

KWALIFIKOWANY DOSTAWCA USŁUG ZAUFANIA „CENCERT”

POLITYKA DLA KWALIFIKOWANYCH USŁUG ZAUFANIA

Wersja: 1.3

Karta dokumentu:

Tytuł dokumentu	Polityka dla kwalifikowanych usług zaufania
Właściciel dokumentu	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Wersja	1.3
Status dokumentu	Zatwierdzony
Data zatwierdzenia	2020-10-06
Liczba stron	54

zatwierdzone przez:

Wersja	zatwierdzający
1.3	Zarząd Enigma Systemy Ochrony Informacji Sp. z o.o.

historia wersji

Nr wersji	Sporządził	Opis zmian	Obowiązuje od
1.0	Jacek Pokraśniewicz	Wersja początkowa, zastępuje <i>Politykę certyfikacji dla certyfikatów kwalifikowanych w. 2.3</i> oraz <i>Politykę znakowania czasem i innych kwalifikowanych usług certyfikacyjnych w. 1.1.</i>	2017-05-20
1.1	Jacek Pokraśniewicz, Piotr Popis	Wprowadzenie uwag audytora, dodanie algorytmu ECDSA	2017-06-14
1.2	Jacek Pokraśniewicz	Dodanie możliwości generowania certyfikatu na podstawie dostarczonego klucza publicznego, dodanie możliwości realizacji usługi pieczęci w trybie zdalnym, dostosowanie do RODO Usunięcie nieaktualnych już przepisów przejściowych	2019-04-01
1.3	Jacek Pokraśniewicz	Dodanie możliwości realizacji usługi podpisu w trybie zdalnym (serwerowym) rSign. Nowa usługa wystawiania certyfikatów do pieczęci zaawansowanej (w tym certyfikatów do PSD2) oraz do uwierzytelnienia witryn internetowych. Możliwość uwierzytelnienia za pomocą potwierdzenia notarialnego lub podpisu kwalifikowanego. Możliwość wystawiania certyfikatów zawierających pseudonim.	Po audycie eIDAS

Spis treści

1. WSTĘP	5
1.1. WPROWADZENIE	5
1.2. IDENTYFIKATOR POLITYKI CERTYFIKACJI	5
1.3. OPIS SYSTEMU CERTYFIKACJI I UCZESTNICZĄCYCH W NIM PODMIOTÓW	6
1.4. ZAKRES ZASTOSOWAŃ	7
1.5. ZASADY ADMINISTROWANIA POLITYKĄ CERTYFIKACJI	8
1.6. SŁOWNIK UŻYWANYCH TERMINÓW I AKRONIMÓW	9
2. ZASADY DYSTRYBUCJI I PUBLIKACJI INFORMACJI.....	11
3. IDENTYFIKACJA I UWIERZYTELNIENIE	12
3.1. STRUKTURA NAZW PRZYDZIELANYCH SUBSKRYBENTOM	12
3.1.1 Certyfikat do podpisu elektronicznego.....	12
3.1.2 Certyfikat do pieczęci elektronicznej.....	14
3.1.3 Certyfikat do uwierzytelnienia stron WWW	15
3.2. UWIERZYTELNIENIE SUBSKRYBENTA PRZY WYSTAWIENIU PIERWSZEGO CERTYFIKATU	16
3.3. UWIERZYTELNIENIE SUBSKRYBENTA PRZY WYSTAWIANIU KOLEJNYCH CERTYFIKATÓW	17
3.4. SPOSOBY UWIERZYTELNIENIA SUBSKRYBENTA PRZY ZGŁASZANIU ŻĄDANIA UNIEWAŻNIENIA, ZAWIESZENIA I UCHYLENIA ZAWIESZENIA CERTYFIKATU	17
3.5. ZARZĄDZANIE UPRAWNIENIAMI OSÓB DO SKŁADANIA PIECZĘCI W TRYBIE ZDALNYM.....	18
4. CYKL ŻYCIA CERTYFIKATU – WYMAGANIA OPERACYJNE.....	19
4.1. WNIOSEK O WYSTAWIENIE CERTYFIKATU.....	19
4.2. PRZETWARZANIE WNIOSKU	20
4.3. WYSTAWIENIE CERTYFIKATU	20
4.4. AKCEPTACJA CERTYFIKATU.....	21
4.5. KORZYSTANIE Z PARY KLUCZY I CERTYFIKATU	21
4.5.1 Korzystanie z certyfikatu.....	21
4.5.2 Korzystanie z klucza prywatnego	21
4.6. WYMIANA CERTYFIKATU	24
4.7. WYMIANA CERTYFIKATU POŁĄCZONA Z WYMIANĄ PARY KLUCZY	24
4.8. ZMIANA TREŚCI CERTYFIKATU.....	24
4.9. UNIEWAŻNIENIE I ZAWIESZENIE CERTYFIKATU	25
4.10. USŁUGI INFORMOWANIA O STATUSIE CERTYFIKATÓW	26
4.11. ZAKOŃCZENIE REALIZACJI USŁUGI ZAUFANIA DLA SUBSKRYBENTA	27
4.12. POWIERZANIE I ODTWARZANIE KLUCZY PRYWATNYCH	27
5. ZABEZPIECZENIA ORGANIZACYJNE, OPERACYJNE I FIZYCZNE.....	28
5.1. ZABEZPIECZENIA FIZYCZNE	28
5.2. ZABEZPIECZENIA PROCEDURALNE	28
5.3. ZABEZPIECZENIA OSOBOWE.....	29
5.4. PROCEDURY TWORZENIA LOGÓW AUDYTOWYCH.....	30
5.5. ARCHIWIZACJA ZAPISÓW	30
5.6. WYMIANA PARY KLUCZY CENTRUM CERTYFIKACJI.....	30
5.7. UTRATA POUFNOŚCI KLUCZA PRYWATNEGO I DZIAŁANIE W PRZYPADKU KATASTROF	31
5.7.1 Utrata poufności klucza prywatnego.....	31
5.7.2 Osłabienie algorytmów kryptograficznych.....	31
5.7.3 Katastrofy	32
5.8. ZAKOŃCZENIE DZIAŁALNOŚCI	32

6.	ZABEZPIECZENIA TECHNICZNE	33
6.1.	GENEROWANIE I INSTALOWANIE PAR KLUCZY	33
6.1.1	<i>Generowanie par kluczy</i>	<i>33</i>
6.1.2	<i>Dostarczenie klucza prywatnego Subskrybentowi</i>	<i>33</i>
6.1.3	<i>Dostarczenie klucza publicznego Subskrybenta</i>	<i>34</i>
6.1.4	<i>Dostarczenie klucza publicznego CenCert</i>	<i>34</i>
6.1.5	<i>Parametry kryptograficzne kluczy</i>	<i>34</i>
6.1.6	<i>Cel użycia klucza</i>	<i>35</i>
6.2.	OCHRONA KLUCZY PRYWATNYCH	35
6.3.	INNE ASPEKTY ZARZĄDZANIA PARĄ KLUCZY	37
6.4.	DANE AKTYWUJĄCE	37
6.5.	ZABEZPIECZENIA KOMPUTERÓW	38
6.6.	ZABEZPIECZENIA ZWIĄZANE Z CYKLEM ŻYCIA SYSTEMU INFORMATYCZNEGO	38
6.7.	ZABEZPIECZENIA SIECI KOMPUTEROWEJ	39
6.8.	ZNAKOWANIE CZASEM	39
7.	PROFIL CERTYFIKATÓW, LIST CRL I TOKENÓW OCSP	40
7.1.	PROFIL CERTYFIKATÓW I ZAŚWIADCZEŃ	40
7.1.1	<i>Nazwy wyróżniające (Distinguished Names)</i>	<i>40</i>
7.1.2	<i>Profil certyfikatów subskrybentów</i>	<i>41</i>
7.1.3	<i>Certyfikaty do podpisywania tokenów OCSP, certyfikaty kluczy infrastruktury, oraz certyfikaty testowe</i>	<i>44</i>
7.2.	PROFIL LIST CRL	45
7.3.	PROFIL OCSP	45
7.4.	PROFIL ZNACZNIKA CZASU	46
8.	AUDYT	47
9.	INNE POSTANOWIENIA	48
9.1.	OPLATY	48
9.2.	ODPOWIEDZIALNOŚĆ FINANSOWA	48
9.3.	POUFNOŚĆ INFORMACJI	48
9.4.	OCHRONA DANYCH OSOBOWYCH	49
9.5.	ZABEZPIECZENIE WŁASNOŚCI INTELEKTUALNEJ	49
9.6.	UDZIELANE GWARANCJE	49
9.7.	ZWOLNIENIA Z DOMYŚLNIE UDZIELANYCH GWARANCJI	50
9.8.	OGRANICZENIA ODPOWIEDZIALNOŚCI	50
9.9.	PRZENOSZENIE ROSZCZEŃ ODSZKODOWAWCZYCH	52
9.10.	PRZEPISY PRZEJŚCIOWE I OKRES OBOWIĄZYWANIA POLITYKI CERTYFIKACJI	52
9.11.	OKREŚLANIE TRYBU I ADRESÓW DORĘCZANIA PISM	52
9.12.	ZMIANY W POLITYCE CERTYFIKACJI	53
9.13.	ROZSTRZYGANIE SPORÓW	53
9.14.	OBOWIĄZUJĄCE PRAWO	53
9.15.	PODSTAWY PRAWNE	53
9.16.	INNE POSTANOWIENIA	54

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę opisującą realizację przez Centrum Certyfikacji **CenCert** prowadzone przez firmę Enigma Systemy Ochrony Informacji Sp. z o.o. kwalifikowanych usług zaufania polegających na:

- 1) wystawianiu i unieważnianiu kwalifikowanych certyfikatów oraz
- 2) wystawianiu kwalifikowanych znaczników czasu.

Usługi zaufania świadczone na podstawie niniejszej polityki spełniają wymagania rozporządzenia UE 910/2014 (eIDAS).

Struktura dokumentu została oparta na standardzie RFC 3647 "*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework*".

1.2. Identyfikator polityki certyfikacji

Nazwa polityki	POLITYKA DLA KWALIFIKOWANYCH USŁUG ZAUFANIA
Kwalifikator polityki	Brak
Numer OID (ang. Object Identifier)	1.3.6.1.4.1.10214.99.1.1.1.4
Data wprowadzenia	3.12.2020, w zakresie usługi wystawiania certyfikatów do uwierzytelnienia stron WWW (QWAC) –od dokonania wpisu usługi na listę TSL
Data wygaśnięcia	Do odwołania

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

CenCert jest kwalifikowanym dostawcą usług zaufania (QTSP - *Qualified Trust Service Provider*), działającym zgodnie z rozporządzeniem eIDAS, w tym zgodnie z aktami wykonawczymi oraz zgodnie z prawem krajowym, czyli ustawą o usługach zaufania (Dz. Ust. z 2016 r., poz. 1579) i aktami wykonawczymi.

Klucze publiczne do weryfikacji świadczonych usług zaufania:

- klucz do podpisywania certyfikatów i list CRL,
- klucz do podpisywania znaczników czasu

- są dostępne w postaci certyfikatów wydanych przez krajowy root (NCCert) oraz na liście TSL.

CenCert nie wystawia certyfikatów dla podległych dostawców usług zaufania (SubCA). CenCert wystawia certyfikat klucza do realizacji usługi OCSP.

CenCert obsługuje Subskrybentów poprzez punkty rejestracji (RA – Registration Authorities):

- Centralny Punkt Rejestracji (CPR), którego dane znajdują się w rozdziale 1.3 poniżej.
- Terenowe Punkty Rejestracji.

Lista terenowych Punktów Rejestracji jest modyfikowana adekwatnie do aktualnych potrzeb Subskrybentów i możliwości CenCert. Dane kontaktowe terenowych punktów rejestracji znajdują się na WWW.

Większość terenowych Punktów Rejestracji (mobilne Punkty Rejestracji) oferuje możliwość realizacji usługi wystawienia kwalifikowanego certyfikatu w domu Subskrybenta lub miejscu jego pracy.

CPR stanowi punkt kontaktowy dla wszelkich zapytań i wniosków związanych z działaniem CenCert.

Punktem kontaktowym dla obsługi wszelkich spraw związanych z realizacją niniejszej polityki certyfikacji przez CenCert jest:

Centralny Punkt Rejestracji *CenCert*
ENIGMA Systemy Ochrony Informacji Sp. z o.o.

biuro@cencert.pl

Aktualny adres pocztowy, telefony kontaktowe i numer faksu są publikowane na stronie <https://www.cencert.pl>.

Elektroniczne wnioski o zmianę statusu certyfikatów (unieważnienie, zawieszenie, uchylenie zawieszenia) oraz o zmianę osób uprawnionych do inicjowania sesji składania pieczęci w trybie zdalnym - powinny być przysyłane na adres rev@cencert.pl. Poprawne wnioski przesłane na inne adresy CenCert (np. biuro@cencert.pl) będą w miarę możliwości obsługiwane, ale CenCert nie ponosi odpowiedzialności za ich terminową obsługę, ani za to, że w ogóle będą obsłużone.

Subskrybentem usług zaufania w zakresie:

- kwalifikowanego certyfikatu do podpisu elektronicznego - może być każda osoba fizyczna posiadająca pełną zdolność do czynności prawnych,
- kwalifikowanego certyfikatu do pieczęci elektronicznej - może być każda osoba prawna w rozumieniu prawa krajowego, jak też inna jednostka o podobnym charakterze (jednostka organizacyjna nieposiadająca osobowości prawnej, spółka cywilna itd.),
- kwalifikowanego znacznika czasu, kwalifikowanego certyfikatu do uwierzytelnienia stron internetowych - może być każda osoba fizyczna, osoba prawna w rozumieniu prawa krajowego, jak też inna jednostka o podobnym charakterze (jednostka organizacyjna nieposiadająca osobowości prawnej, spółka cywilna itd.).

1.4. Zakres zastosowań

CenCert, realizując niniejszą politykę certyfikacji wystawia:

- kwalifikowane certyfikaty do realizacji kwalifikowanego podpisu elektronicznego,
- kwalifikowane certyfikaty do realizacji kwalifikowanej bądź zaawansowanej pieczęci elektronicznej,
- kwalifikowane certyfikaty do uwierzytelnienia stron internetowych,
- kwalifikowane znaczniki czasu,
- certyfikaty infrastruktury używane wewnątrz w Centrum Certyfikacji,
- certyfikaty do realizacji usługi OCSP,
- listy CRL i tokeny OCSP,
- certyfikaty testowe.

CenCert, jako kwalifikowany dostawca usług zaufania, może świadczyć usługi:

- 1) składania kwalifikowanej pieczęci elektronicznej oraz

2) składania kwalifikowanego podpisu elektronicznego

- w imieniu subskrybenta, na zasadach określonych niniejszą polityką, obowiązującymi procedurami i umowami handlowymi.

Certyfikaty infrastruktury są wyraźnie odróżnione od certyfikatów kwalifikowanych poprzez odpowiednie rozszerzenia.

Certyfikaty testowe są wyraźnie odróżnione poprzez użycie identyfikatora DN zawierającego pola „TEST” (ewentualnie inne podobne, jak „TEST1”, „TEST2”, „TEST <znaki innych alfabetów>” itd.) we wszystkich miejscach przeznaczonych na dane tekstowe (imię, nazwisko, nazwa powszechna itd.) oraz przykładowych numerów (typu 1234...) w miejscach przeznaczonych na dane numeryczne (PESEL, NIP itd.).

Zgodnie z eIDAS:

1. Kwalifikowany podpis elektroniczny ma skutek prawny równoważny podpisowi własnoręcznemu.
2. Kwalifikowany podpis elektroniczny oparty na kwalifikowanym certyfikacie wydanym w jednym państwie członkowskim jest uznawany za kwalifikowany podpis elektroniczny we wszystkich pozostałych państwach członkowskich.
3. Kwalifikowany elektroniczny znacznik czasu korzysta z domniemania dokładności daty i czasu, jakie wskazuje, oraz integralności danych, z którymi wskazywane data i czas są połączone.
4. Kwalifikowany elektroniczny znacznik wydany w jednym państwie członkowskim jest uznawany za kwalifikowany elektroniczny znacznik czasu we wszystkich państwach członkowskich.

1.5. Zasady administrowania polityką certyfikacji

Podmiotem uprawnionym do administrowania polityką certyfikacji, w tym zatwierdzania zmian jest Zarząd ENIGMA Systemy Ochrony Informacji Sp. z o.o.

Wszelkie zmiany niniejszej polityki certyfikacji, z wyjątkiem takich, które naprawiają oczywiste błędy redakcyjne lub stylistyczne, wymagają nadania nowego numeru wersji.

Zgodnie z art. 24.2.a) eIDAS, CenCert informuje organ nadzoru o wszelkich zmianach w świadczeniu kwalifikowanych usług zaufania oraz o zamiarze zaprzestania swej działalności (patrz też rozdz. 5.8).

1.6. Słownik używanych terminów i akronimów

W niniejszym dokumencie następujące sformułowania użyte będą w wymienionym poniżej znaczeniu. Należy zwrócić uwagę, że opisy tu umieszczone nie zawsze są ogólnymi definicjami danego terminu, lecz raczej wyjaśniają znaczenie danego terminu lub akronimu w kontekście używanym w CenCert.

Termin/akronim	Opis
eIDAS	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 uchylające dyrektywę 1999/93/WE.
Ustawa	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.
QTSP	(<i>Qualified Trust Service Provider</i>) kwalifikowany dostawca usług zaufania
PKI	<i>Public Key Infrastructure</i> – infrastruktura klucza publicznego – system obejmujący Centra Certyfikacji, Punkty Rejestracji oraz użytkowników końcowych, służący do dystrybucji certyfikatów klucza publicznego oraz zapewnienia możliwości ich wiarygodnej weryfikacji
Osoba prawna	Osoba prawna w rozumieniu prawa krajowego lub inna jednostka o podobnym charakterze (jednostka organizacyjna nieposiadająca osobowości prawnej, spółka cywilna itd.)
Dokument tożsamości	Dokument tożsamości wydany w kraju członkowskim Unii Europejskiej (w tym Polskę) lub paszport wydany przez kraj nienależący do Unii Europejskiej.
Subskrybent	Osoba fizyczna bądź Osoba prawna, której wystawiono kwalifikowany certyfikat na podstawie niniejszej polityki certyfikacji (której dane są wpisane w certyfikacie jako dane właściciela certyfikatu). Osoba fizyczna bądź Osoba prawna, której wystawiono kwalifikowany znaczek czasu.
CPR	Centralny Punkt Rejestracji CenCert.
Punkt rejestracji	RA (Registration Authority) – Jednostka organizacyjna CenCert lub firma trzecia posiadająca umowę z Enigma – wykonująca, poprzez upoważnionych Inspektorów ds. rejestracji, czynności przewidziane do realizacji niniejszą polityką i procedurami pracy, zgodnie z uprawnieniami Inspektorów ds. rejestracji (np. potwierdzanie tożsamości osób ubiegających się o certyfikaty, przekazywanie kart elektronicznych z kluczami itd.)

Termin/akronim	Opis
DN	Identyfikator DN – <i>Distinguished Name</i> – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500.
NCCert	Root krajowego systemu PKI, prowadzony przez Narodowy Bank Polski, na podstawie upoważnienia właściwego ministra.
TSL	EU Trust service Status List – listy wydawane elektronicznie przez Komisję Europejską (lista list) oraz kraje członkowskie EU (w tym Polskę), zawierające informacje o podmiotach świadczących usługi zaufania, ich statusie (czy „kwalifikowany”) oraz dane umożliwiające weryfikację „tokenów” wystawianych przez podmioty świadczące usługi zaufania (czyli weryfikację kwalifikowanych certyfikatów, znaczników czasu itd.).
CRL	<i>Certificate Revocation List</i> - Lista unieważnionych certyfikatów, wystawiana, pieczętowana elektronicznie i publikowana przez CenCert.
OCSP	<i>Online Certificate Status Protocol</i> - usługi informowania o statusie unieważnienia certyfikatu, o który pyta osoba ufająca certyfikatowi.
Klucz prywatny	Dane służące do składania podpisu/pieczęci elektronicznej.
Klucz publiczny	Dane służące do weryfikacji podpisu/pieczęci elektronicznej, zazwyczaj dystrybuowane w postaci certyfikatu.
HSM	<i>Hardware Security Module</i> – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego do generowania podpisów/pieczęci elektronicznych (np. przy wystawianiu certyfikatów, list CRL).
QSCD	QSCD - <i>Qualified Signature Creation Device</i> (kwalifikowane urządzenie do składania podpisu elektronicznego) – urządzenie do składania podpisu elektronicznego lub pieczęci elektronicznej, które a) znajduje się na liście, o której mowa w art. 31.2 eIDAS, bądź b) uznane jest za takie na mocy art. 51.1 eIDAS.
rSeal	(remote seal). Pieczęć elektroniczna składana przez CenCert w imieniu właściciela certyfikatu.
rSign	(remote sign). Podpis elektroniczny składany przez CenCert w imieniu właściciela certyfikatu.
PSD2	Dyrektywa Parlamentu Europejskiego i Rady (UE) 2015/2366 z dnia 25 listopada 2015 r. w sprawie usług płatniczych w ramach rynku wewnętrznego, zmieniająca dyrektywy 2002/65/WE, 2009/110/WE, 2013/36/UE i rozporządzenie (UE) nr 1093/2010 oraz uchylająca dyrektywę 2007/64/WE

2. Zasady dystrybucji i publikacji informacji

CenCert publikuje następujące informacje:

1. Aktualny klucz/klucze publiczne CenCert (w postaci certyfikatów wystawionych przez NCCert).
2. Aktualną listę CRL
3. Archiwalne listy CRL.
4. Aktualne polityki certyfikacji, materiały marketingowe, komunikaty bieżące itd.

CenCert nie publikuje certyfikatów Subskrybentów. Archiwalne listy CRL są publikowane w postaci skompresowanych archiwów zawierających listy CRL z danego okresu.

Powyższe informacje dostępne są w repozytorium dostępnym pod adresem www.cencert.pl za pomocą protokołu HTTP/HTTPS.

3. Identyfikacja i uwierzytelnienie

Niniejszy rozdział opisuje zasady identyfikacji i uwierzytelnienia stosowane przez CenCert przy operacjach tego wymagających – w szczególności przy wystawianiu i zmianie statusu certyfikatów.

3.1. Struktura nazw przydzielanych Subskrybentom

Subskrybenci identyfikowani są w certyfikatach przy użyciu identyfikatorów wyróżniających (ang. Distinguished Names) zdefiniowanych w Zaleceniach ITU z serii X.500.

CenCert potwierdza tożsamość i wiarygodność informacji wpisywanych do certyfikatu, zgodnie z zapisami rozdz. 3.2, ale nie sprawdza praw do posługiwania się zastrzeżonymi znakami towarowymi (w szczególności praw patentowych), nie odpowiada za nieuprawnione wykorzystywanie znaków towarowych i nie jest stroną w przypadku tego typu sporów. W przypadku utraty przez Subskrybenta prawa do posługiwania się daną nazwą lub innym oznaczeniem zamieszczonym w certyfikacie, jest on zobowiązany do zgłoszenia tego faktu celem unieważnienia certyfikatu z powodu nieaktualności danych zawartych w certyfikacie.

3.1.1 Certyfikat do podpisu elektronicznego

3.1.1.1 Certyfikat do podpisu elektronicznego zawierający dane osobowe

Identyfikator wyróżniający Subskrybenta składa się z następujących atrybutów:

Kraj (countryName) = PL

Imię (givenName) = <imię lub imiona Subskrybenta>

Nazwisko (sureName) = <nazwisko Subskrybenta>

Numer seryjny (serialNumber) = <dotkowne dane identyfikujące Subskrybenta, np. PESEL, NIP albo nr dokumentu tożsamości>

Nazwa powszechna (commonName) = <nazwa Subskrybenta>

Numer seryjny może być zapisany w postaci zgodnej z ETSI EN 319 412-1. W takim przypadku odpowiednie rozszerzenie certyfikatu wskazuje zgodność z tą normą.

Nazwa powszechna może zawierać imię i nazwisko Subskrybenta lub jego nieformalne określenie - np. przyjazną formę imienia, pseudonim, przydomek, nazwisko zapisywane inaczej niż w dokumentach formalnych itd.

W przypadku Subskrybentów posiadających kilka imion, dopuszczalne jest wpisanie do certyfikatu tylko jednego imienia

Identyfikator DN może zawierać następujące opcjonalne atrybuty dodatkowe (pola mogą występować wielokrotnie):

Pozycja zawodowa (title)

Organizacja (organizationName)

Nazwa jednostki organizacyjnej (organizationalUnitName)

Adres (pola ze zbioru: postalAddress, localityName, stateOrProvinceName, postalCode)

Pozycja zawodowa może określać stanowisko zawodowe, ale także uprawnienia do wykonywania określonego zawodu (np. wraz z numerem uprawnień), upoważnienie do wykonywania określonych czynności.

Atrybut *Organizacja* zawiera nazwę podmiotu, z którym Subskrybent jest związany, zgodną z wpisem w odpowiednim rejestrze, ewidencji, statucie lub innym dokumencie tego typu, odpowiednim dla rodzaju podmiotu.

Atrybut *Nazwa jednostki organizacyjnej* zawiera nazwę jednostki organizacyjnej będącej częścią organizacji, której nazwa widnieje w atrybucie *Organizacja*.

Pola adresu zawierają dane adresowe służące do lepszej identyfikacji podmiotu, którego nazwa widnieje w atrybucie *Organizacja*. Nie musi to być kompletny adres pocztowy podmiotu.

3.1.1.2 Certyfikat do podpisu elektronicznego zawierający pseudonim

Identyfikator wyróżniający Subskrybenta składa się z następujących atrybutów:

Kraj (countryName) = <kraj>

Pseudonim (pseudonym) = <pseudonim>

Nazwa powszechna (commonName) = <pseudonim>

Pole *nazwa powszechna* ma taką samą zawartość, jak pole *pseudonim*.

Identyfikator DN może zawierać następujące opcjonalne atrybuty dodatkowe (pola mogą występować wielokrotnie):

Organizacja (organizationName)

Nazwa jednostki organizacyjnej (organizationalUnitName)

Adres (pola ze zbioru: postalAddress, localityName, stateOrProvinceName, postalCode)

Atrybut *Organizacja* zawiera nazwę podmiotu, z którym Subskrybent jest związany, zgodną z wpisem w odpowiednim rejestrze, ewidencji, statucie lub innym dokumencie tego typu, odpowiednim dla rodzaju podmiotu.

Atrybut *Nazwa jednostki organizacyjnej* zawiera nazwę jednostki organizacyjnej będącej częścią organizacji, której nazwa widnieje w atrybucie *Organizacja*.

Pola adresu zawierają dane adresowe służące do lepszej identyfikacji podmiotu, którego nazwa widnieje w atrybucie *Organizacja*. Nie musi to być kompletny adres pocztowy podmiotu.

3.1.2 Certyfikat do pieczęci elektronicznej

Identyfikator wyróżniający Subskrybenta składa się z następujących atrybutów:

Kraj (countryName) = PL

Organizacja (organizationName) = <oficjalna nazwa podmiotu>

Identyfikator organizacji (organizationIdentifier) = <identyfikator podmiotu>

Nazwa powszechna (commonName) = <nazwa podmiotu>

Pole *Organizacja* zawiera oficjalną nazwę organizacji, zgodną z wpisem w odpowiednim rejestrze, ewidencji, statucie lub innym dokumencie tego typu odpowiednim dla rodzaju podmiotu.

Identyfikator organizacji zawiera identyfikator organizacji (np. NIP), w postaci zgodnej z ETSI EN 319 412-1.

Nazwa powszechna powinna zawierać nazwę najczęściej używaną przez organizację. Nie musi być to nazwa oficjalna, zgodna z zapisem w rejestrze czy statucie.

Identyfikator DN może zawierać następujące opcjonalne atrybuty dodatkowe (pola mogą występować wielokrotnie):

Nazwa jednostki organizacyjnej (organizationalUnitName)

Adres (pola ze zbioru: postalAddress, localityName, stateOrProvinceName, postalCode)

Atrybut *Nazwa jednostki organizacyjnej* - zawiera nazwę jednostki organizacyjnej będącej częścią organizacji, której nazwa widnieje w atrybucie *Organizacja*.

Pola adresu zawierają dane adresowe służące do lepszej identyfikacji podmiotu, którego nazwa widnieje w atrybucie *Organizacja*. Nie musi to być kompletny adres pocztowy podmiotu.

3.1.3 Certyfikat do uwierzytelnienia stron WWW

Identyfikator wyróżniający Subskrybenta składa się z następujących atrybutów:

Kraj (countryName) = <kraj Subskrybenta>

localityName = <miasto Subskrybenta>

Imię (givenName) = <imię lub imiona Subskrybenta>

Nazwisko (sureName) = <nazwisko Subskrybenta>

albo

Organizacja (organizationName) = <oficjalna nazwa podmiotu>

Identyfikator organizacji (organizationIdentifier) = <identyfikator podmiotu>

Nazwa powszechna (commonName) = <nazwa/nazwy domen, którymi się posługuje Subskrybent>

Identyfikator DN może zawierać również inne atrybuty identyfikujące Subskrybenta (np. dodatkowe pola adresu pocztowego, nazwa jednostki organizacyjnej itd.)

Identyfikator organizacji jest zapisany w postaci zgodnej z ETSI EN 319 412-1.

3.2. Uwierzytelnienie Subskrybenta przy wystawieniu pierwszego certyfikatu

Sprawdzenie tożsamości **osoby fizycznej** ubiegającej się o certyfikat - dokonywane jest przez Inspektora ds. rejestracji lub notariusza na podstawie ważnego Dokumentu tożsamości lub na podstawie ważnego podpisu kwalifikowanego. Jeśli certyfikat ma zawierać dane organizacji, wymagane jest upoważnienie (chyba że umocowanie danej osoby w organizacji wynika ze statutu, zapisów rejestrowych organizacji itp.). Jeśli certyfikat ma zawierać specyficzne dane określające np. uprawnienia zawodowe, wymagany jest dokument potwierdzający uprawnienia.

Osoba lub osoby występujące w imieniu **Osoby prawnej** ubiegającej się o certyfikat muszą być uprawnione do reprezentacji danej Osoby prawnej zgodnie z zapisami odpowiedniego rejestru lub statutu organizacji, lub na podstawie pełnomocnictwa, wystawionego przez osoby uprawnione do reprezentacji. Sprawdzenie tożsamości osoby odbierającej certyfikat (jeśli klucze są generowane przez CenCert) albo składającej klucz publiczny do umieszczenia w certyfikacie – są dokonywane jest przez Inspektora ds. rejestracji na podstawie ważnego Dokumentu tożsamości lub na podstawie podpisu elektronicznego.

Jeśli certyfikat ma zawierać specyficzne informacje dotyczące określonych uprawnień Subskrybenta (np. pełnienia ról określonych w dyrektywie PSD2), uprawnienia są sprawdzane na podstawie odpowiednich dokumentów lub rejestrów.

Sprawdzenie informacji o adresach DNS domen umieszczanych w **certyfikacie do uwierzytelnienia witryn internetowych** jest dokonywane poprzez potwierdzenie faktu zarządzania domeną przez osobę składającą wniosek.

3.3. Uwierzytelnienie Subskrybenta przy wystawianiu kolejnych certyfikatów

W przypadku wystawienia kolejnego certyfikatu do podpisu elektronicznego, uwierzytelnienie może być wykonywane w sposób uproszczony, na podstawie podpisu kwalifikowanego złożonego przy użyciu ważnego, poprzedniego certyfikatu wystawionego przez CenCert. Nowy certyfikat zawiera te same dane identyfikujące Subskrybenta, co certyfikat poprzedni. Nie wykonuje się ponownego sprawdzenia prawa do użycia ewentualnych dodatkowych atrybutów certyfikatu (np. dane organizacji, uprawnienia zawodowe itd.).

Nie realizuje się uproszczonej procedury dla certyfikatów do pieczęci, ani dla certyfikatów do uwierzytelnienia witryn internetowych.

3.4. Sposoby uwierzytelnienia Subskrybenta przy zgłaszaniu żądania unieważnienia, zawieszenia i uchylenia zawieszenia certyfikatu

Unieważnienie lub zawieszenie certyfikatu do podpisu elektronicznego jest realizowane:

1. na stronie WWW CenCert, na podstawie imienia i nazwiska oraz hasła Subskrybenta, ustalonego przy wydawaniu certyfikatu albo
2. na podstawie wniosku podpisanego przez Subskrybenta.

Uchylenie zawieszenia certyfikatu do podpisu elektronicznego jest realizowane na podstawie wniosku podpisanego przez Subskrybenta.

Unieważnienie certyfikatu do podpisu elektronicznego, zawierającego dane organizacji, z którą jest związany Subskrybent, zostanie także zrealizowane na wniosek wystosowany przez tę organizację, podpisany przez osoby upoważnione.

Unieważnienie certyfikatu do pieczęci elektronicznych jest realizowane na wniosek wystosowany przez Subskrybenta (Osobę prawną), podpisany przez osobę upoważnioną.

Unieważnienie certyfikatu, zawierającego dane specyficzne dla PSD2, zostanie także zrealizowane na wniosek wystosowany przez uprawnioną instytucję sprawującą nadzór nad rynkiem finansowym.

Wniosek o zmianę statusu certyfikatu musi być dostarczony w postaci papierowego oryginału lub dokumentu elektronicznego podpisanego podpisem kwalifikowanym.

3.5. Zarządzanie uprawnieniami osób do składania pieczęci w trybie zdalnym

W ramach usługi składania kwalifikowanych pieczęci elektronicznych rSeal, CenCert składa pieczęcie w imieniu Subskrybenta, na zlecenie Subskrybenta, w ramach sesji pieczętowania inicjowanych przez jedną z upoważnionych przez Subskrybenta osób.

Każda sesja jest inicjowana z użyciem ważnego kwalifikowanego podpisu upoważnionej osoby. Osoba upoważniona ma również możliwość zakończenia aktywnej sesji pieczętowania.

Subskrybent może zarządzać danymi osobowymi osób uprawnionych do zarządzania sesjami, składając wnioski papierowe lub elektroniczne, podpisane przez upoważnioną osobę, zgodnie z danymi kontaktowymi zapisanymi w rozdziale 1.3.

CenCert gwarantuje realizację poprawnie złożonego wniosku (w tym podpisanego przez odpowiednią osobę/osoby) do końca następnego dnia roboczego po odebraniu wniosku.

4. Cykl życia certyfikatu – wymagania operacyjne

4.1. Wniosek o wystawienie certyfikatu

Zgłoszenie potrzeby wystawienia certyfikatu może złożyć osoba (podmiot) ubiegająca się o wystawienie certyfikatu lub podmiot finansujący realizację usługi, w dowolnej formie akceptowanej przez dany Punkt rejestracji. Taką rolę spełnia także umowa lub zamówienie na realizację usługi wystawienia certyfikatów, zawierające dane osób, którym mają być wystawione certyfikaty.

W przypadku, gdy dane osobowe do wystawienia certyfikatu są przekazane nie przez osobę, której dotyczą, podmiot przekazujący jest odpowiedzialny za uzyskanie zgody osoby, której dane dotyczą, na przekazanie danych osobowych w celu realizacji usługi zaufania.

Inspektor ds. rejestracji, dysponując danymi osoby ubiegającej się o certyfikat, przygotowuje wniosek o wystawienie certyfikatu oraz protokół przekazania. W przypadku gdy wystawienie certyfikatu nie wiąże się z przekazaniem karty procesorowej, wniosek o wystawienie certyfikatu może być także przygotowany i wysłany w inny sposób, bez udziału Inspektora ds. rejestracji.

Wniosek zawiera informację o warunkach realizacji usługi zaufania, w tym ograniczeniach odpowiedzialności CenCert – poprzez wskazanie na obowiązującą wersję *Polityki kwalifikowanych usług zaufania*. Wniosek zawiera także wymagane informacje oraz zgody osoby ubiegającej się o certyfikat – w szczególności informacje i zgody wymagane przez przepisy o ochronie danych osobowych oraz potwierdzenie przyporządkowania danych służących do weryfikacji podpisu elektronicznego, które są zawarte w wydanym certyfikacie.

W przypadku certyfikatu do pieczęci elektronicznej – wniosek zawiera wskazanie (imię, nazwisko, numer dokumentu tożsamości) osoby uprawnionej do odbioru klucza do składania pieczęci i/lub danych aktywujących klucz.

W przypadku jednoczesnego zakupu certyfikatu do podpisu i pieczęci elektronicznej, na tej samej karcie QSCD:

- 1) We wniosku o wystawienie certyfikatu, jako osoba uprawniona do odbioru karty QSCD z kluczami do generowania pieczęci, musi być wskazana osoba nabywająca certyfikat do podpisu elektronicznego (to musi być ta sama osoba).

- 2) Inspektor generuje na tej samej karcie - parę kluczy do realizacji podpisu oraz parę kluczy do realizacji pieczęci.

W przypadku wystawienia kwalifikowanego certyfikatu do kwalifikowanego podpisu/pieczęci elektronicznej na podstawie klucza publicznego wygenerowanego przez Subskrybenta, CenCert potwierdza posiadanie certyfikatu QSCD przez urządzenie posiadane przez Subskrybenta. Do wniosku o wystawienie certyfikatu dołączany jest klucz publiczny oraz odpowiednie dokumenty (w tym certyfikat SSCD/QSCD urządzenia oraz oświadczenia Subskrybenta).

4.2. Przetwarzanie wniosku

Wniosek o wystawienie certyfikatu może być przetwarzany w postaci papierowej lub elektronicznej.

Wniosek o wystawienie certyfikatu do podpisu elektronicznego w postaci papierowej jest podpisywany przez osobę ubiegającą się o wystawienie certyfikatu w obecności Inspektora ds. rejestracji lub notariusza. Wniosek w postaci elektronicznej jest podpisywany przez osobę ubiegającą się o wystawienie certyfikatu (wymagany jest podpis kwalifikowany), przy użyciu już posiadanego przez tę osobę certyfikatu kwalifikowanego.

4.3. Wystawienie certyfikatu

Podpisany wniosek o wystawienie certyfikatu jest zatwierdzany do realizacji przez Inspektora ds. rejestracji posiadającego uprawnienie do generowania certyfikatów. W przypadku gdy jest możliwa automatyczna weryfikacja poprawności wniosku (wyłącznie wnioski w postaci elektronicznej), wniosek może być zatwierdzony przez system komputerowy CenCert. Po zatwierdzeniu wniosku generowany jest certyfikat.

Po zatwierdzeniu wniosku o wystawienie certyfikatu:

- 1) Wystawiany jest kwalifikowany certyfikat, który zostaje wysłany do Subskrybenta lub udostępniony mu w inny sposób.
- 2) W przypadku podpisu lub pieczęci „na karcie” - wysyłany jest do Subskrybenta kod transportowy umożliwiający aktywowanie karty (plik z kodem transportowym zawiera także certyfikat).
- 3) W przypadku pieczęci rSeal - wysyłany jest do Subskrybenta certyfikat oraz PIN do danych aktywujących klucz do składania pieczęci.

Aktywacja karty procesorowej jest procesem jednorazowym i nieodwracalnym. Przed aktywacją karty, nie jest możliwe użycie zapisanych na niej kluczy do realizacji podpisu bądź pieczęci elektronicznej. Otrzymując kartę elektroniczną w postaci nieaktywnej, Subskrybent ma pewność że zapisane na niej klucze nie zostały wcześniej użyte.

4.4. Akceptacja certyfikatu

Do sprawdzenia i akceptacji certyfikatu zobowiązany jest Subskrybent niezwłocznie po otrzymaniu certyfikatu, a przed jego użyciem (w szczególności przed wykonaniem pierwszego podpisu weryfikowanego przy użyciu tego certyfikatu). W przypadku nieprawdziwości danych zawartych w certyfikacie (w szczególności danych identyfikacyjnych Subskrybenta lub danych osoby lub organizacji, której dane są także zawarte w certyfikacie Subskrybenta) Subskrybent jest zobowiązany do niezwłocznego poinformowania CenCert, zgodnie z procedurami obowiązującymi przy unieważnianiu certyfikatów, w celu unieważnienia certyfikatu i otrzymania nowego, zawierającego poprawne dane.

Posługiwanie się certyfikatem zawierającym nieprawdziwe dane naraża Subskrybenta na odpowiedzialność karną.

4.5. Korzystanie z pary kluczy i certyfikatu

4.5.1 Korzystanie z certyfikatu

Certyfikaty Subskrybentów mogą być wykorzystywane wyłącznie do weryfikowania podpisów lub pieczęci elektronicznych, lub uwierzytelnienia domen internetowych, zgodnie z niniejszą polityką certyfikacji, z uwzględnieniem ewentualnych ograniczeń zapisanych w certyfikacie.

Jedynym sposobem potwierdzenia ważności certyfikatu Subskrybenta pod kątem ewentualnego unieważnienia bądź zawieszenia, jest sprawdzenie statusu certyfikatu na odpowiedniej liście CRL albo za pomocą usługi OCSP.

Z faktu nieukazania się w określonym czasie nowej listy CRL nie można wnioskować o braku unieważnień certyfikatów.

4.5.2 Korzystanie z klucza prywatnego

Klucz prywatny związany z certyfikatem Subskrybenta może służyć wyłącznie do celów wynikających z zastosowań zapisanych w związanym z nim certyfikacie.

Klucz prywatny do podpisu elektronicznego powinien pozostawać w wyłącznej dyspozycji Subskrybenta – osoby fizycznej, której dane są umieszczone w certyfikacie. Nie jest dopuszczalne, aby kluczem tym posługiwała się inna osoba.

Klucz prywatny do pieczęci elektronicznej powinien pozostawać w wyłącznej dyspozycji osoby lub osób upoważnionych przez daną organizację Osobę prawną.

W przypadku usług rSign i rSeal - klucz prywatny do składania podpisu lub pieczęci jest przechowywany na HSM CenCert i jest używany przez CenCert wyłącznie do składania podpisu lub pieczęci w imieniu Subskrybenta, na jego zlecenie.

W przypadku powzięcia uzasadnionego podejrzenia, że dostęp do klucza prywatnego ma osoba nieupoważniona, Subskrybent powinien natychmiast unieważnić związany z tym kluczem certyfikat (a jeśli z kluczem było związane kilka certyfikatów – unieważnione powinny być wszystkie certyfikaty).

Podanie kodu PIN do karty elektronicznej zawierającej klucze służące do składania kwalifikowanych podpisów lub pieczęci, może się odbywać jedynie w bezpiecznym środowisku – to jest na komputerze, do którego dostęp mają jedynie osoby zaufane przez Subskrybenta, zabezpieczonym przed wszelkiego rodzaju niebezpiecznym oprogramowaniem, przy użyciu w szczególności odpowiednich programów antywirusowych oraz zapory firewall.

Warunki użycia karty elektronicznej do składania podpisów/pieczęci:

- W każdym przypadku gdy jest wymagane uwierzytelnianie przed złożeniem podpisu elektronicznego, kod PIN osoby podpisującej powinien być przesłany do karty elektronicznej przez zaufany kanał (secure messaging) ustanowiony pomiędzy aplikacją do tworzenia podpisu a kartą inteligentną.
- Zmiana kodu PIN powinna być wykonywana pod wyłączną kontrolą właściciela karty (podpisującego) i za pośrednictwem bezpiecznego kanału (secure messaging) pomiędzy aplikacją do tworzenia podpisu, a kartą inteligentną.
- Podpis elektroniczny może być wykonywany wyłącznie pod wyłączną kontrolą subskrybenta, który powinien się upewnić, że dane, które mają być podpisane, pochodzą z aplikacji do tworzenia podpisu.
- Dane, które mają zostać podpisane, powinny być wysyłane na kartę inteligentną za pośrednictwem zaufanego kanału (secure messaging) utworzonego pomiędzy aplikacją do tworzenia podpisu a kartą elektroniczną, z zapewnieniem uwierzytelnienia podpisującego.

W przypadku, gdy karta elektroniczna Subskrybenta zawiera, poza danymi służącymi do składania kwalifikowanych podpisów, również inne dane, w szczególności inne klucze prywatne (np. klucz do szyfrowania poczty, klucz do logowania do systemu operacyjnego itd.), karta powinna być tak zorganizowana, aby w celu wykonania podpisu kwalifikowanego karta wymagała podania oddzielnego kodu PIN. Kod PIN do składania podpisów/pieczęci

kwalfikowanych powinien mieć inną wartość niż kody uruchamiające inne usługi dostępne przy użyciu karty.

W przypadku używania do składania podpisów lub pieczęci urządzenia HSM posiadanego przez Subskrybenta, dane aktywujące klucz do podpisywania (np. PIN, hasło lub karty aktywujące), muszą być przechowywane w bezpieczny sposób, z zabezpieczeniem poufności, oraz wprowadzane do urządzenia HSM w sposób przewidziany w dokumentacji (w szczególności dokumentacji certyfikacyjnej) danego urządzenia HSM.

W przypadku usług rSign i rSeal, na Subskrybencie spoczywają następujące obowiązki:

- Zapewnia poufność danych aktywujących klucz prywatny do podpisywania, otrzymanych od CenCert.
 - W szczególności: W ramach sesji składania podpisu/pieczęci w trybie zdalnym, dane aktywujące klucz są przekazywane do serwera CenCert świadczącego usługę rSign/rSeal. Przed przekazaniem danych aktywujących, aplikacja Subskrybenta musi potwierdzić nawiązanie zabezpieczonego kanału transmisji (TLS) z serwerem CenCert oraz poprawnie zidentyfikować serwer CenCert na podstawie certyfikatu SSL/TLS. Właściwy certyfikat serwera CenCert świadczącego usługę składania pieczęci opublikowany jest na stronie <https://www.cencert.pl>.
- Używa wiarygodnej aplikacji do składania podpisu/pieczęci, która:
 - generuje skrót kryptograficzny danych prezentowanych jako dane przeznaczone do podpisania (które zamierza podpisać), w formie odpowiedniej dla usługi rSign/rSeal ;
 - dołącza do podpisywanych danych podpis/pieczęć wytworzoną przez usługę rSign/rSeal lub udostępnia podpis/pieczęć oddzielnie od danych.
- Zapewnia, że bezpieczeństwo oraz integralność elementów systemu służącego do składania podpisu/pieczęci, znajdujących się po stronie Subskrybenta (tzn. poza CenCert), jest utrzymywana w całości pod jego kontrolą.
- Zapewnia, że aplikacja do składania podpisu/pieczęci, znajdująca się po stronie Subskrybenta (poza CenCert), zapewnia poufność, integralność i autentyczność danych przesyłanych pomiędzy użytkownikiem końcowym i tą aplikacją (w tym w szczególności poufność wszelkich wrażliwych danych uwierzytelniających oraz integralność i autentyczność skrótu kryptograficznego z danych do podpisania).
- Zapewnia zgodność z dokumentem opisanym w rozdziale 9.16 odpowiednio dla usługi rSign lub rSeal.

4.6. Wymiana certyfikatu

Dopuszcza się wymianę ważnego certyfikatu kwalifikowanego bez zmiany klucza prywatnego Subskrybenta – o ile bezpieczeństwo kryptograficzne klucza jest wciąż wystarczające dla nowego okresu ważności certyfikatu.

Wymiana (odnowienie) certyfikatu następuje z inicjatywy Subskrybenta. Centrum Certyfikacji, w miarę możliwości będzie informowało Subskrybenta, przed upływem terminu ważności certyfikatu, o konieczności jego wymiany, przy użyciu dostępnych danych kontaktowych.

4.7. Wymiana certyfikatu połączona z wymianą pary kluczy

Wymiana certyfikatu połączona z wymianą pary kluczy jest możliwa przy spełnieniu wymagań rozdziału 3.2.

Wymiana (odnowienie) certyfikatu następuje z inicjatywy Subskrybenta. Centrum Certyfikacji, w miarę możliwości będzie informowało Subskrybenta, przed upływem terminu ważności certyfikatu, o konieczności jego wymiany, przy użyciu dostępnych danych kontaktowych.

4.8. Zmiana treści certyfikatu

Zmiana treści certyfikatu wymaga wystawienia nowego certyfikatu, zawierającego nową treść. Dotychczasowy certyfikat – o ile dane w nim zawarte stały się nieaktualne i zawierają nieprawdziwą informację o Subskrybencie – jest unieważniany.

Za zgłoszenie potrzeby aktualizacji danych zawartych w certyfikacie oraz za określenie, czy zmiana danych pociąga za sobą konieczność unieważnienia certyfikatu dotychczasowego, odpowiedzialny jest Subskrybent.

Dopuszcza się zmianę treści certyfikatu przez CenCert (to jest wystawienie nowego certyfikatu i unieważnienie starego) bez ponownego uwierzytelnienia subskrybenta, dla tego samego klucza publicznego, w przypadku poprawek oczywistych omyłek pisarskich lub błędów

technicznych certyfikatu. O poprawieniu certyfikatu niezwłocznie informowany jest Subskrybent.

4.9. Unieważnienie i zawieszenie certyfikatu

Podmiotem uprawnionym do unieważnienia certyfikatu jest:

- Subskrybent.
- Organizacja, której dane umieszczono w certyfikacie do podpisu elektronicznego.
- Dla certyfikatów zawierających dane specyficzne dla PSD2 - instytucja sprawująca nadzór nad rynkiem finansowym, której dane zapisano w certyfikacie.
- CenCert.

Certyfikat może być unieważniony wyłącznie przed datą końca jego okresu ważności. Unieważnienie certyfikatu jest nieodwracalne – unieważniony certyfikat nie może się stać ponownie ważny.

Subskrybent oraz organizacja, którego dane umieszczono w certyfikacie do podpisu elektronicznego, ma prawo unieważnić certyfikat z dowolnej przyczyny.

Subskrybent certyfikatu jest zobowiązany do niezwłocznego unieważnienia certyfikatu gdy:

- utracił wyłączną kontrolę nad kluczem prywatnym związanym z certyfikatem (np. utracił kartę elektroniczną lub została ona zniszczona, zablokowana itd.),
- dane zawarte w certyfikacie są nieprawidłowe lub nieaktualne.

Organizacja, której dane umieszczono w certyfikacie do podpisu elektronicznego, jest zobowiązana do niezwłocznego unieważnienia certyfikatu gdy:

- dane podmiotu zawarte w certyfikacie są nieprawidłowe lub nieaktualne,
- ustała okoliczność uzasadniająca zamieszczenie danych organizacji w certyfikacie Subskrybenta (np. zwolnienie pracownika, zmiana zakresu obowiązków itd.).

CenCert ma prawo do zmiany statusu certyfikatu jedynie w uzasadnionych przypadkach.

Centrum Certyfikacji zapewnia możliwość zgłoszenia żądania unieważnienia, zawieszenia bądź uchylecia zawieszenia certyfikatu w trybie 365/24/7.

W przypadku zawieszenia certyfikatu – okres zawieszenia trwa maksymalnie 7 dni, po czym certyfikat jest automatycznie unieważniany.

Zgodnie z artykułami 28.5, 38.5 of eIDAS, okres zawieszenia certyfikatu jest czytelnie oznaczony w bazach danych CenCert, a status zawieszenia jest widoczny poprzez listy CRL i tokeny OCSP publikowane w okresie zawieszenia.

Zgodnie z art. 24.3 eIDAS - jeżeli Centrum Certyfikacji postanowi unieważnić certyfikat, rejestruje ono takie unieważnienie w swojej bazie danych dotyczącej certyfikatów i publikuje informację o statusie unieważnienia certyfikatu w odpowiednim czasie, ale w każdym razie w ciągu 24 godzin po otrzymaniu wniosku. Unieważnienie staje się skuteczne natychmiast po jego opublikowaniu.

Procedury związane ze zmianą statusu certyfikatu znajdują się na stronach WWW CenCert.

W przypadku unieważnienia bądź zawieszenia certyfikatu na podstawie hasła Subskrybenta – operacja jest wykonywana na portalu WWW CenCert, którego dane znajdują się w rozdziale 1.3.

Subskrybent jest niezwłocznie informowany o zmianie statusu certyfikatu za pośrednictwem poczty elektronicznej.

4.10. Usługi informowania o statusie certyfikatów

Centrum Certyfikacji informuje o statusie certyfikatów poprzez listę CRL oraz usługę OCSP. Lista CRL jest wystawiana co najmniej raz na 24 godziny.

W celu zbadania statusu unieważnienia certyfikatu należy:

- pobrać token OCSP dla tego certyfikatu i sprawdzić status certyfikatu zapisany w tym tokenie, albo
- pobrać listę CRL wydaną po momencie, na który badamy ważność certyfikatu i sprawdzić status certyfikatu na CRL.

Ważność podpisów pod tokenem OCSP oraz listą CRL należy sprawdzać w oparciu o bieżącą listę TSL.

Odpowiedzi OCSP i listy CRL zawierają prawidłowe informacje o unieważnieniach nawet po upływie okresu ważności certyfikatu.

Centrum Certyfikacji publikuje archiwalne listy CRL, najpóźniej po zakończeniu ważności klucza, którym zostały podpisane.

4.11. Zakończenie realizacji usługi zaufania dla Subskrybenta

Jeśli nie określono inaczej – relacja pomiędzy CenCert a Subskrybentem bądź podmiotem finansującym, dotycząca realizacji przez CenCert usługi zaufania, kończy się wraz z upływem terminu ważności określonego w certyfikacie. W przypadku znakowania czasem – w terminie 24 miesięcy po wystawieniu znacznika czasu.

W przypadku świadczenia usługi składania pieczęci w imieniu subskrybenta, usługa przestaje być świadczona niezwłocznie po zakończeniu ważności certyfikatu (unieważnienie bądź upływ terminu ważności).

4.12. Powierzenie i odtwarzanie kluczy prywatnych

Centrum Certyfikacji nie powierza swojego klucza prywatnego innym podmiotom.

W przypadku usług rSign/rSeal, Subskrybent powierza CenCert swój klucz prywatny. Powierzony klucz nie jest przez CenCert przekazywany nikomu - w tym nie może być przekazany Subskrybentowi.

5. Zabezpieczenia organizacyjne, operacyjne i fizyczne

5.1. Zabezpieczenia fizyczne

Serwery CenCert znajdują się w klimatyzowanych serwerowniach, zabezpieczonych przed zalaniem, wyposażonych w system ochrony przed pożarem, zanikami zasilania, a także w system kontroli dostępu oraz system alarmowy włamania i napadu.

Fizyczny dostęp do urządzeń serwerowych CenCert (w tym urządzeń HSM) jest możliwy tylko dla upoważnionych osób, przy zachowaniu zasady dostępu dwuosobowego, pod kontrolą Inspektora bezpieczeństwa CenCert. Każdorazowy fakt dostępu do urządzeń jest odnotowywany.

Centrum Certyfikacji jest wyposażone w centrum zapasowe, umiejscowione w lokalizacji oddalonej od centrum podstawowego.

Wszelkie dane i urządzenia istotne dla bezpieczeństwa Centrum Certyfikacji i usług przez nie świadczonych (w szczególności karty elektroniczne i inne elementy sprzętowe pozwalające na aktywację klucza prywatnego CenCert, kody dostępu do urządzeń, kart i systemów, nośniki archiwizacyjne) są zabezpieczone i dostępne tylko dla osób upoważnionych.

5.2. Zabezpieczenia proceduralne

W Centrum Certyfikacji występują następujące funkcje mające bezpośredni wpływ na realizację usług certyfikacyjnych:

Nazwa funkcji	Rodzaj obowiązków
Administrator systemu	Konfigurowanie systemu CenCert w zakresie polityki certyfikacji, zarządzanie uprawnieniami dla operatorów systemu. Zarządzanie infrastrukturą IT, wykonywanie kopii zapasowych.
Operator systemu	Nadzór nad systemem teleinformatycznym, zarządzanie uprawnieniami (w tym certyfikatami) Inspektorów ds. rejestracji

Nazwa funkcji	Rodzaj obowiązków
Inspektor ds. rejestracji	Weryfikacja tożsamości Subskrybentów, wydawanie dyspozycji wydawania certyfikatów Subskrybentów, unieważnianie certyfikatów Subskrybentów
Inspektor ds. audytu	Analizowanie zapisów rejestrów zdarzeń w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
Inspektor ds. bezpieczeństwa	Nadzór nad wdrożeniem i stosowaniem wszystkich procedur bezpiecznej eksploatacji przy świadczeniu usług certyfikacyjnych, nadzór nad dostępem fizycznych do urządzeń chronionych.

Co do zasady – każdy Inspektor ds. rejestracji jest również Inspektorem ds. unieważniania.

Funkcja Inspektora ds. bezpieczeństwa nie może być łączona z funkcją Administratora Systemu ani z funkcją Operatora Systemu. Funkcja Inspektora ds. audytu nie może być łączona z żadną z pozostałych wymienionych funkcji.

Osoby pełniące funkcje Inspektorów ds. rejestracji mogą posiadać różnego rodzaju uprawnienia zawierające się w pełnych uprawnieniach Inspektora ds. rejestracji. W szczególności niektóre osoby pełniące tę rolę mogą mieć prawo jedynie do potwierdzania tożsamości Subskrybenta lub tylko prawo do unieważniania certyfikatów.

5.3. Zabezpieczenia osobowe

Wszystkie osoby pełniące co najmniej jedną z funkcji wymienionych w rozdz. 5.2 spełniają następujące wymagania:

- posiadają pełną zdolność do czynności prawnych,
- posiadają niezbędną dla pracy na danym stanowisku wiedzę i umiejętności w zakresie technologii realizacji usług certyfikacyjnych świadczonych przez Centrum Certyfikacji.

Wszystkie osoby pełniące wymienione funkcje, przed dopuszczeniem do wykonywania obowiązków, są szkolone w zakresie odpowiednim dla określonego stanowiska pracy, w tym w zakresie procedur i regulaminów pracy obowiązujących w CenCert oraz odpowiedzialności karnej związanej ze świadczeniem usług certyfikacyjnych.

W przypadku gdy określoną funkcję pełni osoba pracująca na innych zasadach niż umowa o pracę z Enigma, Enigma zawiera umowę z tą osobą lub z firmą, w której jest ona zatrudniona, określającą zasady odpowiedzialności. W przypadku osób zatrudnionych w Enigma na podstawie umowy o pracę, odpowiedzialność tej osoby regulowana jest obowiązującymi przepisami Kodeksu pracy.

Niezależnie od ewentualnej odpowiedzialności finansowej, osoby wykonujące nierzetelnie swoje obowiązki związane ze świadczeniem usług certyfikacyjnych lub nieprzestrzegające wymagań nałożonych przez przepisy o usługach zaufania (w szczególności wymagań o poufności, wymagań w zakresie wystawiania i unieważniania certyfikatów) podlegają sankcjom karnym określonym w Ustawie.

5.4. Procedury tworzenia logów audytowych

Centrum Certyfikacji zapewnia rejestrowanie wszelkich istotnych zdarzeń związanych z realizacją świadczonych przez siebie usług certyfikacyjnych.

Logi są zabezpieczone przed modyfikacją i są archiwizowane.

Logi są przechowywane przez 3 lata od daty ich wytworzenia.

5.5. Archiwizacja zapisów

Centrum Certyfikacji archiwizuje następujące zapisy papierowe i elektroniczne związane ze świadczeniem usług:

- podpisane przez Subskrybentów wnioski o wystawienie certyfikatu,
- wystawione certyfikaty oraz listy CRL,
- żądania unieważnienia kwalifikowanego certyfikatu,
- politykę świadczenia usług

- przez 20 lat od ich wytworzenia.

5.6. Wymiana pary kluczy Centrum Certyfikacji

Wygenerowanie i wymiana pary kluczy Centrum Certyfikacji może następować w planowych terminach lub wcześniej.

Planowa wymiana pary kluczy CenCert następuje:

- nie wcześniej niż na 8 lat i nie później niż na 6 lat przed upływem ważności aktualnej pary kluczy – dla kluczy RSA 4096 oraz ECDSA 256, ważnych 11 lat.

5.7. Utrata poufności klucza prywatnego i działanie w przypadku katastrof

5.7.1 Utrata poufności klucza prywatnego

CenCert posiada odpowiednie procedury obowiązujące w wypadku utraty poufności klucza prywatnego CenCert lub uzasadnionego podejrzenia zajścia takiego zdarzenia.

W przypadku kompromitacji klucza, procedury te przewidują w szczególności:

1. Zgłoszenie incydentu zgodnie z eIDAS, poinformowanie Subskrybentów o zaistniałej sytuacji oraz o planie dalszego działania.
2. Wytworzenie nowych kluczy CenCert i zgłoszenie ich odpowiedniemu ministrowi w celu wystawienia nowego certyfikatu NCCert oraz umieszczenia na liście TSL.
3. Jeśli to będzie w danej sytuacji możliwe (w szczególności bazy danych CenCert pozostaną wiarygodne) – wystawienie nowych certyfikatów Subskrybentów na posiadane przez Subskrybentów klucze, w oparciu o nowe klucze CenCert, z okresami ważności co najmniej takimi samymi, jakie miały unieważnione certyfikaty.

W przypadku utraty poufności kluczy prywatnych powierzonych przez Subskrybentów (usługa pieczęci w trybie zdalnym), CenCert niezwłocznie unieważnia certyfikaty kluczy oraz informuje o sytuacji Subskrybentów.

5.7.2 Osłabienie algorytmów kryptograficznych

W przypadku, gdy okaże się, że używane przez CA lub Subskrybentów algorytmy kryptograficzne lub ich parametry są niewystarczające dla zamierzonego okresu ich użytkowania, CA poinformuje wszystkich Subskrybentów oraz udostępni taką informację publicznie oraz zaplanuje unieważnienie dotkniętych tym certyfikatów. Jeśli to będzie możliwe, certyfikaty będą wymienione na inne, z użyciem nowych algorytmów kryptograficznych i/lub ich parametrów.

5.7.3 Katastrofy

Centrum Certyfikacji posiada plany ciągłości działania, przewidujące w szczególności niedostępność i brak możliwości funkcjonowania Centrum Podstawowego i/lub Centralnego Punktu Rejestracji i/lub wyłączenie repozytorium lub serwera usług OCSP.

5.8. Zakończenie działalności

W przypadku zamiaru zakończenia działalności w zakresie kwalifikowanych usług zaufania, Zarząd Spółki podejmie starania w celu przejęcia tej działalności przez innego kwalifikowanego dostawcę tych usług. Jeśli osiągnięcie takiego porozumienia nie okaże się możliwe, Zarząd Spółki podejmie decyzję o planowym zakończeniu działalności CenCert.

O planowanym zakończeniu działalności niezwłocznie informowany jest organ rządowy sprawujący nadzór nad świadczeniem usług zaufania, z co najmniej 3-miesięcznym wyprzedzeniem.

O planowanym zakończeniu działalności informowani są także:

- Subskrybenci – w terminie umożliwiającym im nabycie nowych certyfikatów u innego kwalifikowanego dostawcy usług zaufania oraz
- podmioty współpracujące przy realizacji przez CenCert usług zaufania (w tym prowadzące Punkty rejestracji) – w terminie zgodnym z zawartymi umowami.

W okresie kończenia działalności, CenCert wypowie wszystkie upoważnienia do działania w jego imieniu (w szczególności w zakresie obsługi Punktów Rejestracji)

Po zakończeniu działalności wszystkie wystawione certyfikaty (będące jeszcze w okresie ważności) są unieważniane, a po wystawieniu ostatniej listy CRL klucz prywatny CA jest niszczone.

Dokumenty i zapisy, co do których jest wymagana archiwizacja, są przekazywane po zakończeniu działalności podmiotowi wskazanemu przez organ rządowy sprawujący nadzór nad świadczeniem usług zaufania.

W przypadku zakończenia realizacji tylko jednej z kwalifikowanych usług zaufania (i utrzymania świadczenia pozostałej kwalifikowanej usługi) zapisy powyższe stosuje się odpowiednio.

6. Zabezpieczenia techniczne

6.1. Generowanie i instalowanie par kluczy

6.1.1 Generowanie par kluczy

Pary kluczy Centrum Certyfikacji generowane są przez personel CPR zgodnie z udokumentowaną procedurą, przy obecności co najmniej dwóch osób pełniących funkcje związane z realizacją usług zaufania, w tym Inspektora ds. bezpieczeństwa. Z ceremonii generowania kluczy sporządza się protokół.

Klucze Inspektorów ds. Rejestracji służące do dostępu do systemu CenCert, są generowane samodzielnie przez inspektorów lub przez personel CPR, na karcie elektronicznej spełniającej wymagania QSCD.

Klucze Subskrybentów są generowane przez Inspektora ds. rejestracji lub przez Subskrybenta, dla certyfikatów do podpisów lub pieczęci kwalifikowanych - na karcie elektronicznej (lub HSM) spełniającej wymagania QSCD.

Klucze Subskrybentów dla usług rSign/rSeal są generowane przez system CenCert na urządzeniu HSM.

Przy generowaniu kluczy zastosowanie mają wszystkie wymagania wynikające z dokumentacji certyfikacyjnej danego urządzenia HSM (lub karty procesorowej). CenCert sprawdza spełnienie tych wymagań również w przypadku generowania kluczy na urządzeniu posiadanym przez Subskrybenta.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Karta elektroniczna, na której są zapisane klucze Subskrybenta, jest technicznie zabezpieczona w sposób umożliwiający złożenie podpisu elektronicznego wyłącznie po aktywacji karty poprzez wprowadzenie kodu transportowego. Kod transportowy jest dostarczany Subskrybentowi inną przesyłką niż karta. Aktywacja karty jest jednorazowa i nieodwracalna.

Karta elektroniczna jest dostarczona Subskrybentowi lub (w przypadku pieczęci –uprawnionej osobie) przez Inspektora ds. rejestracji, po weryfikacji tożsamości.

W przypadku usługi rSeal, osoba upoważniona przez Subskrybenta otrzymuje od Inspektora ds. rejestracji (osobiście), na nośniku wymiennym (np. pamięć USB), plik zawierający m.in. hasło zabezpieczające klucz prywatny („Passphrase”). Hasło to ma postać losowej liczby o

długości 128 bitów i jest zapisane w postaci zaszyfrowanej. Klucz do odszyfrowania hasła (również o długości 128 bitów) jest wysyłany przez serwer CenCert na adres mailowy osoby upoważnionej, po wystawieniu certyfikatu do składania pieczęci.

W przypadku usługi rSign, Subskrybent otrzymuje hasło zabezpieczające klucz prywatny („Passphrase”) zapisane, wraz z innymi danymi, w postaci QR-kodu na Wniosku o wystawienie certyfikatu. Hasło to ma postać losowej liczby o długości 128 bitów i jest zapisane w postaci zaszyfrowanej. Klucz do odszyfrowania hasła (również o długości 128 bitów) jest wysyłany przez serwer CenCert do aplikacji mobilnej Subskrybenta, po instalacji tego QR-kodu w aplikacji i po potwierdzeniu przez serwer CenCert, że nikt wcześniej nie uzyskał tego klucza (kod QR jest jednorazowy). Certyfikat do klucza prywatnego jest wystawiany dopiero po potwierdzeniu poprawnej instalacji danych w aplikacji mobilnej Subskrybenta na podstawie jednorazowego kodu, nie ma więc możliwości, żeby inna osoba posiadała kod dostępu do klucza prywatnego Subskrybenta.

6.1.3 Dostarczenie klucza publicznego Subskrybenta

W przypadku generowania certyfikatu do pieczęci kwalifikowanej na podstawie klucza publicznego, jest on dostarczany do CPR przez Inspektora ds. rejestracji albo Administratora systemu CenCert, obecnego przy generowaniu pary kluczy przez Subskrybenta na urządzeniu QSCD.

W przypadku generowania certyfikatu do pieczęci zaawansowanej lub uwierzytelnienia stron WWW, klucz publiczny jest dostarczany do CenCert w postaci podpisanej podpisem kwalifikowanym lub jest dostarczany razem z wnioskiem o wystawienie certyfikatu.

6.1.4 Dostarczenie klucza publicznego CenCert

Klucz publiczny Centrum Certyfikacji jest dostępny w postaci certyfikatu wystawionego przez NCCert oraz wpisu na listę krajową TSL.

Wskazanie na krajową listę TSL znajduje się na stronie WWW CenCert.

6.1.5 Parametry kryptograficzne kluczy

Klucze RSA Centrum Certyfikacji mają długość 4096 bitów, za wyjątkiem:

- kluczy wytworzonych w okresie obowiązywania wcześniejszych wersji polityki certyfikacji, które mogą mieć długość 2048 bitów.

Klucze ECDSA Centrum Certyfikacji mają długość 256 bitów.

Klucze Subskrybentów mają długość 2048 (klucze RSA) lub 256 (ECDSA) bitów.

Klucze infrastruktury:

- klucze RSA do ochrony komunikacji pomiędzy CenCert a punktami rejestracji mają długość 2048 bity lub większą, klucze ECDSA (jeśli występują), mają długość 256 bitów lub większą.
- klucze Inspektorów ds. rejestracji mają długość 2048 bitów (RSA).

Wszystkie klucze algorytmu ECDSA są generowane w dziedzinach krzywych eliptycznych określonych w normach NIST, wykorzystujących liczby pierwsze.

Do składania przez CenCert pieczęci (w tym do podpisywania certyfikatów oraz innych struktur danych wydawanych przez CenCert) są używane algorytmy skrótu z rodziny SHA-2.

6.1.6 Cel użycia klucza

Klucz prywatny Centrum Certyfikacji do pieczętowania certyfikatów - może być wykorzystywany tylko do pieczętowania certyfikatów i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów i list CRLi.

Klucz prywatny Centrum Certyfikacji do pieczętowania znaczników czasu - może być wykorzystywany tylko do tego celu. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania znaczników czasu.

Klucz prywatny Centrum Certyfikacji do pieczętowania tokenów OCSP - może być wykorzystywany tylko do tego celu. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania tokenów OCSP.

Klucze prywatne Subskrybentów mogą być używane wyłącznie do składania kwalifikowanych podpisów bądź pieczęci elektronicznych.

6.2. Ochrona kluczy prywatnych

Klucze prywatne Centrum Certyfikacji są generowane i przetwarzane w urządzeniach HSM posiadających jeden z certyfikatów:

- 1) Common Criteria (norma ISO/IEC 15408) dla poziomu EAL4 albo bezpieczniejszego,
- 2) FIPS PUB 140-2 dla poziomu 3 albo bezpieczniejszego.
- 3) QSCD

Niezależnie od powyższych wymagań, klucze prywatne Centrum Certyfikacji używane do świadczenia usług zaufania, wygenerowane na urządzeniach CompCrypt Delta-1R/2048 i

wprowadzone do użytku przed 1.05.2017, mogą być używane na tych urządzeniach do końca okresu ważności certyfikatów związanych z tymi kluczami, chyba że okaże się konieczne wcześniejsze wycofanie kluczy z użytku z powodu słabości stosowanego algorytmu kryptograficznego lub długości kluczy.

Klucze prywatne Subskrybentów do podpisów/pieczeni kwalifikowanych oraz klucze prywatne Inspektorów ds. rejestracji są generowane i przetwarzane na kartach elektronicznych lub HSM spełniających wymagania QSCD.

CenCert nie stawia żadnych wymagań na urządzenie (lub oprogramowanie) do generowania i przetwarzania kluczy prywatnych Subskrybentów do kwalifikowanych certyfikatów do pieczęci zaawansowanych (niekwalifikowanych) oraz kwalifikowanych certyfikatów do uwierzytelnienia witryn internetowych. Analiza ryzyka i wybór właściwych rozwiązań leży w takich przypadkach po stronie subskrybentów.

Kopie zapasowe kluczy prywatnych CenCert są tworzone, przy zachowaniu takich samych wymagań bezpieczeństwa, jak dla kluczy w oryginalnej lokalizacji tych kluczy.

Kopie zapasowe kluczy prywatnych Inspektorów ds. rejestracji nie są tworzone.

Kopie zapasowe kluczy prywatnych Subskrybentów używanych dla usług rSign/rSeal są tworzone w sposób zgodny z certyfikatem urządzenia HSM. Kopie zapasowe kluczy są przechowywane w zabezpieczonych pomieszczeniach i przechowywane maksymalnie 7 dni.

Klucze prywatne Subskrybentów ani Centrum Certyfikacji nie są archiwizowane.

Uaktywnienie kluczy Centrum Certyfikacji wymaga jednoczesnej obecności co najmniej dwóch uprawnionych osób.

Klucze prywatne Subskrybentów oraz Inspektorów ds. rejestracji przechowane na kartach QSCD są aktywowane kodem PIN. W przypadku usług rSign/rSeal klucze prywatne Subskrybentów są aktywowane za pomocą mechanizmów przewidzianych w dokumentacji certyfikacyjnej HSM.

Niszczenie kluczy prywatnych Subskrybentów i Inspektorów ds. rejestracji wykonywane jest przez posiadacza danej karty, poprzez logiczne usunięcie klucza z karty elektronicznej lub fizyczne zniszczenie karty. W przypadku usługi pieczęci w trybie zdalnym - niszczenie klucza odbywa się poprzez usunięcie zaszyfrowanego klucza z urządzenia HSM i miejsc przechowywania klucza w postaci zaszyfrowanej (w tym z kopii zapasowych).

Niszczenie kluczy prywatnych Centrum Certyfikacji, służących do realizacji usług zaufania, wykonywane jest komisyjnie zgodnie z udokumentowaną procedurą.

Centrum Certyfikacji nie nakłada formalnych wymagań na badania pod kątem ujawniającego ulotu elektromagnetycznego urządzeń lub pomieszczeń, w których są generowane i przetwarzane klucze CenCert, Inspektorów ds. rejestracji i Subskrybentów.

6.3. Inne aspekty zarządzania parą kluczy

Okres ważności certyfikatów Subskrybentów wynosi maksymalnie 5 lat.

Okres ważności certyfikatów Inspektorów ds. rejestracji jest nie dłuższy niż 2 lata.

Po unieważnieniu bądź przeterminowaniu ostatniego certyfikatu związanego z kluczem prywatnym dla usługi rSign lub rSeal, jest on niszczone (w tym usuwany z kopii zapasowych) w terminie 7 dni.

6.4. Dane aktywujące

CenCert przyjął i przestrzega udokumentowanych procedur postępowania z wszelkimi danymi aktywującymi. Ogólne zasady, na których zbudowane są szczegółowe procedury są następujące:

1. Uaktywnienie klucza CenCert wymaga jednoczesnej obecności co najmniej dwóch osób pełniących funkcje związane ze świadczeniem usług zaufania.
2. Wszelkie dane aktywujące powinny być zapamiętane lub zapisane w bezpieczny sposób przez osoby rutynowo je używające. Hasła są archiwizowane w zabezpieczony sposób.
3. Dane aktywujące potrzebne – choćby potencjalnie – w obu lokalizacjach (Centrum Podstawowe i Zapasowe), są zapisywane w dwóch kopiach i przechowywane w obu lokalizacjach.

Klucze prywatne Subskrybentów dla usług rSign/rSeal są przechowywane w trybie nieaktywnym, poza sesjami podpisywania/pieczetowania. Aktywacja klucza wymaga każdorazowo zainicjowania sesji składania pieczęci przez Subskrybenta, w tym: podania hasła zabezpieczającego klucz ("Passphrase"). W przypadku rSeal dodatkowo jest wymagane zatwierdzenie sesji podpisem kwalifikowanym jednej z osób upoważnionych przez Subskrybenta. Sesja składania pieczęci kończy się po upływie czasu, na który została ustanowiona lub w dowolnej chwili - na żądanie Subskrybenta. W przypadku rSign, uruchomienie sesji podpisywania wymaga użycia urządzenia mobilnego z aplikacją spełniającą warunki opisane w dokumencie wymienionym w rozdziale 9.16.

Hasło zabezpieczające klucz dla usług rSeal/rSign jest przekazywane Subskrybentowi przez CenCert przed wystawieniem certyfikatu. CenCert stosuje zabezpieczenia techniczne i proceduralne gwarantujące, że jedynym posiadaczem i dysponentem hasła zabezpieczającego klucz do składania podpisu/pieczęci jest Subskrybent. Utrata dostępu przez Subskrybenta do hasła oznacza techniczny brak możliwości składania podpisu/pieczęci (hasła nie da się odtworzyć ani odczytać z systemu CenCert).

6.5. Zabezpieczenia komputerów

Nie jest wymagane używanie przez Centrum Certyfikacji serwerów posiadających certyfikaty bezpieczeństwa na sprzęt lub oprogramowanie systemu operacyjnego.

Centrum Certyfikacji przeprowadza regularne testy podatności oraz testy penetracyjne używanego systemu informatycznego, nie rzadziej niż co 6 miesięcy. Wyniki testów nie są publikowane.

Wszystkie operacje przewidziane do wykonania na komputerach i serwerach Centrum Certyfikacji można wykonać po uprzednim uwierzytelnieniu się i kontroli uprawnień. Wykonywane operacje są zapisywane w dziennikach zdarzeń.

6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

W Centrum Certyfikacji przyjęto udokumentowaną procedurę dokonywania modyfikacji lub zmian 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.

Procedura gwarantuje testowanie nowych wersji oprogramowania w środowisku testowym. Do realizacji jakichkolwiek prac w środowisku testowym nie mogą być używane klucze prywatne CenCert służące do świadczenia usług zaufania.

6.7. Zabezpieczenia sieci komputerowej

Serwery wykorzystywane przez CenCert do świadczenia usług certyfikacyjnych zgodnie z niniejszą polityką certyfikacji są połączone za pomocą logicznie wydzielonej, dwusegmentowej sieci wewnętrznej, oddzielonej od sieci zewnętrznej zaporami firewall.

6.8. Znakowanie czasem

Do wydawania znaczników czasu, a także oznaczania czasem certyfikatów, zaświadczeń certyfikacyjnych, list CRL oraz zapisów w logach urządzeń i oprogramowania stosuje się wskazanie bieżącego czasu pochodzące z zegarów wbudowanych w urządzenia lub stacje robocze.

Zegary stacji roboczych są synchronizowane protokołem NTP z czasem UTC(pl) udostępnianym publicznie na serwerach Głównego Urzędu Miar.

Synchronizacja zapewnia dokładność czasu nie mniejszą niż 1s.

CenCert gwarantuje dostępność usługi znakowania czasem na poziomie 99,9% mierzonej w ujęciu rocznym.

Usługi znakowania czasem świadczone są w odpowiedzi na żądanie zawierające podpis zaawansowany podmiotu uprawnionego do otrzymania znacznika. CenCert, po uzgodnieniu z klientem, może udostępnić także inne metody uwierzytelnienia (np. login/hasło).

7. Profil certyfikatów, list CRL i tokenów OCSP

7.1. Profil certyfikatów i zaświadczeń

7.1.1 Nazwy wyróżniające (Distinguished Names)

Identyfikator DN związany ze świadczeniem usługi wystawiania kwalifikowanych certyfikatów do podpisu i pieczęci:

Kraj (countryName) = *PL*

Nazwa organizacji (organizationName) = *Enigma Systemy Ochrony Informacji Sp. z o.o.*

Nazwa powszechna (commonName) = *CenCert QTSP CA*

Identyfikator organizacji (organizationIdentifier) = *VATPL-5261029614*

Identyfikatory DN związane ze świadczeniem usługi wystawiania kwalifikowanych znaczników czasu:

Kraj (countryName) = *PL*

Nazwa organizacji (organizationName) = *Enigma Systemy Ochrony Informacji Sp. z o.o.*

Nazwa powszechna (commonName) = *CenCert QTSP TSA*

Identyfikator organizacji (organizationIdentifier) = *VATPL-5261029614*

Kraj (countryName) = *PL*

Nazwa organizacji (organizationName) = *Enigma Systemy Ochrony Informacji Sp. z o.o.*

Nazwa powszechna (commonName) = *CenCert QTSP TSA ECC*

Identyfikator organizacji (organizationIdentifier) = *VATPL-5261029614*

Identyfikatory DN związane ze świadczeniem usługi wystawiania kwalifikowanych certyfikatów do uwierzytelnienia stron internetowych:

Kraj (countryName) = *PL*

Nazwa organizacji (organizationName) = *Enigma Systemy Ochrony Informacji Sp. z o.o.*

Nazwa powszechna (commonName) = *CenCert QTSP WEB CA*

Identyfikator organizacji (organizationIdentifier) = *VATPL-5261029614*

Identyfikatory DN związane ze świadczeniem usług zaufania, dla kluczy wygenerowanych i zapisanych w krajowym TSL przed wejściem w życie niniejszej polityki:Kraj (countryName) = **PL**Nazwa organizacji (organizationName) = **ENIGMA SOI Sp. z o.o.**Nazwa powszechna (commonName) = **CenCert Centrum Certyfikatów Kwalifikowanych**Numer seryjny (serialNumber) = **Nr wpisu: 11**Kraj (countryName) = **PL**Nazwa organizacji (organizationName) = **ENIGMA SOI Sp. z o.o.**Nazwa powszechna (commonName) = **CenCert Centrum Kwalifikowanych Znaczników Czasu**Numer seryjny (serialNumber) = **Nr wpisu: 12****7.1.2 Profil certyfikatów subskrybentów**

Centrum Certyfikacji wystawia certyfikaty w formacie X.509 v.3, zgodnym ze standardem RFC 5280.

Numery wystawianych certyfikatów są pseudolosowe i unikalne w ramach Centrum certyfikacji. Unikalność numerów certyfikatów zapewnia oprogramowanie generujące certyfikaty wraz z używanymi bazami danych.

CenCert stosuje następujące identyfikatory usług kryptograficznych: sha256-with-RSA, sha384-with-RSA, sha512-with-RSA, sha1-with-RSA¹, sha256-with-ecdsa, sha384-with-ecdsa, sha512-with-ecdsa. Algorytm ECDSA jest używany i akceptowany dla dziedzin krzywych eliptycznych określonych w normach NIST.

Rozszerzenia kwalifikowanych certyfikatów Subskrybentów:

Rozszerzenie	Opis/wartość	krytyczne ?
<i>AuthorityKeyIdentifier</i>	skrót z klucza publicznego CA	NIE
<i>SubjectKeyIdentifier</i>	skrót z klucza publicznego Subskrybenta	NIE

¹ Algorytm SHA-1 jest używany jedynie w celu weryfikacji, w pieczęciach i podpisach wytworzonych przed 2 lipca 2018 r.

POLITYKA DLA KWALIFIKOWANYCH USŁUG ZAUFANIA

Rozszerzenie	Opis/wartość	krytyczne ?
<i>KeyUsage</i>	<p>nonRepudation – dla certyfikatów do podpisów i pieczęci</p> <p>digitalSignature, keyEnciphering – dla certyfikatów do uwierzytelnienia witryn internetowych</p>	TAK
<i>ExtendedKeyUsage</i>	<p>Tylko dla certyfikatów do uwierzytelnienia witryn internetowych:</p> <p>Server Authentication (1.3.6.1.5.5.7.3.1)</p> <p>Client Authentication (1.3.6.1.5.5.7.3.2)</p>	NIE
<i>CertificatePolicies</i>	<p>1) {1.3.6.1.4.1.10214.99.1.1.1.4}</p> <p>albo (tylko dla certyfikatów wystawianych przy użyciu kluczy CA wprowadzonych do użytku przed wejściem w życie niniejszej polityki)</p> <p>{1.2.616.1.113681.1.1.10.1.1.2}</p>	NIE
<i>basicConstraints</i>	<p>pusta sekwencja</p> <p>(określenie, że subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)</p>	TAK
<i>crlDistributionPoints</i>	zawiera lokalizacje aktualnego CRL	NIE
<i>qcStatement</i>	<p>esi4-qcStatement-1</p> <p>Deklaracja, że certyfikat jest kwalifikowany na obszarze UE</p> <p>id-etsi-qcs-QcCompliance {0.4.0.1862.1.1}</p>	NIE
<i>qcStatement</i>	<p>esi4-qcStatement-4</p> <p>deklaracja, że klucz prywatny związany z certyfikatem znajduje się w urządzeniu QSCD</p> <p>id-etsi-qcs-QcSSCD {0.4.0.1862.1.4}</p> <p>Nie występuje w certyfikatach do pieczęci zaawansowanych (niekwalifikowanych) oraz w certyfikatach do uwierzytelnienia witryn internetowych</p>	

Rozszerzenie	Opis/wartość	krytyczne ?
<i>qcStatement</i>	<p>esi4-qcStatement-6 deklaracja oznaczająca rodzaj certyfikatu</p> <p>id-etsi-qct-esign {0.4.0.1862.1.6.1} – dla certyfikatów do podpisu elektronicznego</p> <p>id-etsi-qct-eseal {0.4.0.1862.1.6.2} – dla certyfikatów do pieczęci elektronicznej</p> <p>id-etsi-qct-web {0.4.0.1862.1.6.3} – dla certyfikatów do uwierzytelnienia witryn internetowych</p>	
<i>qcStatement</i>	<p>esi4-qcStatement-5 Wskazanie (URL) na oświadczenia (PDS - <i>PKI Disclosure Statements</i>)</p> <p>id-etsi-qcs-QcPDS {0.4.0.1862.1.5}</p> <p>URL wskazujący na PDS</p>	
<i>qcStatement</i>	<p>id-etsi-qcs-semanticsId-Natural {0.4.0.194121.1.1}</p> <p>wskazuje zgodność budowy atrybutu serialNumber identyfikatora DN ze składnią i semantyką zdefiniowaną w ETSI EN 319 412-1 dla certyfikatów dla osób fizycznych</p>	NIE, rozszerzenie opcjonalne
<i>qcStatement</i>	<p>id-etsi-qcs-SemanticsId-Legal {0.4.0.194121.1.2}</p> <p>wskazuje zgodność budowy atrybutu organizationIdentifier identyfikatora DN ze składnią i semantyką zdefiniowaną w ETSI EN 319 412-1 dla certyfikatów dla osób prawnych</p>	NIE

Rozszerzenie	Opis/wartość	krytyczne ?
<i>qcStatement</i>	<p>Tylko dla certyfikatów wystawionych zgodnie z PSD2:</p> <p>etsi-psd2-qcStatement {0.4.0.19495.2}</p> <p>Oznaczenie instytucji nadzoru finansowego (NCAName, NCAId) oraz jedna lub więcej ról zdefiniowanych w PSD2, zgodnie z ETSI TS 119 495:</p> <ul style="list-style-type: none"> - PSP_AS id-psd2-role-asp-as {0.4.0.19495.1.1} - PSP_PI id-psd2-role-asp-pi {0.4.0.19495.1.2} - PSP_AI id-psd2-role-asp-ai {0.4.0.19495.1.3} - SP_IC id-psd2-role-asp-ic {0.4.0.19495.1.4} 	NIE
<i>Authority Information Access</i> –	<i>id-ad-caIssuers</i> wskazanie URL na położenie certyfikatu CA wystawionego przez NCCert (protokół HTTP)	NIE
<i>Authority Information Access</i> –	<i>id-ad-ocsp</i> wskazanie URL na serwer OCSP (protokół HTTP)	NIE, rozszerzenie opcjonalne

7.1.3 Certyfikaty do podpisywania tokenów OCSP, certyfikaty kluczy infrastruktury, oraz certyfikaty testowe

Certyfikaty do podpisywania tokenów OCSP posiadają rozszerzenia

- *keyUsage* -> digitalSignature - krytyczne
- *extendedKeyUsage* -> *id-kp-OCSPSigning* (patrz RFC 5280) – niekrytyczne
- *id-pkix-ocsp-nocheck* – niekrytyczne.

Certyfikaty kluczy infrastruktury (klucze dostępu do systemu Inspektorów ds. Rejestracji oraz klucze do ochrony komunikacji) nie są certyfikatami kwalifikowanymi – nie posiadają odpowiednich rozszerzeń QCStatements. Posiadają natomiast rozszerzenie ExtKeyUsage {1.3.6.1.4.1.10214.2.1.1.2} albo {1.3.6.1.4.1.10214.2.1.1.3} świadczące o tym, że są to certyfikaty infrastruktury używane wyłącznie w ramach systemu CenCert i nie mogą być używane poza tym systemem.

Certyfikaty testowe posiadają identyczną budowę jak certyfikaty produkcyjne, z tym że ich identyfikator DN jest zbudowany z pól „TEST” (ewentualnie „TEST TEST”, TEST2”, „TEST <znaki innych alfabetów>” itd.) we wszystkich miejscach przeznaczonych na dane tekstowe (imię, nazwisko, nazwa powszechna itd.) oraz przykładowych numerów (typu 1234...) w miejscach przeznaczonych na dane numeryczne (PESEL, NIP itd.).

7.2. Profil list CRL

Centrum Certyfikacji wystawia listy CRL w formacie zgodnym z Zaleceniem X.509:2000, wersja 2. formatu.

Do wykonania pieczęci Centrum Certyfikacji pod listami CRL wykorzystywany jest algorytm skrótu SHA-2. Do daty określonej Ustawą SHA-1 może być także używany algorytm SHA-1.

Rozszerzenia

Pole	Opis/wartość	krytyczne ?
<i>Extensions</i>		
<i>AuthorityKeyIdentifier</i>		NIE
<i>keyIdentifier</i>	skrót z klucza publicznego	
<i>cRLNumber</i>	numer kolejny listy CRL wystawionej w CenCert	NIE

Listy CRL mogą zawierać również inne rozszerzenia, oznaczone jako niekrytyczne.

7.3. Profil OCSP

Akceptowane są żądania zgodne z RFC 6960. Do przesłania treści żądania oraz pobrania odpowiedzi używany jest protokół HTTP.

Adres usługi OCSP zawarty jest w rozszerzeniu certyfikatu (patrz rozdz. 7.1.2). Dla niezawierających tego rozszerzenia, obowiązują następujące adresy udostępniania usług OCSP:

- <http://ocsp.cencert.pl/2017> (dla certyfikatów weryfikowanych przy użyciu certyfikatu NCCert wystawionego 13.02.2017),

- http://ocsp.cencert.pl/2017_new (dla certyfikatów weryfikowanych przy użyciu certyfikatu NCCert wystawionego 18.05.2017),

Odpowiedź serwera poświadczeń jest zgodna z normą RFC 6960. Dla zapytania o nieznaną numeru certyfikatu, usługa zwraca wartość *unknown*. Usługa zwraca informacje o unieważnieniach niezależnie od daty ważności certyfikatu.

Token OCSP jest opatrzony pieczęcią złożoną przy użyciu klucza służącego wyłącznie do tego celu i zawiera certyfikat tego klucza, wystawiony przy użyciu klucza CenCert służącego do wystawiania certyfikatów.

7.4. Profil znacznika czasu

Akceptowane są żądania znakowania czasem zgodne z RFC 3161, podpisane elektronicznie w celu uwierzytelnienia zgodnie z normą PKCS#7. Do przesłania treści żądania znakowania czasem oraz pobrania znacznika czasu używany jest protokół HTTP.

Jeśli w żądaniu znakowania czasem (wg RFC 3161) występuje opcjonalny atrybut *ReqPolicy*, powinien zawierać identyfikator „{2 5 29 32 0}” (any policy). Opcjonalny atrybut *Extensions* może występować lecz nie jest przetwarzany przez system CCK.

Atrybut *Version* podpisu pod żądaniem (wg PKCS#7) powinien zawierać wartość „1”. Atrybut *Certificates* powinien zawierać listę certyfikatów, składającą się wyłącznie z certyfikatu (zgodnego z X.509v3) klucza, którym został podpisany znacznik czasu. Atrybut *SignerInfos* powinien zawierać listę podpisów, składającą się z dokładnie jednego podpisu. Opcjonalne atrybuty podpisu *SignedAttrs* i *UnsignedAttrs* nie są przetwarzane przez system CCK.

Odpowiedź serwera znakowania czasem na prawidłowo sformułowane żądanie znakowania jest zgodna ze standardem RFC 3161 i jest opatrzona zaawansowaną pieczęcią złożoną kluczem prywatnym Centrum Certyfikacji do pieczętowania znaczników czasu. Pieczęć pod znacznikiem czasu obejmuje m.in. datę i czas oraz dane przysłane przez osobę żądającą usługi (skrót kryptograficzny z danych znakowanych czasem).

8. Audyt

Centrum Certyfikacji podlega audytom zgodnie z art. 20 eIDAS.

9. Inne postanowienia

9.1. Opłaty

CenCert pobiera opłaty za świadczenie swoich usług zgodnie z obowiązującym w danym momencie cennikiem.

CenCert nie pobiera opłat za unieważnienie, zawieszenie bądź uchylenie zawieszenia certyfikatu, a także za dostęp do klucza publicznego CenCert oraz publikowanych (aktualnej i archiwalnych) list unieważnionych certyfikatów.

9.2. Odpowiedzialność finansowa

Odpowiedzialność Centrum Certyfikacji CenCert jest określona w art. 13 eIDAS.

Centrum Certyfikacji, jako kwalifikowany dostawca usług zaufania, jest odpowiedzialny za szkody wyrządzone w sposób zamierzony lub z powodu zaniedbania osobie fizycznej lub prawnej w związku z niewypełnieniem obowiązków określonych w eIDAS, z uwzględnieniem ograniczeń odpowiedzialności określonych w rozdziale 9.8 poniżej.

Domniemywa się zamiar lub zaniedbanie CenCert, chyba że udowodni, że szkoda, o której mowa powyżej, nie powstała z powodu zamierzonego działania lub zaniedbania CenCert.

9.3. Poufność informacji

Zasady ochrony poufności informacji związanych ze świadczeniem usług certyfikacyjnych określone są w ustawie o usługach zaufania oraz identyfikacji elektronicznej, a także w ustawie o ochronie danych osobowych.

Centrum Certyfikacji traktuje jako informacje poufne wszystkie informacje związane z realizowanymi przez siebie usługami poza informacjami następującymi:

- Polityka certyfikacji w wersjach aktualnie obowiązujących,
- Klucz publiczny CenCert,
- Lista unieważnionych certyfikatów, tokeny OCSP,
- Certyfikaty kluczy infrastruktury,

- Informacje bieżące, przeznaczone do publikacji (takie jak cennik usług, oferta handlowa, bieżące komunikaty, dane kontaktowe).

9.4. Ochrona danych osobowych

CenCert przetwarza dane osobowe Subskrybentów zgodnie z Rozporządzeniem Parlamentu Europejskiego i Rady (UE) 679/2016 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 oraz ustawą z dnia 10 maja 2018 r. o ochronie danych osobowych.

CenCert wdrożył i realizuje odpowiednie procedury zapewniające ochronę danych osobowych. Subskrybenci są informowani przy podpisywaniu umowy o przetwarzaniu przez CenCert ich danych osobowych oraz o przysługujących im w związku z tym prawach.

9.5. Zabezpieczenie własności intelektualnej

Firma Enigma Systemy Ochrony Informacji Sp. z o.o. ma pełne prawo do dysponowania majątkowymi prawami autorskimi odnoszącymi się do niniejszej polityki certyfikacji.

Enigma Systemy Ochrony Informacji Sp. z o.o. zezwala na wykorzystywanie polityki (w tym drukowanie i kopiowanie) przez Subskrybentów i innych odbiorców usług certyfikacyjnych, w celach związanych z wykorzystywaniem certyfikatów, tokenów OCSP i znaczników czasu wystawianych przez CenCert.

9.6. Udzielane gwarancje

Nie dotyczy

9.7. Zwolnienia z domyślnie udzielanych gwarancji

Centrum Certyfikacji nie udziela Subskrybentom żadnych domyślnie udzielanych gwarancji, poza gwarancjami które mogą wynikać z obowiązujących przepisów.

Wszelkie gwarancje udzielane przez Centrum Certyfikacji muszą być udzielane w formie pisemnej, pod rygorem nieważności.

9.8. Ograniczenia odpowiedzialności

Centrum Certyfikacji nie odpowiada za szkody wynikające z nieprzestrzegania przez odbiorcę usług zaufania zasad określonych w polityce certyfikacji, w szczególności za szkody wynikające z:

- 1) użycia certyfikatu niezgodnie z zakresem określonym w polityce wskazanej w certyfikacie, w tym za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została wskazana w certyfikacie;
- 2) nieprawdziwości danych zawartych w certyfikacie, podanych przez odbiorcę usług zaufania używającego tego certyfikatu, chyba że szkoda była wynikiem niedołożenia należytej staranności przez dostawcę usług zaufania;
- 3) przechowywania lub używania przez odbiorców usług zaufania kluczy prywatnych do składania podpisu elektronicznego, pieczęci elektronicznej lub uwierzytelnienia witryn internetowych – lub danych chroniących te klucze - w sposób niezapewniający ich ochrony przed nieuprawnionym wykorzystaniem, w szczególności nieprzestrzegania obowiązków wynikających z zapisów rozdz. 4.5.2 niniejszej polityki.

Centrum Certyfikacji nie odpowiada za to, że wystawiony certyfikat będzie odpowiedni dla potrzeb Subskrybenta ani że będzie poprawnie funkcjonował w systemie, w którym Subskrybent chce lub potrzebuje go użyć.

W przypadku skrócenia okresu ważności certyfikatów z winy Centrum Certyfikacji, odpowiedzialność Centrum Certyfikacji ogranicza się do zwrotu kosztów wystawienia certyfikatów, proporcjonalnie do skrócenia okresu ważności.

Centrum Certyfikacji nie odpowiada za niedostępność usługi OCSP, o ile w okresie niedostępności działają poprawnie usługi informowania o statusie certyfikatów na podstawie listy CRL.

Centrum Certyfikacji nie odpowiada za niedostępność usługi znakowania czasem, o ile okres niedostępności nie narusza deklaracji dostępności usługi określonej w rozdziale 6.8..

Centrum Certyfikacji, świadcząc usługi zaufania, nie odpowiada za poprawne działanie oprogramowanie używanego przez Subskrybenta oraz poprawność oraz adekwatność zastosowanych po stronie Subskrybenta zabezpieczeń technicznych i organizacyjnych.

W szczególności przy świadczeniu usługi znakowania czasem, Centrum Certyfikacji nie odpowiada za poprawność wyliczenia skrótu kryptograficznego z danych, które mają być oznaczone czasem.

Przy świadczeniu usługi w trybie serwerowym (rSign/rSeal), Centrum Certyfikacji w szczególności nie odpowiada za poprawność wyliczenia skrótu kryptograficznego z danych, które mają być podpisane/opieczetowane, ani za to że skrót kryptograficzny przesłany do systemu CenCert odpowiada danym, które Subskrybent zamierza podpisać/opieczetować, ponadto nie odpowiada za bezpieczeństwo przetwarzania, poza systemem CenCert, hasła zabezpieczającego klucz do składania podpisu/pieczęci, za zarządzanie przez Subskrybenta uprawnieniami osób upoważnionych do inicjowania sesji składania pieczęci, w tym za zgłaszanie personelowi CenCert zmian uprawnień z odpowiednim wyprzedzeniem

CenCert nie ponosi odpowiedzialności za terminową obsługę wniosku o zmianę statusu certyfikatu (unieważnienie, zawieszenie lub uchylenie zawieszenia), ani za to, że wniosek w ogóle zostanie obsłużony – jeśli nie został on dostarczony do CenCert na wskazany w rozdz. 1.3 adres przeznaczony do przesyłania wniosków o zmianę statusu certyfikatów (adres tradycyjny lub email, w zależności od formy wniosku).

CenCert nie ponosi odpowiedzialności za terminową obsługę wniosku o zmianę w zakresie upoważnień osób do ustanawiania sesji pieczętowania w trybie zdalnym (upoważnienie, usunięcie upoważnienia, zmiana danych), ani za to, że wniosek w ogóle zostanie obsłużony – jeśli nie został on dostarczony do CenCert na wskazany w rozdz. 1.3 adres (adres tradycyjny lub email, w zależności od formy wniosku).

CenCert nie ponosi odpowiedzialności za utratę dostępu Subskrybenta do klucza prywatnego służącego do realizacji podpisów lub pieczęci, spowodowaną blokadą karty elektronicznej z powodu błędnie wprowadzonego kodu PIN i/lub PUK, przy przekroczeniu ustalonego limitu błędnych prób, o którym Subskrybent został poinformowany.

CenCert nie ponosi odpowiedzialności za utratę dostępu do klucza prywatnego służącego do realizacji pieczęci w trybie zdalnym (rSeal), spowodowaną utratą hasła do aktywacji klucza.

CenCert nie ponosi odpowiedzialności za utratę dostępu do klucza prywatnego służącego do realizacji podpisu w trybie zdalnym (rSign), spowodowaną utratą danych „backupu” zapisywanych przez aplikację mobilną, bądź utratą PINu do aplikacji mobilnej, bądź utratą dostępu do wiadomości SMS wysyłanych na zdefiniowany w CenCert numer telefonu.

Łączna odpowiedzialność finansowa ENIGMA SOI Sp. z o.o. z tytułu świadczenia przez CenCert usług certyfikacyjnych nie może przekroczyć 1 000 000 EUR. Wysokość jednorazowego odszkodowania z tytułu użycia nieprawidłowego certyfikatu wydane przez CenCert nie może przekroczyć 250 000 EUR.

9.9. Przenoszenie roszczeń odszkodowawczych

Centrum Certyfikacji zawarło umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, zgodnie z ustawą o usługach zaufania.

9.10. Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych w okresie jej obowiązywania. Certyfikaty wykorzystywane w celach dochodzeniowych lub dowodowych po okresie ich ważności, powinny być wykorzystywane zgodnie z polityką certyfikacji, w ramach której zostały wystawione.

Polityka może być stosowana od momentu zatwierdzenia (przed datą wejścia w życie) do realizacji usług zaufania w celach testowych i związanych z audytem.

9.11. Określanie trybu i adresów doręczania pism

Wszelkie pisma związane z bieżącą działalnością Centrum Certyfikacji powinny być dostarczane pod adresem Centralnego Punktu Rejestracji.

Wszelkie pisma mogą być także dostarczane na adres siedziby Enigma Systemy Ochrony Informacji Sp. z o.o.

9.12. Zmiany w polityce certyfikacji

Zasady zarządzania polityką certyfikacji zostały opisane w rozdziale 1.5.

9.13. Rozstrzyganie sporów

Wszelkie sprawy sporne dotyczące realizacji usług zaufania CenCert, w tym skargi i reklamacje, należy kierować do firmy Enigma Systemy Ochrony Informacji Sp. z o.o. pod adresem biuro@enigma.com.pl.

9.14. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu Rzeczypospolitej Polskiej oraz Unii Europejskiej.

9.15. Podstawy prawne

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

- Rozporządzeniu Parlamentu Europejskiego i Rady (UE) Nr 910/2014 z dnia 23 lipca 2014 r. oraz wydanymi na podstawie tego rozporządzenia decyzjami wykonawczymi Komisji (UE).
- Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.
- Rozporządzeniu Parlamentu Europejskiego i Rady (UE) 679/2016 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 oraz ustawie z dnia 10 maja 2018 r. o ochronie danych osobowych.
- Ustawie Kodeks karny.
- Ustawie Prawo autorskie.

9.16. Inne postanowienia

CenCert udostępnia potencjalnym klientom usługi rSeal, przed rozpoczęciem świadczenia usługi, opis interfejsu usługi składania pieczęci w trybie zdalnym.

CenCert udostępnia potencjalnym producentom aplikacji mobilnej do usługi rSign, po podpisaniu odpowiedniej umowy, opis wymagań bezpieczeństwa i funkcjonalnych dla aplikacji mobilnej.