KWALIFIKOWANY DOSTAWCA USŁUG ZAUFANIA „CENCERT”

POLITYKA DLA KWALIFIKOWANYCH USŁUG ZAUFANIA

Wersja: 1.4

Karta dokumentu:

Tytuł dokumentu	Polityka dla kwalifikowanych usług zaufania
Właściciel dokumentu	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Wersja	1.4
Status dokumentu	**ZATWIERDZONY**
Data zatwierdzenia	2023-04-13
Liczba stron	71

Zatwierdzone przez: 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 *Politykę certyfikacji dla certyfikatów kwalifikowanych* w. 2.3 oraz *Politykę znakowania czasem i innych kwalifikowanych usług certyfikacyjnych* w. 1.1.	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.	2020-12-03
1.31	Jacek Pokraśniewicz	Dodanie deklaracji dostępności bieżących list CRL, uszczegółowienia w zakresie certyfikatów z pseudonimem, inne drobne poprawki.	2021-10-10
1.4	Jacek Pokraśniewicz, Artur Krystosik, Katarzyna Ligenza	Dodanie usługi kwalifikowanej walidacji podpisu elektronicznego. Przegląd polityki, poprawki redakcyjne. Uporządkowanie rozdziału *Ograniczenia odpowiedzialności*, rozszerzenie możliwości unieważnienia certyfikatu przez CenCert.	2023-05-29

Spis treści

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę opisującą realizację kwalifikowanych usług zaufania, świadczonych przez firmę Enigma Systemy Ochrony Informacji Sp. z o.o. pod marką ***CenCert***, polegających na:

1) wystawianiu i unieważnianiu kwalifikowanych certyfikatów,
2) wystawianiu kwalifikowanych znaczników czasu oraz
3) walidacji podpisu elektronicznego i pieczęci elektronicznej

Wszelkie postanowienia odnoszące się do „CenCert" należy rozumieć jako postanowienia odnoszące się do firmy „Enigma Systemy Ochrony Informacji Sp. z o.o.", realizującej usługi zaufania pod marką „CenCert".

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*".

Postanowienia specyficzne dla kwalifikowanej usługi walidacji podpisu lub pieczęci elektronicznej zostały zawarte w Załączniku A, który jest integralną częścią niniejszego dokumentu.

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	**2023-05-29**

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,
- klucz do podpisywania raportów walidacji podpisu i pieczęci elektronicznej

- 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, kwalifikowanej usługi walidacji podpisu i pieczęci - 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,

- raporty z walidacji podpisów i pieczęci elektronicznych,
- certyfikaty infrastruktury używane wewnętrznie w CenCert,
- 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	(*Qualified Trust Service Provider*) kwalifikowany dostawca usług zaufania
PKI	*Public Key Infrastructure* – 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.)

Termin/akronim	Opis
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 znacznik czasu bądź raport z walidacji podpisu/pieczęci.
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.)
DN	Identyfikator DN – *Distinguished Name* – 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	*Certificate Revocation List* - Lista unieważnionych certyfikatów, wystawiana, pieczętowana elektronicznie i publikowana przez CenCert.
OCSP	*Online Certificate Status Protocol* - 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.

Termin/akronim	Opis
HSM	*Hardware Security Module* – 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 - *Qualified Signature Creation Device* (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 postanowieniami rozdz. 3.2, ale nie sprawdza praw do posługiwania się przedmiotami praw własności intelektualnej, w szczególności utworami, zastrzeżonymi znakami towarowymi czy zarejestrowanymi patentami, nie odpowiada za nieuprawnione wykorzystywanie ww. przedmiotów 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) = <dodatkowe 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>

Zawartość pola „Pseudonim" nie może wprowadzać w błąd (w szczególności wywoływać błędnego wrażenia, że certyfikat należy do osoby publicznej lub powszechnie znanej). Pole to nie może też mieć zawartości wulgarnej ani obraźliwej.

Pole *nazwa powszechna* ma taką samą zawartość, jak pole *pseudonim*, ewentualnie uzupełnioną o wskazanie, że zawartość pola jest pseudonimem (np. poprzez dopisek o treści „(pseud.)").

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 – 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.

W przypadku certyfikatów do podpisu elektronicznego zawierających pseudonim zamiast imienia i nazwiska (patrz rozdział 3.1.1.2), CenCert nie weryfikuje praw do posługiwania się

danym pseudonimem ani jego unikalności, bez uszczerbku dla postanowień dotyczących zasad umieszczenia w certyfikacie danych organizacji. CenCert przechowuje dane pozwalające na zidentyfikowanie konkretnej osoby fizycznej posługującej się danym certyfikatem zawierającym pseudonim.

CenCert ma prawo odmówić wystawienia certyfikatu z pseudonimem, jeśli zdaniem CenCert treść wpisu do certyfikatu narusza warunki określone w rozdziale 3.1.1.2.

3.3. Uwierzytelnienie Subskrybenta przy wystawianiu kolejnych certyfikatów

Kolejny certyfikat do podpisu elektronicznego może być wykonany na podstawie ważnego podpisu kwalifikowanego. Nowy certyfikat zawiera te same dane identyfikujące Subskrybenta, co certyfikat poprzedni. Przy przepisaniu do nowego certyfikatu ewentualnych dodatkowych danych Subskrybenta (np. dane organizacji, z którą jest związany Subskrybent, uprawnienia zawodowe itd.), nie wymaga się ponownego sprawdzenia prawa do umieszczenia tych danych. Zakres tych dodatkowych danych, zapisanych w nowym certyfikacie, może być również ograniczony w stosunku do danych zawartych w poprzednim certyfikacie, dane te mogą być również uaktualnione lub uzupełnione, przy czym przy uzupełnianiu lub aktualizacji wymagane są upoważnienia lub potwierdzenia tych danych, jak przy wydaniu pierwszego certyfikatu.

Nie realizuje się procedury wydania certyfikatu na podstawie certyfikatu poprzedniego, 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 wyłącznie pod 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

kwalifikowanych 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. CenCert, w miarę możliwości będzie informował 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. CenCert, w miarę możliwości będzie informował 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, której 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. W szczególności:

- CenCert może unieważnić certyfikat zawierający pseudonim, jeśli okaże się, że pseudonim nie spełnia warunków określonych w rozdziale 3.1.1.2,

- CenCert może zawiesić lub unieważnić certyfikat Subskrybenta na wniosek organizacji, która finansowała wydanie certyfikatu (dotyczy certyfikatów wydanych na podstawie umowy lub umowy ramowej, zawartej pomiędzy CenCert, a daną organizacją),
- CenCert może zawiesić, a następnie unieważnić certyfikat, w przypadku nieopłacenia usługi wystawienia certyfikatu, przez Subskrybenta lub organizację zamawiającą wydanie certyfikatu, po uprzednim bezskutecznym wezwaniu do uregulowania płatności w terminie co najmniej 14 dni. Wystarczającą formą powiadomienia jest mail wysłany na adres podany do przesłania faktury lub na adres elektroniczny Subskrybenta podany w celu wystawienia certyfikatu.

CenCert zapewnia możliwość zgłoszenia żądania unieważnienia, zawieszenia bądź uchylenia 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 CenCert 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

CenCert informuje o statusie certyfikatów poprzez listę CRL oraz usługę OCSP.

Lista CRL jest wystawiana co najmniej raz na 24 godziny, z gwarantowaną dostępnością 99,95% w ujęciu rocznym.

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 badana jest 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.

CenCert 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 polegającej na wystawieniu kwalifikowanego certyfikatu, 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 podpisu lub pieczęci w imieniu subskrybenta, usługa przestaje być świadczona niezwłocznie po zakończeniu ważności certyfikatu (unieważnienie bądź upływ terminu ważności).

W przypadku świadczenia usługi walidacji podpisu lub pieczęci, okres świadczenia usługi określony jest w umowie z subskrybentem, a jeśli zamówienie dotyczy pojedynczej operacji walidacji – w terminie 24 miesięcy po wystawieniu raportu walidacji.

4.12. Powierzanie i odtwarzanie kluczy prywatnych

CenCert nie powierza swojego klucza prywatnego inny 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. Fakt dostępu do urządzeń jest każdorazowo odnotowywany.

CenCert jest wyposażony w centrum zapasowe, umiejscowione w lokalizacji oddalonej od centrum podstawowego.

Wszelkie dane i urządzenia istotne dla bezpieczeństwa CenCert i usług przez niego 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 CenCert 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 CenCert.

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 współpracująca z Enigmą 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 pełnienia tych funkcji na rzecz Enigmy oraz 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

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

Logi są zabezpieczone przed modyfikacją.

5.5. Archiwizacja zapisów

CenCert 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 służących do świadczenia usług zaufania

Wygenerowanie i wymiana pary kluczy CenCert 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

CenCert 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 niszczony.

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 niektórych kwalifikowanych usług zaufania (i utrzymania świadczenia pozostałej kwalifikowanej usługi lub usług) zapisy powyższe stosuje się odpowiednio.

6. Zabezpieczenia techniczne

6.1. Generowanie i instalowanie par kluczy

6.1.1 Generowanie par kluczy

Pary kluczy CenCert 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 CenCert 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 CenCert mają długość 4096 bitów.

Klucze ECDSA CenCert 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, raportów z walidacji podpisów/pieczęci oraz innych struktur danych wydawanych przez CenCert) są używane algorytmy skrótu z rodziny SHA-2.

6.1.6 Cel użycia klucza

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

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

Klucz prywatny CenCert do pieczętowania raportów walidacji podpisu lub pieczęci elektronicznej - może być wykorzystywany tylko do tego celu. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania raportów.

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

6.2. Ochrona kluczy prywatnych

Klucze prywatne CenCert 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

Klucze prywatne Subskrybentów do podpisów/pieczęci 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 CenCert nie są archiwizowane.

Uaktywnienie kluczy CenCert 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 CenCert, służących do realizacji usług zaufania, wykonywane jest komisyjnie zgodnie z udokumentowaną procedurą.

CenCert 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 niszczony (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/pieczętowania. 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

CenCert 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 CenCert można wykonać po uprzednim uwierzytelnieniu się i kontroli uprawnień. Wykonywane operacje są zapisywane w dziennikach zdarzeń.

Część oprogramowania służącego do realizacji usługi walidacji podpisów i pieczęci może być zainstalowana w infrastrukturze IT użytkownika usługi walidacji, w postaci zabezpieczonego dockera lub serwera wirtualnego, dostarczanego i zarządzanego przez CenCert. Użytkownik usługi walidacji jest zobowiązany do zapewnienia bezpiecznego środowiska uruchomienia tego oprogramowania, w szczególności do zabezpieczenia go przed dostępem nieuprawnionych osób, jak również do powstrzymania się od jakiejkolwiek ingerencji w dostarczone oprogramowanie, w tym od prób przełamywania zabezpieczeń zastosowanych przez CenCert.

6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

W CenCert 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, oznaczania czasem zdarzeń związanych z usługą walidacji podpisów i pieczęci oraz do 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 znakowania czasem, zgodne z postanowieniami rozdz. 7.4.

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 usługi walidacji podpisów lub pieczęci elektronicznych:

Kraj (countryName) = ***PL***
Nazwa organizacji (organizationName) = ***Enigma Systemy Ochrony Informacji Sp. z o.o.***
Nazwa powszechna (*commonName*) = ***CenCert QTSP QVal***
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

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

Numery wystawianych certyfikatów są pseudolosowe i unikalne w ramach danej usługi zaufania, identyfikowanej poprzez identyfikator wyróżniający CenCert. 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-RSA[1], sha256-with-ecdsa, sha384-with-

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

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

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

Rozszerzenie	Opis/wartość	krytyczne ?

qcStatement	Tylko dla certyfikatów wystawionych zgodnie z PSD2:
	
	`etsi-psd2-qcStatement {0.4.0.19495.2}`
	Oznaczenie instytucji nadzoru finansowego (NCAName, NCAId) oraz jedna lub więcej ról zdefiniowanych w PSD2, zgodnie z ETSI TS 119 495:
	- `PSP_AS`
	`id-psd2-role-psp-as {0.4.0.19495.1.1}`
	- `PSP_PI`
	`id-psd2-role-psp-pi {0.4.0.19495.1.2}`
	- `PSP_AI`
	`id-psd2-role-psp-ai {0.4.0.19495.1.3}`
	- `SP_IC`
	`id-psd2-role-psp-ic {0.4.0.19495.1.4}`
		NIE

Authority Information Access –	*id-ad-caIssuers* wskazanie URL na położenie certyfikatu CA wystawionego przez NCCert (protokół HTTP)	NIE
Authority Information Access –	*id-ad-ocsp* 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

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

Do wykonania pieczęci CenCert pod listami CRL wykorzystywany jest algorytm skrótu SHA-2.

Rozszerzenia

Pole	**Opis/wartość**	**krytyczne ?**
Extensions		
AuthorityKeyIdentifier		NIE
keyIdentifier	skrót z klucza publicznego	
cRLNumber	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).

Odpowiedź serwera poświadczeń jest zgodna z normą RFC 6960. Dla zapytania o nieznany 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, uwierzytelnione na jeden ze sposobów:

- z użyciem mechanizmu „http basic authentication" i parametrów „login, hasło" uprawniających do pobierania znaczników czasu, albo
- podpisane elektronicznie w celu uwierzytelnienia, zgodnie z normą PKCS#7, przy użyciu certyfikatu uprawnionego do pobierania znaczników czasu.

Do przesłania treści żądania znakowania czasem oraz pobrania znacznika czasu używany jest protokół http lub https, przy czym protokołu http klient powinien używać wyłącznie wtedy, gdy jego system nie obsługuje https oraz gdy używa trybu z podpisanymi żądaniami znakowania czasem (klient nie powinien nigdy inicjować połączenia niezabezpieczonym protokołem http, gdy zamierza używać trybu login/hasło).

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.

W przypadku podpisanych żądań znakowania czasem - 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 zostało podpisane żądanie znakowania czasem. 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 standardami RFC 3161 oraz ETSI EN 319 422 i jest opatrzona zaawansowaną pieczęcią złożoną kluczem prywatnym CenCert 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

CenCert 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 CenCert jest określona w art. 13 eIDAS.

CenCert, 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.

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

1) Polityka certyfikacji w wersjach aktualnie obowiązujących,
2) Klucz publiczny CenCert,
3) Lista unieważnionych certyfikatów, tokeny OCSP,
4) Certyfikaty kluczy infrastruktury,

5) 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

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

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

9.8. Ograniczenia odpowiedzialności

9.8.1 Postanowienia ogólne

CenCert nie odpowiada za szkody wynikające z nieprzestrzegania przez odbiorcę usług zaufania zasad określonych w niniejszej polityce.

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

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 wydanego przez CenCert nie może przekroczyć 250 000 EUR.

9.8.2 Postanowienia szczegółowe związane z usługami wystawiania certyfikatów kwalifikowanych oraz z usługą składania podpisu/pieczęci w imieniu Subskrybenta (rSign/rSeal)

CenCert nie odpowiada za szkody wynikające z:

1) użycia certyfikatu niezgodnie z zakresem określonym w polityce wskazanej 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.

CenCert 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 CenCert, odpowiedzialność CenCert ogranicza się do zwrotu kosztów wystawienia certyfikatów, proporcjonalnie do skrócenia okresu ważności.

CenCert nie odpowiada za skutki wynikające z unieważnienia certyfikatu zawierającego pseudonim, jeśli po wystawieniu certyfikatu okaże się, że pseudonim nie spełnia warunków określonych w rozdziale 3.1.1.2, a fakt ten nie był znany CenCert w momencie wystawiania certyfikatu.

CenCert nie odpowiada za niedostępność usługi OCSP, o ile w okresie niedostępności działały poprawnie usługi informowania o statusie certyfikatów na podstawie listy CRL, zgodnie z deklaracją dostępności określoną w rozdziale 4.10.

CenCert nie odpowiada za niedostępność usługi udostępniania bieżącej listy CRL, o ile okres niedostępności nie narusza deklaracji dostępności usługi, określonej w rozdziale 4.10.

Przy świadczeniu usługi w trybie serwerowym (rSign/rSeal), CenCert nie odpowiada za poprawność wyliczenia skrótu kryptograficznego z danych, które mają być podpisane/opieczętowane, ani za to że skrót kryptograficzny przesłany do systemu CenCert odpowiada danym, które Subskrybent zamierza podpisać/opieczętować, 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.

9.8.3 Postanowienia szczegółowe związane z usługą znakowania czasem

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

CenCert nie odpowiada za poprawność wyliczenia skrótu kryptograficznego z danych, które mają być oznaczone czasem.

9.8.4 Postanowienia szczegółowe związane z usługą walidacji podpisu i pieczęci

CenCert nie ponosi odpowiedzialności za to, czy walidowane podpisy/pieczęcie spełniają wymagania odbiorcy usługi, w szczególności nie odpowiada za to, czy osoby, które złożyły podpisy, były odpowiednio umocowane.

Podpisy i pieczęcie elektroniczne mogą być składane w sposób, który może wprowadzić w błąd osobę walidującą dokument – np. mogą obejmować swoim zakresem tylko część dokumentu, mogą być złożone pod dokumentami zawierającymi aktywną treść, zmieniającą sposób prezentacji dokumentu, itd. CenCert wykazuje należytą staranność w wykrywaniu i informowaniu odbiorcy usługi walidacji o potencjalnych problemach z bezpieczeństwem, jednak nie gwarantuje i nie ponosi odpowiedzialności za wykrywanie wszelkich tego typu przypadków.

Jeśli usługa walidacji jest świadczona przy pomocy oprogramowania CenCert, zainstalowanego częściowo w infrastrukturze zarządzanej przez klienta usługi walidacji (patrz

opis w Załączniku A, rozdział A.2.3), w przypadku naruszenia integralności tego oprogramowania, wystawione przy jego pomocy raporty walidacji mogą być uznane za niezgodne z dokumentami wejściowymi do usługi walidacji (patrz opis sposobu potwierdzenia, czy raport walidacji odpowiada dokumentowi wejściowemu, Załącznik A, rozdział A.1.2.1). CenCert nie odpowiada za szkody, które mogą wyniknąć z tego tytułu

W przypadku gdy, na życzenie klienta, usługa walidacji jest realizowana na podstawie wprowadzonej przez niego daty powstania podpisanego dokumentu – CenCert nie odpowiada za poprawność tej daty i wynikającą stąd poprawność raportu walidacji. Stosowna informacja jest umieszczana w raporcie walidacji.

CenCert nie odpowiada za ewentualne skutki mogące wystąpić z powodu użycia niepoprawnych, to jest niezgodnych z przepisami lub obowiązującymi standardami, informacji takich jak listy CRL, OCSP, znaczniki czasu – publikowanych przez innych kwalifikowanych dostawców kwalifikowanych usług – wykorzystywanych przy realizacji usługi walidacji.

9.9. Przenoszenie roszczeń odszkodowawczych

CenCert zawarł 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 obowiązuje w stosunku do produktów realizacji usług zaufania (certyfikatów, znaczników czasu, raportów walidacji itd.) wystawionych w okresie jej obowiązywania.

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

Usługa kwalifikowanej walidacji kwalifikowanych podpisów i pieczęci elektronicznych jest realizowana po jej wpisaniu na listę TSL.

9.11. Określanie trybu i adresów doręczania pism

Wszelkie pisma związane z bieżącą działalnością CenCert 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 Rzeczpospolitej Polskiej oraz Unii Europejskiej.

9.15. Podstawy prawne

Zasady działania CenCert 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.

Załącznik A – Postanowienia polityki specyficzne dla kwalifikowanej usługi walidacji kwalifikowanych podpisów i pieczęci elektronicznych

A.1 Wprowadzenie

A.1.1 Informacje ogólne

Niniejszy dokument opisuje postanowienia polityki świadczenia kwalifikowanych usług specyficzne dla kwalifikowanej usługi walidacji kwalifikowanych podpisów i pieczęci elektronicznych („Usługa"). W stosunku do Usługi obowiązują także postanowienia zawarte w dokumencie głównym polityki.

Struktura załącznika oparta jest na normie ETSI TS 119 172-1 V1.1.1.

Sposób realizacji usługi walidacji jest zgodny z normą ETSI TS 119 441.

A.1.2 Domena biznesowa lub aplikacyjna

A.1.2.1 Zakres i ograniczenia polityki podpisu

Usługa służy do walidacji kwalifikowanych podpisów i pieczęci elektronicznych we wszelkich zastosowaniach kwalifikowanego podpisu i pieczęci elektronicznej. Usługa może być również używana do walidacji wybranych typów zaawansowanych podpisów i pieczęci elektronicznych. Produktem Usługi jest raport walidacji zawierający wyniki walidacji podpisów i pieczęci zawartych w dokumencie lub dołączonych do dokumentu.

W przypadku potwierdzenia ważności podpisu lub pieczęci, raport walidacji jednoznacznie określa rodzaj walidowanego podpisu/pieczęci, w szczególności czy jest to podpis kwalifikowany lub pieczęć kwalifikowana.

W celu potwierdzenia, czy dany raport walidacji odpowiada danemu dokumentowi (czy stanowi dowód potwierdzający status ważności podpisów lub pieczęci konkretnego dokumentu), należy:

1) potwierdzić zgodność skrótu kryptograficznego z pliku/plików dokumentu ze skrótem umieszczonym w raporcie walidacji ORAZ
2) potwierdzić zgodność skrótów z poszczególnych części dokumentu, objętych poszczególnymi podpisami/pieczęciami, ze skrótami zamieszczonymi w raporcie walidacji (postać XLM raportu walidacji).

CenCert udostępnia na stronie WWW bezpłatną, dostępną dla wszystkich zainteresowanych stron, aplikację, pozwalającą na potwierdzenie zgodności danego dokumentu z danym raportem walidacji.

W niektórych przypadkach, wyraźnie wykazanych w raporcie walidacji, walidacja jest oparta na dowodach istnienia podpisanego dokumentu, leżących po stronie użytkownika Usługi (patrz rozdział A.3.2.3). W takim przypadku, raport potwierdza ważność podpisu/pieczęci wyłącznie w połączeniu z odpowiednim dowodem istnienia dokumentu, posiadanym przez użytkownika.

Przedmiotem działania Usługi jest dokument o dowolnej treści cyfrowej, zawierający podpisy lub pieczęcie elektroniczne, lub podpisy i pieczęcie dołączone do dokumentu jako podpisy/pieczecie zewnętrzne i zapisane w innych plikach.

Wynik walidacji danego podpisu lub pieczęci jest określony jako:

1) POZYTYWNY (TOTAL-PASSED) – co oznacza, że potwierdzono ważność podpisu/pieczęci,
2) NIEOKREŚLONY (INDETERMINATE) – co oznacza, że podpis/pieczęć jest matematycznie poprawna, ale - przy danych wejściowych obecnie dostępnych dla usługi walidacji - nie ma możliwości potwierdzenia ważności podpisu/pieczęci, albo
3) NIEPOPRAWNY (INVALID) – co oznacza, że nie ma możliwości potwierdzenia ważności podpisu/pieczęci (np. podpis matematycznie niepoprawny, certyfikat został unieważniony przed wykonaniem podpisu itd.).

Zgodnie z art. 32.1, art. 40 eIDAS, proces walidacji kwalifikowanego podpisu lub pieczęci elektronicznej potwierdza ważność kwalifikowanego podpisu elektronicznego lub kwalifikowanej pieczęci elektronicznej, pod warunkiem że:

a) certyfikat, który towarzyszy podpisowi/pieczęci, był w momencie składania podpisu kwalifikowanym certyfikatem podpisu elektronicznego zgodnym z Załącznikiem I eIDAS lub kwalifikowanym certyfikatem pieczęci elektronicznej zgodnym z Załącznikiem III eIDAS;
b) kwalifikowany certyfikat został wydany przez kwalifikowanego dostawcę usług zaufania i był ważny w momencie składania podpisu;
c) dane służące do walidacji podpisu lub pieczęci odpowiadają danym dostarczonym stronie ufającej;
d) unikalny zestaw danych reprezentujących podpisującego umieszczony w certyfikacie jest prawidłowo dostarczony stronie ufającej;
e) jeżeli w momencie składania podpisu użyty został pseudonim, zostaje to wyraźnie wskazane stronie ufającej;

f) podpis elektroniczny został złożony za pomocą kwalifikowanego urządzenia do składania podpisu elektronicznego lub pieczęci elektronicznej;
g) integralność podpisanych danych nie została naruszona;
h) wymogi przewidziane w art. 26 dla podpisu, lub art. 36 dla pieczęci, zostały spełnione w momencie składania podpisu/pieczęci.

Zgodnie z art. 32.2, art. 40 eIDAS, system wykorzystany do walidacji kwalifikowanego podpisu i pieczęci elektronicznej zapewnia stronie ufającej prawidłowy wynik procesu walidacji i umożliwia stronie ufającej wykrycie wszelkich problemów związanych z bezpieczeństwem. W szczególności Usługa realizuje działania opisane w rozdz. A.1.2.3 (dostarczenie danych o kontekście operacji podpisu/pieczęci), A.3.2.3 (ewentualna niepewność dowodów związanych z czasem istnienia podpisanego dokumentu), A.3.1.3 (relacja pomiędzy podpisami o podpisanymi danymi), A.3.4.2 (algorytmy kryptograficzne).

A.1.2.2 Zakres stosowania

Nie ogranicza się zakresu stosowania Usługi.

Walidowane dokumenty mogą być używane zarówno w relacjach typu B2B, B2C, Gov2B, Gov2C, a także relacjach opartych na umowach, relacjach finansowych, medycznych, konsumenckich, w ramach jednej organizacji lub relacjach pomiędzy organizacjami, krajowych oraz międzynarodowych.

A.1.2.3 Kontekst operacji

Usługa służy do walidacji dokumentów występujących w różnych kontekstach.

Jeśli walidowany podpis zawiera oznaczenie swojego kontekstu zgodnie z kwalifikatorami zdefiniowanymi w normie ETSI 101 733 (np. rola podpisującego *Proof of origin*, *Proof of creation*, itd.)[2], fakt ten jest wyraźnie uwidoczniony w raporcie walidacji.

A.1.3 Nazwy dokumentów i polityk, zasady identyfikacji i zgodności

A.1.3.1 Nazwa polityki podpisu

Patrz rozdział 1.2.

[2] Oznaczenia kontekstu podpisu są zdefiniowane w normie ETSI TS 101 733 dotyczącej podpisów CAdES, ale są przywołane w odpowiednich normach i obowiązują również dla innych formatów podpisów (np. w normie ETSI TS 101 903 dla podpisów XAdES).

A.1.3.2 Identyfikator polityki podpisu

Patrz rozdział 1.2.

A.1.3.3 Zasady zgodności

Patrz rozdział 1.

A.1.3.4 Punkty dystrybucji

Patrz rozdział 1.3.

A.1.4 Zasady administrowania polityką podpisu

Patrz rozdział 1.5.

A.1.5 Definicje i skróty

DA - Driving Application – część oprogramowania CenCert służącego do realizacji Usługi, instalowana zasadniczo w infrastrukturze IT klienta Usługi (aby uniknąć przekazywania do CenCert dokumentów podlegających walidacji, z uwagi na poufność danych zawartych w dokumentach), odpowiedzialna za wyliczanie reprezentacji (skrótów kryptograficznych) danych objętych podpisami/pieczęciami.

SVA – Signature Validation Application – część oprogramowania CenCert służącego do realizacji Usługi, działająca na serwerach CenCert, odpowiedzialna między innymi za badanie ważności odpowiednich kwalifikowanych certyfikatów w określonych momentach czasu, wydawanie decyzji co do wyniku walidacji podpisów/pieczęci i dokumentu, wystawienie raportu walidacji.

POE – Proof od Existance – Dowód, że w danym momencie podpis/pieczęć już istniał (został złożony w tym momencie lub wcześniej).

A.2 Signature application practices statements

Niniejszy rozdział zawiera zestaw wymagań dotyczących zasad i praktyk bezpieczeństwa, które spełniają aplikacje DA i SVA podczas walidacji podpisów/pieczęci.

A.2.1 Wymagania prawne

Patrz rozdział 9.15.

A.2.2 Wymagania dotyczące systemu zarządzania bezpieczeństwem informacji

Enigma Systemy Ochrony Informacji Sp. z o.o. (właściciel znaku towarowego CenCert) wdrożyła i utrzymuje system zarządzania bezpieczeństwem informacji, certyfikowany na zgodność z wymaganiami normy ISO 27001. System ten obejmuje również świadczenie usług zaufania pod marką "CenCert", w tym usług walidacji podpisu i pieczęci elektronicznych. W ramach tego sytemu zarządzania określono *Politykę Zintegrowanego Systemu Zarządzania*, która jest certyfikowana zgodnie z normami ISO 9001, ISO 27001 i jest dostępna na stronie WWW.

Informacje nt. zabezpieczenia interfejsu sieci komputerowej CenCert określone są w rozdziale 6.7 polityki. Połączenie pomiędzy DA i SVA jest realizowane zabezpieczonym kanałem transmisji (TLS), z uwierzytelnieniem serwera na podstawie certyfikatu TLS. Komponent DA jest również uwierzytelniany, za pomocą mechanizmu „http basic authentication", z odpowiednio długim hasłem.

Postanowienia dotyczące zabezpieczenia systemu informatycznego zapisane są w rozdziale 6.5 polityki.

Postanowienia dotyczące zapewnienia integralności aplikacji w kontekście aktualizacji również określone są w rozdziale 6.5 polityki. Dodatkowo, CenCert prowadzi listę aplikacji służących do realizacji Usługi, wraz z określeniem numerów wersji.

Aplikacje komponentu DA są dystrybuowane przez CenCert do klientów z użyciem technologii zapewniającej, że DA nie jest dostępne dla klientów do modyfikacji np. w postaci obrazu systemu operacyjnego dla maszyny wirtualnej.

Kopie zapasowe danych po stronie CenCert (dotyczy SVA) są regularnie wykonywane na szyfrowanych nośnikach, które są przechowywane w innej lokalizacji niż serwery. Dane są ponadto replikowane pomiędzy Centrum podstawowym i centrum zapasowym.

CenCert nadzoruje wyniki audytów zgodnie z wymaganiami ISO 9001 i ISO 27001, wszelkie ewentualne niezgodności i inne uwagi audytowe są odnotowywane, wraz z przebiegiem postępowania z nimi (w tym podjęte decyzje, status postępowania, ewentualnie analiza przyczyn itd.).

A.2.3 Wymagania dotyczące procesów walidacji podpisu

Usługa jest realizowana w sposób automatyczny przez komponenty programistyczne:

- SVA, w skład którego wchodzi usługa rVer Server oraz usługi pomocnicze,
- DA, rVer Gateway, w skład którego wchodzi usługa rVer Client i komponenty interfejsu użytkownika.

SVA jest zlokalizowany na serwerach CenCert i komunikuje się z DA oraz repozytoriami informacji o unieważnieniach publikowanymi przez dostawców usług zaufania. SVA realizuje część procesu walidacji polegającą na badaniu poprawności oraz statusu certyfikatów wykorzystanych do złożenia danego podpisu/pieczęci oraz wystawia raport końcowy. SVA prowadzi centralną bazę danych usługi walidacji.

Dla klienta usługi walidacji, SVA jest dostępny wyłącznie za pośrednictwem DA. Protokół komunikacyjny pomiędzy SVA i DA jest zgodny z ETSI TS 119 442.

DA, co do zasady, jest przeznaczony do instalacji w infrastrukturze informatycznej klienta Usługi (zapewniając że dane zawarte w walidowanych dokumentach nie opuszczają infrastruktury klienta). DA zapewnia interfejs WWW dla użytkownika Usługi, pozwalający na zlecanie procesów walidacji i odczytywanie statusu operacji oraz jej wyniku (raportów walidacji). DA zapewnia także zarządzanie użytkownikami lokalnymi Usługi oraz udostępnia interfejs rest, pozwalający na integrację z systemami klienta usługi.

Możliwa jest również konfiguracja usługi z instancją DA zainstalowaną w infrastrukturze CenCert. W takim przypadku dokumenty do walidacji i raporty są przekazywane w inny sposób (np. poprzez ze sklep WWW lub szyfrowane maile itd.).

SVA dostarcza użytkownikowi raport walidacji, za pośrednictwem DA, w sposób asynchroniczny - wtedy, kiedy zgromadzi wszystkie potrzebne dane. W przypadku, gdy w momencie złożenia dokumentu do walidacji, nie są jeszcze dostępne wszystkie informacje dotyczące potencjalnego unieważnienia certyfikatu w momencie złożenia podpisu lub pieczęci, SVA samoczynnie ponawia próbę walidacji co określony czas, nie obciążając użytkownika dodatkowymi czynnościami ani kosztami. Raport walidacji jest przygotowywany wtedy, gdy SVA zgromadzi wymagane informacje od zewnętrznych dostawców usług zaufania lub, jeśli to się nie uda, po upływie maksymalnego przewidzianego czasu na realizację usługi, który wynosi nie mniej niż 24 godziny.

CenCert gwarantuje dostępność Usługi na poziomie 99,9% mierzonej w ujęciu rocznym. Powyższy wskaźnik nie obejmuje przerw w działaniu Usługi wynikających z przyczyn leżących poza CenCert (w szczególności, z przyczyn związanych z infrastrukturą IT klienta, w której jest zainstalowana DA).

Usługa obsługuje następujące formaty podpisów/pieczęci:

- XAdES (XML Advanced Electronic Signatures zgodne z ETSI TS 103 171 v.2.1.1),
- PAdES (PDF Advanced Electronic Signatures zgodne z ETSI TS 103 172 v.2.2.2,)
- CadES (CMS Advanced Electronic Signatures zgodne z ETSI TS 103 173 v.2.2.1),
- ASiC (ASiC Electronic Signatures zgodne z ETSI TS 103 174 v.2.2.1).

Obsługiwane są wszystkie poziomy podpisu/pieczęci: B-Level (Basic), T-Level (Timestamped), LT-Level (Long Term) and LTA-Level (Long Term with Archive time-stamps).

Podpisy/pieczęcie mogą być integralne z podpisywaną treścią lub odłączone (w osobnym pliku). Walidowane dokumenty mogą zawierać wiele podpisów/pieczęci, w tym kontrasygnaty.

W celu potwierdzenia ważności podpisu lub pieczęci, Usługa musi dysponować informacjami o unieważnieniach certyfikatów z odpowiedniej daty, w związku z tym istnieją pewne ograniczenia co do możliwości potwierdzenia ważności (TOTAL-PASSED) podpisów/pieczęci historycznych. Potwierdzone mogą być:

- podpisy/pieczęcie złożone przy użyciu certyfikatów, dla których okres ważności jeszcze nie minął w momencie walidacji podpisu/pieczęci,
- podpisy/pieczęcie złożone przy użyciu certyfikatów, których okres ważności już minął w momencie walidacji podpisu/pieczęci, pod warunkiem, że:
    - są to prawidłowo konserwowane podpisy/pieczęcie poziomu LTA-Level albo
    - są to podpisy/pieczęcie złożone z wykorzystaniem certyfikatów - wystawionych przez polskich kwalifikowanych dostawców usług zaufania (znajdujących się na polskiej liście TSL) - których okres ważności minął nie wcześniej niż 28 grudnia 2020 r., albo
    - w ograniczonym zakresie, w miarę dostępności historycznych informacji o unieważnieniach – są to podpisy/pieczęcie złożone z wykorzystaniem certyfikatów, wystawionych przez kwalifikowanych dostawców usług zaufania, znajdujących się na liście TSL jednego z krajów UE, których okres ważności minął nie wcześniej niż 28 grudnia 2020 r.

Integralność i pochodzenie raportu walidacji są gwarantowane poprzez zaawansowaną pieczęć elektroniczną Usługi, złożoną przy użyciu należącego do CenCert klucza i certyfikatu służącego do realizacji Usługi, znajdującego się na krajowej liście TSL.

Raport walidacji jest wystawiany w formatach XML oraz PDF. Raport w postaci XML jest zgodny z normą ETSI TS 119 102-2 v 1.3.1.

Obie postacie raportu walidacji są oznaczone tym samym identyfikatorem i stanowią komplet. Obie postaci raportu są spójne pomiędzy sobą, w szczególności zawierają takie same statusy walidacji podpisów/pieczęci. Postać PDF raportu jest zoptymalizowana pod kątem czytelności w języku naturalnym. Postać XML jest przeznaczona głównie do odczytywania maszynowego i zawiera więcej szczegółów dotyczących procesu walidacji.

Raport zawiera jednoznaczne wskazanie na dane wejściowe Usługi, w tym dane identyfikujące pliki składające się dokument i podpis/podpisy (w tym reprezentacje danych w postaci skrótów kryptograficznych) oraz dane nt. wykorzystanych informacji o unieważnieniach.

A.2.4 Wymagania polityki tworzenia oprogramowania

W miarę możliwości, CenCert uczestniczy w dostępnych testach interoperacyjności oprogramowania służącego do walidacji podpisów/pieczęci, organizowanych przez ETSI i/lub inne organizacje Unii Europejskiej lub krajowe. Wyniki testów są szczegółowo analizowane i mogą być podstawą zmian w realizacji usługi.

A.2.5 Wymagania ogólne

Nie określono dodatkowych wymagań.

A.3 Parametry zakresu biznesowego (BSP)

A.3.1 BSP odnoszące się głównie do danej aplikacji/procesu biznesowego

A.3.1.1 BSP (a): Przepływ procesu, sekwencjonowanie i synchronizacja podpisów

Nie dotyczy.

A.3.1.2 BSP (b): Podpisywane dane

Usługa nie nakłada żadnych ograniczeń na format ani na wielkość podpisanych danych. Ograniczenie na wielkość plików może jednak wynikać z przyczyn technicznych, w tym z infrastruktury IT udostępnianej przez użytkownika do instalacji DA.

A.3.1.3 BSP (c): Relacja pomiędzy podpisami a podpisanymi danymi

Raport z walidacji zawiera informację, jeśli dany podpis nie obejmuje całego dokumentu, przy czym podpis może obejmować treść dokumentu bezpośrednio (odnosząc się do skrótu z dokumentu) lub pośrednio (odnosząc się do wcześniejszego podpisu lub znacznika czasu, który się odnosi do skrótu z dokumentu).

Obsługiwane formaty i poziomy podpisu określone są w rozdziale A.2.3.

A.3.1.4 BSP (d): Społeczność docelowa

Nie dotyczy.

A.3.1.5 BSP (e): Zaadresowanie odpowiedzialności za walidację i rozszerzenie podpisu

W ramach Usługi wykonywana jest walidacja podpisu/pieczęci. Wraz z usługą walidacji, w zależności od ustaleń z klientem, mogą być udostępnione możliwości rozszerzenia podpisu do bardziej zaawansowanych form (znakowanie czasem itd.), ale opcje te nie są częścią usługi walidacji i są ewentualnie inicjowane dla danego dokumentu przez klienta.

A.3.2 BSP zależne głównie od przepisów prawnych/regulacyjnych związanych z daną aplikacją/procesem biznesowym

A.3.2.1 BSP (f): Rodzaj podpisów z prawnego punktu widzenia

Usługa jest przeznaczona do walidacji kwalifikowanych podpisów i pieczęci elektronicznych. Umożliwia również walidację wybranych typów zaawansowanych podpisów/pieczęci elektronicznych, informując wyraźnie o typie podpisu/pieczęci, w szczególności czy jest to podpis/pieczęć kwalifikowana.

Usługa potwierdza ważność podpisu/pieczęci, w jej zakresie nie leży natomiast rozstrzyganie, czy określony typ podpisu/pieczęci jest odpowiedni pod względem prawnym do danego zakresu czynności lub danego dokumentu, jak również za to, czy liczba podpisów/pieczęci jest odpowiednia, czy podpisujące się osoby są odpowiednio umocowane itd.

A.3.2.2 BSP (g): Zobowiązanie przyjęte przez podpisującego

Parz rozdział A.1.2.3.

A.3.2.3 BSP (h): Poziom pewności w odniesieniu do dowodów związanych z czasem

Następujące źródła czasu mogą być użyte jako dowód istnienia danego podpisu/pieczęci w określonym momencie (POE):

1) Kwalifikowane znaczniki czasu,
2) Czas własny serwera CenCert realizującego Usługę, synchronizowany z czasem UTC(pl) zgodnie z zapisami rozdziału 6.8 polityki.
3) Czas wprowadzony przez klienta usługi walidacji.

W przypadku opisanym w pkt. 3) powyżej, fakt pobrania czasu, w którym istniał podpisany dokument, od klienta Usługi, jest wyraźnie odnotowany na raporcie walidacji, wraz z informacją, że raport walidacji stanowi dowód ważności podpisu/pieczęci wyłącznie w połączeniu z dowodem istnienia dokumentu w określonym czasie, który to dowód leży po stronie klienta usługi.

A.3.2.4 BSP (i): Formalności związane z podpisywaniem

Nie dotyczy.

A.3.2.5 BSP (j): Trwałość i odporność na zmiany

Raporty walidacji są pieczętowane kluczem CenCert służącym do realizacji Usługi, z którym jest związany certyfikat zapisany na liście TSL, z okresem ważności kończącym się nie wcześniej niż 8 lat od momentu wystawienia raportu walidacji.

Raporty z walidacji są przechowywane przez CenCert przez 10 lat od momentu wystawienia

A.3.2.6 BSP (k): Archiwizacja

Nie dotyczy.

A.3.3 BSP związane głównie z podmiotami zaangażowanymi w tworzenie/rozszerzanie/walidację podpisów

A.3.3.1 BSP (l): Tożsamość (i role/atrybuty) podmiotów podpisujących

Raport z walidacji jest pieczętowany kluczem CenCert służącym do realizacji Usługi. Dane identyfikacyjne certyfikatu określone są w rozdziale 7.1.1. polityki.

Podmiot, który wykonał podpis lub pieczęć podlegająca walidacji, jest identyfikowany na raporcie z walidacji poprzez prezentację pełnej zawartość identyfikatora DN, w tym w szczególności:

1) dla podpisu elektronicznego opartego na kwalifikowanym certyfikacie:
   a) imię, nazwisko
   b) pseudonim (jeśli certyfikat zawiera pseudonim)
   c) zawartość pola identyfikatora DN „serial numer”
2) dla pieczęci elektronicznej opartej na kwalifikowanym certyfikacie:
   a) nazwę organizacji,
   b) nazwę jednostki organizacyjnej (jeśli jest podana)
   c) zawartość pola identyfikatora DN „serial numer”.

A.3.3.2 BSP (m): Poziom pewności wymagany do uwierzytelnienia podmiotu podpisującego

Raport z walidacji jest pieczętowany w sposób automatyczny, przez system informatyczny służący do realizacji Usługi. Oprogramowanie tego systemu jest zatwierdzane w ramach audytu realizowanego zgodnie z art. 20.1 eIDAS.

A.3.3.3 BSP (n): Urządzenia do tworzenia podpisów

Klucz do podpisywania raportu z walidacji umieszczony jest na hsm zgodnie z zapisami rozdziału 6.2 polityki. Aktywacja klucza jest realizowana zgodnie z zapisami rozdziału 6.4.

A.3.4 Inne BSP

A.3.4.1 BSP (o): Inne informacje, które mają być powiązane z podpisem

Nie zawarto postanowień.

A.3.4.2 BSP (p): Zestawy kryptograficzne

Raport walidacji jest pieczętowany przy użyciu algorytmów podpisu/pieczęci i ich parametrów określonych w rozdziale 6.1.5.

W zakresie walidowanych podpisów/pieczęci, akceptowane są następujące algorytmy kryptograficzne:

1) Akceptuje się następujące algorytmy kryptograficzne podpisu/pieczęci: RSA (PKCS#1 v.1.5, RSA-PSS), ECDSA, DSA.
2) Akceptuje się następujące funkcje skrótu użyte do wystawienia kwalifikowanego certyfikatu i list CRL, tokenów OCSP, znaczników czasu:
    a. SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512
    b. SHA-1 ale tylko do pieczęci/podpisów wystawionych przed 1 lipca 2018 r.
3) Akceptuje się następujące funkcje skrótu zastosowane do walidowanego podpisu / pieczęci:
    a. SHA-224, SHA-256, SHA-384, SHA-512, SHA3-224, SHA3-256, SHA3-384, SHA3-512
    b. SHA-1 ale tylko do podpisów/pieczęci wystawionych przed 1 lipca 2018 r. (patrz rozdział A.3.2.3 w zakresie ustalania czasu złożenia podpisu/pieczęci)

A.3.4.3 BSP (q): Środowisko technologiczne

Nie zawarto postanowień.

A.4 Wymagania i oświadczenia dotyczące mechanizmów technicznych i implementacji standardów

Nie zawarto postanowień.

A.5 Pozostałe kwestie biznesowe i prawne

Nie zawarto postanowień.

A.6 Audyt zgodności i inne oceny

Obowiązują postanowienia zawarte w rozdziałach 8 oraz 6.5.