Dokumentacja Centrum Certyfikacji Ministerstwa Cyfryzacji

Tytuł dokumentu: Polityka świadczenia usług dla certyfikatów użytkowników aplikacji mObywatel

Wersja: 0.4

Data wersji: 2023-07-06

Data ostatniej aktualizacji:

Imię i nazwisko	Stanowisko	Wersja dokumentu	Podpis
Sporządził	Główny architekt	0.4	n/d
Zatwierdził	Dyrektor	0.4	

1. Wstęp

1.1. Wprowadzenie

Dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji Ministerstwa Cyfryzacji (CC MC). Odpowiada ono za szereg polityk certyfikacji, a dla każdej z tych polityk jest określony tzw. podsystem certyfikacji. W ramach każdego podsystemu certyfikacji obowiązują określone dla danej polityki certyfikacji procedury i zasady oraz profile nazw i certyfikatów. CC MC generuje pary kluczy kryptograficznych dla każdego podsystemu certyfikacji, które służą do zapewnienia integralności i autentyczności zaświadczeń certyfikacyjnych, list unieważnionych certyfikatów, certyfikatów kluczy infrastruktury i certyfikatów Subskrybentów. Niniejsza polityka certyfikacji odnosi się do podsystemu certyfikacji, w którym generowane i wydawane certyfikaty, klucze dla systemów teleinformatycznych oraz certyfikaty dla użytkowników aplikacji mObywatel. To osoby fizyczne, które mogą korzystać z aplikacji mObywatel po wcześniejszym ustaleniu tożsamości w sposób określony w ustawie o aplikacji mObywatel. Dokument zawiera również uregulowania szczegółowe w zakresie objętym polityką certyfikacji, pełni zatem jednocześnie rolę dokumentu Certificate Practice Statement w rozumieniu RFC 3647[1] Struktura dokumentu została oparta na dokumencie RFC 3647. W rozdziale 1.6 zamieszczono słownik pojęć stosowanych w dokumencie.

1.2. Identyfikator polityki certyfikacji

Poniższa tabela przedstawia dane identyfikacyjne Polityki świadczenia usług dla certyfikatów użytkowników aplikacji mObywatel wraz z jej identyfikatorem OID, zgodnym z ASN.1.

Nazwa polityki	Polityka świadczenia usług dla certyfikatów użytkowników aplikacji mObywatel
Kwalifikator polityki	Brak
Wersja polityki	1.0
Numer OID (ang. Object Identifier)	0.4.0.2042.1.3
Data zatwierdzenia	
Data ważności	Do odwołania

[1] Chokhani, S., Ford, W., Sabett, R., Merrill, C., and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, DOI 10.17487/RFC3647, November 2003, <https://www.rfc-editor.org/info/rfc3647>.

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

Niniejsza polityka certyfikacji realizowana jest przez CC MC, które w ramach swoich obowiązków świadczy usługi certyfikacyjne dla podmiotów, użytkowników aplikacji mObywatel. Subskrybentami usług certyfikacyjnych realizowanych zgodnie z tą polityką certyfikacji są użytkownicy aplikacji mObywatel oraz podmioty świadczące usługi zintegrowane z systemem mObywatel.

1.4. Zakres zastosowań

Opisana polityka dotyczy podsystemu certyfikacji, w którym są wydawane certyfikaty niekwalifikowane, oparte na modelu Infrastruktury Klucza Publicznego (PKI) dla użytkowników aplikacji mObywatel oraz podmiotów publicznych i niepublicznych zintegrowanych z systemem mObywatel. Klucze prywatne związane z certyfikatami generowanymi zgodnie z tą polityką mogą być wykorzystane do potwierdzenia tożsamości użytkownika lub poświadczenia atrybutów użytkownika instytucji/osobie weryfikującej.

1.5. Administracja polityką certyfikacji

Polityka certyfikacji została opracowana na potrzeby systemu mObywatel. Wszelkie zmiany w tej polityce wymagają zatwierdzenia przez Gestora systemu CC MC. Obowiązująca wersja polityki jest dostępna na stronie BIP MC. O ile Gestor systemu nie postanowi inaczej, wszystkie certyfikaty wystawione w okresie obowiązywania wcześniejszej wersji polityki i nadal ważne w chwili zatwierdzenia nowej wersji, zachowują swoją ważność i podlegają postanowieniom tej wersji polityki certyfikacji zgodnie, z którą zostały wystawione. Wszelkie zmiany niniejszej polityki certyfikacji, z wyjątkiem takich, które dotyczą oczywistych błędów redakcyjnych lub stylistycznych oraz informacji teleadresowych, wymagają zatwierdzenia przez Gestora systemu.

1.5.1 Punkty kontaktowe

Adres:

Centralny Ośrodek Informatyki
Aleje Jerozolimskie 132-136
02-305 Warszawa

Telefon: +48 42 253 54 74

Email: mObywatel-pomoc@coi.gov.pl

1.6. Słownik terminów i pojęć

	Pojęcia lub skrót	Znaczenie
1	**aplikacja mObywatel**	Aplikacja mObywatel, o której mowa w ustawie z dnia 26 maja 2023 r. o aplikacji mObywatel, zwanej dalej „ustawą o aplikacji mObywatel". Warunki udostępniania oraz zapewniania rozwoju oprogramowania aplikacji określają przepisy ww. ustawy oraz Regulamin korzystania z aplikacji mObywatel. Aplikacja mObywatel przeznaczona dla osób fizycznych i jest dostepna w sklepach Google Play oraz App Store. Element front-end'u systemu mObywatel.
2	**profil mObywatel**	Środek identyfikacji elektronicznej, o którym mowa w art. 3 pkt 2 rozporządzenia Parlamentu Europejskiego i Rady (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 oraz uchylającego dyrektywę 1999/93/WE, obsługiwany w aplikacji mObywatel. Identyfikacja działa z wykorzystaniem certyfikatu podstawowego Obywatela, przechowywanym w szyfrowanym kontenerze aplikacji mObywatel.
3	**System CC MC**	System certyfikacji prowadzony w Ministerstwie Cyfryzacji, w ramach którego są świadczone usługi certyfikacyjne dla użytkowników aplikacji mObywatel oraz podmiotów świadczących usługi w aplikacji mObywatel. System CC MC składa się z podsystemów certyfikacji realizujących odrębne polityki i posługujących się odrębnymi kluczami do generowania certyfikatów i list CRL
4	**certyfikat**	Elektroniczne zaświadczenie, za pomocą którego klucz publiczny jest przyporządkowany do Subskrybenta; umożliwia jego jednoznaczną identyfikację
5	**DN**	Identyfikator wyróżniający (ang. Distinguished Name) zgodny z zaleceniami zdefiniowanymi w ITU z serii X.500. Jednoznacznie identyfikuje on Subskrybenta usług certyfikacyjnych
6	**Gestor systemu**	Gestor (właściciel) oznacza kierownika komórki organizacyjnej w Ministerstwie Cyfryzacji, wskazanej w Regulaminie Organizacyjnym do realizacji spraw związanych z nadzorem, kontrolą i eksploatacją Centrum Certyfikacji MC. Gestor (właściciel) ponosi odpowiedzialność kierowniczą przed Ministrem Cyfryzacji za nadzór nad eksploatacją, rozwojem, utrzymaniem, bezpieczeństwem i dostępem do systemu.
7	**HSM**	Sprzętowy moduł kryptograficzny, który realizuje operacje z użyciem kluczy prywatnych
8	**ITU**	Międzynarodowy Związek Telekomunikacyjny

	Pojęcia lub skrót	Znaczenie
9	**Operator Punktu Rejestracji**	Osoba upoważniona do pracy w PR, odpowiedzialna za: obsługę wniosków certyfikacyjnych, wydawanie certyfikatów dla Subskrybentów, unieważnianie certyfikatów
10	**LDAP**	Baza danych przechowująca informacje o subskrybentach dostępna za pomocą protokołu LDAP (Lightweight Directory Access Protocol) – protokół przeznaczony do korzystania z usług katalogowych, bazujący na standardzie X.500
11	**Lista CRL**	Lista zawieszonych i unieważnionych certyfikatów i zaświadczeń certyfikacyjnych
12	**PR**	Punkt Rejestracji Centrum Certyfikacji MC
13	**Subskrybent**	Podmiot lub osoba, dla których wystawiany jest certyfikat w ramach systemu certyfikacji
14	**Zaświadczenie certyfikacyjne**	Elektroniczne zaświadczenie, za pomocą którego dane do weryfikacji certyfikatu są przyporządkowane do podsystemu certyfikacji
15	**X.500**	Zbiór standardów stworzonych przez ITU

2. Zasady dystrybucji i publikacji informacji

2.1. Repozytorium

W ramach podsystemu certyfikacji działają repozytorium certyfikatów oraz usługa OCSP. Są one dostępne za pośrednictwem protokołu HTTP(S) w formie usługi zarządzania oraz OCSP. Publicznie dostępna jest wyłącznie usługa OCSP.

2.2. Częstotliwość publikacji informacji

Informacja o unieważnionych certyfikatach jest dostępna poprzez protokół OCSP niezwłocznie. Treść aktualnej wersji polityki certyfikacji z zaznaczeniem okresu jej obowiązywania publikowana jest na stronie internetowej BIP Ministra Cyfryzacji, w sekcji poświęconej aplikacji mObywatel. Nowe wersje polityki certyfikacji publikowane są niezwłocznie po ich zatwierdzeniu przez Gestora systemu.

3. Identyfikacja i uwierzytelnienie

3.1. Struktura nazw przydzielanych Subskrybentom

Zawartość certyfikatu jednoznacznie identyfikuje Subskrybenta usług certyfikacyjnych przy użyciu identyfikatora wyróżniającego DN zgodnego z zaleceniami zdefiniowanymi w ITU z serii X.500.

Centrum certyfikacji obsługuje 5 typów subskrybentów:

3.1.1. Certyfikat podstawowy Obywatela, tj. certyfikat podstawowy, o którym mowa w art. 10 ustawy o aplikacji mObywatel

Pole	Opis		Wartość/maska
Version Number	Wersja certyfikatu		v3 (definiowane przez liczbę całkowitą 2)
Serial Number	Unikalny numer seryjny dla każdego certyfikatu wystawionego przez system mDokumenty (zgodnie z 4.1.2.2. RFC 5280 https://www.ietf.org/rfc/rfc5280.txt)		Unikalny numer seryjny
Signature Algorithm	Algorytm podpisu		SHA256 RSA (1.2.840.113549.1.1.11)
Subject	Pole podmiot składające się z poniższych atrybutów :		
	countryName (OID value: 2.5.4.6)	Kraj (*ang. Country*)	PL
	serialNumber (OID value: 2.5.4.5)	Numer identyfikujący Obywatela zgodnie z normą ETSI EN 319 412-1 V1.1.1 (2016-02)	PNOPL-XXXXXXXXXXX gdzie : XXXXXXXXXXX odpowiada numerowi PESEL Obywatela.
	sn (OID value: 2.5.4.4)	Nazwisko Obywatela	Nazwisko Obywatela
	givenName (OID value: 2.5.4.42)	Imiona Obywatela	Imiona Obywatela
	cn (OID value: 2.5.4.3)	Identyfikacja obiektu zgodnie z rekomendacją ITU-T X.520 6.2.2	cn=givenName+" "+sn
Authority Information Access	Dostęp do informacji o urzędach (AIA) to rozszerzenie certyfikatu X.509 v3 zgodnie z RFC5280. Rozszerzenie wskazuje, w jaki sposób uzyskać dostęp do informacji i usług dla wystawcy certyfikatu, w którym pojawia się rozszerzenie. Zawiera co najwyżej dwa rodzaje informacji: – Informacje o tym, jak pozyskać informację o wystawcy tego certyfikatu (*ang. CA issuer access method*) – Adres dla protokołu OCSP, gdzie można sprawdzić odwołanie		Adres pod którym można pozyskać klucz publiczny wystawcy. Adres usługi OCSP. Przykładowo : Method = OCSP URI = https://mobywatel.gov.pl/ocsp Method = Certification Authority Issuer URI = https://mobywatel.gov.pl/MTmid_2.cer

	certyfikatu (*ang. OCSP access method*)	
X509v3 Certificate Policies	Identyfikator OID polityki certyfikacji oraz informacja dla użytkownika o miejscu publikacji niniejszej polityki certyfikacji.	Policy: 0.4.0.2042.1.3 CPS: https://mobywatel.gov.pl/polityka

Przykładowa struktura pola Subject:

c=PL,
serialNumber=PNOPL-00021995693,
sn=Kozłowski,
givename=Jan Maria,
cn=Jan Maria Kozłowski

Certyfikat podstawowy Obywatela posiada parametry :

- algorytm kryptograficzny: RSA
- długość klucza: 2048 bitów
- czas ważności certyfikatu: 1 rok

3.1.2. Certyfikat Studenta, o którym mowa w art. 12 ustawy o aplikacji mObywatel

Pole	Opis		Wartość/maska
Version Number	Wersja certyfikatu		v3 (definiowane przez liczbę całkowitą 2)
Serial Number	Unikalny numer seryjny dla każdego certyfikatu wystawionego przez system mDokumenty (zgodnie z 4.1.2.2. RFC 5280 https://www.ietf.org/rfc/rfc5280.txt)		Unikalny numer seryjny
Signature Algorithm	Algorytm podpisu		SHA256 RSA (1.2.840.113549.1.1.11)
Subject	Pole podmiot składające się z poniższych atrybutów :		
	countryName (OID value: 2.5.4.6)	Kraj (*ang. Country*)	PL
	localityName (OID value: 2.5.4.7)	Lokalizacja (*ang. Locality Name*)	Lokalizacja siedziby Uczelni (*np. Warszawa*)
	organizationIdentifier (OID value: 2.5.4.97)	Numer identyfikujący Uczelnie zgodnie z normą ETSI EN 319 412-1 V1.1.1 (2016-02) oraz rekomendacj	BR:PL-*XXXXXXXXX* gdzie : *XXXXXXXXX* odpowiada numerowi REGON Instytucji, dla REGON 9 znakowego, lub BR:PL-*XXXXXXXXXXXXXX* gdzie : *XXXXXXXXXXXXXX* odpowiada numerowi REGON Instytucji, dla REGON 14 znakowego

		ą ITU-T X.520 6.4.4	
	organizationName (OID value: 2.5.4.10)	Pełna nazwa Uczelni zgodnie z rekomendacją ITU-T X.520 6.4.1	Pełna nazwa Uczelni
	organizationalUnitName (OID value: 2.5.4.11)	Nazwa jednostki Uczelni zgodnie z rekomendacją ITU-T X.520 6.4.2	Nazwa jednostki Uczelni (pole opcjonalne)
	serialNumber (OID value: 2.5.4.5)	Numer identyfikujący Studenta zgodnie z normą ETSI EN 319 412-1 V1.1.1 (2016-02)	PNOPL-*XXXXXXXXXXX* gdzie : *XXXXXXXXXXX* odpowiada numerowi PESEL Studenta
	serialNumber (OID value: 2.5.4.5)	Numer identyfikujący legitymację Studenta	SC:PL-*NumerLegitymacji* gdzie : *NumerLegitymacji* odpowiada numerowi legitymacji nadanej przez Uczelnię
	sn (OID value: 2.5.4.4)	Nazwisko Studenta	Nazwisko Studenta
	givenName (OID value: 2.5.4.42)	Imiona Studenta	Imiona Studenta
	cn (OID value: 2.5.4.3)	Identyfikacja obiektu zgodnie z rekomendacją ITU-T X.520 6.2.2	cn=givenName+" "+sn
Authority Information Access	Dostęp do informacji o urzędach (AIA) to rozszerzenie certyfikatu X.509 v3 zgodnie z RFC5280. Rozszerzenie wskazuje, w jaki sposób uzyskać dostęp do informacji i usług dla wystawcy certyfikatu, w którym pojawia się rozszerzenie. Zawiera co najwyżej dwa rodzaje informacji: – Informacje o tym, jak pozyskać informację o wystawcy tego certyfikatu (*ang. CA issuer access method*)		Adres pod którym można pozyskać klucz publiczny wystawcy. Adres usługi OCSP. Przykładowo : Method = OCSP URI = https://mobywatel.gov.pl/ocsp Method = Certification Authority Issuer URI = https://mobywatel.gov.pl/MTmid_2.cer

	– Adres dla protokołu OCSP, gdzie można sprawdzić odwołanie certyfikatu (*ang. OCSP access method*)	
X509v3 Certificate Policies	Identyfikator OID polityki certyfikacji oraz informacja dla użytkownika o miejscu publikacji niniejszej polityki certyfikacji.	Policy: 0.4.0.2042.1.3 CPS: https://mobywatel.gov.pl/polityka

Przykładowa struktura pola Subject:

c=PL,
l=Warszawa,
organizationIdentifier=BR:PL-000001258,
O=Uniwersytet Warszawski,
serialNumber=PNOPL-00021995693,
serialNumber=SC:PL-124567686,
sn=Kozłowski,
givename=Jan Maria,
cn=Jan Maria Kozłowski

Certyfikat roboczy Studenta posiada parametry :

- algorytm kryptograficzny RSA
- długość klucza 2048 bitów
- czas ważności certyfikatu zgodny z czasem ważności semestru (maksymalnie 14 miesięcy)

3.1.3. Certyfikat Ucznia, o którym mowa w art. 11 ustawy o aplikacji mObywatel

Pole	Opis		Wartość/maska
Version Number	Wersja certyfikatu		v3 (definiowane przez liczbę całkowitą 2)
Serial Number	Unikalny numer seryjny dla każdego certyfikatu wystawionego przez system mDokumenty (zgodnie z 4.1.2.2. RFC 5280 *https://www.ietf.org/rfc/rfc5280.txt*)		Unikalny numer seryjny
Signature Algorithm	Algorytm podpisu		SHA256 RSA (1.2.840.113549.1.1.11)
Subject	Pole podmiot składające się z poniższych atrybutów :		
	countryName (OID value: 2.5.4.6)	Kraj (*ang. Country*)	PL
	localityName (OID value: 2.5.4.7)	Lokalizacja (*ang. Locality Name*)	Lokalizacja siedziby szkoły (*np. Warszawa*)

	organizationIdentifier (OID value: 2.5.4.97)	Numer identyfikujący szkołę zgodnie z normą ETSI EN 319 412-1 V1.1.1 (2016-02) oraz rekomendacją ITU-T X.520 6.4.4	RS:PL-*NumerRSPO* gdzie : *NumerRSPO* odpowiada numerowi RSPO nadanemu szkole zgodnie Ustawą z dnia 15 kwietnia 2011 r. o systemie informacji oświatowej
	organizationName (OID value: 2.5.4.10)	Pełna nazwa Szkoły zgodnie z rekomendacją ITU-T X.520 6.4.1	Pełna nazwa Szkoły
	organizationalUnitName (OID value: 2.5.4.11)	Nazwa jednostki Szkoły zgodnie z rekomendacją ITU-T X.520 6.4.2	Nazwa jednostki Szkoły (pole opcjonalne)
	serialNumber (OID value: 2.5.4.5)	Numer identyfikujący Ucznia zgodnie z normą ETSI EN 319 412-1 V1.1.1 (2016-02)	PNOPL-*XXXXXXXXXXX* gdzie : *XXXXXXXXXXX* odpowiada numerowi PESEL Ucznia
	serialNumber (OID value: 2.5.4.5)	Numer identyfikujący legitymację Ucznia	SI:PL-*NumerLegitymacji* gdzie : *NumerLegitymacji* odpowiada numerowi legitymacji nadanej przez Szkołę
	Sn	Nazwisko Ucznia	Nazwisko Ucznia
	givenName	Imiona Ucznia	Imiona Ucznia
	Cn	Identyfikacja obiektu zgodnie z rekomendacją ITU-T X.520 6.2.2	cn=givenName+" "+sn
Authority Information Access	Dostęp do informacji o urzędach (AIA) to rozszerzenie certyfikatu X.509 v3 zgodnie z RFC5280. Rozszerzenie wskazuje, w jaki sposób uzyskać dostęp do informacji i usług dla wystawcy		Adres pod którym można pozyskać klucz publiczny wystawcy. Adres usługi OCSP. Przykładowo : Method = OCSP

	certyfikatu, w którym pojawia się rozszerzenie. Zawiera co najwyżej dwa rodzaje informacji: – Informacje o tym, jak pozyskać informację o wystawcy tego certyfikatu (*ang. CA issuer access method*) – Adres dla protokołu OCSP, gdzie można sprawdzić odwołanie certyfikatu (*ang. OCSP access method*)	URI = https://mobywatel.gov.pl/ocsp Method = Certification Authority Issuer URI = https://mobywatel.gov.pl/MTmid_2.cer
X509v3 Certificate Policies	Identyfikator OID polityki certyfikacji oraz informacja dla użytkownika o miejscu publikacji niniejszej polityki certyfikacji.	Policy: 0.4.0.2042.1.3 CPS: https://mobywatel.gov.pl/polityka

Przykładowa struktura pola Subject:

c=PL,
l=Grodzisk Mazowiecki,
organizationIdentifier=RS:PL-6164,
O=SZKOŁA PODSTAWOWA NR 2 IM. M. KONOPNICKIEJ,
serialNumber=PNOPL-00021995693,
serialNumber=SI:PL-4567686,
sn=Kozłowski,
givename=Jan Maria,
cn=Jan Maria Kozłowski

Certyfikat roboczy Ucznia posiada parametry :

- algorytm kryptograficzny: RSA
- długość klucza: 2048 bitów
- czas ważności certyfikatu: zgodny z okresem roku szkolnego lub semestru, w którym jest wydawana, związana z tym certyfikatem, legitymacja szkolna w postaci dokumentu mobilnego (maksymalnie 14 miesięcy).

3.1.4. Certyfikaty Instytucji, tj. podmiotu publicznego lub niepublicznego, o którym mowa w ustawie o aplikacji mObywatel

Certyfikaty wydawane Instytucjom mają postać :

<table>
<tr><th>Pole</th><th colspan="2">Opis</th><th>Wartość/maska</th></tr>
<tr><td>Version Number</td><td colspan="2">Wersja certyfikatu</td><td>v3
(definiowane przez liczbę całkowitą 2)</td></tr>
<tr><td>Serial Number</td><td colspan="2">Unikalny numer seryjny dla każdego certyfikatu wystawionego przez system mObywatel (zgodnie z 4.1.2.2. RFC 5280 https://www.ietf.org/rfc/rfc5280.txt)</td><td>Unikalny numer seryjny</td></tr>
<tr><td>Signature Algorithm</td><td colspan="2">Algorytm podpisu</td><td>SHA256 RSA (1.2.840.113549.1.1.11)</td></tr>
<tr><td rowspan="6">Subject</td><td colspan="3">Pole podmiot składające się z poniższych atrybutów :</td></tr>
<tr><td>countryName
(OID value: 2.5.4.6)</td><td>Kraj (ang. Country)</td><td>PL</td></tr>
<tr><td>organizationIdentifier
(OID value: 2.5.4.97)</td><td>Numer identyfikujący Instytucję zgodnie z normą ETSI EN 319 412-1 V1.1.1 (2016-02) oraz rekomendacją ITU-T X.520 6.4.4</td><td>BR:PL-XXXXXXXXX
gdzie : XXXXXXXXX odpowiada numerowi REGON Instytucji, dla REGON 9 znakowego, lub
BR:PL-XXXXXXXXXXXXXX
gdzie : XXXXXXXXXXXXXX odpowiada numerowi REGON Instytucji, dla REGON 14 znakowego</td></tr>
<tr><td>organizationName
(OID value: 2.5.4.10)</td><td>Pełna nazwa Instytucji zgodnie z rekomendacją ITU-T X.520 6.4.1</td><td>Pełna nazwa Instytucji</td></tr>
<tr><td>organizationalUnitName
(OID value: 2.5.4.11)</td><td>Nazwa jednostki Instytucji zgodnie z rekomendacją ITU-T X.520 6.4.2</td><td>Nazwa jednostki Instytucji
(pole opcjonalne)</td></tr>
<tr><td>commonName
(OID value: 2.5.4.3)</td><td>Identyfikacja obiektu zgodnie z rekomendacją ITU-T X.520 6.2.2</td><td>Zwyczajowa nazwa Instytucji</td></tr>
<tr><td>businessCategory
(OID value: 2.5.4.15)</td><td>Typ organizacji zgodnie z rekomendacj</td><td>Typ organizacji, przyjmujący wartości słownikowe:<table><tr><th>Wartość</th><th>Opis</th></tr></table></td></tr>
</table>

<table>
<tr><td></td><td></td><td>ą ITU-T X.520 6.5.4</td><td><table><tr><td>I</td><td>Instytucja</td></tr><tr><td>G</td><td>Instytucje publiczne</td></tr><tr><td>S</td><td>Szkoła</td></tr><tr><td>U</td><td>Uczelnia</td></tr></table></td></tr>
<tr><td>Authority Information Access</td><td>Dostęp do informacji o urzędach (AIA) to rozszerzenie certyfikatu X.509 v3 zgodnie z RFC5280. Rozszerzenie wskazuje, w jaki sposób uzyskać dostęp do informacji i usług dla wystawcy certyfikatu, w którym pojawia się rozszerzenie. Zawiera co najwyżej dwa rodzaje informacji:
– Informacje o tym, jak pozyskać informację o wystawcy tego certyfikatu (ang. CA issuer access method)
– Adres dla protokołu OCSP, gdzie można sprawdzić odwołanie certyfikatu (ang. OCSP access method)</td><td>Adres pod którym można pozyskać klucz publiczny wystawcy.
Adres usługi OCSP.
Przykładowo :
Method = OCSP
URI = https://mobywatel.gov.pl/ocsp
Method = Certification Authority Issuer
URI = https://mobywatel.gov.pl/MTmid_2.cer</td></tr>
<tr><td>X509v3 Certificate Policies</td><td>Identyfikator OID polityki certyfikacji oraz informacja dla użytkownika o miejscu publikacji niniejszej polityki certyfikacji.</td><td>Policy: 0.4.0.2042.1.3
CPS: https://mobywatel.gov.pl/polityka</td></tr>
</table>

Przykładowa struktura pola Subject:

c=PL,
organizationIdentifier=BR:PL-012261725,
O=Kancelaria Prezesa Rady Ministrów,
OU=Departament Zarządzania Systemami,
cn=Kancelaria Prezesa Rady Ministrów,
businessCategory=G

lub

c=PL,
organizationIdentifier=BR:PL-012261725,
O=Kancelaria Prezesa Rady Ministrów,
cn=Kancelaria Prezesa Rady Ministrów,
businessCategory=G

3.1.5. Certyfikat Diia.pl, o którym mowa w art. 10 ustawy z dnia 12 marca 2022 r. o pomocy obywatelom Ukrainy w związku z konfliktem zbrojnym na terytorium tego państwa

Pole	Opis		Wartość/maska
Version Number	Wersja certyfikatu		v3 (definiowane przez liczbę całkowitą 2)
Serial Number	Unikalny numer seryjny dla każdego certyfikatu wystawionego przez system mDokumenty (zgodnie z 4.1.2.2. RFC 5280 https://www.ietf.org/rfc/rfc5280.txt)		Unikalny numer seryjny
Signature Algorithm	Algorytm podpisu		SHA256 RSA (1.2.840.113549.1.1.11)
Subject	Pole podmiot składające się z poniższych atrybutów :		
	countryName (OID value: 2.5.4.6)	Kraj (*ang. Country*)	Kod kraju zgodny z normą ISO 3166-1 alfa-2 zależny od kodu obywatelstwa przekazanego przez interfejs rejestru PESEL w atrybucie obywatelstwo@kod
	serialNumber (OID value: 2.5.4.5)	Numer identyfikujący Obywatela zgodnie z normą ETSI EN 319 412-1 V1.1.1 (2016-02)	PNOPL-XXXXXXXXXXX gdzie : XXXXXXXXXXX odpowiada numerowi PESEL Obywatela.
	Sn (OID value: 2.5.4.4)	Nazwisko Obywatela	Nazwisko Obywatela
	givenName (OID value: 2.5.4.42)	Imiona Obywatela	Imiona Obywatela
	Cn (OID value: 2.5.4.3)	Identyfikacja obiektu zgodnie z rekomendacją ITU-T X.520 6.2.2	cn=givenName+" "+sn
Authority Information Access	Dostęp do informacji o urzędach (AIA) to rozszerzenie certyfikatu X.509 v3 zgodnie z RFC5280. Rozszerzenie wskazuje, w jaki sposób uzyskać dostęp do informacji i usług dla wystawcy certyfikatu, w którym pojawia się rozszerzenie. Zawiera co najwyżej dwa rodzaje informacji: Informacje o tym, jak pozyskać informację o wystawcy tego certyfikatu (*ang. CA issuer access method*) Adres dla protokołu OCSP, gdzie można sprawdzić odwołanie certyfikatu (*ang. OCSP access method*)		Adres pod którym można pozyskać klucz publiczny wystawcy. Adres usługi OCSP. Przykładowo : Method = OCSP URI = https://mobywatel.gov.pl/ocsp Method = Certification Authority Issuer URI = https://mobywatel.gov.pl/MTmid_2.cer

X509v3 Certificate Policies	Identyfikator OID polityki certyfikacji oraz informacja dla użytkownika o miejscu publikacji niniejszej polityki certyfikacji.	Policy: 0.4.0.2042.1.3 CPS: https://mobywatel.gov.pl/polityka

Przykładowa struktura pola Subject:

c=UA,
serialNumber=PNOPL-00021995693,
sn=Kozłowski,
givename=Jan Maria,
cn=Jan Maria Kozłowski

Certyfikat roboczy diia.pl posiada parametry :

algorytm kryptograficzny: RSA

długość klucza: 2048 bitów

czas ważności certyfikatu: 1 rok

3.2. Rejestracja i uwierzytelnienie Subskrybenta

3.2.1. Sposoby uwierzytelnienia

Certyfikat podstawowy Obywatela jest wydawany wraz z wydaniem dokumentu mObywatel, o którym mowa w ustawy o aplikacji mObywatel (funkcjonującego pod biznesową nazwa mDowód) w systemie mObywatela. Potwierdzenie tożsamości użytkownika odbywa się w oparciu o krajowy schemat identyfikacji z wykorzystaniem środka identyfikacji elektronicznej na poziomie co najmniej średnim. Alternatywnie Obywatel będzie miał możliwość uzyskania certyfikatu profilu mObywatel, gdy potwierdzi swoją tożsamość za pomocą innego dokumentu tożsamości w Urzędzie Gminy.

Uchodźca może uzyskać certyfikat Diia.pl jeśli potwierdzi swoją tożsamość w oparciu o krajowy schemat identyfikacji i użyje środka identyfikacji elektronicznej na poziomie co najmniej średnim.

Certyfikat Ucznia i certyfikat Studenta wydawany jest po potwierdzeniu tożsamości przez szkołę lub uczelnię, w której osoba posiada status studenta lub ucznia.

Certyfikat instytucji wydawany jest podmiotom, które podpisały porozumienie lub spełniły warunki określone w ogólnych warunkach świadczenia (OWU), o których mowa w art. 15 ustawy o aplikacji mObywatel i spełniły wszystkie wymagania dotyczące integracji z systemem mObywatel. Weryfikacja podmiotu odbywa się na podstawie procedur manualnych.

3.2.2. Sposoby udowodnienia posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu zawartemu w certyfikacie

Klucz prywatny Subskrybenta jest generowany w momencie wydawania certyfikatu.

3.3. Sposoby uwierzytelnienia Subskrybenta przy wystawianiu kolejnych certyfikatów

Przed upływem ważności certyfikatu podstawowego Obywatela lub Diia.pl Subskrybent ma możliwość wymiany certyfikatu na nowy (o dłuższym okresie ważności) z wykorzystaniem

uwierzytelnienia za pomocą aktualnego certyfikatu. Po upływie ważności niezbędne jest ponowne potwierdzenie tożsamości stosując metody wymienione w rozdziale 3.2.1.

Odnowienie certyfikatów Studenta, Ucznia oraz Instytucji przebiega tak samo jak proces ich uzyskania za pierwszym razem opisany w rozdziale 3.2.1.

3.4. Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia certyfikatu

Certyfikat użytkownika aplikacji mObywatel unieważniany jest:

- przez posiadacza za pomocą przeznaczonej do tego funkcjonalności w aplikacji mObywatel,

- w przyszłości poprzez usługę webową po potwierdzeniu tożsamości użytkownika przy użyciu środka identyfikacji elektronicznej na poziomie co najmniej średnim, przyłączonego do węzła krajowej identyfikacji elektronicznej,

- Obywatel ma też możliwość unieważnienia certyfikatu, gdy potwierdzi swoją tożsamość poprzez kontakt telefoniczny z infolinią.

Uchodźca ma możliwość unieważnienia certyfikatu Diia.pl:

- za pomocą przeznaczonej do tego funkcjonalności w aplikacji mObywatel,

- gdy potwierdzi swoją tożsamość poprzez kontakt telefoniczny z infolinią.

Certyfikaty Studenta i Ucznia mogą zostać unieważnione przez uczelnie lub szkołę, która wydała związany z tym certyfikatem dokument elektroniczny – mLegitymację szkolną lub mLegitymację studencką.

Certyfikaty Instytucji są unieważniane na wniosek podmiotu. Weryfikacja podmiotu odbywa się w oparciu o procedury manualne.

Zgodnie z art. 13 ust. 1 ustawy o aplikacji mObywatel, w przypadku uzasadnionego podejrzenia naruszenia bezpieczeństwa certyfikatu użytkownika aplikacji mObywatel, odpowiednio do rodzaju podejrzewanego naruszenia, Minister Cyfryzacji unieważnia certyfikaty, których dotyczy podejrzewane naruszenie, oraz zawiesza świadczenie usług związanych z wykorzystaniem tych certyfikatów do czasu przywrócenia stanu bezpieczeństwa tych certyfikatów. Ponadto zgodnie z art. 13 ust. 2 ustawy o aplikacji mObywatel Minister Cyfryzacji ogłasza niezwłocznie, w drodze obwieszczenia, w Dzienniku Urzędowym Rzeczypospolitej Polskiej „Monitor Polski" informacje odpowiednio o unieważnieniu certyfikatów użytkowników aplikacji mObywatel i zawieszeniu oraz przywróceniu świadczenia usług związanych z tymi certyfikatami.

4. Cykl życia certyfikatu – wymagania operacyjne

4.1. Wniosek

Certyfikaty: podstawowy Obywatela, Studenta, Ucznia i Diia.pl wydawane są w sposób automatyczny do aplikacji mObywatel po wcześniejszym potwierdzeniu tożsamości (zgodnie z rozdziałem 3.2.1).

4.2. Przetwarzanie wniosków

Wniosek jest weryfikowany przez podsystem certyfikacji pod kątem poprawności i zgodności z wymaganiami określonymi w niniejszej polityce oraz zgodności danych przekazanych w treści wniosku ze stanem faktycznym.

Niniejsza polityka nakłada ograniczenie posiadania maksymalnie jednego aktywnego certyfikatu użytkownika aplikacji mObywatel danego rodzaju w tym samym momencie. Jednakże dopuszcza posiadanie jednocześnie certyfikaty podstawowy Obywatela, Ucznia, Studenta jeśli spełnione są warunki niezbędne do wydania dokumentu elektronicznego związane z danym certyfikatem użytkownika aplikacji mObywatel. W związku z tym podsystem certyfikacji w sposób automatyczny po złożonym nowym wniosku unieważnia istniejący aktywny certyfikat.

4.3. Wystawienie certyfikatu

Po stwierdzeniu poprawności wniosku podsystem w sposób automatyczny tworzy i wydaje żądany certyfikat, który następnie przekazywany jest do urządzenia końcowego/Subskrybenta w formie zaszyfrowanej.

W przypadku certyfikatów Ucznia i Studenta to szkoła lub uczelnia inicjuje proces wydania certyfikatu. Certyfikat Ucznia lub Studenta może zostać utworzony i pobrany tylko w ograniczonym przedziale czasowym od momentu zgłoszenia przez szkołę lub uczelnię.

4.4. Akceptacja certyfikatu

Certyfikaty, do których nie zgłoszono zastrzeżeń, uznaje się za dostarczone do Subskrybenta.

4.5. Korzystanie z pary kluczy i certyfikatu

Subskrybent jest zobowiązany do przestrzegania postanowień, wymagań i procedur opisanych w niniejszej polityce certyfikacji oraz stosowania się do zasad korzystania z aplikacji mobilnej i systemu mObywatel. Subskrybent zobowiązany jest do wykorzystywania certyfikatu i związanego z nim klucza prywatnego wyłącznie zgodnie z przeznaczeniem. Subskrybent zobowiązany jest do niezwłocznego unieważnienia wydanego certyfikatu w przypadku ujawnienia lub zgubienia klucza prywatnego związanego z certyfikatem wystawionym w ramach niniejszej polityki certyfikacji.

4.6. Wymiana certyfikatu

W niniejszym podsystemie certyfikacji nie przewiduje się wystawiania nowego certyfikatu dla pary kluczy, dla której istnieje ważny certyfikat w ramach tej polityki certyfikacji. Wymagane jest wydanie nowego certyfikatu powiązanego z nową parą kluczy.

4.7. Wymiana certyfikatu połączona z wymianą pary kluczy

Wymiana certyfikatu przed upływem ważności aktywnego certyfikatu odbywa się automatycznie w oparciu o istniejący certyfikat. Po upływie ważności istniejącego certyfikatu wymiana nie jest możliwa i Subskrybent musi złożyć wniosek o wygenerowanie nowego certyfikatu zgodnie z opisami z wcześniejszych rozdziałów.

4.8. Zmiana treści certyfikatu

Zmiana danych zawartych w certyfikacie wymaga wystawienia nowego certyfikatu (zawierającego nową treść) i unieważnienia dotychczasowego certyfikatu (zawierającego starą treść). Wystawienie nowego certyfikatu odbywa się w sposób określony powyżej.

4.9. Unieważnienie certyfikatu

Subskrybent będący użytkownikiem aplikacji mObywatel ma możliwość unieważnienia certyfikatu za pomocą aplikacji mObywatel również w innym urządzeniu poprzez aktywację nowego certyfikatu, co skutkuje automatycznym unieważnieniem istniejącego certyfikatu.

Certyfikat może być unieważniony, jeżeli Subskrybent nie przestrzega postanowień niniejszej polityki certyfikacji, w szczególności gdy używa certyfikatów i związanych z nimi kluczy prywatnych niezgodnie z taą polityką certyfikacji.

Certyfikat może być także unieważniony, jeżeli zmianie ulega polityka certyfikacji i konieczne jest zaprzestanie używania dotychczasowych certyfikatów ze względu na sprzeczność z postanowieniami nowej polityki certyfikacji (zgodnie z rozdziałem 1.5).

4.10 Sprawdzanie statusu certyfikatu

Podsystem certyfikacji udostępnia usługę weryfikacji ważności certyfikatu online dostępną publicznie w internecie.

4.11 Powierzanie i odtwarzanie kluczy prywatnych

Nie dopuszcza się powierzania kluczy prywatnych Subskrybentów. Nie jest możliwe odtwarzanie kluczy prywatnych Subskrybentów w przypadku ich utraty lub niedostępności.

5. Zabezpieczenia organizacyjne, operacyjne i fizyczne

5.1 Zabezpieczenia fizyczne

Zabezpieczenia stosowane przez CC MC określone są w dokumentacji bezpieczeństwa oraz dokumentacji technicznej systemu mObywatel.

5.2 Zabezpieczenia proceduralne

Zabezpieczenia stosowane przez CC MC określone są w dokumentacji bezpieczeństwa oraz dokumentacji technicznej systemu mObywatel.

5.3 Zabezpieczenia osobowe

Zabezpieczenia stosowane przez CC MC określone są w dokumentacji bezpieczeństwa oraz dokumentacji technicznej systemu mObywatel.

5.4 Procedury rejestrowania zdarzeń

Zabezpieczenia stosowane przez CC MC określone są w dokumentacji bezpieczeństwa oraz dokumentacji technicznej systemu mObywatel.

5.5 Archiwizacja zapisów

Zabezpieczenia stosowane przez CC MC określone są w dokumentacji bezpieczeństwa oraz dokumentacji technicznej systemu mObywatel.

5.6. Wymiana pary kluczy podsystemu certyfikacji

Wymiana pary kluczy podsystemu certyfikacji może następować w planowych terminach (przed upływem ważności dotychczasowego zaświadczenia certyfikacyjnego) lub w przypadku wykrycia zwiększonego ryzyka utraty klucza prywatnego (np. na skutek uszkodzenia niektórych nośników klucza prywatnego przechowujących dane niezbędne do odtworzenia klucza prywatnego w stosowanym schemacie podziału sekretu). Nie dopuszcza się wystawiania nowych zaświadczeń certyfikacyjnych dla dotychczasowej pary kluczy podsystemu certyfikacji. Planowa wymiana pary kluczy podsystemu certyfikacji powinna nastąpić nie później niż w terminie określonym w rozdziale

5.6.1. Postępowanie w przypadku wymiany pary kluczy podsystemu certyfikacji jest następujące:

1) CC MC generuje nową parę kluczy i nowe zaświadczenia certyfikacyjne;
2) nowe zaświadczenia certyfikacyjne instalowane są jako tzw. punkty zaufania w tych modułach systemu certyfikacji, które tego wymagają w taki sposób, aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim kluczem prywatnym podsystemu certyfikacji. Oznacza to, że moduły w okresie zakładkowym powinny traktować oba zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania;
3) podsystem certyfikacji dostarcza Subskrybentom nowe zaświadczenia certyfikacyjne w sposób zapewniający autentyczność dostarczonych zaświadczeń certyfikacyjnych.

5.7 Postępowanie po ujawnieniu lub utracie klucza prywatnego podsystemu certyfikacji

Przez ujawnienie klucza prywatnego podsystemu certyfikacji należy rozumieć sytuację, w której zaistniała by możliwość użycia tego klucza w sposób niezgodny z niniejszą polityką certyfikacji i dokumentacją bezpieczeństwa. Procedury obowiązujące przy ujawnieniu klucza należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie ujawnienia klucza. W przypadku zaistnienia sytuacji, w której nastąpiło podejrzenie naruszenia lub naruszenie poufności, integralności bądź dostępności klucza prywatnego podsystemu certyfikacji, należy:

1) Zgłosić incydent zgodnie z zasadami określonymi w dokumentacji bezpieczeństwa;
2) Zidentyfikować okoliczności i osoby mające wpływ na zaistnienie nieprawidłowości;
3) Zebrać i zabezpieczyć materiał dowodowy;
4) Wyciągnąć wnioski, przedstawić i realizować zalecenia minimalizując możliwość zaistnienia podobnych sytuacji w przyszłości;
5) Pociągnąć osoby winne do odpowiedzialności dyscyplinarnej i/lub karnej.

5.7.1 Postępowanie po ujawnieniu klucza prywatnego podsystemu certyfikacji

Wykrycie ujawnienia klucza prywatnego podsystemu certyfikacji lub uzasadnione podejrzenie takiego ujawnienia powoduje następujące, niezwłocznie podejmowane działania:

1) Gestor systemu zawiadamia Subskrybentów o zaistniałej sytuacji oraz postępuje zgodnie z zapisami określonymi w dokumentacji bezpieczeństwa;
2) CC MC tworzy listę i unieważnia wszystkie aktywne certyfikaty i zaświadczenia certyfikacyjne;
3) Subskrybenci przestają wykorzystywać unieważnione certyfikaty oraz zaświadczenie certyfikacyjne;
4) CC MC generuje nową parę kluczy oraz nowe zaświadczenie certyfikacyjne zgodnie z obowiązującymi procedurami operacyjnymi;
5) nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu certyfikacji, które tego wymagają;
6) zaświadczenie certyfikacyjne związane z ujawnionym kluczem powinno być usunięte z systemów, w których stanowią tzw. punkty zaufania;
7) PR dostarcza Subskrybentom nowe zaświadczenie certyfikacyjne w sposób zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego;
8) dotychczasowy (ujawniony) klucz prywatny jest niszczony (sposób niszczenia jest określony w procedurach operacyjnych);
9) Subskrybenci za pomocą aplikacji mogą uzyskać nowe certyfikaty w sposób opisany w rozdziałach 3 i 4;
10) Dla certyfikatów instytucji, PR, działając w porozumieniu z Subskrybentami, wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków, zastępujące wszystkie

dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje na podstawie ponowienia zleceń certyfikacyjnych, o których mowa w rozdziale 4.3.

Jeśli baza danych podsystemu certyfikacji jest wiarygodna pomimo ujawnienia klucza, decyzją Gestora systemu nowe certyfikaty instytucji mogą zostać wygenerowane w oparciu o certyfikaty znajdujące się w tej bazie danych – bez powtórnego analizowania wniosków.

5.7.2. Postępowanie po utracie klucza prywatnego podsystemu certyfikacji

Utrata klucza prywatnego podsystemu certyfikacji, w przypadku braku podejrzeń dotyczących jego ujawnienia, powoduje następujące, niezwłocznie podejmowane działania:

1) CC MC generuje nową parę kluczy oraz nowe zaświadczenie certyfikacyjne zgodnie z obowiązującymi procedurami operacyjnymi;
2) Nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu certyfikacji, które tego wymagają, w taki sposób aby akceptowane były również certyfikaty Subskrybentów poświadczone poprzednim, utraconym kluczem prywatnym podsystemu certyfikacji (oznacza to, że moduły powinny traktować oba zaświadczenia certyfikacyjne – dotychczasowe i nowe – jako punkty zaufania);
3) PR dostarcza Subskrybentom nowe zaświadczenie certyfikacyjne w sposób zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego.

5.7.3. Postępowanie po jednoczesnym ujawnieniu i utracie klucza prywatnego podsystemu certyfikacji

Wykrycie jednoczesnego ujawnienia (lub uzasadnionego podejrzenia ujawnienia) i utraty klucza prywatnego podsystemu certyfikacji powoduje następujące, niezwłocznie podejmowane działania:

1) Gestor systemu zawiadamia Subskrybentów o zaistniałej sytuacji oraz postępuje zgodnie z zapisami określonymi w dokumentacji bezpieczeństwa;
2) Subskrybenci przestają wykorzystywać unieważnione certyfikaty oraz zaświadczenie certyfikacyjne;
3) CC MC generuje nową parę kluczy oraz nowe zaświadczenie certyfikacyjne zgodnie z obowiązującymi procedurami operacyjnymi;
4) nowe zaświadczenie certyfikacyjne instalowane jest jako tzw. punkt zaufania w tych modułach systemu certyfikacji, które tego wymagają;
5) zaświadczenie certyfikacyjne związane z ujawnionym i utraconym kluczem powinno być usunięte z systemów, w których stanowią tzw. punkty zaufania;
6) PR dostarcza Subskrybentom nowe zaświadczenie certyfikacyjne w sposób zapewniający autentyczność dostarczonego zaświadczenia certyfikacyjnego;
7) Subskrybenci za pomocą aplikacji mogą uzyskać nowe certyfikaty w sposób opisany w rozdziałach 3 i 4;
8) Dla instytucji – PR działając w porozumieniu z Subskrybentami – wystawia nowe zlecenia certyfikacyjne na podstawie posiadanych wniosków, zastępujące wszystkie dotychczas wystawione certyfikaty. Wydawanie nowych certyfikatów następuje na podstawie ponowienia zleceń certyfikacyjnych, o których mowa w rozdziale 4.3.

5.8. Zakończenie działalności podsystemu certyfikacji

Decyzję o zakończeniu działalności podsystemu certyfikacji podejmuje Gestor systemu. Subskrybenci zostaną poinformowani o planowanym zakończeniu działalności podsystemu certyfikacji niezwłocznie po podjęciu takiej decyzji, w miarę możliwości z co najmniej 3-miesięcznym

wyprzedzeniem. Nie później niż z chwilą zaprzestania działalności wszystkie wystawione certyfikaty zostaną unieważnione.

6. Zabezpieczenia techniczne

Zabezpieczenia stosowane przez CC MC określone są w dokumentacji bezpieczeństwa. W niniejszym rozdziale zawarto jedynie niektóre aspekty dotyczące zabezpieczeń technicznych i organizacyjnych.

6.1. Generowanie i instalowanie par kluczy

6.1.1. Generowanie par kluczy

Pary kluczy podsystemu certyfikacji generowane są przez personel CC MC zgodnie z procedurami operacyjnymi CC MC. Generowanie par kluczy podsystemu certyfikacji odbywa się w bezpiecznym module kryptograficznym HSM. Pary kluczy Subskrybentów generowane są z wykorzystaniem bezpiecznego, sprzętowego generatora liczb losowych modułu kryptograficznego HSM w systemie centralnym mObywatel.

6.1.2. Dostarczenie klucza prywatnego Subskrybentowi

Certyfikaty wraz z kluczem prywatnym są przekazywane do Subskrybentów w postaci zaszyfrowanej kluczem publicznym, przekazanym w żądaniu certyfikacyjnym. Dodatkowo cała komunikacja pomiędzy aplikacją, a systemem centralnym wykorzystuje szyfrowany protokół TLS.

Klucze prywatne Subskrybentów są kasowane z systemu centralnego tuż po ich dostarczeniu Subskrybentowi.

6.1.3. Dostarczenie klucza publicznego Subskrybenta do PR

Klucze Subskrybentów są bezpiecznie generowane w podsystemie certyfikacji dlatego nie ma konieczności dostarczania kluczy prywatnych do PR w procesie rejestracji.

6.1.4. Dostarczenie klucza publicznego podsystemu certyfikacji

Klucz publiczny podsystemu certyfikacji jest publikowany w formie zaświadczenia certyfikacyjnego w formacie X509. Zaświadczenie certyfikacyjne jest wykorzystywane jako punkt zaufania w aplikacji mobilnej ale również w systemach zintegrowanych do których użytkownicy aplikacji mObywatel mają możliwość przekazywania swoich danych.

6.1.5. Rozmiary kluczy

Centrum certyfikacji stosuje klucze RSA o długości nie mniejszej niż 2048 bitów, z wyjątkiem certyfikatu służącego do znaczenia czasem gdzie ze względów wydajnościowych minimalna długość klucza może wynosić 1024 bity.

6.1.6. Cel użycia klucza

Pole rozszerzenia keyUsage w certyfikatach zgodnych z Zaleceniem X.509:2000 określa zastosowanie (jedno lub kilka) klucza publicznego zawartego w certyfikacie.

Klucz prywatny podsystemu certyfikacji może być wykorzystywany tylko do podpisywania certyfikatów i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów i list CRL.

Klucze prywatne Subskrybentów mogą być używane tylko do podpisywania komunikatów przesyłanych do systemu oraz do ochrony transmisji komunikatów w ramach systemu mObywatel. Odpowiadające im klucze publiczne mogą być używane do weryfikacji podpisu Subskrybenta, i uwierzytelnienia Subskrybenta podczas komunikacji z systemami zintegrowanymi z systemem mObywatel. Certyfikaty wyżej wymienionych kluczy mają ustawione odpowiednie wartości (digitalSignature, keyEncipherment, dataEncipherment, keyAgreement lub pewien podzbiór tych wartości) w polu keyUsage.

6.2. Ochrona kluczy prywatnych

6.2.1. Standardy dla modułów kryptograficznych

Klucze prywatne podsystemu certyfikacji są generowane, a następnie przechowywane w bezpiecznym urządzeniu kryptograficznym HSM posiadającym certyfikat zgodności z wymaganiami normy FIPS 140-3 poziom 3 lub normy ISO/IEC 15408 Evaluation criteria for IT Security, poziom EAL-4, które zapewniają odpowiedni poziom bezpieczeństwa przechowywania kluczy wewnątrz urządzenia oraz przeprowadzania operacji z użyciem klucza prywatnego.

Klucze prywatne Subskrybentów są generowane za pomocą generatora liczb losowych modułu kryptograficznego HSM posiadającego certyfikat zgodności z wymaganimi normy FIPS 140-3 poziom 3 lub normy ISO/IEC 15408 Evaluation criteria for IT Security, poziom EAL-4.

6.2.2. Wieloosobowe zarządzanie kluczem

Klucze prywatne podsystemu certyfikacji są przechowywane z wykorzystaniem mechanizmu podziału sekretów.

6.2.3. Powierzenie klucza prywatnego (key-escrow)

Nie występuje.

6.2.4. Kopia bezpieczeństwa klucza prywatnego

Kopia bezpieczeństwa klucza prywatnego podsystemu certyfikacji wynika z realizacji procedury podziału sekretów. Kopie bezpieczeństwa kluczy prywatnych Subskrybenta nie powinny być tworzone.

6.2.5. Archiwizowanie klucza prywatnego

Nie przewiduje się archiwizowania kluczy prywatnych.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Klucze prywatne podsystemu certyfikacji są wprowadzane do modułu kryptograficznego przez personel PR zgodnie z procedurami operacyjnymi.

6.2.7. Metoda aktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji jest uaktywniany w sposób automatyczny przez aplikację za pomocą hasła dostępowego. Polityka certyfikacji nie nakłada wymagań na metodę aktywacji kluczy prywatnych Subskrybentów.

Klucz prywatny Subskrybentów korzystających z aplikacji mObywatel odblokowywany jest przy pomocy hasła, bądź użyciu biometrii urządzenia i kodu PIN lub tylko biometrii.

Polityka certyfikacji nie nakłada wymagań na metodę aktywacji kluczy prywatnych certyfikatów Instytucji.

6.2.8. Metoda dezaktywacji klucza prywatnego

Klucz prywatny podsystemu certyfikacji może zostać dezaktywowany przez personel PR poprzez usunięcie z modułu kryptograficznego wczytanych kluczy kryptograficznych.

W przypadku Subskrybentów korzystających z aplikacji mObywatel klucz jest automatycznie blokowany na skutek nieaktywności użytkownika lub po zamknięciu aplikacji.

Polityka certyfikacji nie nakłada wymagań na metodę dezaktywacji kluczy prywatnych Subskrybentów korzystających z certyfikatów Instytucji.

6.2.9. Metoda niszczenia klucza prywatnego

Klucze prywatne podsystemu certyfikacji niszczone są poprzez fizyczne zniszczenie nośników kluczy kryptograficznych zawierających fragmenty tych kluczy, zgodnie z procedurami określonymi w odrębnym dokumencie.

Klucz prywatny wykorzystywany przez aplikację mObywatel niszczony jest przez aplikację poprzez bezpieczne usunięcie.

Subskrybent korzystający z certyfikatu instytucji powinien opracować zasady, według których niszczone są należące do niego klucze prywatne i nośniki kluczy kryptograficznych.

6.3. Inne aspekty zarządzania parą kluczy

6.3.1. Długoterminowa archiwizacja kluczy publicznych

CC MC prowadzi długoterminową archiwizację kluczy publicznych podsystemu certyfikacji oraz wszystkich wystawionych przez siebie certyfikatów i zaświadczeń certyfikacyjnych, zgodnie z dokumentacją bezpieczeństwa.

6.3.2. Okresy ważności kluczy

Okres ważności pary kluczy i zaświadczeń certyfikacyjnych podsystemu certyfikacji może wynosić maksymalnie 5 lat. Okres ważności certyfikatów kluczy Subskrybentów wynosi 1 rok, z wyjątkiem uczniów i studentów.

6.4. Dane aktywujące

Subskrybenci korzystający z aplikacji mObywatel aktywują klucz prywatny z użyciem hasła lub mechanizmu biometrycznego systemu operacyjnego urządzenia z dodatkowym kodem PIN.

Dane aktywujące są zarządzane zgodnie z procedurami umieszczonymi w odrębnych dokumentach zgodnych z utrzymaniem procedur certyfikacji w CC MC.

6.5. Zabezpieczenia komputerów

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

6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

6.6.1. Środki przedsięwzięte dla zapewnienia bezpieczeństwa rozwoju systemu

W CC MC przyjęto zasady dokonywania modyfikacji w systemie teleinformatycznym. W szczególności dotyczy to testów nowych wersji oprogramowania i/lub wykorzystania do tego celu istniejących baz danych. Zasady te gwarantują nieprzerwaną pracę systemu teleinformatycznego, integralność jego zasobów oraz zachowanie poufności danych.

6.6.2. Zarządzanie bezpieczeństwem

Za realizację procesów bezpieczeństwa odpowiedzialny jest personel CC MC oraz personel wykonawcy obsługujący system mObywatel. Środki bezpieczeństwa zostały określone w dokumentacji bezpieczeństwa CC MC oraz dokumentacji technicznej systemu mObywatel.

6.7. Zabezpieczenia sieci komputerowej

Zastosowane zabezpieczenia są zgodne z zasadami określonymi w dokumentacji bezpieczeństwa CC MC oraz dokumentacji technicznej systemu mObywatel.

6.8. Oznaczanie czasem

Do oznaczania czasem certyfikatów, zaświadczeń certyfikacyjnych oraz zapisów w logach urządzeń i oprogramowania stosuje się wskazanie bieżącego czasu pochodzące z zegarów wbudowanych w urządzenia lub stacje robocze, synchronizowanymi ze sprzętowym źródłem czasu UTC z dokładnością do 1s.

7. Profile certyfikatów i list CRL

Rozdział zawiera informacje o profilu certyfikatów kluczy publicznych generowanych zgodnie z niniejszą polityką certyfikacji.

7.1. Profil certyfikatów

CC MC wystawia certyfikaty i zaświadczenia certyfikacyjne w formacie zgodnym z zaleceniem X.509:2000, wersja 3 formatu.

7.1.1. Struktura certyfikatów

Wszystkie certyfikaty wydawane przez podsystem certyfikacji mają strukturę podstawowych atrybutów zgodną z poniższym opisem:

Atrybut	Przykładowa wartość	Uwagi	Wymagany
Wersja - Version	V3	Zgodny z zaleceniem X.509:2000, wersja 3 formatu	TAK
Numer seryjny - serialNumber	00 01 02 03 04 05 06 07 08 09 0A 0B 0C 0D 0E 0F	Jednoznaczny w ramach urzędu certyfikacji podpisującego certyfikat. Numer nadawany przez ten urząd.	TAK
Algorytm podpisu signatureAlgorithm	sha256WithRSAEncryption	Identyfikator algorytmu stosowanego do	TAK

		elektronicznego poświadczenia certyfikatu. Minimum SHA256 z szyfrowaniem RSA	
Okres ważności certyfikatu - Validity			
not before	not before: 2018-0102 00:00:00 GMT	Data i godzina wydania certyfikatu. Minimalny okres to dwa lata od wydania certyfikatu.	
not after	not after: 2020-01-02 23:59:59 GMT	Data i godzina wydania certyfikatu + <okres ważności certyfikatu>	
Klucz publiczny	Klucz publiczny RSA rsaEncryption	Szyfrowanie RSA	TAK
Długość klucza	2048 bit RSA	Minimalna długość klucza 2048 bit.	TAK

7.1.2. Rozszerzenia certyfikatów i ich krytyczność

Certyfikaty wydawane Subskrybentom mają następujące rozszerzenia:

Rozszerzenie	Krytyczny	Wymagany	Wartość	Uwagi
Key Usage	TAK	TAK		Podstawowe warunki użycia certyfikatu X509v3
digitalSignature			1	Uwierzytelnianie
keyEncipherment			0	Szyfrowanie klucza
dataEncipherment			1	Szyfrowanie danych
keyAgreement			0	Uzgadnianie klucza
Authority Key Identifier	NIE	TAK	np. 89:56:DD:D3:B5:F7:10:65:FF:14:4F:24:A9:9F:B6:62:DF:C9:75:93	Identyfikator klucza zaświadczenia certyfikacyjnego
Subject Key Identifier	NIE	TAK	np. 89:56:DD:D3:B5:F7:10:65:FF:14:4F:24:A9:9F:B6:62:DF:C9:75:93	Identyfikator klucza Subskrybenta
Authority Information Access	NIE	NIE	np. CA Issuers – URI:https://www.mobywatel.gov.pl/MTInt.cer OCSP – URI:https://www.mobywatel.gov.pl/ocsp	Informacja na temat punktów informacyjnych służących do weryfikacji certyfikatu.
Document Type	NIE	NIE	np. MOBILE_ID_CARD	Rozszerzenie niestandardowe OID:

				2.25.119573321019488463162866753412488583781.1.1.1

7.1.3. Identyfikatory algorytmów kryptograficznych

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

Nazwa	Identyfikator
Sha512WithRSAEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) sha512WithRSAEncryption(13)}
RsaEncryption	{iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) rsaEncryption(1)}

7.1.4. Formaty identyfikatorów podsystemu certyfikacji oraz Subskrybentów

7.1.4.1. Identyfikator wyróżniający podsystemu certyfikacji

Kraj (countryName) = PL

Nazwa organizacji (organizationName) = Kancelaria Prezesa Rady Ministrów

Nazwa powszechna (commonName) = MTMid

7.1.4.2. Struktura identyfikatorów wyróżniających Subskrybentów

Budowa identyfikatora wyróżniającego Subskrybenta opisana jest w rozdziale 3.1.

7.1.5. Identyfikatory zgodnych polityk certyfikacji

Brak.

7.2. Profil list CRL

Podsystem certyfikacji wykorzystuje mechanizm OCSP do weryfikacji ważności certyfikatów online. Nie są wykorzystywane listy CRL.

8. Zasady audytu

CC MC podlega regularnym audytom wewnętrznym, prowadzonym przez osoby niezajmujące się bieżącą obsługą CC MC. CC MC posiada dokument określający procedury audytu.

9. Inne postanowienia

9. Opłaty

Nie dotyczy.

9.2. Odpowiedzialność finansowa

Nie dotyczy.

9.3. Poufność informacji

Rodzaje informacji podlegające ochronie oraz sposoby ich ochrony są zdefiniowane w dokumentach bezpieczeństwa opracowanych dla CC MC w tym dokumentacji technicznej systemu mObywatel. Pracownicy CC MC są zobowiązani do ochrony poufności informacji podlegających ochronie.

Subskrybenci są zobowiązani do ochrony poufności posiadanych kluczy kryptograficznych (dla użytkowników aplikacji mObywatel oznacza to stosowanie wyłącznie oficjalnej aplikacji dostępnej w repozytorium aplikacji systemu operacyjnego dostarczonej przez MC) oraz innych danych z tym związanych (jak hasła i kody PIN). Certyfikaty, zaświadczenia certyfikacyjne są traktowane jako informacje jawne.

9.4. Ochrona danych osobowych

Dane zawarte we wnioskach i certyfikatach są przetwarzane w sposób określony w niniejszej polityce i w dokumentacji technicznej systemu mObywatel.

9.5. Zabezpieczenie własności intelektualnej

Niniejsza polityka certyfikacji stanowi własność intelektualną MC. Z punktu widzenia prawa autorskiego polityka może być bez żadnych ograniczeń wykorzystywana (w tym drukowana i kopiowana) przez osoby, którym została udostępniona za zgodą MC. Certyfikaty wystawione przez CC MC są jego własnością. Subskrybenci mają prawo do wykorzystywania certyfikatów w systemie mObywatel, zgodnie z zasadami opisanymi w niniejszej polityce certyfikacji.

9.6. Udzielane gwarancje

Nie występują.

9.7. Zwolnienia z domyślnie udzielanych gwarancji

Nie występują.

9.8. Ograniczenia odpowiedzialności

Nie występują.

9.9. Przenoszenie roszczeń odszkodowawczych

Nie występuje.

9.10. Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Przepisy przejściowe nie występują. Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią do utraty ważności tych certyfikatów (z powodu zakończenia okresu ważności lub unieważnienia). Certyfikaty wykorzystywane w celach dochodzeniowych lub dowodowych po okresie ich ważności powinny być używane zgodnie z polityką certyfikacji w ramach której zostały wystawione. W stosunku do nowo wystawianych certyfikatów stosuje się najnowszą obowiązującą politykę certyfikacji zatwierdzoną przez Gestora systemu.

9.11. Określanie trybu i adresów doręczania pism

Tryb i adres doręczania pism związanych ze sprawami niniejszej polityki certyfikacji i wystawianych w jej ramach certyfikatów określają odrębne przepisy.

9.12. Zmiany w polityce certyfikacji

Zasady zarządzania polityką certyfikacji zostały opisane w rozdziale 1.5.

9.13. Rozstrzyganie sporów

Wszelkie spory dotyczące spraw związanych z niniejszą polityką certyfikacji będą rozstrzygane przez Gestora systemu. Wiążące interpretacje postanowień niniejszej polityki certyfikacji wydaje Gestor systemu.

9.14. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega polskiemu prawu.

9.15. Podstawy prawne

Zasady działania CC MC są zgodne z obowiązującym prawem, a w szczególności z przepisami zawartymi w następujących aktach prawnych:

1) ustawa z dnia 26 maja 2023 r. o aplikacji mObywatel (Dz. U. poz. 1234);

2) ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. z 2023 r. 57);

3) ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz. U. 2021 r. poz. 1797);

4) rozporządzenie Parlamentu Europejskiego i Rady (UE) 2016/679 z dnia 27 kwietnia 2016 r. w sprawie ochrony osób fizycznych w związku z przetwarzaniem danych osobowych i w sprawie swobodnego przepływu takich danych oraz uchylenia dyrektywy 95/46/WE (ogólne rozporządzenie o ochronie danych) (Dz. Urz. UE L 119 z 04.05.2016, str. 1);

5) rozporządzenie Parlamentu Europejskiego i Rady (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 oraz uchylającego dyrektywę 1999/93/WE (Dz. Urz. UE L 257 z 28.08.2014, str. 73).

9.16. Inne postanowienia

Nie występują.