Polityka świadczenia usług dla dowodu osobistego z warstwą elektroniczną

Spis treści

Polityka certyfikacji EDO ... 3
1. Wstęp ... 3
1.1. Wprowadzenie ... 3
1.2. Nazwa dokumentu i wersjonowanie ... 3
1.3. Uczestnicy PKI ... 4
1.4. Zakres stosowania certyfikatów ... 6
1.5. Zarządzanie polityką certyfikacji ... 7
1.6. Słownik ... 7
2. Publikowanie i repozytorium ... 10
2.1. Repozytorium ... 10
2.2. Publikowanie w postaci elektronicznej ... 11
2.3. Częstotliwość publikacji ... 11
2.4. Dostęp do repozytoriów ... 11
3. Zasady identyfikacji i uwierzytelnienia ... 11
3.1. Zasady nadawania nazw ... 12
3.2. Pierwsza rejestracja ... 14
3.3. Wystawienie kolejnego certyfikatu ... 14
3.4. Zawieszenie, cofnięcie zawieszenia i unieważnienie certyfikatu ... 14
4. Wymagania dotyczące cyklu życia certyfikatów ... 15
4.1. Zgłoszenie certyfikacyjne ... 15
4.2. Obsługa zgłoszenia certyfikacyjnego ... 15
4.3. Wydanie certyfikatu ... 15
4.4. Akceptacja certyfikatu ... 16
4.5. Zasady używania certyfikatu i pary kluczy ... 16
4.6. Odnowienie certyfikatu ... 16
4.7. Odnowienie certyfikatu z wymianą klucza ... 16
4.8. Modyfikacja zawartości certyfikatu ... 17
4.9. Zawieszenie, cofnięcie zawieszenia i unieważnienie certyfikatu ... 17
4.10. Usługi weryfikacji statusu certyfikatu ... 18
5. Obiekt, zarządzanie i kontrola operacyjna ... 18
5.1. Bezpieczeństwo fizyczne ... 18
5.2. Zabezpieczenia organizacyjne ... 19
5.3. Nadzorowanie personelu ... 20
5.4. Rejestracja zdarzeń ... 22

5.5. Archiwizacja danych 24
5.6. Wymiana kluczy urzędu 24
5.7. Naruszenie bezpieczeństwa kluczy urzędu i procedury odtwarzania po awarii (Compromise and Disaster Recovery) 24
5.8. Zakończenie działalności CA lub punktów rejestracji 26
6. Środki ochrony technicznej 26
6.1. Generowanie pary kluczy i instalacja 26
6.2. Ochrona, aktywacja, dezaktywacja i niszczenie kluczy 29
6.3. Dane aktywujące 31
6.4. Zarządzanie bezpieczeństwem systemu informatycznego 31
6.5. Zarządzanie bezpieczeństwem cyklu życia procesu wytwórczego 32
6.6. Zarządzanie bezpieczeństwem sieciowym 33
7. Profil certyfikatu i list CRL 33
7.1. Struktura certyfikatu 33
7.2. Struktura odpowiedzi OCSP 44
8. Audyt zgodności 45
8.1. Częstotliwość i okoliczności audytu 45
8.2. Kwalifikacje audytorów 46
8.3. Związek audytora z audytowaną jednostką 46
8.4. Zakres kontroli/audytu 46
8.5. Podejmowanie działań w przypadku wykrycia niezgodności 46
8.6. Informowanie o wynikach audytu 46
9. Postanowienia ogólne 46
9.1. Opłaty 46
9.2. Synchronizacja czasu 47
9.3. Ochrona informacji 47
9.4. Ochrona danych osobowych 47
9.5. Prawo do własności intelektualnej 47
9.6. Ograniczenie odpowiedzialności 47
9.7. Okres obowiązywania i wypowiedzenie 48
9.8. Powiadamianie 48
9.9. Rozstrzyganie sporów 48
9.10. Prawo właściwe 48
9.11. Inne postanowienia 49

Polityka certyfikacji EDO

1. Wstęp

1.1. Wprowadzenie

Niniejszą politykę stosuje się do usług certyfikacji w zakresie wydawania środka identyfikacji elektronicznej zwanego dalej EDO (Elektroniczny Dowód Osobisty) wydawanego zgodnie z wymaganiami określonymi w Rozporządzenie 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 Certyfikacji określa ogólne zasady stosowane przez MSWiA w trakcie świadczenia usług zaufania w szczególności:

- Wydawania środka identyfikacji elektronicznej zawierającego:
    - Certyfikat do identyfikacji i uwierzytelnienia
    - Certyfikat dla zaawansowanego podpisu elektronicznego
    - Certyfikat do potwierdzania obecności
- Zawieszenia, cofnięcia zawieszenia i unieważnienia certyfikatów

EDO w zakresie wydawania certyfikatów niekwalifikowanych zostało zaprojektowane i wdrożone w taki sposób, aby spełnić wymagania nałożone przez krajową Ustawę o Usługach Zaufania 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 RFC 3647 "Certificate Policy and Certification Practices Framework".

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

1.2. Nazwa dokumentu i wersjonowanie

Identyfikator niniejszego dokumentu Polityki świadczenia usług zaufania.

Nazwa Polityki	**Polityka Certyfikacji dowodu osobistego z warstwą elektroniczną.**
Wersja Polityki	1.0
Status wersji	Archiwalny
Numer referencyjny/OID (ang. Object Identifier)	1.2.616.1.101.5.2.1.1.1.0.1.0
Data wprowadzenia w życie Polityki	4 marca 2019 r.

Data wygaśnięcia	30 grudnia 2020 r.

Niniejszy dokument Polityki Certyfikacji dowodu osobistego z warstwą elektroniczną jest zbiorem polityk i regulaminów stosowanych przez MSWiA przy wydawaniu dowodu osobistego z warstwą elektroniczną. Identyfikator Polityki Certyfikacji nie jest umieszczany w treści wystawianych certyfikatów. W wydawanych przez siebie certyfikatach dla EDO, MSWiA umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru identyfikatorów polityk certyfikacji określanych w rozdz. 7.1 niniejszego dokumentu. Niniejsza Polityka Certyfikacji 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 EDO:

	Parametr	**Wartość**
Level1 - Root CA	Nazwa DN	CN=pl.ID Root CA SERIALNUMBER=2019 C=PL
	Numer seryjny	2e96f5990b4d0b93e0e6c13c8271cd4b
	Identyfikator klucza	55d15232bcefcaecfe33b018e737eee3b82fab47
	Odcisk palca [SHA-1]	d073b9d766a73785dd5ba67c32f21183a60f1379
Level2 - OCSP	Nazwa DN	CN=pl.ID Root CA OCSP SERIALNUMBER=2019 C=PL
	Numer seryjny	63545144e9e3f3a0791a89feb082cb21
	Identyfikator klucza	c1ff5f0837b0bdc9729d71e6c0d1aede59e3ac7d
	Odcisk palca [SHA-1]	5525b45d3a960c1a4fb7dbd9f0583db9b5f5ab94

Level2 - Sub CA	Nazwa DN	CN=pl.ID Authentication CA O=MSWiA OU=CPD C=PL SERIALNUMBER=20190221
	Numer seryjny	24fd34b5ee415389e367a5262167d6b7
	Identyfikator klucza	453dddd3108328a8a1830c67ac7bdfb686b8725d
	Odcisk palca [SHA-1]	e1fd93f7bff44e7d5e3ad8567d302ab691231aff
Level3 - OCSP	Nazwa DN	CN=pl.ID Authentication CA OCSP O=MSWiA OU=CPD C=PL SERIALNUMBER=20190221
	Numer seryjny	6abd13f78e4547e5b8fb9280ea0dc670
	Identyfikator klucza	6dd404e46ab8079fbac6b24c2a2ec5646e0758a4
	Odcisk palca [SHA-1]	b08abbf25ee629a4cc03cedcfe9c11d9b997c029
Level2 - Sub CA	Nazwa DN	CN=pl.ID Authorization CA O=MSWiA OU=CPD C=PL SERIALNUMBER=20190221
	Numer seryjny	20ac6380ff1f7220fd3224bc83467616
	Identyfikator klucza	fae95b03b06d7656301fc69a1789894f7ca604dd
	Odcisk palca [SHA-1]	1a6dc93e941e8ab01a63b25ad236d5bcb39eab89
Level3 - OCSP	Nazwa DN	CN=pl.ID Authorization CA OCSP O=MSWiA OU=CPD C=PL SERIALNUMBER=20190221
	Numer seryjny	47c804761403344203d8f379d1f2c9ef
	Identyfikator klucza	53d7acdc7277d6228126d25bbb287dc9f1bb33e4
	Odcisk palca [SHA-1]	723c6949a81776ae0b2135da4a19b2db9c170e5d

Level2 - Sub CA	Nazwa DN	CN=pl.ID Presence CA O=MSWiA OU=CPD C=PL SERIALNUMBER=20190221
	Numer seryjny	1455c38ae1a7f3cfff01b3d72571f6cb
	Identyfikator klucza	ad189e8a65d09e71c856b583ac9d1ffb2b67e369
	Odcisk palca [SHA-1]	5eaf3e85c864c667bd3715375794afb93631bf76
Level3 - OCSP	Nazwa DN	CN=pl.ID Presence CA OCSP O=MSWiA OU=CPD C=PL SERIALNUMBER=20190221
	Numer seryjny	3a5d3ca4d37e43bb66ff5f539f41e718
	Identyfikator klucza	1f103fc6122a094a8f1ed994839bd9802bc8322b
	Odcisk palca [SHA-1]	f991ddc0e0dab45c2a8434bbc2bc825f26716cb2

1.4. Zakres stosowania certyfikatów

W ramach Polityki Certyfikacyjnej dowodu osobistego z warstwą elektroniczną 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 certyfikacji. 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 certyfikacji

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: 22 60 17 956

1.5.3.Podmioty określające aktualność zasad określonych w dokumencie

Za ocenę aktualności i przydatności niniejszej Polityki Certyfikacji dowodu osobistego z warstwą elektroniczną 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 Certyfikacji dowodu osobistego z warstwą elektroniczną

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

1.6. Słownik

1. 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}".

2. Bezpieczne urządzenie służące do weryfikacji podpisu elektronicznego - urządzenie służące do weryfikacji podpisu elektronicznego spełniające wymagania określone w Ustawie.
3. Blankiet - Niespersonalizowany blankiet Dowodu Osobistego wytwarzany i dostarczany przez PWPW do CPD MSWiA. Po spersonalizowaniu Blankiet staje się Dowodem Osobistym.
4. Centrum Certyfikacji CPD MSWiA - jednostka wystawiająca certyfikaty znajdująca się w Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji.
5. Certyfikat klucza publicznego - certyfikat klucza weryfikującego podpis lub certyfikat klucza szyfrującego.
6. 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; certyfikat klucza weryfikującego podpis jest certyfikatem w rozumieniu Ustawy.
7. CPD MSWiA - Centrum Personalizacji Dokumentów Ministerstwa Spraw Wewnętrznych i Administracji. Jednostka administracji państwowej odpowiedzialna za personalizację dokumentów takich jak dowód osobisty, paszport i inne.
8. 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 stanowiący środek identyfikacji elektronicznej obywatela oraz służący do składania 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.
9. eDO - Dowód osobisty z warstwą elektroniczną.
10. 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.
11. Klucz - liczba, symbol lub ciąg liczb lub symboli jednoznacznie wyznaczający przekształcenie kryptograficzne spośród rodziny przekształceń zdefiniowanej przez algorytm kryptograficzny.
12. Klucz podpisujący - klucz prywatny służący do składania podpisu elektronicznego; klucz podpisujący stanowi dane służące do składania podpisu elektronicznego w rozumieniu Ustawy.
13. 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.
14. Klucze infrastruktury - klucze kryptograficzne algorytmów kryptograficznych stosowane do innych celów niż składanie lub weryfikacja kwalifikowanego podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane:
    14.1. w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych,

14.2. do zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń,

14.3. do weryfikacji dostępu do urządzeń, oprogramowania weryfikującego lub podpisującego.

15. Komponent techniczny - sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.
16. 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.
17. Moduł kluczowy - urządzenie współpracujące z komponentem technicznym, przechowujące klucze infrastruktury lub dane służące do składania bezpiecznych podpisów elektronicznych lub poświadczeń elektronicznych, lub klucze chroniące te dane, lub przechowujące części tych kluczy lub danych.
18. MSWiA - Ministerstwo Spraw Wewnętrznych i Administracji.
19. NIST - (ang. National Institute of Standards and Technology) - amerykańska agencja federalna spełniająca funkcję Narodowego Biura Standaryzacji).
20. 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.
21. PESEL - Powszechny Elektroniczny System Ewidencji Ludności.
22. 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.
23. Polityka - niniejsza polityka usług zaufania.
24. Poświadczenie elektroniczne - dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne, oraz spełniają następujące wymagania:

    24.1. są sporządzone za pomocą podlegających wyłącznej kontroli podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne kwalifikowanych urządzeń służących do składania podpisu elektronicznego i danych służących do składania poświadczenia elektronicznego,

    24.2. jakakolwiek zmiana danych poświadczonych jest rozpoznawalna.

25. Rozporządzenie Ministra Cyfryzacji z dnia 5 października 2016 r. w sprawie krajowej infrastruktury zaufania (Dz. U. 2016 poz. 1632), zwane dalej „Rozporządzenie MC".
26. 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.
27. SPD - System Personalizacji Dokumentów używany przez CPD MSWiA do personalizacji dowodów osobistych.
28. Strona ufająca - osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej, która w granicach określonych w polityce certyfikacji może działać w oparciu o certyfikat lub zaświadczenie certyfikacyjne. Stroną ufającą jest również

Subskrybent, jeśli wykonuje działania w oparciu o wystawiony zgodnie z Polityką certyfikat lub zaświadczenie certyfikacyjne.

29. Ścieżka certyfikacji - uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i certyfikatu utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i certyfikatu poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego „punktem zaufania".
30. TLS - (ang. *Transport Layer Security*). Jest to protokół, który służy do bezpiecznej wymiany danych za pośrednictwem Internetu.
31. 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
32. Usługi certyfikacyjne - szeroka klasa usług dotyczących TTP obejmująca działania polegające na poświadczeniu wybranych informacji przez wygenerowanie podpisanego elektronicznie zaświadczenia certyfikacyjnego, jak certyfikacja kluczy publicznych, certyfikacja istnienia danych elektronicznych w określonym czasie, certyfikacja przedstawienia danych elektronicznych przez określonych użytkowników w określonym czasie.
33. Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej. (Dz. U. 2016 Poz. 1579), zwaną dalej „Ustawa".
34. Uwierzytelnienie - Oznacza proces elektroniczny, który umożliwia identyfikację elektroniczną osoby fizycznej lub prawnej, lub potwierdzenie pochodzenia oraz integralności weryfikowanych danych w postaci elektronicznej.
35. Zaświadczenie certyfikacyjne - elektroniczne zaświadczenie, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub ministra właściwego do spraw gospodarki i które umożliwia identyfikację tego podmiotu lub organu.
36. X.509 - Standard definiujący konstrukcję certyfikatu klucza publicznego i listy certyfikatów unieważnionych.

Określenia wykorzystywane w niniejszej polityce certyfikacji, 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 certyfikowanych.
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/e-dowod/polityka-certyfikacji.

W postaci elektronicznej publikowane są następujące dokumenty:

1. wszystkie wersje Polityki, z podaniem okresu ich obowiązywania
2. Certyfikaty podpisów elektronicznych klucza publicznego:
    1. Urzędów EDO służących 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, ale nie później niż 24 godziny od momentu odebrania unieważnienia.
3. Nowe wersje Polityk, Regulaminów są publikowane niezwłocznie po zatwierdzeniu**.**

2.4. Dostęp do repozytoriów

1. Repozytorium EDO 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 osobiście w formie pisemnej lub w formie dokumentu elektronicznego 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 prawny lub kurator. Tożsamość osoby ubiegającej się o wydanie dowodu osobistego ustala się na podstawie przedłożonego przez wnioskodawcę dotychczasowego 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. dokumentu, organ gminy ustala jej tożsamość na podstawie danych zawartych w dostępnych rejestrach publicznych (RDO i PESEL). W

przypadku, gdy wniosek jest składany w postaci elektronicznej, tożsamość osoby ubiegającej się o wydanie dowodu osobistego potwierdza się przy odbiorze dowodu osobistego.

Dowód osobisty odbiera się osobiście. Odbioru dowodu osobistego wydanego osobie nieposiadającej zdolności do czynności prawnych lub posiadającej ograniczoną zdolność do czynności prawnych dokonuje przedstawiciel ustawowy tej osoby w jej obecności, chyba że osoba ta nie ma ukończonych 5 lat lub była obecna przy składaniu wniosku o dowód osobisty. Odbioru dowodu osobistego wydanego osobie posiadającej ograniczoną zdolność do czynności prawnych może dokonać osobiście ta osoba. Odbioru dowodu osobistego może dokonać pełnomocnik legitymujący się pełnomocnictwem szczególnym do dokonania tej czynności w przypadku, gdy wnioskodawca, nie może osobiście odebrać dowodu osobistego z powodu choroby, niepełnosprawności lub innej niedającej się pokonać przeszkody. Niemniej dotyczy to sytuacji, gdy wnioskodawca osobiście składał wniosek: w urzędzie lub z powodu ww. okoliczności wniosek był przyjęty w miejscu pobytu tej osoby.

Przepisy prawa gwarantują, że tożsamość osoby, której dotyczy wniosek o wydanie dowodu osobistego, co najmniej raz jest weryfikowana osobiście przez urzędnika przyjmującego wniosek.

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.

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 RFC 5280 Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, z uwzględnieniem wymagań ze standardów europejskich ETSI EN 319 412-(1 do 2).

Budowa numerów identyfikacyjnych osób fizycznych, dla których wydawane będą dowody osobiste z warstwą elektroniczną, będzie zgodna ze składnią zdefiniowaną w normie 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 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 do 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:** numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „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 dla zaawansowanego podpisu elektronicznego:

- 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:** numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „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 do potwierdzania obecności:

- 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:** numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „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.
Organ gminy, 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 będzie zamieszczony w dowodach osobistych osób posiadających pełną zdolność do czynności prawnych oraz osób posiadających ograniczoną zdolność do czynności prawnych. Certyfikat podpisu osobistego będą posiadały 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, oraz osobom małoletnim, które w okresie ważności dowodu osobistego ukończą 18 rok życia – jeżeli rodzic, opiekun prawny lub kurator tej osoby przy składaniu wniosku o wydanie dowodu osobistego wyraził zgodę na zamieszczenie tego certyfikatu.

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. Na podstawie przesłanych danych generowane są certyfikaty, które w procesie personalizacji blankietu nagrywane są w warstwę elektroniczną dowodu osobistego. Po zakończeniu personalizacji dowód osobisty oraz korespondencja z kodem PUK zostaje wysłana do urzędów, gdzie czeka na odbiór przez wnioskującego.

4.3. Wydanie certyfikatu

Po otrzymaniu żądania wygenerowania certyfikatu z SPD, urząd certyfikujący weryfikuje poprawność danych i po pozytywnej weryfikacji generuje certyfikat.

Wygenerowany certyfikat zapisywany jest w bazie danych i przekazywany jest do SPD w celu osadzenia go na blankiecie w kontenerze, na którym jest osadzony klucz prywatny powiązany z kluczem publicznym certyfikatu.

Centrum Certyfikacji zapisuje do logu wszystkie znaczące zdarzenia związane z wystawieniem certyfikatu

Nowy dowód osobisty może być odebrany po 30 dniach od złożenia wniosku, jednak zazwyczaj jest gotowy wcześniej. Tylko w szczególnych przypadkach termin może się wydłużyć. Istnieje możliwość sprawdzenia przy pomocy usługi zamieszczonej na stronie internetowej www obywatel.gov.pl, czy dowód osobisty jest już gotowy do odbioru. Wymaga to jedynie wskazania numeru wniosku, który jest zamieszczony na potwierdzeniu złożenia wniosku o wydanie dowodu osobistego.

4.4. Akceptacja certyfikatu

Z przepisów ustawy o dowodach osobistych wynika wprost, że wszystkie dowody osobiste są wyposażone w certyfikat potwierdzenia obecności. Natomiast certyfikat identyfikacji i uwierzytelnienia będzie zamieszczony w dowodach osobistych osób posiadających pełną zdolność do czynności prawnych oraz osób posiadających ograniczoną zdolność do czynności prawnych. Certyfikat podpisu osobistego będą posiadały 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, oraz osobom małoletnim, które w okresie ważności dowodu osobistego ukończą 18 rok życia – jeżeli rodzic, opiekun prawny lub kurator tej osoby przy składaniu wniosku o wydanie dowodu osobistego wyraził zgodę na zamieszczenie tego 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 Certyfikacji 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 nie wie, gdzie jest dokument) będzie 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 będzie powodowało zawieszenie ważności dowodu osobistego. Czynności dokonane w okresie zawieszenia albo unieważnienia certyfikatów nie wywołają skutków prawnych. Po upływie 14 dni i nie cofnięciu przez posiadacza dowodu zawieszenia certyfikatów, dowód osobisty automatycznie zostanie unieważniony. Późniejsze cofnięcie zawieszenia certyfikatów nie wpływa na ważność czynności dokonanej w okresie zawieszenia.

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:

1. zgłoszenia utraty lub uszkodzenia dowodu osobistego;
2. utraty przez posiadacza dowodu osobistego obywatelstwa polskiego;
3. ubezwłasnowolnienia całkowitego lub częściowego posiadacza dowodu osobistego, w którego dowodzie osobistym w warstwie elektronicznej został zamieszczony certyfikat podpisu osobistego;
4. zgonu posiadacza dowodu osobistego;

5. zmiany danych zawartych w dowodzie osobistym (4 miesiące od zmiany danych, jeżeli wcześniej dowód nie został unieważniony);
6. 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

Zapewnia się kontrolę dostępu do pomieszczeń, w których zlokalizowane jest Centrum Certyfikacji poprzez indywidualne karty dostępowe oraz uwierzytelnienie kodem PIN. Dostęp do elementów systemu mają wyłącznie osoby uprawnione.

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. Pełni jednocześnie funkcje Inspektora ds. rejestracji oraz Inspektora ds. unieważniania.

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	Lista osób wymaganych
1.	Uruchomienie systemu	Operator Systemu, Administrator Systemu, Inspektor Bezpieczeństwa Systemu
2.	Wczytanie kluczy urzędów RootCA	trzech Operatorów Systemu, Inspektor Bezpieczeństwa Systemu
2.	Wczytanie kluczy urzędów SubCA i OCSP	dwóch Operatorów Systemu, Inspektor Bezpieczeństwa Systemu
3.	Odtworzenie kopii zapasowej systemu	Operator Systemu, Administrator Systemu, Inspektor Bezpieczeństwa Systemu
4.	Zamknięcie systemu	Operator Systemu, Inspektor Bezpieczeństwa Systemu
5.	Wykonanie kopii zapasowej	Operator Systemu, Inspektor Bezpieczeństwa Systemu
6.	Odnowienie kluczy urzędów i OCSP	dwóch Operatorów Systemu, Administrator Systemu, Inspektor Bezpieczeństwa Systemu

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 jego pracownicy wykonujący 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,
- personel Centrum Certyfikacji, zwłaszcza osoby piastujące tzw. zaufane role, zobowiązane są postępować zgodnie z przepisami *Rozporządzenia eIDAS i Ustawy z dnia 5 września o usługach zaufania oraz identyfikacji elektronicznej*.

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 Certyfikacji nie określa wymagań w tym zakresie.

5.3.6. Kwestie dyscyplinarne

W przypadku wykrycia, że pracownik Centrum Certyfikacji wykonał nieuprawnione działania, może się on narazić na sankcje wynikające z Kodeksu Pracy oraz innych przepisów, w tym m.in. z Ustawy o podpisie elektronicznym czy 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 pracownikom niezbędną dokumentację, wymaganą do realizacji obowiązków służbowych. W szczególności obejmuje ona:

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

5.4. Rejestracja zdarzeń

5.4.1. Typy rejestrowanych zdarzeń

W celu zapewniania jak najwyższego poziomu bezpieczeństwa 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. 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:

Serwery Centrum Certyfikacji, w tym bazy danych przechowujące informacje o Subskrybentach i wystawionych certyfikatach.

Serwery Repozytorium.

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

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. Tworząc kopie zapasowe, archiwizacji podlega cała zawartość dysków twardych serwerów Centrum Certyfikacji.

5.6. Wymiana kluczy urzędu

Niniejsza polityka nie opisuje przedmiotowego zakresu.

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 Subskrybentów i Strony ufające. Następnie unieważnianie są wszystkie ważne certyfikaty Subskrybentów i Zaświadczenie certyfikacyjne Centrum Certyfikacji. 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 nowej pary 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

Pary kluczy urzędów EDO generowane są zgodnie z udokumentowaną procedurą generacji, zapewniającą integralność i poufność kluczy. Generacja pary kluczy odbywa się w siedzibie CPD MSWiA w środowisku bezpiecznym fizycznie, w obecności co najmniej dwóch uprawnionych 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 wszystkich 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.

Pary kluczy dla Obywateli generowane są podczas procesu personalizacji dowodu osobistego w module kryptograficznym.

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 subskrybentów, których klucze publiczne są certyfikowane zgodnie z niniejsza polityką, są przechowywane tylko i wyłącznie na blankietach dowodów osobistych.

6.1.2.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

6.1.3.Parametry generowania klucz publicznego

Klucze publiczne urzędów CA oraz użytkowników końcowych generowane są za pomocą sprzętowych modułów kryptograficznych, które zapewniają odpowiednią jakość otrzymanych kluczy.

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 urzędu są używane wyłącznie do podpisywania certyfikatów Obywateli.

Klucze 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 komponentu technicznego (module kryptograficznym) w sposób zapewniający jego ochronę i bezpieczne przekazanie na blankiet dowodu osobistego.

Klucze prywatne wszystkich urzędów i usług EDO przechowywane są w komponencie technicznym (module kryptograficznym).

6.2.1.Kontrola klucza prywatnego przez wiele osób

Klucze prywatne wszystkich Urzędów Certyfikacji są chronione przez podział klucza na części. Zarządzanie kluczami prywatnymi urzędów wymaga współpracy przynajmniej dwóch uprawnionych administratorów i wykorzystania co najmniej dwóch części klucza.

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 kluczem symetrycznym, który jest podzielony na sekrety współdzielone przechowywane w bezpiecznych lokalizacjach. Dostęp do zapasowych zestawów sekretów wymaga podwójnej kontroli.

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 modułu kryptograficznego

Klucz prywatny urzędu certyfikacji w postaci jawnej może być przetwarzany wyłącznie w module kryptograficznym. Transfer kluczy prywatnych urzędów CPD MSWiA do modułu kryptograficznego następuje w procedurze ładowania kluczy. Klucz w postaci jawnej nie jest transferowany poza moduł kryptograficzny.

Klucze prywatne Obywateli generowane są w module kryptograficznym 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 klucza prywatnego Obywatela wymaga obecności w urzędzie gminy gdzie kod aktywujący w sposób bezpieczny będzie automatycznie wprowadzony do komponentu technicznego. Kod PIN nadawany jest przez Obywatela w momencie obioru dowodu osobistego 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 modułu kryptograficznego 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
- 11 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 (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),
- kontrola dostępu zarówno w zakresie dostępu do pomieszczeń jak i poszczególnych elementów systemu login, hasło (np. imienne konta w systemie operacyjnym i aplikacjach),
- możliwość prowadzenia 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 obejmujące kwestie dotyczące bezpieczeństwa komputerów specyficzne dla działalności e-Dowodu. Zabezpieczenia są realizowane w aplikacjach, systemach operacyjnych, sieci teleinformatycznej oraz zabezpieczeniach fizycznych.

6.4.2.Poziom zabezpieczeń komputerów

Zabezpieczenia komputerów stosowane w infrastrukturze e-Dowodu spełniają wymagania stawiane systemom eksploatowanym w MSWiA.

6.4.3.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.

6.4.4.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 bezpiecznym konwojem do CPD MSWiA, gdzie składowane są w odpowiednio przygotowanym magazynie (kontrola dostępu oraz monitoring przemysłowy CCTV). Następnie blankiety z warstwą elektroniczną przekazywane są dyspozytorowi, który rozdziela je na produkcję. Po spersonalizowaniu graficznym oraz elektronicznym na hali personalizacyjnej która również jest chroniona poprzez monitoring przemysłowy CCTV oraz kontrolę dostępu, gotowe dowody osobiste trafiają na spedycję w celu spakowania oraz rozesłania ich Pocztą Specjalną do wnioskujących urzędów. gmin, Czynność ta wykonywana jest również pod nadzorem

kamer, dodatkowo proces przekazania dowodów Poczcie Specjalnej nadzorowany jest przez pracownika ochrony wewnętrznej budynku. Do urzędów gmin wysyłane są także, osobną przesyłką, w postaci bezpiecznej korespondencji kody PUK nadawane w procesie personalizacji dokumentu, w osobnym nie połączonym z halą personalizacyjną pomieszczeniu o równie restrykcyjnych zabezpieczeniach jak w przypadku hali personalizacyjnej. Wysyłane są do urzędów gmin osobną przesyłką, w zabezpieczonych kopertach, 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 Centrum Certyfikacji 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 Certyfikacji dowodu osobistego z warstwą elektroniczną certyfikaty zawierają następujące elektroniczne struktury danych:

1. Treść certyfikatu (**tbsCertificate**),
2. Informacja o algorytmie użytym do podpisania certyfikatu (**signatureAlgorithm**),
3. 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 EDO przedstawiono w tabeli:

Certyfikat dla 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	-
3	SignatureAlgorithm	informacja o algorytmie użytym do podpisania certyfikatu	1.2.840.10045.4.3.2 (SHA512 with ECDSA Encryption)
4	Issuer	identyfikator (nazwa DN) wydającego certyfikat	CN=PL.ID Root CA SN=<YYYY> gdzie <YYYY> oznacza rok wystawienia Centrum Autoryzacji C=PL
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	-
6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	**C - pole obowiązkowe:** Wartość PL **CN - pole obowiązkowe:** Nazwa powszechna urzędu**;** **O - pole obowiązkowe:** Nazwa organizacji **OU -pole obowiązkowe:** Jednostka organizacyjna **SN - pole obowiązkowe:** Data wystawienia urzędu certyfikacji w formacie <YYYYMMDD>

7	SubjectPublicKeyInfo	określenie algorytmu używanego przez posiadacza certyfikatu oraz jego klucz publiczny	-

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. OCSP -adres usługi OCSP

        ii. caIssuers - adres publikacji certyfikatów urzędów

1. Basic Constraints

    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	-
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> gdzie <YYYYMMDD> oznacza datę wystawienia Centrum Autoryzacji C=PL
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	-

6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	**C - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Obywatelstwo” **CN - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko**”;** **SURNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko” z rozdziału 3.1.2 Zawartość warstwy graficznej; **GIVENNAME – pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Imię pierwsze”;** **GIVENNAME – pole nie obowiązkowe: wartość na podstawie danych dotyczących osoby – Drugie imię”; SN - pole obowiązkowe:** numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „numer PESEL”. Zawartość warstwy graficznej. 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	-

Poniżej wskazano zakres i wartość pól rozszerzonych certyfikatów:

1. Rozszerzenie standardowe
    1. AuthorityKeyIdentifier

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

    2. SubjecKeyIdentifier

       Skrót klucza certyfikatu - rozszerzenie niekrytyczne

3. KeyUsage: digitalSignature

   Definiuje dozwolone użycie klucza - rozszerzenie krytyczne.

4. CertificatePolicies

   Rozszerzenie zawiera informację o polityce certyfikacji (identyfikator, adreselektroniczny) 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 Certyfikacji 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 zaawansowanego podpisu elektronicznego:

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	-
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> gdzie <YYYYMMDD> oznacza datę ustawienia Centrum Autoryzacji C=PL
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	-

6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	**C - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Obywatelstwo” **CN - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko**”;** **SURNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko” z rozdziału 3.1.2 Zawartość warstwy graficznej; **GIVENNAME – pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Imię pierwsze”;** **GIVENNAME – pole nie obowiązkowe: wartość na podstawie danych dotyczących osoby – Drugie imię”; SN - pole obowiązkowe:** numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „numer PESEL”. Zawartość warstwy graficznej. 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	-

Poniżej wskazano zakres i wartość pól rozszerzonych certyfikatów:

2. 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: 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 Certyfikacji 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

3. 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	-

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> gdzie <YYYYMMDD> oznacza datę ustawienia Centrum Autoryzacji C=PL
5	Validity	data ważności certyfikatu, określona jako data i czas początku okresu ważności certyfikatu (notBefore) oraz data i czas końca okresu ważności certyfikatu (notAfter)	-

6	Subject	identyfikator (nazwa DN) posiadacza certyfikatu	**C - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Obywatelstwo” **CN - pole obowiązkowe:** Jest to połączenie pól „Imię/Imiona” +„ ” + „Nazwisko**”;** **SURNAME - pole obowiązkowe:** wartość na podstawie danych dotyczących osoby - „Nazwisko” z rozdziału 3.1.2 Zawartość warstwy graficznej; **GIVENNAME – pole obowiązkowe: wartość na podstawie danych dotyczących osoby - „Imię pierwsze”;** **GIVENNAME – pole nie obowiązkowe: wartość na podstawie danych dotyczących osoby – Drugie imię”; SN - pole obowiązkowe:** numer PESEL, będzie zawierać wartość na podstawie danych dotyczących dowodu osobistego - „numer PESEL”. Zawartość warstwy graficznej. 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	-

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: 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 Certyfikacji 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

4. 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 odpowiedzi OCSP

W ramach EDO 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 zaawansowanego podpisu oraz certyfikat do potwierdzania obecności, jak też informacji o statusie certyfikatu każdego z urzędów wchodzących w skład infrastruktury Urzędu EDO. Zawartość i format odpowiedzi OCSP zgodny jest z zapisami normy RFC 6960.

Dla każdego Urzędu Certyfikacji wchodzącego w skład infrastruktury EDO tworzona jest w ramach usługi OCSP oddzielna para kluczy, podpisana 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.

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**)

7.2.1.Opis poszczególnych struktur przedstawiono poniżej

L.p.	Pole	Opis	Zawartość
1.	Version	wersja formatu usługi zgodna z RFC6990	V1
2.	Responder	identyfikator urzędu certyfikacji dostawcy usługi	--
3.	ProducedAt	Data/czas wygenerowania odpowiedzi	--
4.	Responses	lista aktualnych statusów certyfikatów, pojedynczy certyfikat opisany jest następującymi atrybutami: numer seryjny unieważnionego certyfikatu (certID), status certyfikatu (certStatus), data/czas, dla której zweryfikowano statusu (thisUpdate), data/czas następnej aktualizacji statusu	--
5.	ResponseExtensions	rozszerzona informacja o odpowiedzi OCSP	--

8. Audyt zgodności

8.1. Częstotliwość i okoliczności audytu

Działalność Centrum Certyfikacji podlega kontroli wewnętrznej i zewnętrznej.

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

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

8.4. Zakres kontroli/audytu

Kontrolą 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 certyfikacji,
- Zgodność realizacji działań z przyjętymi procedurami.

Kontrola realizowana jest zgodnie z przyjętą procedurą audytu.

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 ponownej kontroli.

8.6. Informowanie o wynikach audytu

Raport końcowy z przeprowadzonej kontroli nie podlega publikacji i jest uważany za dokument wewnętrzny Centrum Certyfikacji.

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

Wszyscy pracownicy CPD MSWiA, wykonujący zadania związane ze świadczeniem usług zaufania, są zobowiązani do zachowania poufności informacji. Obowiązek ochrony poufności informacji przez pracowników firm zewnętrznych, wykonujących zadania na rzecz CPD MSWiA, jest regulowany w umowach zawartych przez CPD MSWiA z tymi firmami.

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

1. sądom i prokuraturze w związku z toczącym się postępowaniem;
2. ministrowi właściwemu do spraw informatyzacji w związku ze sprawowaniem przez niego nadzoru nad działalnością dostawców usług zaufania;
3. 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 przekazywane Centrum Certyfikacji przez Subskrybentów Usług certyfikacyjnych 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 certyfikacji 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 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.

Poza tym ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. poz. 1579 oraz z 2018 r. poz. 650 z późn. zm.) przewiduje sankcje karne za posługiwanie się cudzym

środkiem identyfikacji elektronicznej, wydawanym w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, w celu uzyskania nieuprawnionego dostępu do usługi online, oraz za bezprawne kopiowanie lub przechowywanie nieprzyporządkowanych do niego danych pozwalających na identyfikowanie się z wykorzystaniem środka identyfikacji elektronicznej, wydawanym w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego, oraz za wydawanie środka identyfikacji elektronicznej w systemie identyfikacji elektronicznej przyłączonym do węzła krajowego osobie nieuprawnionej.

9.7. Okres obowiązywania i wypowiedzenie

Niniejsza Polityka świadczenia usług dla dowodu osobistego z warstwą elektroniczną obowiązuje od momentu nadania mu statusu aktualny i opublikowania go w repozytorium CPD MSWiA.

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

W momencie wygaśnięcia ważności bieżącego dokumentu użytkownicy certyfikatów wydanych w okresie jego obowiązywania są dalej ograniczeni zapisami niniejszego dokumentu aż do momentu utraty ważności certyfikatu.

9.8. Powiadamianie

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

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.