mswia/polityka-certyfikacji

W postaci elektronicznej publikowane są następujące dokumenty:

1. wszystkie wersje Polityki, z podaniem okresu ich obowiązywania
2. certyfikaty urzędów certyfikacji służące do weryfikacji certyfikatów kluczy publicznych wystawionych zgodnie z Polityką
3. zasady i warunki świadczenia usług

2.3. Częstotliwość publikacji

1. Status certyfikatu w usłudze OCSP jest aktualizowany każdorazowo i niezwłocznie, gdy nastąpi wydanie nowego certyfikatu.
2. W przypadku wystąpienia zdarzenia unieważnienia/zawieszenia/cofnięcia zawieszenia status certyfikatu w usłudze OCSP jest aktualizowany niezwłocznie, zgodnie z zapisami Ustawy o dowodach.
3. Nowe wersje Polityk, Regulaminów są publikowane niezwłocznie po zatwierdzeniu**.**

2.4. Dostęp do repozytoriów

1. Repozytorium plików jest ogólnodostępne w trybie "do odczytu", w celu pobrania opublikowanych tam danych lub dokumentów.
2. Realizuje się kontrolę dostępu uniemożliwiającą dokonywanie nieautoryzowanych zmian statusów certyfikatów lub innych dokumentów umieszczonych w repozytorium.

3. Zasady identyfikacji i uwierzytelnienia

Wniosek o wydanie dowodu osobistego składa osoba posiadająca pełną zdolność do czynności prawnych. W imieniu osoby nieposiadającej zdolności do czynności prawnych lub posiadającej ograniczoną zdolność do czynności prawnych ubiegającej się o wydanie dowodu osobistego wniosek składa rodzic, opiekun lub kurator. Wniosek o wydanie dowodu osobistego składa się osobiście w siedzibie organu gminy na piśmie utrwalonym w postaci papierowej. Wniosek o wydanie dowodu osobistego osobie do 12. roku życia można złożyć na piśmie utrwalonym w postaci elektronicznej. Tożsamość osoby ubiegającej się o wydanie dowodu osobistego ustala się na podstawie ważnego dowodu osobistego lub ważnego dokumentu paszportowego tej osoby, a w przypadku osób, które nabyły obywatelstwo polskie, na podstawie posiadanego dokumentu podróży lub innego dokumentu stwierdzającego tożsamość. Jeżeli osoba ubiegająca się o wydanie dowodu osobistego nie posiada ww. dokumentów, organ gminy ustala jej tożsamość na podstawie danych zawartych w dostępnym rejestrze PESEL oraz w Rejestrze Dowodów Osobistych.

Przepisy prawa gwarantują, że tożsamość osoby, której dotyczy wniosek o wydanie dowodu osobistego, co najmniej raz jest weryfikowana osobiście przez urzędnika przyjmującego wniosek, z wyjątkiem osoby, która nie ukończyła 5. roku życia.

Dowód osobisty odbiera się osobiście. Dowód osobisty osoby nieposiadającej zdolności do czynności prawnych odbiera rodzic albo opiekun, a dowód osobisty osoby posiadającej ograniczoną zdolność do czynności prawnych odbiera osoba ubiegająca się o wydanie dowodu

osobistego, rodzic albo kurator. Odbiór dowodu osobistego wydanego osobie nieposiadającej zdolności do czynności prawnych albo posiadającej ograniczoną zdolność do czynności prawnych wymaga obecności tej osoby, z wyjątkiem osoby, która nie ukończyła 5. roku życia albo ukończyła 5. rok życia i nie ukończyła 12. roku życia, jeżeli osoba ta była obecna przy składaniu wniosku w siedzibie organu gminy. Odbioru dowodu osobistego może dokonać pełnomocnik, składając pełnomocnictwo szczególne do dokonania tej czynności, w przypadku gdy wniosek o wydanie dowodu osobistego został złożony w miejscu pobytu wnioskodawcy albo gdy osoba ubiegająca się o wydanie dowodu osobistego powiadomi organ gminy o niemożności osobistego odebrania dowodu osobistego z powodu choroby, niepełnosprawności lub innej niedającej się pokonać przeszkody, która powstała po dniu złożenia tego wniosku.

Poza tym, wyłącznie posiadacz dowodu osobistego jest uprawniony do odbioru koperty z kodem umożliwiającym odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego oraz do ustalenia kodów umożliwiających identyfikację elektroniczną i złożenie podpisu osobistego.

W przypadku gdy osoba ubiegająca się o wydanie dowodu osobistego nie może osobiście odebrać dowodu osobistego z powodu choroby, niepełnosprawności lub innej niedającej się pokonać przeszkody i wyrazi wolę ustalenia przy odbiorze dowodu osobistego kodów umożliwiających identyfikację elektroniczną i złożenie podpisu osobistego, odbiór dowodu osobistego, ustalenie tych kodów oraz odbiór kodu umożliwiającego odblokowanie certyfikatu identyfikacji i uwierzytelnienia oraz certyfikatu podpisu osobistego w miejscu pobytu tej osoby, po uprzednim powiadomieniu, zapewnia, po spełnieniu ustalonych warunków, właściwy organ gminy.

3.1. Zasady nadawania nazw

Certyfikaty wydawane w ramach dowodu z warstwą elektroniczną są certyfikatami w standardzie x.509v3, tworzonymi w zgodzie z wymogami zawartymi w standardach europejskich ETSI EN 319 412-(1 do 2), a także RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile.

Budowa numerów identyfikacyjnych osób fizycznych, dla których wydawane będą dowody osobiste z warstwą elektroniczną, będzie zgodna ze składnią zdefiniowaną w standardzie ETSI EN 319-412-1.

3.1.1.Typy nazw

Pole identyfikatora podmiotu ‘subject’ umożliwia zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu. Pole ‘subject’ musi zawierać niepustą nazwę wyróżniającą podmiotu. Zawartość pola Odbiorca certyfikatu będzie zgodna z wytycznymi standardu ETSI EN 319-412-2 oraz rekomendacji ITU-T X.520.

3.1.2.Konieczność używania nazw znaczących

W celu zapewnienia możliwości jednoznacznej identyfikacji Odbiorcy certyfikatu, w polu identyfikatora podmiotu ‘subject’ wystąpią co najmniej atrybuty:

Zawartość certyfikatu identyfikacji i uwierzytelnienia:

- Kraj **(countryName) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, 2 literowy kod zgodny z ISO 3166;
- Nazwa wyróżniająca **(commonName) - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona” + „ ” + „Nazwisko**”;**
- Nazwisko **(Surname) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko”;
- Pierwsze Imię **(givenName) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Pierwsze imię”;
- Drugie Imię **(givenName) - pole nie obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Drugie imię”;
- Numer seryjny **(serialNumber) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „numer PESEL”. Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

Zawartość certyfikatu podpisu osobistego:

- Kraj **(countryName) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, 2 literowy kod zgodny z ISO 3166;
- Nazwa wyróżniająca **(commonName) - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko**”;**
- Nazwisko **(Surname) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko”;
- Pierwsze Imię **(givenName) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Pierwsze imię”;
- Drugie Imię **(givenName) - pole nie obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Drugie imię”;
- Numer seryjny **(serialNumber) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „numer PESEL”. Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

Zawartość certyfikatu potwierdzania obecności:

- Kraj **(countryName) - pole obowiązkowe:** wartość określająca kraj weryfikacji tożsamości i utrzymywania rejestru, 2 literowy kod zgodny z ISO 3166;
- Nazwa wyróżniająca **(commonName) - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona" +„ " + „Nazwisko**";**
- Nazwisko **(Surname) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko";
- Pierwsze Imię **(givenName) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Pierwsze imię";
- Drugie Imię **(givenName) - pole nie obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Drugie imię";
- Numer seryjny **(serialNumber) - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „numer PESEL". Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures" Rozdział „5.1.3 Natural person semantics identifier". Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

3.1.3. Unikalność nazw

CPD MSWiA zapewnia unikalność nazw w domenie wystawcy certyfikatów, poprzez weryfikację już na poziomie rejestracji użytkowników, że nie zostaną zarejestrowani różni odbiorcy z tym samym zakresem danych w nazwie wyróżniającej certyfikatu (DN). Raz wykorzystana nazwa DN, nie może być wykorzystana przez innego Odbiorcę certyfikatu przez cały okres życia wystawcy certyfikatów.

3.2. Pierwsza rejestracja

Proces wystawienia pierwszego dowodu osobistego, w tym uwierzytelnienie osoby składającej wniosek o wydanie dowodu osobistego, przebiega zgodnie z zapisami Ustawy z dnia 6 sierpnia 2010 r. o dowodach osobistych wraz z późniejszymi zmianami.

3.3. Wystawienie kolejnego certyfikatu

Proces wystawienia certyfikatów dla kolejnego dowodu osobistego z warstwą elektroniczną dla obywatela przebiega identycznie jak proces wystawienia pierwszego dowodu, łącznie z procesem pełnej identyfikacji i uwierzytelniania wnioskodawcy. Przy wystawianiu kolejnych certyfikatów generowana jest każdorazowo nowa para kluczy.

3.4. Zawieszenie, cofnięcie zawieszenia i unieważnienie certyfikatu

Zgłoszenia zawieszenia, cofnięcia zawieszenia lub unieważnienia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego dokonuje osobiście, w postaci dokumentu elektronicznego lub przy użyciu dedykowanej usługi elektronicznej udostępnionej przez ministra właściwego do spraw informatyzacji, posiadacz dowodu osobistego mający pełną zdolność do czynności prawnych, który czasowo utracił kontrolę nad dokumentem. W imieniu osoby nieposiadającej zdolności do czynności prawnych lub posiadającej ograniczoną zdolność do

czynności prawnych, zgłoszenia dokonuje rodzic, opiekun prawny lub kurator. Zgłoszenia, może dokonać pełnomocnik legitymujący się pełnomocnictwem szczególnym do dokonania takiej czynności.

Zgłoszenia dokonuje się do organu dowolnej gminy na terenie Rzeczypospolitej Polskiej lub placówki konsularnej Rzeczypospolitej Polskiej. Organ, do którego zgłoszono zawieszenie, cofnięcie zawieszenia, lub unieważnienie certyfikatów zamieszczonych w dowodzie osobistym, ustala zgodność danych posiadacza dowodu osobistego z danymi zawartymi w dostępnych rejestrach publicznych oraz na podstawie innych dokumentów tożsamości, jeśli są dostępne.

W przypadku zgłoszenia zawieszenia, cofnięcia zawieszenia lub unieważnienia certyfikatów zamieszczonych w dowodzie osobistym, dokonanego przy użyciu dedykowanej usługi elektronicznej udostępnionej przez ministra właściwego do spraw informatyzacji, ustalenie zgodności danych następuje automatycznie w oparciu o dane zawarte w rejestrach (RDO i PESEL).

4. Wymagania dotyczące cyklu życia certyfikatów

4.1. Zgłoszenie certyfikacyjne

Wszystkie dowody osobiste są wyposażone w certyfikat potwierdzenia obecności. Natomiast certyfikat identyfikacji i uwierzytelnienia jest zamieszczany w dowodach osobistych osób posiadających pełną zdolność do czynności prawnych oraz osób posiadających ograniczoną zdolność do czynności prawnych. Certyfikat podpisu osobistego posiadają dowody osobiste wydane osobom, które posiadają pełną zdolność do czynności prawnych i przy składaniu wniosku o wydanie dowodu osobistego wyraziły zgodę na zamieszczenie tego certyfikatu, albo – w przypadku osób małoletnich, które ukończyły 13 rok życia – zgodę tę wyraził rodzic, opiekun prawny lub kurator tej osoby.

W dowodzie osobistym jest przestrzeń umożliwiająca zamieszczenie, na podstawie indywidulanej umowy zawartej przez posiadacza dowodu osobistego z dostawcą usług zaufania - kwalifikowanego certyfikatu podpisu elektronicznego.

4.2. Obsługa zgłoszenia certyfikacyjnego

Po zweryfikowaniu tożsamości wnioskodawcy przez urzędnika w gminie, wniosek jest przesyłany z RDO do SPD celem personalizacji dokumentu, w tym wydania certyfikatów osadzonych na dokumencie.

4.3. Wydanie certyfikatu

Na podstawie przesłanych danych generowane są certyfikaty, które w procesie personalizacji blankietu nagrywane są w warstwie elektronicznej dowodu osobistego. Po zakończeniu personalizacji dowód osobisty oraz korespondencja z opcjonalnie kodem PUK zostaje wysłany do urzędu, gdzie czeka na odbiór przez wnioskującego.

Centrum Certyfikacji zapisuje wszystkie znaczące zdarzenia związane z wystawieniem certyfikatu.

Nowy dowód osobisty jest wydawany w ciągu 30 dni od momentu złożenia wniosku. Istnieje możliwość sprawdzenia przy pomocy usługi zamieszczonej na stronie internetowej www obywatel.gov.pl, gotowości dokumentu do odbioru.

4.4. Akceptacja certyfikatu

Potwierdzając odbiór dowodu osobistego, a w przypadku dowodu osobistego wyposażonego w certyfikat identyfikacji i uwierzytelnienia oraz podpisu osobistego (jeżeli wnioskodawca wyraził zgodę na zamieszczenie tego certyfikatu) również koperty z kodem odblokowującym certyfikaty (PUK), posiadacz dowodu osobistego świadomie potwierdza odbiór dowodu z odpowiednimi certyfikatami.

4.5. Zasady używania certyfikatu i pary kluczy

Obywatele są zobowiązani do używania kluczy prywatnych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszej Polityce i zgodnym z treścią certyfikatu (pól keyUsage oraz extendedKeyUsage, patrz rozdz. 7.1),
- zgodnie z treścią ustawy o dowodzie osobistym z dnia 6 sierpnia 2010 r. o dowodach osobistych oraz rozporządzeniem Ministra Spraw Wewnętrznych i Administracji w sprawie warstwy elektronicznej dowodu osobistego,
- tylko w okresie ich ważności,
- tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego.

4.6. Odnowienie certyfikatu

Proces odnowienia certyfikatów dla dowodu osobistego z warstwą elektroniczną dla obywatela jest realizowane przez proces wystawienia nowego dowodu, łącznie z procesem pełnej identyfikacji i uwierzytelniania wnioskodawcy.

4.7. Odnowienie certyfikatu z wymianą klucza

Proces odnowienia certyfikatów z wymianą klucza dla dowodu osobistego z warstwą elektroniczną dla obywatela jest realizowane przez proces wystawienia nowego dowodu, łącznie z procesem pełnej identyfikacji i uwierzytelniania wnioskodawcy.

4.8. Modyfikacja zawartości certyfikatu

Proces modyfikacji zawartości certyfikatu dla dowodu osobistego z warstwą elektroniczną dla obywatela jest realizowane przez proces wystawienia nowego dowodu, łącznie z procesem pełnej identyfikacji i uwierzytelniania wnioskodawcy.

4.9. Zawieszenie, cofnięcie zawieszenia i unieważnienie certyfikatu

W przypadku czasowej utraty kontroli nad dowodem osobistym posiadacz ma możliwość zgłoszenia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego, maksymalnie na 14 dni. Zgłoszenie powinno nastąpić niezwłocznie po stwierdzeniu utraty kontroli nad dokumentem. Zawieszenie certyfikatów zawsze powoduje zawieszenie ważności dowodu osobistego. Czynności dokonane w okresie zawieszenia albo unieważnienia certyfikatów nie wywołają skutków prawnych. Jeżeli w okresie 14 dni nie nastąpi cofnięcie zawieszenia przez posiadacza dowodu, dowód osobisty automatycznie zostanie unieważniony.

Zgłoszenia zawieszenia lub cofnięcia zawieszenia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego dokonuje, osobiście, w postaci dokumentu elektronicznego lub przy użyciu dedykowanej usługi elektronicznej udostępnionej przez ministra właściwego do spraw informatyzacji, posiadacz dowodu osobistego mający pełną zdolność do czynności prawnych. W imieniu osoby nieposiadającej zdolności do czynności prawnych lub posiadającej ograniczoną zdolność do czynności prawnych zgłoszenia dokonuje rodzic, opiekun prawny lub kurator. Zgłoszenia, może dokonać pełnomocnik legitymujący się pełnomocnictwem szczególnym do dokonania takiej czynności.

Unieważnienie dowodu osobistego zawsze skutkuje unieważnieniem certyfikatów zamieszczonych w warstwie elektronicznej dowodu przez ministra właściwego do spraw wewnętrznych. Poza unieważnieniem dowodu osobistego w wyniku zgłoszenia zawieszenia certyfikatów i nie cofnięcia tego zawieszenia w terminie 14 dni, unieważnienie dowodu osobistego następuje w przypadku:

- zgłoszenia utraty lub uszkodzenia dowodu osobistego;
- utraty przez posiadacza dowodu osobistego obywatelstwa polskiego;
- ubezwłasnowolnienia całkowitego lub częściowego posiadacza dowodu osobistego, w którego dowodzie osobistym w warstwie elektronicznej został zamieszczony certyfikat podpisu osobistego;
- zgonu posiadacza dowodu osobistego;
- zmiany danych zawartych w dowodzie osobistym (4 miesiące od zmiany danych, jeżeli wcześniej dowód nie został unieważniony);
- wydania nowego dowodu osobistego przed upływem terminu ważności wcześniej posiadanego dowodu osobistego.

Poza tym, minister właściwy do spraw wewnętrznych w przypadku uzasadnionego podejrzenia naruszenia praw obywateli związanego z naruszeniem bezpieczeństwa wykorzystania warstwy elektronicznej dowodu osobistego, unieważnia certyfikaty zamieszczone w warstwie elektronicznej dowodu osobistego, przy zachowaniu ważności warstwy graficznej dowodu osobistego oraz może określić czas, w którym będą wydawane dowody osobiste niezawierające w warstwie elektronicznej certyfikatów. Unieważnienie, może dotyczyć wszystkich posiadaczy dowodów osobistych lub grupy posiadaczy dowodów osobistych o tych samych cechach zabezpieczeń. Unieważnienie certyfikatów przez ministra nie obejmuje certyfikatu kwalifikowanego, zamieszczonego w przeznaczonej do tego przestrzeni, na podstawie

indywidualnej umowy zawartej pomiędzy posiadaczem dowodu osobistego a dostawcą usług zaufania.

4.10. Usługi weryfikacji statusu certyfikatu

CPD MSWiA świadczy usługę weryfikacji statusu certyfikatu, nieodpłatnie w sposób ciągły. Status certyfikatu można zweryfikować: w usłudze OCSP dostępnej pod adresem wskazanym w certyfikacie.

5. Obiekt, zarządzanie i kontrola operacyjna

5.1. Bezpieczeństwo fizyczne

5.1.1.Lokalizacja Centrum Certyfikacji

Sieciowy system komputerowy, terminale operatorskie oraz zasoby informacyjne CPD MSWiA znajdują się w wydzielonych pomieszczeniach, fizycznie chronionych przed nieupoważnionym dostępem, zniszczeniem oraz zakłóceniami ich pracy. W zapisach zdarzeń systemu kontroli dostępu (logach systemowych) rejestrowane jest każde wejście i wyjście. Poprzez wewnętrzne systemy monitoringu nadzorowana jest stabilność zasilania, temperatura oraz wilgotność.

System informatyczny Centrum Certyfikacji eksploatowany jest w odpowiednio przystosowanym pomieszczeniu, zlokalizowanym na terenie Centrum Personalizacji Dokumentów MSWiA.

W ramach pomieszczeń eksploatacji Centrum Certyfikacji wyróżnione zostały pomieszczenia:

- Eksploatacji systemu informatycznego (serwerownia)
- Administratorów i operatorów systemu

5.1.2.Dostęp fizyczny

Dostęp do elementów systemu mają wyłącznie osoby uprawnione. Zapewnia się kontrolę dostępu do pomieszczeń oraz rozliczalność wejść i wyjść.

5.1.3.Zasilanie oraz klimatyzacja

W celu przeciwdziałania przerwaniu działalności na skutek przerw w dopływie energii elektrycznej CPD MSWiA posiada system zasilania awaryjnego. Odpowiednia temperatura oraz wilgotność powietrza w pomieszczeniach ośrodka zapewnione są przez całodobowe systemy monitorujące.

5.1.4.Zagrożenie zalaniem

Krytyczne elementy Centrum Certyfikacji, są rozmieszczone w pomieszczeniach o małym ryzyku zalania, w tym w wyniku uszkodzenia instalacji budynku. W przypadku wystąpienia zagrożenia zalaniem, postępuje się zgodnie z procedurami obowiązującymi w CPD MSWiA oraz uruchamia się procedury zapewnienia ciągłości działania Centrum Certyfikacji.

5.1.5.Ochrona przeciwpożarowa

System ochrony przeciwpożarowej, zainstalowany w budynku CPD MSWiA, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. W serwerowi zainstalowano urządzenia gaśnicze (gazowe), które załączają się automatycznie w przypadku wykrycia pożaru w chronionym obszarze.

5.1.6.Przechowywanie nośników danych

Wszystkie nośniki danych przechowywane są w pomieszczeniach chroniących je przed wpływem czynników środowiskowych takich jak temperatura, wilgotność i pole magnetyczne.

5.2. Zabezpieczenia organizacyjne

5.2.1.Zaufane role

W Centrum Certyfikacji funkcjonują następujące role:

1. **Inspektor Bezpieczeństwa Systemu**, który nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemu teleinformatycznego Centrum Certyfikacji;

2. **Administrator Systemu**, który instaluje, konfiguruje i zarządza systemem teleinformatycznym oraz odtwarza dane z kopii zapasowej;

3. **Operator Systemu** wykonujący codzienną obsługę systemu, w tym wykonuje kopie zapasowe.

4. **Inspektor ds. Audytu** analizujący zapisy rejestrów zdarzeń mających miejsce w Centrum Certyfikacji.

5.2.2.Liczba osób wymaganych do realizacji zadań

Zgodnie z procedurami Centrum Certyfikacji część zadań wymaga obecności więcej niż jednego pracownika CPD MSWiA pełniącego rolę w Centrum Certyfikacji.

Lp.	Nazwa zadania	Liczba osób wymaganych
1.	Uruchomienie systemu	trzy uprawnione osoby/role
2.	Wczytanie kluczy urzędów RootCA	cztery uprawnione osoby/role
2.	Wczytanie kluczy urzędów SubCA i OCSP	trzy uprawnione osoby/role
3.	Odtworzenie kopii zapasowej systemu	trzy uprawnione osoby/role
4.	Zamknięcie systemu	dwie uprawnione osoby/role

5.	Wykonanie kopii zapasowej	dwie uprawnione osoby/role
6.	Odnowienie kluczy urzędów i OCSP	cztery uprawnione osoby/role

5.2.3.Identyfikacja oraz uwierzytelnianie każdej roli

Identyfikacja oraz uwierzytelnienie osób pełniących role jest dokonywane dzięki systemowi zabezpieczeń fizycznych i organizacyjnych obejmujących w szczególności:

1. kontrolę i ograniczenie dostępu do poszczególnych pomieszczeń zajmowanych przez Centrum Certyfikacji;
2. przydział indywidualnych imiennych kont w systemie i określony zakres uprawnień uzasadniony zakresem wykonywanych obowiązków;
3. zastosowanie kart elektronicznych do uaktywniania elementów systemu.

5.2.4.Role, które nie mogą być łączone

Żadne role w Centrum Certyfikacji nie mogą być łączone.

5.3. Nadzorowanie personelu

5.3.1.Kwalifikacje, doświadczenie i poświadczenia bezpieczeństwa

CPD MSWiA gwarantuje, że osoby wykonujące zadania w ramach Centrum Certyfikacji:

- posiadają pełną zdolność do czynności prawnych;
- posiadają minimum wykształcenie średnie;
- zawarły umowę o pracę lub inną umowę cywilno-prawną precyzującą rolę, którą mają pełnić i określającą wynikające z niej prawa i obowiązki;
- przeszły niezbędne przeszkolenie z zakresu obowiązków, które będą wykonywały;
- zostały przeszkolone w zakresie ochrony danych osobowych;
- w umowie zawarto klauzule o nieujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa urzędu certyfikacji lub poufności danych subskrybenta;
- nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem certyfikacji a działającymi w jego imieniu punktami rejestracji;
- zobowiązane są postępować zgodnie z przepisami *Rozporządzenia eIDAS i Ustawy o usługach zaufania*.

5.3.2.Procedury weryfikacji personelu

Kontrola przygotowania do pracy na danym stanowisku wiążącym się z pełnieniem zaufanej roli przeprowadzana jest w stosunku do każdego nowego pracownika zgodnie z wewnętrzną procedurą obowiązującą w CPD MSWiA.

5.3.3. Wymagania szkoleniowe

Osoby pełniące role w Centrum Certyfikacji są przeszkolone, w szczególności w zakresie:

1. technologii tworzenia certyfikatów i świadczenia innych usług związanych z podpisem elektronicznym i pieczęcią elektroniczną;
2. obsługi sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych, automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych;
3. przestrzegania zasad bezpieczeństwa systemów teleinformatycznych;
4. przestrzegania procedur awaryjnych;
5. przestrzegania procedur stosowanych w czasie wykonywania czynności służbowych.

5.3.4. Wymagania i częstotliwość szkoleń

Szkolenia obejmują zakres wiedzy wymagany na danym stanowisku pracy. Osoby pełniące role w Centrum Certyfikacji przechodzą szkolenia udoskonalające, zgodnie z zasadami szkoleń obowiązującymi w CPD MSWiA. W przypadku zmiany w funkcjonowaniu Centrum Certyfikacji, pracownicy CPD MSWiA przechodzić będą szkolenia dodatkowe.

5.3.5. Częstotliwość i sekwencja rotacji zadań

Niniejsza Polityka nie określa wymagań w tym zakresie.

5.3.6. Kwestie dyscyplinarne

W przypadku naruszenia zasad wynikających z niniejszej Polityki, osoby wykonującej określone funkcje w ramach Centrum Certyfikacji podlegają sankcjom wynikającym z Kodeksu Pracy, Ustawy o Usługach Zaufania i Kodeksu Karnego.

5.3.7. Wymagania dla podwykonawców

Dopuszcza się pracę w systemie osób niebędących pracownikami CPD MSWiA (serwis zewnętrzny, wykonawcy podsystemów i oprogramowania, itp.), w związku z realizacją zadań określonych w umowach, zawartych przez CPD MSWiA. W takim przypadku, jeśli osoby trzecie realizujące zapisy umowy będą stałymi pracownikami wyznaczonymi do realizacji warunków umowy wtedy ich dane w celach weryfikacyjnych i dostępowych powinny się znaleźć w zapisach umowy. Jeśli natomiast następowała będzie rotacja pracowników podwykonawcy umowy w zapisach powinna się znaleźć informacja o przekazywaniu do CPD MSWiA listy pracowników, którzy w danym okresie będą realizować zakres zadań zapisany w umowie. Wszelkie prace, które są wykonywane w Centrum Certyfikacji nadzorowane są przez osoby pełniące role w Centrum Certyfikacji CPD MSWiA.

5.3.8. Dokumentacja dla personelu

W ramach realizacji obowiązków służbowych, udostępnia się osobom realizującym zadania w ramach Centrum Certyfikacji niezbędną dokumentację, wymaganą do realizacji obowiązków służbowych. W szczególności obejmuje ona:

- niniejszą Politykę,
- wzory umów związanych ze świadczeniem usług certyfikacyjnych,
- zakres obowiązków i uprawnień wynikających z pełnionej roli
- procedury i instrukcje

5.4. Rejestracja zdarzeń

5.4.1.Typy rejestrowanych zdarzeń

W celu zapewniania jak najwyższego poziomu bezpieczeństwa infrastruktury i zaufania do Centrum Certyfikacji, jest ono zobowiązane do archiwizowania wszystkich istotnych zdarzeń związanych z funkcjonowaniem systemu. W szczególności są to zdarzenia:

- Systemowe (generowane przez sprzęt i oprogramowanie Centrum Certyfikacji),
- Błędy (zdarzenia krytyczne dla funkcjonowania Centrum Certyfikacji),
- Audytu (związane z przeglądem rejestrów zdarzeń Centrum Certyfikacji).

Rejestry przechowywane są w postaci elektronicznej oraz w postaci papierowej. Tam, gdzie jest to możliwe, rejestry zdarzeń prowadzone są w postaci elektronicznej. Każdy z rejestrów powinien przechowywać przynajmniej następujące informacje:

- Miejsce wystąpienia zdarzenia,
- Rodzaj zdarzenia jakie wystąpiło,
- Dokładną datę i czas wystąpienia zdarzenia,

Rejestry zdarzeń tworzone są w oparciu o zdarzenia jakie miały miejsce w następujących elementach Architektury PKI:

- Centrum Certyfikacji (na warstwie sprzętowej, sieciowej i aplikacyjnej systemu),
- Urzędzie rejestracji (szczególnie zdarzenia związane z wystawieniem, zawieszeniem, unieważnieniem i odwieszeniem certyfikatu Subskrybenta),
- Zdarzenia wynikające z eksploatacji zabezpieczeń fizycznych i logicznych Centrum Certyfikacji).

5.4.2.Częstotliwość przeglądu rejestrów zdarzeń

Rejestry zdarzeń powinny być przeglądane w sposób ciągły, jednakże nie rzadziej niż raz dziennie przez Administratora systemu.

5.4.3.Czas przechowywania archiwalnych kopii rejestrów zdarzeń

Archiwalne kopie rejestrów zdarzeń powinny być przechowywane przynajmniej przez okres 5 lat.

5.4.4.Ochrona zapisów rejestrowanych zdarzeń

Rejestry zdarzeń przechowywane są w środowisku zapewniającym odpowiedni poziom bezpieczeństwa. Zapewnia się integralność plików w rejestrach zdarzeń.

Tworzy się kopie zapasowe rejestrów zdarzeń. Kopie zapasowe tworzy się z wykorzystaniem technik zapewniających integralność danych. Przy tworzeniu kopii zapasowych powinny być obecne, co najmniej dwie spośród osób, o których mowa w rozdziale 5.2.1 niniejszej Polityki. Czynności polegające na tworzeniu kopii zapasowych nadzoruje bezpośrednio Inspektor Bezpieczeństwa Systemu.

5.4.5.Procedury tworzenia kopii zapasowych

Kopie rejestrów zdarzeń są tworzone wraz z kopiami bezpieczeństwa systemu. Powstałe w ten sposób kopie zapasowe tworzy się z wykorzystaniem technik zapewniających integralność danych. Przy tworzeniu kopii zapasowych powinny być obecne, co najmniej dwie spośród osób, o których mowa w rozdziale 5.2.1 niniejszej Polityki. Czynności polegające na tworzeniu kopii zapasowych nadzoruje bezpośrednio Inspektor Bezpieczeństwa Systemu.

5.4.6.Oszacowanie podatności na zagrożenia

Dokonuje się okresowej oceny poziomu ryzyka systemu, w celu identyfikacji zagrożeń, oszacowania prawdopodobieństwa ich wystąpienia oraz podatności na nie. Na podstawie wyników analizy ryzyka wprowadzone zostają rozwiązania mające na celu eliminację lub zmniejszenie podatności systemu na zagrożenia.

5.5. Archiwizacja danych

5.5.1.Rodzaje zasobów podlegających tworzeniu kopii zapasowych

Tworzenie kopii bezpieczeństwa ma na celu zapewnienie ciągłości działania Centrum Certyfikacji. Tworzeniu kopii zapasowych podlegają wszystkie istotne elementy infrastruktury informatycznej systemu Centrum Certyfikacji. W szczególności są to następujące elementy:

- bazy danych przechowujące informacje o wystawionych certyfikatach,
- konfiguracje systemów i aplikacji,
- repozytoria danych.

5.5.2.Częstotliwość tworzenia kopii zapasowych

Kopie zapasowe zasobów, o których mowa w rozdziale 5.5.1 tworzone są raz na tydzień.

5.5.3.Czas przechowywania kopii zapasowych

Tygodniowe kopie zapasowe przechowywane są przez okres jednego miesiąca. Wyjątkiem są kopie tworzone w ostatnim tygodniu miesiąca i roku kalendarzowego, które przechowywane są przez okres 5 lat.

5.5.4.Przechowywanie i dostęp do kopii zapasowych

Kopie zapasowe są umieszczane na oddzielnych zestawach nośników.

Zasady przechowywania kopii zapasowych określono w rozdziale 5.1.6.

5.5.5. Techniczna realizacja tworzenia kopii zapasowych

Kopie zapasowe tworzone są z użyciem narzędzi informatyczno-sprzętowych i podlegają zapisowi na magnetycznych nośnikach danych. Trwałość zapisu na wspomnianych nośnikach wynosi 5 lat.

5.6. Wymiana kluczy urzędu

Wymiana kluczy urzędu następuje wraz z wydaniem nowych certyfikatów i jest realizowana wg. wewnętrznej procedury.

5.7. Naruszenie bezpieczeństwa kluczy urzędu i procedury odtwarzania po awarii (Compromise and Disaster Recovery)

5.7.1. Procedura postępowania po wystąpienie incydentu

W przypadku wykrycia incydentu naruszającego bezpieczeństwo Centrum Certyfikacji, podejmowane są działania mające na celu ich zidentyfikowanie i wyeliminowanie. Środkami zapobiegawczymi podejmowanymi w celu uniknięcia zaistnienia incydentu w Centrum Certyfikacji są odpowiednio wdrożone procedury awaryjne reagowania na zagrożenie. Procedury są uruchamiane w momencie zaistnienia zagrożenia. Dodatkowo zbierane są informacje na temat zasobów Centrum Certyfikacji, które uległy incydentowi, oraz przypadek poddawany jest analizie w celu przeciwdziałania jego wystąpieniu w przyszłości.

5.7.2. Postepowanie po uszkodzeniu zasobów sprzętowych, programowych i danych

W przypadku wystąpienia awarii zasobów Centrum Certyfikacji, zespół bezpieczeństwa w skład którego wchodzą Inspektor Bezpieczeństwa Systemu, Administrator Systemu oraz Operator Systemu zobowiązany jest do określenia i oszacowania zasobów, które uległy uszkodzeniu. Zasoby te obejmują sprzęt, oprogramowanie, środowisko sieciowe oraz środowisko fizyczne, w którym funkcjonuje Centrum Certyfikacji. Wystąpienie awarii zasobów uruchamia procedurę awaryjną pozwalającą na reagowanie na uszkodzenie odpowiednich zasobów.

Działania podejmowane w tym zakresie zmierzają do jak najszybszego odtworzenia działalności Centrum Certyfikacji.

5.7.3. Postępowanie po naruszeniu ochrony klucza prywatnego Centrum Certyfikacji

W przypadku wystąpienia incydentu naruszającego bezpieczeństwo klucza prywatnego Centrum Certyfikacji, personel Centrum Certyfikacji zobowiązany jest do podjęcia działań zmierzających w kierunku powiadomienia o zaistniałym incydencie kierownictwo CPD MSWiA oraz Obywateli i Strony ufające. Następnie unieważnianie są wszystkie ważne certyfikaty obywateli i urzędów. W dalszej kolejności określane jest źródło, które spowodowało zagrożenie i podejmowane są działania zmierzające do zniwelowania zagrożeń wypływających z tegoż źródła. Po ich usunięciu następuje wygenerowanie nowych par kluczy Centrum Certyfikacji.

5.7.4.Możliwość zapewniania ciągłości działania po wystąpieniu incydentu

Za zapewnienie ciągłości działania Centrum Certyfikacji po wystąpieniu incydentu odpowiada kierownictwo CPD MSWiA. W swych działaniach opiera się o Plan Ciągłości Działania Centrum Certyfikacji oraz zbiór procedur awaryjnych pozwalających reagować na odpowiednie incydenty. Procedury tworzone są w oparciu o analizę ryzyka funkcjonowania Centrum Certyfikacji. Przynajmniej raz do roku następuje przegląd analizy ryzyka funkcjonowania Centrum Certyfikacji i dokumentacji z tym związanej. W miarę wystąpienia nowych zagrożeń, dokumentacja ta jest modyfikowana i aktualizowana.

5.8. Zakończenie działalności CA lub punktów rejestracji

Centrum Certyfikacji zobowiązane jest do wdrożenia procedur i środków minimalizujących wpływ skutków zakończenia działalności Centrum Certyfikacji na Subskrybentów.

W przypadku zakończenia działalności, Centrum Certyfikacji zobowiązane jest do powiadomienia o tym fakcie Subskrybentów i Strony ufające. Subskrybenci informowani są za pośrednictwem portalu informatycznego, zaś Strony ufające za pośrednictwem stosownego komunikatu zamieszczonego w Repozytorium. Powiadomienie powinno nastąpić przynajmniej z miesięcznym wyprzedzeniem. Zakończenie działalności wiąże się z unieważnieniem wszystkich ważnych certyfikatów Subskrybentów oraz unieważnieniem Zaświadczenia certyfikacyjnego Centrum Certyfikacji.

6. Środki ochrony technicznej

6.1. Generowanie pary kluczy i instalacja

Bezpieczeństwo generacji oraz instalacji pary kluczy zapewniają procedury operacyjne stosowane w MSWiA.

6.1.1.Generacja par kluczy urzędów certyfikacji

Pary kluczy urzędów certyfikacji generowane są w HSM, zgodnie z udokumentowaną procedurą generacji, zapewniającą integralność i poufność kluczy. Ceremonia generacji par kluczy odbywa się w siedzibie CPD MSWiA w środowisku bezpiecznym fizycznie, w obecności wymaganej liczby osób pełniących zaufane role, przy czym jedną z nich musi być Inspektor ds. bezpieczeństwa. Z czynności wykonywanych podczas generacji kluczy sporządzany jest raport, który jest podpisywany przez uczestników procedury generacji kluczy. Inspektor ds. bezpieczeństwa zaświadcza swoim podpisem, że proces generowania kluczy przebiegał zgodnie z udokumentowaną procedurą z zachowaniem poufności i integralności kluczy. Po wygenerowaniu kluczy, generowane są certyfikaty dla urzędów wystawiających certyfikaty dla obywateli. Po otrzymaniu certyfikatu następuje weryfikacja poprawności podpisu i ścieżki zaufania.

6.1.2.Generacja par kluczy Obywateli

Pary kluczy Obywateli generowane są podczas personalizacji dowodu osobistego za pomocą HSM'a, które zapewniają odpowiednią jakość otrzymanych kluczy.

Parametry generowanych kluczy muszą spełniać wymagania postawione w normie ETSI TS 119 312: "Electronic Signatures and Infrastructures (ESI); Cryptographic Suites" lub w przepisach krajowych.

MSWiA zapewnia, że wszystkie klucze prywatne Obywateli, których klucze publiczne są certyfikowane zgodnie z niniejsza Polityką, są zapisywane wyłącznie na blankietach dowodów osobistych.

6.1.3.Parametry kluczy

Urzędy certyfikacji MSWiA używają kluczy:

Root CA:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA512 WithECDSA

SubCa dla certyfikatów do uwierzytelnienia:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA512WithECDSA

SubCa dla certyfikatów do zaawansowanego podpisu elektronicznego:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA512WithECDSA

SubCa dla certyfikatów do potwierdzenia obecności:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA512WithECDSA

Usługa OCSP używa następujących kluczy dla poszczególnych responderów:

Responder dla RootCA

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA256WithECDSA

Responder dla certyfikatów do uwierzytelnienia:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA256WithECDSA

Responder dla certyfikatów do zaawansowanego podpisu elektronicznego:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA256WithECDSA

Responder dla certyfikatów do zaawansowanego podpisu elektronicznego:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA256WithECDSA

Dla użytkownika końcowego certyfikat do uwierzytelnienia:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA256WithECDSA

Dla użytkownika końcowego certyfikat do zaawansowanego podpisu elektronicznego:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384
- Długość klucza: 384
- Algorytm podpisu: SHA256WithECDSA

Dla użytkownika końcowego certyfikat do potwierdzenia obecności:

- Klucze algorytmu ECDSA
- Typ: secp384r1/P-384

- Długość klucza: 384
- Algorytm podpisu: SHA256WithECDSA

6.1.4.Zastosowanie kluczy

Sposób użycia klucza zdefiniowany jest w polu KeyUsage oraz ExtendedKeyUsage rozszerzeń standardowych certyfikatu (X.509 v3). Pole powinno być weryfikowane przez aplikacje korzystające z certyfikatu.

Klucze głównego urzędu certyfikacji są używane do podpisywania certyfikatów pośrednich urzędów certyfikacji, certyfikatu usługi OCSP oraz list CRL.

Klucze pośrednich urzędów certyfikacji są używane do podpisywania certyfikatów Obywateli, certyfikatu usługi OCSP oraz list CRL.

Klucze usługi OCSP są używane wyłącznie do podpisywania odpowiedzi OCSP.

6.2. Ochrona, aktywacja, dezaktywacja i niszczenie kluczy

Klucze prywatne certyfikatów do uwierzytelnienia, zaawansowanego podpisu elektronicznego oraz potwierdzenia obecności generowane są w procesie personalizacji dowodu, w środowisku bezpiecznym przy użyciu HSM'a w sposób zapewniający jego ochronę i bezpieczne przekazanie na blankiet dowodu osobistego.

Klucze prywatne wszystkich urzędów odtwarzane i przetwarzane są jedynie w HSM'ach.

6.2.1.Kontrola klucza prywatnego przez wiele osób

Klucze prywatne wszystkich Urzędów Certyfikacji są chronione przez podział dostępu na części „n" z „m", przy czym sposób podziału regulują wewnętrzne procedury. Zarządzanie kluczami prywatnymi urzędów wymaga współpracy odpowiedniej liczby osób uprawnionych.

6.2.2.Deponowanie klucza prywatnego

CPD MSWiA nie przechowuje w depozycie kluczy prywatnych obywateli

6.2.3.Kopia zapasowa klucza prywatnego

CPD MSWiA tworzy kopie kluczy prywatnych urzędów na wypadek awaryjnej procedury odzyskiwania kluczy. Kopie zapasowe kluczy przechowywane są w postaci zaszyfrowanej z dostępem w postaci dzielonego sekretu..

CPD MSWiA nie tworzy kopii zapasowych kluczy prywatnych Obywateli.

6.2.4.Archiwizacja klucza prywatnego

Nie dopuszcza się archiwizacji żadnych kluczy prywatnych wydanych Obywatelowi.

6.2.5.Transfer klucza prywatnego do/z HSM'a

Klucz prywatny urzędu certyfikacji w postaci jawnej może być przetwarzany wyłącznie w HSM'e. Transfer kluczy prywatnych urzędów CPD MSWiA do HSM'a następuje w procedurze ładowania kluczy. Klucz w postaci jawnej nie jest transferowany poza moduł kryptograficzny.

Klucze prywatne Obywateli generowane są w HSM'e i przekazywane są w bezpiecznym środowisku na blankiet dowodu osobistego w procesie personalizacji dokumentu.

6.2.6.Sposób aktywacji klucza prywatnego

Materiał kryptograficzny zawierający klucze przechowywany jest w systemie plików w postaci zaszyfrowanej. Aktywacja kluczy prywatnych urzędów MSWiA wymaga współdziałania dwóch osób pełniących zaufaną rolą, posiadających współdzielone sekrety na kartach elektronicznych oraz hasła do tych kart.

Aktywacja kodów PIN chroniących klucze prywatne Obywatela następuje w momencie odbioru dowodu przez Obywatela lub w czasie późniejszym.

6.2.7.Sposób dezaktywacji klucza prywatnego

Dezaktywacja kluczy prywatnych urzędów MSWiA następuje pod kontrolą dwóch uprawnionych administratorów. Dezaktywacja klucza prywatnego polega na zakończeniu działania aplikacji wykorzystującej HSM w systemie operacyjnym.

Dezaktywacja klucza prywatnego Obywatela następuje w wyniku zakończenia działania aplikacji korzystającej z klucza.

6.2.8.Sposób niszczenia klucza prywatnego

Klucze prywatne wszystkich urzędów i usług MSWiA są niszczone wraz z fizycznym zniszczeniem kart zawierających sekrety współdzielone. Z czynności wykonywanych podczas niszczenia kluczy sporządzany jest raport, który jest podpisywany przez wszystkich uczestników procedury zniszczenia.

Klucze prywatne Obywatela są niszczone wraz z fizycznym zniszczeniem blankietem dowodu osobistego.

6.2.9.Archiwizacja klucza publicznego

Wszystkie klucze publiczne są archiwizowane przez CPD MSWiA. Certyfikaty, których okres ważności wygasł, są archiwizowane przez okres, co najmniej 20 lat od daty powstania, włącznie z kluczem publicznym.

6.2.10. Okresy funkcjonowania certyfikatów i okresy funkcjonowania par kluczy

Okresy ważności certyfikatów CPD MSWiA oraz certyfikatów Obywateli, wynoszą nie więcej niż:

- 25 lat dla głównego urzędu certyfikacji,
- 12 lat dla certyfikatów pośrednich urzędów certyfikacji MSWiA,
- 10 lat dla certyfikatów Obywateli.

Okres ważności klucza prywatnego może być krótszy niż okres ważności certyfikatu.

6.3. Dane aktywujące

W przypadku Obywateli dane aktywujące stanowią kody PIN.

W przypadku urzędów certyfikacji dane aktywujące stanowią specjalne karty kryptograficzne z przypisanymi do nich hasłami.

6.4. Zarządzanie bezpieczeństwem systemu informatycznego

Zgodnie z polityką bezpieczeństwa CPD MSWiA, przepisami prawa powszechnego oraz wewnętrznymi regulacjami CPD MSWiA, w systemie teleinformatycznym CPD MSWiA wykorzystuje się wiarygodne oprogramowanie i sprzęt wdrożony na podstawie istniejących procedur zapewniających bezpieczną eksploatację.

Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń systemu informatycznego, używanego w Centrum Certyfikacji CPD MSWiA. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery funkcjonujące w Centrum Certyfikacji CPD MSWiA wyposażone są w następujące funkcje zabezpieczające:

- obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji,
- kontrola dostępu zarówno w zakresie dostępu do pomieszczeń jak i poszczególnych elementów systemu login, hasło (np. imienne konta w systemie operacyjnym i aplikacjach),
- prowadzenie audytu zabezpieczeń,
- pracownik, który pełni zaufaną role jest zobowiązany do blokowania swojej stacji roboczej zawsze, jeśli pozostają one poza jego nadzorem,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- wymuszanie wylogowania użytkownika po okresie bezczynności,
- identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
- wykonywanie kopii zapasowych i archiwalnych,

- monitorowanie i alarmowanie w przypadku nieautoryzowanego dostępu do systemu teleinformatycznego,
- mechanizm monitorowani i alarmowania w przypadku wystąpienia zdarzenia przekroczenia parametrów wydajności systemów i dostępności usług.

6.4.1.Specjalne wymagania techniczne odnośnie bezpieczeństwa komputerów

Zostały wdrożone techniczne i środowiskowe mechanizmy bezpieczeństwa dotyczące komputerów, specyficzne dla działalności Centrum Certyfikacji. Zabezpieczenia są realizowane w aplikacjach, systemach operacyjnych, sieci teleinformatycznej oraz zabezpieczeniach fizycznych.

6.4.2.Uprawnienia użytkowników

Nadanie uprawnień użytkownikom w systemie teleinformatycznym e-Dowodu wymaga formalnej akceptacji wniosku zgodnie z udokumentowaną procedurą zarządzania uprawnieniami. Konfiguracja praw dostępu odbywa się w oparciu o zasadę najmniejszych uprawnień oraz podział ról. Konta użytkowników, którzy zmienili stanowisko lub zakończyli zatrudnienie są niezwłocznie modyfikowane lub blokowane.

6.4.3.Zabezpieczenie przed szkodliwym oprogramowaniem

Zabezpieczenie przed szkodliwym oprogramowaniem jest realizowane przez zabezpieczenia techniczne (separacja systemów, oprogramowanie antywirusowe oraz uniemożliwienie instalacji aplikacji przez nieupoważnionych użytkowników) i organizacyjne (zwiększanie świadomości użytkowników, wewnętrzne instrukcje opisujące sposób postępowania w przypadku infekcji złośliwym kodem), których zadaniem jest ograniczenie ryzyka infekcji przez złośliwe oprogramowanie.

6.5. Zarządzanie bezpieczeństwem cyklu życia procesu wytwórczego

Blankiety do produkcji dowodów osobistych dostarczane są do CPD MSWiA w sposób kontrolowany. Personalizacja odbywa się w środowisku kontrolowanym i monitorowanym. Po spersonalizowaniu graficznym oraz elektronicznym gotowe dowody osobiste trafiają na spedycję, celem dystrybucji w sposób kontrolowany do wnioskujących urzędów gmin. Do urzędów gmin wysyłane są także, osobną przesyłką, w postaci zabezpieczonej kody PUK, gdzie wydawane są bezpośrednio obywatelowi wraz z dowodem osobistym.

6.6. Zarządzanie bezpieczeństwem sieciowym

Sieć teleinformatyczna e-Dowodu została podzielona na segmenty przy użyciu zapór sieciowych, na których dodatkowo zostały uruchomione moduły wykrywające włamania. Reguły na zaporach sieciowych pozwalają tylko na zdefiniowany ruch, poprzez listy kontroli dostępu, pozostałe połączenia są odrzucane. Zapisy zdarzeń sieciowych są regularnie monitorowane przez personel pełniący zaufane role.

Komunikacja pomiędzy komponentami wchodzącymi w skład e-dowodu jest zabezpieczona za pomocą dwustronnego protokołu SSL/TLS z uwierzytelnieniem klienta.

W przypadku stwierdzenia potrzeby wprowadzenia zmian konfiguracyjnych w urządzeniach sieciowych lub dokonania innych modyfikacji w systemie, Administrator systemu zobowiązany jest do wykorzystania procedury wprowadzania zmian w systemie. Wykonana zmiana podlega przetestowaniu na środowisku testowym, celem weryfikacji poprawności jej działania. Decyzję o wprowadzeniu zmiany akceptuje dyrektor CPD MSWiA. Jeżeli wprowadzona zmiana powoduje zmiany w dokumentacji i konfiguracji systemu informatycznego oraz w procedurach funkcjonowania, to zmiany te są niezwłocznie wprowadzane, a dokumentacja jest udostępniana upoważnionym pracownikom.

7. Profil certyfikatu i list CRL

Profile certyfikatów są zgodne z formatami opisanymi normą ITU-T X.509. Dodatkowo certyfikaty są zgodne z profilami certyfikatów zdefiniowanych w normie ETSI-EN 319 412-2.

7.1. Struktura certyfikatu

W ramach Polityki certyfikaty zawierają następujące elektroniczne struktury danych:

- Treść certyfikatu (tbsCertificate),
- Informacja o algorytmie użytym do podpisania certyfikatu (signatureAlgorithm),
- Poświadczenie certyfikatu, składane przez organ wydający certyfikat (signatureValue).

7.1.1.Treść certyfikatu

Zgodnie ze standardem X.509 na treść certyfikatu składają się pola standardowe i rozszerzone

Zakres i wartość pól standardowych certyfikatów wydawanych przez Centrum Certyfikacji przedstawiono w tabeli:

Certyfikat dla głównego urzędu certyfikacji:

l.p.	Pole	Opis	Zawartość
1	Version	wersja formatu certyfikatu zgodna z X.509	V3
2	SerialNumber	numer seryjny certyfikatu, unikalny w ramach urzędu wydającego certyfikat	Unikalny identyfikator
3	SignatureAlgorithm	informacja o algorytmie użytym do podpisania certyfikatu	1.2.840.10045.4.3.4 (SHA512 with ECDSA Encryption)

4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	CN=pl.ID Root CA SN=<YYYY> C=PL gdzie: <YYYY> oznacza rok wystawienia certyfikatu
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	Zakres dat
6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	CN=pl.ID Root CA SN=<YYYY> C=PL gdzie: <YYYY> oznacza rok wystawienia certyfikatu
7	SubjectPublicKeyInfo	określenie algorytmu używanego przez posiadacza certyfikatu oraz jego klucz publiczny	Klucz publiczny oraz użyty algorytm

Certyfikat dla pośrednich urzędów certyfikacji:

l.p.	**Pole**	**Opis**	**Zawartość**
1	Version	wersja formatu certyfikatu zgodna z X.509	V3
2	SerialNumber	numer seryjny certyfikatu, unikalny w ramach urzędu wydającego certyfikat	Unikalny identyfikator
3	SignatureAlgorithm	informacja o algorytmie użytym do podpisania certyfikatu	1.2.840.10045.4.3.4 (SHA512 with ECDSA Encryption)

4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	CN=pl.ID Root CA SN=<YYYY> C=PL gdzie: <YYYY> oznacza rok wystawienia certyfikatu
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	Zakres dat
6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	CN=<Nazwa powszechna urzędu> O=<Nazwa organizacji> OU=<Jednostka organizacyjna> OU SN=<YYYYMMDD> C=PL gdzie: <YYYYMMDD> oznacza datę wystawienia certyfikatu
7	SubjectPublicKeyInfo	określenie algorytmu używanego przez posiadacza certyfikatu oraz jego klucz publiczny	Klucz publiczny oraz użyty algorytm

Poniżej wskazano zakres i wartość pól rozszerzonych certyfikatów:

1. Rozszerzenie standardowe
    1. AuthorityKeyIdentifier

        Identyfikator klucza urzędu**:** 20-to bajtowy identyfikator klucza publicznego wystawcy certyfikatu - rozszerzenie niekrytyczne

2. Skrót klucza certyfikatu - rozszerzenie niekrytyczne

3. KeyUsage: certificateSigning, CRLSigning

   Definiuje dozwolone użycie klucza - rozszerzenie krytyczne.

4. Authority Information Access

   Rozszerzenie zawiera wskazanie lokalizacji i metody dostępu do informacji lub usług udostępnianych przez wystawcę certyfikatu, w którym zawarte jest to rozszerzenie - rozszerzenie nie jest krytyczne i nie występuje w certyfikacie głównego urzędu certyfikacji

   i. OCSP - adres usługi OCSP

   ii. caIssuers - adres publikacji certyfikatów urzędów

2. Basic Constraints - rozszerzenie krytyczne

   Subject is a CA. Path Length Constraint: 0

   Informacja o tym, że jest to certyfikat urzędu, z którego bezpośrednio wystawiane są certyfikaty końcowe.

Certyfikat do identyfikacji i uwierzytelnienia:

l.p.	Pole	Opis	Zawartość
1	Version	wersja formatu certyfikatu zgodna z X.509	V3
2	SerialNumber	numer seryjny certyfikatu, unikalny w ramach urzędu wydającego certyfikat	Unikalny identyfikator
3	SignatureAlgorithm	informacja o algorytmie użytym do podpisania certyfikatu	1.2.840.10045.4.3.2 (SHA256 with ECDSA Encryption)
4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	CN=PL.ID Authentication CA O=MSWiA OU=CPD SN=<YYYYMMDD> C=PL gdzie <YYYYMMDD> oznacza datę wystawienia certyfikatu urzędu
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	Zakres dat

6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	**C - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, zapisane jako 2 literowy kod zgodny z ISO 3166; **CN - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona” + „ ” + „Nazwisko**”;** **SURNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko” **GIVENNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Pierwsze imię”; **GIVENNAME - pole nie obowiązkowe:** wartość na podstawie danych dotyczących osoby - Drugie imię”; **SN - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „numer PESEL”. Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;
7	SubjectPublicKeyInfo	określenie algorytmu używanego przez posiadacza certyfikatu oraz jego klucz publiczny	Klucz publiczny oraz użyty algorytm

Poniżej wskazano zakres i wartość pól rozszerzonych certyfikatów:

1. Rozszerzenie standardowe
    1. AuthorityKeyIdentifier

       Identyfikator klucza wystawcy certyfikatu - rozszerzenie niekrytyczne

    2. SubjectKeyIdentifier

Identyfikator klucza certyfikatu - rozszerzenie niekrytyczne

3. KeyUsage: digitalSignature

   Definiuje dozwolone użycie klucza - rozszerzenie krytyczne.

4. CertificatePolicies

   Rozszerzenie zawiera informację o polityce certyfikacji (identyfikator, adres elektroniczny) przyjętej przez urząd certyfikacji - rozszerzenie krytyczne.

   - Identyfikator polityki **(policyIdentifier)**: 1.2.616.1.101.5.2.1.1.1.1
   - Typ kwalifikatora polityki **(policyQualifierId)**: id-qt-unotice
   - **User notice: Explicit Text:** Treść Polityki znajduje się pod adresem http://e-dowod.gov.pl

5. Extended Key Usage

   Rozszerzone użycie klucza **- rozszerzenie niekrytyczne:** id-kp-clientAuth

6. SubjectDirectoryAttributes

   Rozszerzenie to zawiera dodatkowe atrybuty powiązane z subskrybentem i dopełniające informacje zawarte w polu **Subject** - rozszerzenie nie krytyczne.

   Zawiera następujące atrybuty:

   DateOfBirth - zawiera datę urodzenia posiadacza certyfikatu,

   PlaceOfBirth - określa miejsce urodzenia posiadacza certyfikatu.

7. Authority Information Access

   Rozszerzenie zawiera wskazanie lokalizacji i metody dostępu do informacji lub usług udostępnianych przez wystawcę certyfikatu, w którym zawarte jest to rozszerzenie -

   rozszerzenie nie jest krytyczne.

   i. OCSP -adres usługi OCSP

   ii. caIssuers - adres publikacji certyfikatów urzędów

2. Basic Constraints - rozszerzenie krytyczne

   Subject is not a CA. Path Length Constraint: None

Jest to certyfikat końcowy.

Certyfikat dla podpisu osobistego:

l.p.	Pole	Opis	Zawartość
1	Version	wersja formatu certyfikatu zgodna z X.509	V3
2	SerialNumber	numer seryjny certyfikatu, unikalny w ramach urzędu wydającego certyfikat	Unikalny identyfikator
3	SignatureAlgorithm	informacja o algorytmie użytym do podpisania certyfikatu	1.2.840.10045.4.3.2 (SHA256 with ECDSA Encryption)
4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	CN=PL.ID Authorization CA O=MSWiA OU=CPD SN=<YYYYMMDD> C=PL gdzie <YYYYMMDD> oznacza datę wystawienia certyfikatu urzędu

5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	Zakres dat
6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	**C - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Obywatelstwo”, zapisane jako 2 literowy kod zgodny z ISO 3166; **CN - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko**”;** **SURNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko” **GIVENNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Pierwsze imię”; **GIVENNAME - pole nie obowiązkowe:** wartość na podstawie danych dotyczących osoby - Drugie imię”; **SN - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „numer PESEL”. Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures” Rozdział „5.1.3 Natural person semantics identifier”. Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

7	SubjectPublicKeyInfo	określenie algorytmu używanego przez posiadacza certyfikatu oraz jego klucz publiczny	Klucz publiczny oraz użyty algorytm

Poniżej wskazano zakres i wartość pól rozszerzonych certyfikatów:

1. Rozszerzenie standardowe
    1. AuthorityKeyIdentifier

       Identyfikator klucza urzędu - rozszerzenie niekrytyczne

    2. SubjectKeyIdentifier

       Identyfikator klucza certyfikatu - rozszerzenie niekrytyczne

    3. KeyUsage: contentCommitment

       Definiuje dozwolone użycie klucza - rozszerzenie krytyczne.

    4. CertificatePolicies

       Rozszerzenie zawiera informację o polityce certyfikacji (identyfikator, adres elektroniczny) przyjętej przez urząd certyfikacji - rozszerzenie krytyczne.

       - Identyfikator polityki **(policyIdentifier)**: 1.2.616.1.101.5.2.1.1.1.2
       - Typ kwalifikatora polityki **(policyQualifierId)**: id-qt-unotice
       - **User notice: Explicit Text:** Treść Polityki znajduje się pod adresem http://e-dowod.gov.pl

    5. Authority Information Access

       Rozszerzenie zawiera wskazanie lokalizacji i metody dostępu do informacji lub usług udostępnianych przez wystawcę certyfikatu, w którym zawarte jest to rozszerzenie -

       rozszerzenie nie jest krytyczne.

       i. OCSP -adres usługi OCSP

       ii. caIssuers - adres publikacji certyfikatów urzędów

2. Basic Constraints - rozszerzenie krytyczne

Subject is not a CA. Path Length Constraint: None

Jest to certyfikat końcowy.

Certyfikat do potwierdzenia obecności:

l.p.	Pole	Opis	Zawartość
1	Version	wersja formatu certyfikatu zgodna z X.509	V3
2	SerialNumber	numer seryjny certyfikatu, unikalny w ramach urzędu wydającego certyfikat	Unikalny identyfikator
3	SignatureAlgorithm	informacja o algorytmie użytym do podpisania certyfikatu	1.2.840.10045.4.3.2 (SHA256 with ECDSA Encryption)
4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	CN=PL.ID Presence CA O=MSWiA OU=CPD SN=<YYYYMMDD> C=PL gdzie <YYYYMMDD> oznacza datę wystawienia certyfikatu urzędu

5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	Zakres dat
6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	**C - pole obowiązkowe:** wartość określająca kraj weryfikacji tożsamości i utrzymywania rejestru, 2 literowy kod zgodny z ISO 3166 **CN - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona" +„ " + „Nazwisko**";** **SURNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko"; **GIVENNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Imię pierwsze"; **GIVENNAME - pole nie obowiązkowe: w**artość na podstawie danych dotyczących osoby - Drugie imię"; **SN - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „numer PESEL". Składnia pola będzie zgodna z zapisami Normy Europejskiej „ETSI EN 319 412-1 V1.1.1 Certificate Profiles; Part 1: Overview and common data structures" Rozdział „5.1.3 Natural person semantics identifier". Dla numeru seryjnego bazującego na krajowym numerze identyfikacyjnym przykładowa składnia to: PNOPL-76050912345;

7	SubjectPublicKeyInfo	określenie algorytmu używanego przez posiadacza certyfikatu oraz jego klucz publiczny	Klucz publiczny oraz użyty algorytm

Poniżej wskazano zakres i wartość pól rozszerzonych certyfikatów:

1. Rozszerzenie standardowe
    1. AuthorityKeyIdentifier

       Identyfikator klucza urzędu- rozszerzenie niekrytyczne

    2. SubjectKeyIdentifier

       Identyfikator klucza certyfikatu - rozszerzenie niekrytyczne

    3. KeyUsage: digitalSignature

       Definiuje dozwolone użycie klucza - rozszerzenie krytyczne.

    4. CertificatePolicies

       Rozszerzenie zawiera informację o polityce certyfikacji (identyfikator, adres elektroniczny) przyjętej przez urząd certyfikacji - rozszerzenie krytyczne.

       - Identyfikator polityki **(policyIdentifier)**: 1.2.616.1.101.5.2.1.1.1.3
       - Typ kwalifikatora polityki **(policyQualifierId)**: id-qt-unotice
       - **User notice: Explicit Text:** Treść Polityki znajduje się pod adresem http://e-dowod.gov.pl

    5. Authority Information Access

       Rozszerzenie zawiera wskazanie lokalizacji i metody dostępu do informacji lub usług udostępnianych przez wystawcę certyfikatu, w którym zawarte jest to rozszerzenie - rozszerzenie nie jest krytyczne.

       i. OCSP -adres usługi OCSP

       ii. caIssuers - adres publikacji certyfikatów urzędów

2. Basic Constraints - rozszerzenie krytyczne

Subject is not a CA. Path Length Constraint: None

Jest to certyfikat końcowy.

Wymienione powyżej pola rozszerzeń certyfikatu zostały określone jako krytyczne lub niekrytyczne.
W przypadku pól krytycznych od systemu wykorzystującego certyfikat wymagana jest jego poprawna interpretacja. Jeżeli system wykorzystującego certyfikat nie obsługuje pól wskazanych jako krytyczne certyfikat nie może być poprawnie przetwarzany.

Pola niekrytyczne mogą zostać zignorowane, jeżeli system wykorzystujący certyfikat nie potrafi ich poprawnie interpretować.

7.2. Struktura zapytania oraz odpowiedzi OCSP

Usługa świadczenia statusu certyfikatu w czasie rzeczywistym. Moduł OCSP udostępniać będzie usługę informowania o statusie certyfikatów wydanych przez każdy z urzędów podrzędnych. OCSP jest usługą dostępną publicznie.

W ramach działalności Centrum Certyfikacji udostępniona jest usługa weryfikacji statusu certyfikatu w trybie online (OCSP). Umożliwia ona uzyskanie informacji zarówno o statusie każdego z certyfikatów wydawanych w ramach PL.ID: certyfikat do uwierzytelniania, certyfikat do podpisu osobistego oraz certyfikat do potwierdzania obecności, jak też informacji o statusie certyfikatu każdego z pośrednich urzędów certyfikacji. Zawartość i format odpowiedzi OCSP zgodny jest z zapisami normy RFC 6960.

Dla każdego Urzędu Certyfikacji obsługiwanego przez Centrum Certyfikacji tworzona jest w ramach usługi OCSP oddzielna para kluczy i certyfikat usługi podpisany kluczem danego Urzędu. Odpowiedź na zapytanie o status certyfikatu wystawionego z danego Urzędu Certyfikacji podpisywana jest kluczem z usługi OCSP dedykowanym dla tego Urzędu i podpisanym przez ten Urząd.

Zapytanie OCSP jest zbiorem pól, których znaczenie przedstawiono poniżej:

L.p.	Pole	Opis
1.	Version	Wersja formatu usługi zgodna z RFC6990
2.	Request	Zapytanie do OCSP zawiera m.in informacje dotyczące: 1. Użyta funkcja skrótu 2. Skrót nazwy wystawcy certyfikatu, który wystawił weryfikowany certyfikat

		3. Skrót klucza wystawcy certyfikatu, który wystawił weryfikowany certyfikat 4. Numer seryjny weryfikowany certyfikatu
5.	RequestExtensions	Rozszerzona informacja o zapytaniu OCSP

Odpowiedź OCSP jest zbiorem pól, których znaczenie przedstawiono poniżej:

- Informacja o statusie certyfikatu (tbsResponseData)
- Informacja o algorytmie użytym do podpisania odpowiedzi (signatureAlgorithm)
- Poświadczenie elektroniczne, składane przez organ wydający odpowiedź (signature)
- Certyfikaty załączone do odpowiedzi (certs) opcjonalnie

Opis poszczególnych struktur przedstawiono poniżej:

L.p.	**Pole**	**Opis**
1.	Version	Wersja formatu usługi zgodna z RFC6990
2.	Responder Id	Identyfikator certyfikatu usługi OCSP
3.	Produced At	Data/czas podpisania odpowiedzi
4.	Responses	Pole zawiera statusy certyfikatów dla których zostało wysłane zapytanie, zawierające: 1. Użyta funkcja skrótu w zapytaniu 2. Skrót nazwy wystawcy certyfikatu, który wystawił weryfikowany certyfikat 3. Skrót klucza wystawcy certyfikatu, który wystawił weryfikowany certyfikat 4. Numer seryjny weryfikowany certyfikatu 5. Status certyfikatu 6. Data unieważnienia (dla certyfikatów unieważnionych) 7. Powód unieważniania (dla certyfikatów unieważnionych) 8. Data sprawdzenia statusu
5.	ResponseExtensions	Rozszerzona informacja o odpowiedzi OCSP

7.3. Struktura listy CRL

Lista CRL to plik z listą unieważnionych i zawieszonych certyfikatów klucza publicznego wystawionych przez urząd certyfikacji. Lista jest poświadczona elektronicznie przez podmiot świadczący usługi certyfikacyjne. Profile certyfikatów są zgodne z formatami opisanymi normą

ITU-T X.509. Dodatkowo certyfikaty są zgodne z profilami certyfikatów zdefiniowanych w normie ETSI-EN 319 412-2.

Lista unieważnionych i zawieszonych certyfikatów jest zbiorem pól, których znaczenie przedstawiono poniżej:

Pole	Opis/wartość
tbsCertList	Poświadczona elektronicznie treść Listy CRL
signatureAlgorithm	Algorytm podpisu: EcdsaWithSHA512 (1.2.840.10045.4.3.4)
signatureValue	Wartość poświadczenia elektronicznego.

Poświadczona elektronicznie treść Listy CRL:

Pole	Opis/wartość	Pole krytyczne
version	„1” (X.509 v2 CRL)	
signature	Algorytm podpisu: EcdsaWithSHA512 (1.2.840.10045.4.3.4)	
issuer	Identyfikator wystawcy listy CRL, zgodny z identyfikatorem określonym w profilu certyfikatów	
thisUpdate	Data wydania listy CRL	
nextUpdate	Data następnej aktualizacji listy CRL	
revokedCertificates	Sekcja zawierająca listę unieważnionych certyfikatów	
▪ userCertificate	Numer seryjny zawieszonego lub unieważnionego certyfikatu lub unieważnionego zaświadczenia certyfikacyjnego	
▪ revocationDate	Data zawieszenia bądź unieważnienia certyfikatu lub unieważnienia zaświadczenia certyfikacyjnego	
▪ cRLReason	Kod przyczyny unieważnienia lub wskazanie, że certyfikat został zawieszone (opcjonalne)	NIE
crlExtensions	Rozszerzenia listy CRL (dotyczą całej listy)	
▪ authorityKeyIdentifier	EcdsaWithSHA512 (1.2.840.10045.4.3.4)	NIE
▪ cRLNumber	Numer kolejny listy CRL	NIE

Pole	Opis/wartość	Pole krytyczne
▪ ExpiredCertsOnCRL	Rozszerzenie ExpiredCertsOnCRL (2.5.29.60) oznacza, że lista CRL zawiera także certyfikaty, które wygasły. ExpiredCertsOnCRL zawiera datę od której lista CRL przechowuje informacje o wygasłych certyfikatach.	

8. Audyt zgodności

8.1. Częstotliwość i okoliczności audytu

Działalność Centrum Certyfikacji podlega audytowi wewnętrznemu i zewnętrznemu.

Audyt wewnętrzny przeprowadzany jest w miarę bieżących potrzeb lub w przypadku dokonywania znaczących zmian w Centrum Certyfikacji.

Audyt zewnętrzny może być przeprowadzony również na wniosek ministra właściwego ds. informatyzacji.

8.2. Kwalifikacje audytorów

Audytorzy powinni posiadać niezbędną wiedzę i doświadczenie do prawidłowego przeprowadzenia audytu.

8.3. Związek audytora z audytowaną jednostką

Audytu nie mogą dokonywać pracownicy bezpośrednio związani z funkcjonowaniem Centrum Certyfikacji CPD MSWiA.

8.4. Zakres audytu

Audytem mogą być objęte są wszystkie istotne aspekty świadczenia usług certyfikacyjnych przez Centrum Certyfikacji, a w szczególności:

- Bezpieczeństwo fizyczne,
- Bezpieczeństwo logiczne,
- Realizacja usług zgodnie z przyjętymi regułami zapisanymi w Polityce,
- Zgodność realizacji działań z przyjętymi procedurami.

Audyt realizowany jest zgodnie z przyjętą procedurą.

8.5. Podejmowanie działań w przypadku wykrycia niezgodności

W przypadku wykrycia niezgodności, audytorzy zobowiązani są do:

- Sporządzenia notatki opisującej charakter niezgodności i jej wpływ na funkcjonowanie Centrum Certyfikacji,
- Przedstawienia notatki Dyrektorowi CPD MSWiA, które podejmuje decyzję o podjęciu działań korygujących oraz priorytecie ich realizacji,
- Po wdrożeniu działań korygujących i usunięciu niezgodności, obszar zmian zostaje poddany ponownemu audytowi.

8.6. Informowanie o wynikach audytu

Raport końcowy z przeprowadzonego audytu nie podlega publikacji i jest uważany za dokument wewnętrzny CPD MSWiA.

9. Postanowienia ogólne

9.1. Opłaty

Dowód osobisty wydawany jest nieodpłatnie.

9.2. Synchronizacja czasu

Wszystkie zegary urządzeń synchronizacji czasu urządzeń wykorzystywanych w procesie świadczenia usług są synchronizowane z międzynarodowym wzorcem czasu.

9.3. Ochrona informacji

Wszystkie osoby wykonujący zadania związane ze świadczeniem usług zaufania w CPD MSWiA, są zobowiązane do zachowania poufności informacji. Obowiązek ochrony poufności informacji dotyczy także pracowników podmiotów zewnętrznych, wykonujących zadania na rzecz CPD MSWiA i jest regulowany w umowach zawartych przez CPD MSWiA z tymi podmiotami.

CPD MSWiA ujawnia dane związane z funkcjonowaniem Centrum Certyfikacji i objęte tajemnicą wyłącznie następującym podmiotom:

- sądom i prokuraturze w związku z toczącym się postępowaniem;
- ministrowi właściwemu do spraw informatyzacji w związku ze sprawowaniem przez niego nadzoru nad działalnością dostawców usług zaufania;
- innym upoważnionym organom w związku z prowadzonym przez te organy postępowaniem.

Zgodnie z art. 15 ust. 4 ustawy o usługach zaufania nie udostępnia się danych wykorzystywanych przez Centrum Certyfikacji służących do składania pieczęci elektronicznej.

9.4. Ochrona danych osobowych

Dane osobowe Obywateli przekazywane do Centrum Certyfikacji są objęte ochroną określoną przez Ustawę o ochronie danych osobowych. Dane osobowe są wykorzystywane tylko w związku ze świadczeniem Usług certyfikacyjnych.

9.5. Prawo do własności intelektualnej

Niniejsza Polityka stanowi własność intelektualną CPD MSWiA. Z punktu widzenia prawa autorskiego Polityka może być bez żadnych ograniczeń wykorzystywana (w tym drukowana i kopiowana) przez osoby, którym została udostępniona za zgodą CPD MSWiA.

9.6. Ograniczenie odpowiedzialności

Zamieszczenie w dowodzie osobistym (w przeznaczonej do tego przestrzeni) kwalifikowanego certyfikatu podpisu elektronicznego wraz z danymi do składania podpisu oraz korzystanie z tego podpisu odbywa się na podstawie umowy posiadacza dowodu osobistego oraz kwalifikowanego dostawcy usługi zaufania. W przypadku unieważnienia dowodu osobistego z przyczyn określonych w ustawie skutkującego niemożnością korzystania z tego certyfikatu, Skarb Państwa nie ponosi kosztów związanych z zakupem nowego kwalifikowanego certyfikatu podpisu elektronicznego.

9.7. Okres obowiązywania i wypowiedzenie

Niniejsza Polityka obowiązuje od momentu nadania jej statusu aktualnej i opublikowania w repozytorium określonym w pkt. 2.2.

Niniejszy dokument obowiązuje do momentu zastąpienia go nową wersją i utraty statusu aktualny.

9.8. Powiadamianie

Minister właściwy do spraw wewnętrznych określi i opublikuje na swojej stronie internetowej Politykę świadczenia usług dla dowodu osobistego z warstwą elektroniczną.

W sytuacji opisanej w art. 12g Ustawy o dowodach osobistych, Minister właściwy do spraw wewnętrznych ogłosi, w drodze obwieszczenia, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski", informację o seriach i numerach dowodów osobistych, w których unieważniono certyfikaty: potwierdzenia obecności, identyfikacji i uwierzytelnienia, podpisu osobistego, zamieszczone w warstwie elektronicznej, informację o seriach i numerach dowodów osobistych, których ważność została przedłużona oraz harmonogram wymiany dowodów osobistych, a także informację o okresie, w którym będą wydawane dowody osobiste niezawierające w warstwie elektronicznej ww. certyfikatów. Jeżeli unieważnienie certyfikatów dotyczy dowodów osobistych wydanych w ściśle określonym czasie, obwieszczenie zawiera również daty wydania tych dowodów osobistych.

9.9. Rozstrzyganie sporów

Postępowania w sprawach dowodów osobistych rozpatrywane są zgodnie z procedurą przewidzianą w ustawie z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2017 r. poz. 1257, z 2018 r. poz. 149, 650).

9.10. Prawo właściwe

W zakresie niniejszej Polityki stosuje się prawo obowiązujące na terenie Rzeczypospolitej Polskiej

9.11. Inne postanowienia

Minister właściwy do spraw wewnętrznych w przypadku uzasadnionego podejrzenia naruszenia praw obywateli związanego z naruszeniem bezpieczeństwa wykorzystania warstwy elektronicznej dowodu osobistego, unieważnia certyfikaty zamieszczone w warstwie elektronicznej dowodu osobistego, przy zachowaniu ważności warstwy graficznej dowodu osobistego oraz może określić czas, w którym będą wydawane dowody osobiste niezawierające w warstwie elektronicznej certyfikatów. Unieważnienie, może dotyczyć wszystkich posiadaczy dowodów osobistych lub grupy posiadaczy dowodów osobistych o tych samych cechach zabezpieczeń. Unieważnienie, może dotyczyć wszystkich posiadaczy dowodów osobistych lub grupy posiadaczy dowodów osobistych o tych samych cechach zabezpieczeń. Minister właściwy do spraw wewnętrznych w przypadku unieważnienia certyfikatów zamieszczonych w warstwie elektronicznej dowodu osobistego, może przedłużyć ważność dowodów osobistych w zakresie warstwy graficznej, jeżeli data wymiany określona w harmonogramie wymiany dowodów osobistych jest późniejsza niż data ważności dowodu osobistego. Minister właściwy do spraw wewnętrznych przekazuje niezwłocznie ministrowi właściwemu do spraw informatyzacji informację o unieważnieniu certyfikatów oraz ogłasza w drodze obwieszczenia, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski”, informację o seriach i numerach dowodów osobistych, w których unieważniono certyfikaty zamieszczone w warstwie elektronicznej, informację o seriach i numerach dowodów osobistych, których ważność została przedłużona oraz harmonogram wymiany dowodów osobistych, a także informację o okresie, w którym będą wydawane dowody osobiste niezawierające w warstwie elektronicznej certyfikatów. Jeżeli unieważnienie certyfikatów dotyczy dowodów osobistych wydanych w ściśle określonym czasie, obwieszczenie zawiera również daty wydania tych dowodów osobistych

Unieważnienie certyfikatów przez ministra nie obejmuje certyfikatu kwalifikowanego, zamieszczonego w przeznaczonej do tego przestrzeni, na podstawie indywidualnej umowy zawartej pomiędzy posiadaczem dowodu osobistego a dostawcą usług zaufania.