KWALIFIKOWANE CENTRUM CERTYFIKACJI „CENCERT”

POLITYKA CERTYFIKACJI DLA CERTYFIKATÓW KWALIFIKOWANYCH

Wersja: 2.3

Karta dokumentu:

Tytuł dokumentu	Polityka certyfikacji dla certyfikatów kwalifikowanych
Właściciel dokumentu	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Wersja	2.3
Status dokumentu	Zatwierdzony
Data zatwierdzenia	7 grudnia 2016 r.
Liczba stron	45

zatwierdzone przez:

Wersja	**zatwierdzający**
2.3	Zarząd Enigma Systemy Ochrony Informacji Sp. z o.o.

historia wersji

Wersja	**Data**	**Komentarze**
1.0	2008-09-17	Wersja początkowa; Do zatwierdzenia.
1.1	2009-06-22	Wersja obowiązująca.
1.2	2009-09-07	Wprowadzenie poprawek wynikających z uwag ministerstwa
1.21	2010-01-11	Poprawienie numeru OID, inne drobne poprawki; zmiana sposobu uwierzytelnienia przy unieważnianiu i zawieszaniu certyfikatów
1.22	2010-03-15	Zmiana rozszerzenia certyfikatu *CertificatePolicies* na „anyPolicy”
1.23	2010-08-26	Zmiana sposobu zapisu imienia i nazwiska w certyfikacie – w atrybucie commonName oraz dodatkowo w atrybutach sureName i givenName
2.0	2011-01-19	Zmiany wynikające z przejęcia firmy Safe Technologies S.A. przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o.
2.01	2011-10-19	Zmiana OID polityki na 1.2.616.1.113681.1.1.10.1.1.2 (OID umieszczony w TSL). Zmiana rozszerzenia certyfikatu *CertificatePolicies* na OID polityki. Dodanie możliwości uwierzytelnienia Subskrybenta na podstawie Karty pobytu. Drobne poprawki gramatyczne.
2.02	2012-04-11	Dodanie opcjonalnego drugiego atrybutu CommonName (w celu lepszej identyfikacji Subskrybenta w określonym środowisku), poprawienie błędnego nr wpisu do Rejestru kwalifikowanych

		podmiotów (w identyfikatorze DN CCK CenCert), poprawki redakcyjne w zakresie zasad odpowiedzialności finansowej,
2.1	2014-10-15	Zmiana adresu Centralnego Punktu Rejestracji (na ul. Jagiellońską 78). Przegląd i uaktualnienie całego dokumentu, liczne drobne poprawki redakcyjne, usunięcie uszczegółowień w celu poprawienia czytelności dokumentu.
2.2	2016-06-27	Powołanie się na eIDAS, zmiana niektórych odwołań do przepisów oraz zapisu o audytach (rozdz. 8). Dodanie możliwości wygenerowania kluczy subskrybenta na podstawie pisemnej umowy/zamówienia, przed jego identyfikacją (rozdz. 4.2, 6.1.2). Usunięcie możliwości generowania klucza na podstawie PKCS#10 (rozdz. 6.1.3), zamieszczenie zapisów o generowaniu klucza Subskrybenta w jego obecności. Dodanie możliwości umieszczania w certyfikacie tylko jednego imienia (rozdz. 3.1). Inne drobne poprawki.
2.3	2016-12-02	Aktualizacja całej polityki w związku z ustawą o usługach zaufania.

Spis treści

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji Kluczy ***CenCert*** prowadzone przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o. w celu realizacji usług zaufania polegających na wystawianiu kwalifikowanych certyfikatów.

Centrum Certyfikacji Kluczy realizujące niniejszą politykę stanowi kwalifikowany podmiot świadczący usługi certyfikacyjne, zgodnie z *Rozporządzeniem 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 uchylającym dyrektywę 1999/93/WE* oraz *ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej*.

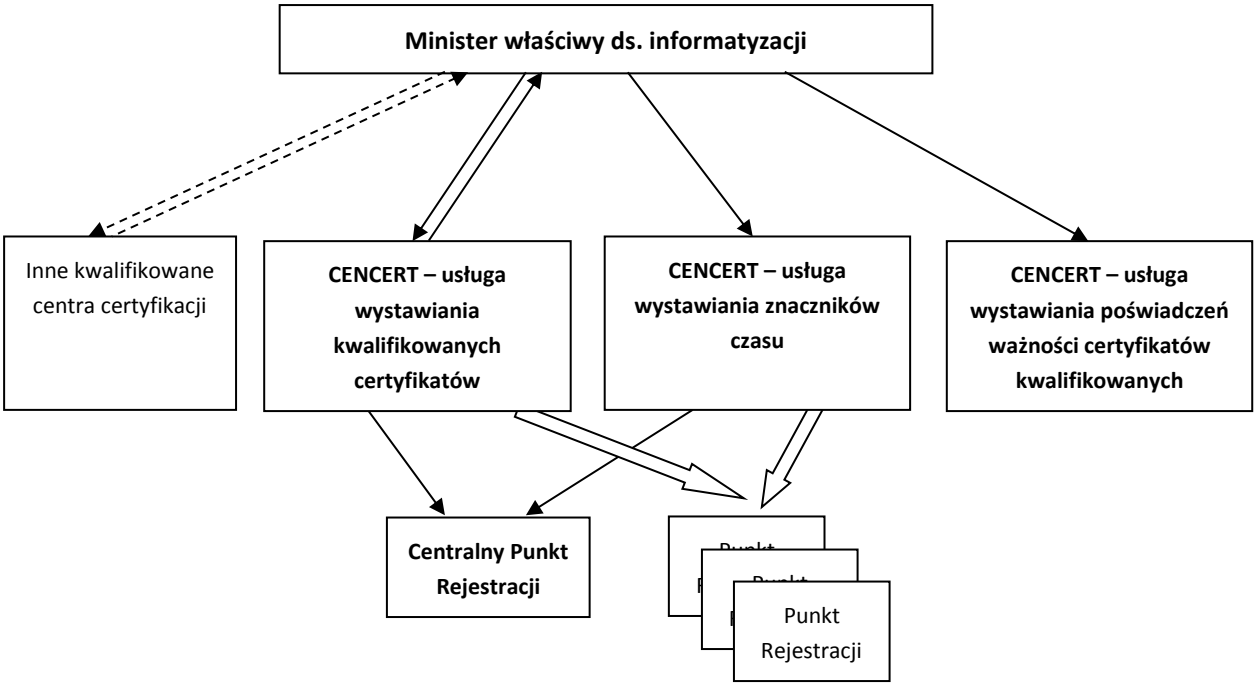
Struktura dokumentu została oparta na dokumencie RFC 3647 "*Internet X.509 Public Key Infrastructure Certification Policy and Certification Practices Framework*".

1.2. Identyfikator polityki certyfikacji

Nazwa polityki	Polityka certyfikacji dla certyfikatów kwalifikowanych
Kwalifikator polityki	Brak
Numer OID (ang. *Object Identifier*)	1.2.616.1.113681.1.1.10.1.1.2
Data wprowadzenia	9 grudnia 2016 r.
Data wygaśnięcia	Do odwołania

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

CCK CenCert, zgodnie z przepisami o podpisie elektronicznym, jest częścią systemu PKI obejmującego kwalifikowane podmioty certyfikacyjne. Rolę Nadrzędnego CCK (tzw. „*Root CA*") pełni Minister właściwy do spraw informatyzacji lub podmiot, któremu Minister powierzył to zadanie. CCK CenCert, wraz z innymi kwalifikowanymi podmiotami, pełni rolę „operacyjnego urzędu certyfikacji" w ramach struktury PKI i wystawia certyfikaty dla użytkowników końcowych (Subskrybentów). CCK CenCert nie wystawia certyfikatów dla żadnych podległych centrów certyfikacji.



CCK CenCert obsługuje Subskrybentów poprzez:

- Centralny Punkt Rejestracji (CPR), którego dane znajdują się w rozdziale 1.5.
- Inne Punkty Rejestracji,
- Inne punkty prowadzące pełną lub częściową obsługę Subskrybentów (np. w zakresie potwierdzania tożsamości Subskrybentów przy zawieraniu umów), zgodnie z aktualnymi potrzebami Subskrybentów i możliwościami CCK CenCert.

Punkty rejestracji oraz inne punkty prowadzące obsługę Subskrybentów są tworzone adekwatnie do aktualnych potrzeb Subskrybentów i możliwości CCK CenCert. Wyjątkiem jest Centralny Punkt Rejestracji (CPR), który może być zlikwidowany jedynie przy spełnieniu

wszystkich wymagań obowiązujących przepisów o podpisie elektronicznym (w tym przy zapewnieniu dalszego spełniania przez CCK wszystkich wymagań związanych z obsługą Subskrybentów).

CPR prowadzi całodobowy dostęp do usług unieważniania i zawieszania certyfikatów dla CCK CenCert.

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

Subskrybentem usług certyfikacyjnych może być każda osoba fizyczna posiadająca pełną zdolność do czynności prawnych.

Stroną ufającą może być każda osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej mająca potrzebę weryfikacji kwalifikowanego podpisu elektronicznego weryfikowanego przy użyciu certyfikatu wystawionego zgodnie z niniejszą polityką certyfikacji.

1.4. Zakres zastosowań

Kwalifikowane certyfikaty wystawiane zgodnie z niniejszą polityką certyfikacji mogą służyć wyłącznie do weryfikacji kwalifikowanych podpisów elektronicznych.

1.5. Zasady administrowania polityką certyfikacji

Podmiotem uprawnionym do administrowania polityką certyfikacji, w tym zatwierdzania, zatwierdzania zmian itd., jest 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.

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

Centralny Punkt Rejestracji
Centrum Certyfikacji Kluczy *CenCert*
ENIGMA Systemy Ochrony Informacji Sp. z o.o.
03-301 Warszawa
ul. Jagiellońska 78

Telefony kontaktowe i numer faksu są publikowane na stronie www.cencert.pl.

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 są ogólnymi definicjami danego terminu, lecz wyjaśniają znaczenie danego terminu lub akronimu w kontekście używanym w CCK CenCert.

Termin/akronim	Opis
CCK	Centrum Certyfikacji Kluczy – dostawca usługi zaufania polegającej na wystawianiu kwalifikowanych certyfikatów.
CPR	Centralny Punkt Rejestracji CenCert. Dane kontaktowe CPR zamieszczone są w rozdziale 1.5.
CRL	Lista unieważnionych certyfikatów. Jest wystawiana, podpisywana elektronicznie i publikowana przez CCK.
DN	Identyfikator DN – *Distinguished Name* – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500
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).
Klucz prywatny	Dane służące do składania podpisu/pieczęci elektronicznej.
Klucz publiczny	Dane służące do weryfikacji podpisu/pieczęci elektronicznej, zazwyczaj dystrybuowane w postaci certyfikatu.
OCSP	*Online Certificate Status Protocol* - protokół i nazwa usługi PKI służącej do informowania o statusie konkretnych certyfikatów, o które pyta usługobiorca (czy certyfikat jest ważny, czy unieważniony)

Termin/akronim	Opis
PKI	*Public Key Infrastructure* – infrastruktura klucza publicznego – system obejmujący Centra Certyfikacji Kluczy, Punkty Rejestracji oraz użytkowników końcowych, służący do dystrybucji certyfikatów klucza publicznego oraz zapewnienia możliwości ich wiarygodnej weryfikacji
Subskrybent	Osoba, której wystawiono (lub która ubiega się o wystawienie) kwalifikowany certyfikat, zgodnie z niniejszą polityką certyfikacji.
Dokument tożsamości	Dowód osobisty, paszport (w tym paszport wydany przez inny kraj) albo karta pobytu, wydana na podstawie Ustawy z dnia 12 grudnia 2013 r. o cudzoziemcach.
Ustawa	Ustawa z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej.
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
NCCert	Root krajowego systemu PKI, prowadzony przez Narodowy Bank Polski, na podstawie upoważnienia ministra właściwego ds. informatyzacji.
TSL	EU Trust service Status List – listy wydawane przez Komisję Europejską (lista list) oraz kraje członkowskie EU, 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.).
SSCD/QSCD	*SSCD - Secure Signature Creation Device* – urządzenie posiadające certyfikat umożliwiający użycie do wystawiania bezpiecznego podpisu elektronicznego, na podstawie *Dyrektywy Parlamentu Europejskiego i Rady 1999/93/WE. z dnia 13 grudnia 1999 r. w sprawie wspólnotowych ram w zakresie podpisów elektronicznych*. QSCD - *Qualified Signature Creation Device* – urządzenie posiadające certyfikat umożliwiający użycie do wystawiania kwalifikowanego pieczęci/podpisu elektronicznego, na podstawie eIDAS.

2. Zasady dystrybucji i publikacji informacji

CCK publikuje następujące informacje:

- Aktualny klucz/klucze publiczne CCK (w postaci certyfikatów wystawionego przez NCCert).
- Aktualną listę CRL.
- Aktualną politykę certyfikacji, materiały marketingowe, komunikaty bieżące itd.

CCK nie publikuje certyfikatów Subskrybentów.

Powyższe informacje dostępne są w repozytorium dostępnym pod adresem **www.cencert.pl** za pomocą protokołu HTTP/HTTPS. Protokół HTTPS zapewnia uwierzytelnienie serwera WWW, na którym znajduje się repozytorium, z poziomu popularnych przeglądarek internetowych.

3. Identyfikacja i uwierzytelnienie

Niniejszy rozdział opisuje zasady identyfikacji i uwierzytelnienia stosowane przez CCK przy operacjach tego wymagających – w szczególności przy wystawianiu, unieważnianiu i zawieszaniu 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.

CCK CenCert nie wystawia certyfikatów anonimowych (w szczególności certyfikatów zawierających wyłącznie pseudonim).

CCK CenCert na życzenie Subskrybenta, po przedstawieniu odpowiednich dokumentów, zawiera w certyfikacie Subskrybenta dodatkowo dane osoby prawnej lub innej jednostki organizacyjnej.

CCK CenCert nie sprawdza prawa do posługiwania się zastrzeżonymi znakami towarowymi, nie odpowiada za nieuprawnione wykorzystywanie znaków towarowych i nie jest stroną w przypadku tego typu sporów. W przypadku utraty przez Subskrybenta prawa do posługiwania się daną nazwą lub innym oznaczeniem zamieszczonym w certyfikacie, jest on zobowiązany do zgłoszenia tego faktu celem unieważnienia certyfikatu z powodu nieaktualności danych zawartych w certyfikacie.

Identyfikator wyróżniający Subskrybenta składa się z następujących atrybutów:

Wariant I

Kraj (countryName) = PL

Imię (givenName) = <imiona Subskrybenta>

Nazwisko (sureName) = <nazwisko Subskrybenta>

(opcjonalnie) **Nazwa powszechna (commonName)** = <imiona i nazwisko Subskrybenta>

(opcjonalnie) **Nazwa powszechna (commonName)** = <dane mogące mieć znaczenie dla identyfikacji Subskrybenta w danym środowisku>

Numer seryjny (serialNumber) = <PESEL lub NIP Subskrybenta>

Imię (imiona) i nazwisko (nazwiska) Subskrybenta zapisywane są w brzmieniu zgodnym z zawartym w Dokumencie tożsamości. W przypadku Subskrybentów posiadających kilka imion, dopuszczalne jest wpisanie do certyfikatu tylko jednego imienia, jeśli nie prowadzi to do możliwości popełnienia błędu w identyfikacji Subskrybenta (gdy jest wypełniony poprawnie parametr PESEL lub NIP).

Dane mogące mieć znaczenie dla identyfikacji Subskrybenta w danym środowisku są to dane dodatkowe wpisywane na wniosek Subskrybenta, służące do jego lepszej identyfikacji w środowisku, w którym funkcjonuje. W szczególności taką daną może być np. numer uprawnień do wykonywania zawodu.

Atrybut *Numer seryjny* zawiera numer PESEL lub NIP Subskrybenta w formacie „PESEL: XXXXXXXXXXX" lub „NIP: XXXXXXXXXX".

Wariant II

Kraj (countryName) = PL

Imię (givenName) = <imiona Subskrybenta>

Nazwisko (sureName) = <nazwisko Subskrybenta>

(opcjonalnie) **Nazwa powszechna (commonName)** = <imiona i nazwisko Subskrybenta>

(opcjonalnie) **Nazwa powszechna (commonName)** = <dane mogące mieć znaczenie dla identyfikacji Subskrybenta w danym środowisku>

Numer seryjny (serialNumber) = <PESEL lub NIP Subskrybenta>

Organizacja (organization) = <nazwa firmy>

(opcjonalne) **Nazwa jednostki organizacyjnej (organizationalUnitName)** = <nazwa jednostki organizacyjnej>

Województwo (stateOrProvinceName) = <województwo>

Nazwa miejscowości (*localityName*) = <nazwa miejscowości>

Adres (postalAddress) = <adres pocztowy>

Imię (imiona) i nazwisko (nazwiska) Subskrybenta zapisywane są w brzmieniu zgodnym z zawartym w Dokumencie tożsamości. W przypadku Subskrybentów posiadających kilka imion, dopuszczalne jest wpisanie do certyfikatu tylko jednego imienia, jeśli nie prowadzi to do możliwości popełnienia błędu w identyfikacji Subskrybenta (gdy jest wypełniony poprawnie parametr PESEL lub NIP).

Dane mogące mieć znaczenie dla identyfikacji Subskrybenta w danym środowisku są to dane dodatkowe wpisywane na wniosek Subskrybenta, służące do jego lepszej identyfikacji w środowisku, w którym funkcjonuje. W szczególności taką daną może być np. numer uprawnień do wykonywania zawodu.

Atrybut *Numer seryjny* zawiera numer PESEL lub NIP Subskrybenta w formacie „PESEL: XXXXXXXXXXX" lub „NIP: XXXXXXXXXX".

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* – o ile występuje - zawiera nazwę jednostki organizacyjnej będącej częścią organizacji, której nazwa widnieje w atrybucie *Organizacja*.

Atrybuty *Województwo, Nazwa miejscowości, Adres* zawierają dane podmiotu, którego nazwa widnieje w atrybucie Organizacja. Atrybut *Adres* powinien być w takiej postaci, w jakiej adresy są umieszczane na przesyłkach.

3.2. Uwierzytelnienie Subskrybenta przy wystawieniu pierwszego certyfikatu

Uwierzytelnienie Subskrybenta dokonywane jest przez Inspektora ds. rejestracji na podstawie Dokumentu tożsamości. Inspektor ds. rejestracji poświadcza dokonanie uwierzytelnienia Subskrybenta własnoręcznym podpisem oraz podaniem swojego numeru PESEL, w pisemnym oświadczeniu o potwierdzeniu tożsamości wnioskodawcy.

Dla certyfikatu zawierającego wyłącznie dane osoby fizycznej (certyfikat bez atrybutu *Organizacja*), w celu weryfikacji tożsamości wymagane są następujące dokumenty:

- Ważny Dokument tożsamości (patrz definicja w rozdz. 1.6).
- Jeśli certyfikat ma zawierać numer NIP - oryginał dokumentu przyznającego numer NIP.

Dla certyfikatu zawierającego dane osoby fizycznej oraz dane innej osoby (certyfikat z atrybutem Organizacja), w celu weryfikacji tożsamości wymagane są następujące dokumenty:

- Ważny Dokument tożsamości (patrz definicja w rozdz. 1.6).
- Jeśli certyfikat ma zawierać numer NIP - oryginał dokumentu przyznającego numer NIP Subskrybenta (osoby fizycznej).
- Uwierzytelnioną kopię lub odpis dokumentu określającego zasady reprezentacji organizacji (np. wyciąg z Rejestru KRS, statut itd.) - przy czym w przypadku rejestrów KRS i CEDG wystarczający jest odpowiednio wydruk z systemu KRS pobrany na podstawie art. 4 ust. 4aa *Ustawy z dnia 20 sierpnia 1997 r. o Krajowym Rejestrze Sądowym* (https://ems.ms.gov.pl) albo wydruk z systemu CEDG zgodny z art. 38 ust. 4 *Ustawy z dnia 2 lipca 2004 r o swobodzie działalności gospodarczej* (https://prod.ceidg.gov.pl)
- Upoważnienie do wystawienia certyfikatu podpisane przez uprawniona osobę. Upoważnienie powinno dotyczyć konkretnego Subskrybenta.

Dla certyfikatu zawierającego dodatkowy atrybut *Nazwa powszechna*, zawierający *dane mogące mieć znaczenie dla identyfikacji Subskrybenta w danym środowisku*, przed wydaniem certyfikatu następuje weryfikacja prawdziwości tych danych, w sposób zależny od rodzaju danych, np. dla danych zawierających numer uprawnień do wykonywania danego zawodu wymaga się okazania dokumentu przyznającego to uprawnienie.

3.3. Uwierzytelnienie Subskrybenta przy wystawianiu kolejnych certyfikatów

W przypadku, gdy w momencie uzyskiwania nowego certyfikatu Subskrybent posiada ważny kwalifikowany certyfikat, wystawiony zgodnie z niniejszą polityką certyfikacji, wszelkie dokumenty związane z otrzymaniem nowego certyfikatu mogą być podpisane elektronicznie.

Uwierzytelnienie Subskrybenta opiera się w takim przypadku na weryfikacji ważności złożonego przez niego kwalifikowanego podpisu elektronicznego.

W każdym przypadku można realizować procedury przewidziane dla wystawienia pierwszego certyfikatu Subskrybenta.

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

Unieważnienie certyfikatu jest realizowane na wniosek Subskrybenta lub podmiotu, którego dane są zawarte w certyfikacie Subskrybenta. Certyfikat może być też unieważniony z innych powodów, przewidzianych przepisami o podpisie elektronicznym.

Podmiot, którego dane są zawarte w certyfikacie Subskrybenta, unieważnia certyfikat poprzez przesłanie do Centralnego Punktu Rejestracji wniosku o unieważnienie certyfikatu, podpisanego przez osobę (osoby) upoważnioną.

Subskrybent może unieważnić, zawiesić bądź przywrócić ważność zawieszonego certyfikatu certyfikat poprzez osobistą wizytę lub kontakt telefoniczny z CPR.

W przypadku wizyty osobistej tożsamość Subskrybenta jest weryfikowana na podstawie Dokumenty tożsamości.

W przypadku kontaktu telefonicznego - tożsamość Subskrybenta jest weryfikowana na podstawie hasła ustalonego przy wystawieniu certyfikatu, a przy zawieszaniu certyfikatu, na podstawie hasła lub danych osobowych podanych przy wystawieniu certyfikatu.

Uchylenie zawieszenia certyfikatu jest możliwe jedynie przed upłynięciem 7 dni od zawieszenia. Po tym terminie certyfikaty są automatycznie unieważniane.

4. Cykl życia certyfikatu – wymagania operacyjne

4.1. Zgłoszenie certyfikacyjne

Centrum Certyfikacji Kluczy wystawia certyfikat każdorazowo na podstawie zgłoszenia certyfikacyjnego, podpisanego elektronicznie przez uprawnioną osobę pełniącą funkcję Inspektora ds. Rejestracji.

Zgłoszenie certyfikacyjne jest wystawiane przez Inspektora ds. Rejestracji:

1. po poprawnej identyfikacji Subskrybenta zgodnie z rozdz. 3.2 niniejszej polityki certyfikacji oraz podpisaniu przez niego stosownych, wymaganych prawem, dokumentów, lub
2. po poprawnej identyfikacji Subskrybenta zgodnie z rozdz. 3.3 niniejszej polityki certyfikacji oraz podpisaniu przez niego (w formie elektronicznej) stosownych, wymaganych prawem, dokumentów, lub
3. na podstawie pisemnego zamówienia lub umowy zawierającej dane Subskrybenta do umieszczenia w certyfikacie.

W przypadku wystawienia zgłoszenia certyfikacyjnego na podstawie pisemnego zamówienia/umowy, karta elektroniczna zawierająca parę kluczy Subskrybenta oraz jego certyfikat, jest zabezpieczona oraz następnie niezwłocznie dostarczona Subskrybentowi zgodnie z zapisami rozdziału 6.1.2 polityki. Wydanie karty Subskrybentowi możliwe jest jedynie po jego identyfikacji przez Inspektora ds. rejestracji, zgodnie z rozdz. 3.2 niniejszej polityki oraz podpisaniu przez niego stosownych, wymaganych prawem, dokumentów.

W przypadku opisanym w pkt. 2 powyżej (identyfikacja Subskrybenta zgodnie z rozdz. 3.3 polityki) wystawia się certyfikat zawierający te same dane identyfikacyjne Subskrybenta (w tym ewentualnie dane firmy/organizacji zawarte w certyfikacie), co certyfikat pierwotny. Nie jest wymagana ponowna zgoda firmy/organizacji na umieszczenie jej danych w certyfikacie.

4.2. Przetwarzanie zgłoszeń certyfikacyjnych

Po wypełnieniu wymogów formalnych określonych w rozdziale 4.1 inspektor ds. rejestracji wprowadza do systemu informatycznego Centrum Certyfikacji Kluczy zgłoszenie certyfikacyjne.

System informatyczny Centrum Certyfikacji Kluczy niezwłocznie po odebraniu zgłoszenia weryfikuje podpis elektroniczny oraz uprawnienia Inspektora ds. rejestracji, a następnie generuje certyfikat oraz udostępnia go Inspektorowi ds. rejestracji.

Zgłoszenie jest automatycznie odrzucane w przypadku niepoprawnego podpisu elektronicznego Inspektora ds. rejestracji, jego niewystarczających uprawnień lub zawarcia w zgłoszeniu błędnych wartości parametrów certyfikatu, powodujących niezgodność z polityką CCK (np. niewłaściwa długość klucza, zbyt długi okres ważności certyfikatu itd.).

4.3. Wystawienie certyfikatu

Po wprowadzeniu poprawnego zgłoszenia certyfikacyjnego przez Inspektora ds. rejestracji, certyfikat jest automatycznie wystawiany i przesyłany Inspektorowi ds. rejestracji.

4.4. Akceptacja certyfikatu

Wstępna akceptacja certyfikatu jest wykonywana przez Inspektora ds. rejestracji niezwłocznie po wystawieniu certyfikatu, a przed nagraniem go na jakikolwiek nośnik. Inspektor sprawdza, czy dane zawarte w certyfikacie są prawidłowe. W przypadku niezaakceptowania certyfikatu jest on natychmiast unieważniany.

Do sprawdzenia i akceptacji certyfikatu zobowiązany jest Subskrybent niezwłocznie po otrzymaniu certyfikatu, a przed jego użyciem (w szczególności przed wykonaniem pierwszego podpisu elektronicznego 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 CCK, 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 elektronicznych składanych przez Subskrybentów, zgodnie z niniejszą polityką certyfikacji i ewentualnymi ograniczeniami zastosowań danego certyfikatu zapisanymi w certyfikacie.

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

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

Osoba weryfikująca podpis elektroniczny, w celu zapewnienia wartości dowodowej podpisu powinna zapewnić możliwość udowodnienia, że podpis elektroniczny został złożony nie później niż w określonym momencie. Na ten moment powinna być badana ważność certyfikatu służącego do weryfikacji podpisu. Najprostszą metodą uzyskania możliwej do udowodnienia daty podpisu jest oznaczenie podpisu znacznikiem czasu wystawionym przez kwalifikowanego dostawcę usług zaufania.

W celu zabezpieczenia wartości dowodowej podpisu po upłynięciu ważności klucza CenCert, którym był opieczętowany certyfikat, znacznik czasu lub token OCSP, należy stosować tzw. wyższe formy podpisu elektronicznego, określone w odpowiednich normach międzynarodowych określających formaty podpisu. Formy te polegają na dołączeniu do podpisu elektronicznego dodatkowych danych, takich jak certyfikat używany do weryfikacji, znacznik czasu, dodatkowe certyfikaty ścieżki certyfikacji, lista CRL lub odpowiedź OCSP.

4.5.2 Korzystanie z klucza prywatnego

Klucz prywatny związany z certyfikatem Subskrybenta może służyć wyłącznie do składania podpisów kwalifikowanych i powinien podlegać odpowiedniej ochronie.

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

Odblokowanie karty elektronicznej w celu złożenia kwalifikowanego podpisu, poprzez podanie kodu PIN, 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.

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

Subskrybent ponosi wszelką odpowiedzialność za dokumenty elektroniczne opatrzone kwalifikowanym podpisem elektronicznym, jak za dokumenty podpisane własnoręcznie.

4.6. Wymiana certyfikatu

Dopuszcza się wymianę ważnego certyfikatu kwalifikowanego bez zmiany klucza prywatnego Subskrybenta.

Zaleca się, aby Subskrybent przestrzegał maksymalnego okresu ważności klucza prywatnego, o ile okres taki określono dla danej długości klucza w polityce.

Wymiana certyfikatu może się odbyć zdalnie, przy pomocy narzędzi dostarczonych przez Centrum Certyfikacji Kluczy. Wszelkie niezbędne dokumenty formalne mogą być podpisywane przy użyciu dotychczasowego, ważnego w momencie składania podpisów, kwalifikowanego certyfikatu.

Nie ma możliwości wymiany certyfikatu unieważnionego, certyfikatu po upływie terminu ważności oraz w przypadku zmiany jakichkolwiek danych identyfikacyjnych zawartych w certyfikacie. W takim przypadku należy postępować według zasad przewidzianych przy wydawaniu pierwszego certyfikatu.

Wymiana certyfikatu następuje z inicjatywy Subskrybenta.

4.7. Wymiana certyfikatu połączona z wymianą pary kluczy

Wymiana certyfikatu może się odbyć zdalnie, przy pomocy narzędzi dostarczonych przez Centrum Certyfikacji Kluczy. Wszelkie niezbędne dokumenty formalne mogą być podpisywane przy użyciu dotychczasowego, ważnego w momencie składania podpisów, kwalifikowanego certyfikatu.

Nie ma możliwości wymiany certyfikatu unieważnionego, certyfikatu po upływie terminu ważności oraz w przypadku zmiany jakichkolwiek danych identyfikacyjnych zawartych w certyfikacie. W takim przypadku należy postępować według zasad przewidzianych przy wydawaniu pierwszego certyfikatu.

Wymiana certyfikatu następuje z inicjatywy Subskrybenta.

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.

4.9. Unieważnienie i zawieszenie certyfikatu

Podmiotem uprawnionym do unieważnienia certyfikatu jest:

- Subskrybent.
- Organizacja, której dane umieszczono w certyfikacie.
- Centrum Certyfikacji Kluczy.

Subskrybent oraz organizacja, którego dane umieszczono w certyfikacie, ma prawo unieważnić certyfikat w dowolnym czasie (lecz w okresie ważności certyfikatu) z dowolnej przyczyny. Kod powodu unieważnienia, jeśli został podany, umieszczany jest na liście CRL.

Subskrybent jest zobowiązany do niezwłocznego unieważnienia certyfikatu w następujących przypadkach:

- Gdy utracił wyłączną kontrolę nad kluczem prywatnym związanym z certyfikatem kwalifikowanym (np. gdy utracił kartę elektroniczną lub została ona zniszczona, zablokowana itd.)
- Gdy utracił pełną zdolność do czynności prawnych.
- Gdy dane zawarte w certyfikacie są nieprawidłowe.
- W przypadku dezaktualizacji danych Subskrybenta lub podmiotu, z którym związany jest Subskrybent, zawartych w certyfikacie.

Organizacja, której dane umieszczono w certyfikacie, jest zobowiązana do niezwłocznego unieważnienia certyfikatu w następujących przypadkach:

- Gdy dane podmiotu zawarte w certyfikacie są nieprawidłowe.
- W przypadku dezaktualizacji danych podmiotu zawartych w certyfikacie.
- W przypadku utraty okoliczności uzasadniającej zamieszczenie danych organizacji w certyfikacie (np. zwolnienie pracownika, zmiana zakresu obowiązków itd.).

Centrum Certyfikacji Kluczy ma prawo do unieważnienia certyfikatu jedynie w uzasadnionych przypadkach.

Podmiotem uprawnionym do zawieszenia certyfikatu jest Centrum Certyfikacji Kluczy, które zawiesza certyfikat niezwłocznie po powzięciu uzasadnionego podejrzenia, że istnieją przesłanki do zawieszenia bądź unieważnienia certyfikatu, w szczególności na wniosek złożony przez Subskrybenta. W przypadku niepotwierdzenia się przesłanek uzasadniających zawieszenie certyfikatu, Centrum Certyfikacji Kluczy uchyla zawieszenie certyfikatu. W przypadku potwierdzenia podejrzenia oraz w przypadku, gdy Centrum Certyfikacji Kluczy nie jest w stanie wyjaśnić wątpliwości w terminie 7 dni od zawieszenia certyfikatu, certyfikat zostaje unieważniony.

Po unieważnieniu lub zawieszeniu certyfikatu Subskrybenta, jest on niezwłocznie o tym informowany za pośrednictwem poczty elektronicznej.

4.10. Usługi informowania o statusie certyfikatów

Formami informowania przez Centrum Certyfikacji Kluczy o statusie certyfikatów jest lista unieważnionych i zawieszonych certyfikatów (lista CRL) oraz usługa OCSP.

Lista CRL jest wystawiana co około 30 minut, poza okresami ewentualnych przerw technicznych. Niezależnie od okoliczności, CCK gwarantuje wystawianie i publikację list CRL co najmniej raz dziennie, a w przypadku zaistnienia unieważnienia lub zawieszenia certyfikatu, nie później niż w ciągu 1 godziny od momentu unieważnienia bądź zawieszenia certyfikatu.

CenCert udostępnia także usługę OCSP, w ramach której udzielane są elektroniczne, opieczętowane przez CenCert odpowiedzi zawierające status danego certyfikatu. Odpowiedzi te zawierają określenie czasu, na który dana odpowiedź jest udzielona. Czas ten może być wcześniejszy niż moment dostarczenia odpowiedzi lub zadania pytania.

Odpowiedzi OCSP i listy CRL, wystawione po upływie okresu ważności certyfikatu, nie dają miarodajnych odpowiedzi o status certyfikatu.

4.11. Zakończenie umowy certyfikacyjnej

Umowa certyfikacyjna pomiędzy Centrum Certyfikacji Kluczy a Subskrybentem, dotycząca wystawienia certyfikatu, kończy się wraz z upłynięciem terminu ważności określonego w certyfikacie.

Subskrybent oraz podmiot którego dane zawarto w certyfikacie (o ile takie dane zawarto) mogą ponadto zakończyć umowę w każdym czasie, poprzez unieważnienie certyfikatu.

4.12. Powierzanie i odtwarzanie kluczy prywatnych

Centrum Certyfikacji Kluczy nie powierza swojego klucza prywatnego inny podmiotom.

5. Zabezpieczenia organizacyjne, operacyjne i fizyczne

5.1. Zabezpieczenia fizyczne

Centrum Certyfikacji Kluczy jest umiejscowione w pomieszczeniach użytkowanych przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o.

Serwery CCK znajdują się w klimatyzowanej serwerowni, wyposażonej w system ochrony przed zalaniem, pożarem oraz zanikami zasilania, a także system kontroli dostępu oraz system alarmowy włamania i napadu klasy SA3.

Dostęp do pomieszczenia serwerowni jest możliwy tylko dla upoważnionych osób, a każdorazowy fakt dostępu jest odnotowywany.

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

Wszelkie dane i urządzenia istotne dla bezpieczeństwa Centrum Certyfikacji Kluczy i usług przez nie świadczonych (w szczególności karty elektroniczne z elementami klucza prywatnego CCK, kody dostępu do urządzeń, kart i systemów, nośniki archiwizacyjne) są przechowywane w pomieszczeniach CCK o kontrolowanym dostępie, w zamkniętych szafach metalowych.

5.2. Zabezpieczenia proceduralne

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

Nazwa funkcji	Rodzaj obowiązków
Administrator Systemu	Konfigurowanie systemu CCK w zakresie polityki certyfikacji, zarządzanie uprawnieniami dla operatorów systemu.

Nazwa funkcji	Rodzaj obowiązków
Operator Systemu	Stała obsługa systemu teleinformatycznego, w tym wykonywanie kopii zapasowych, zarządzanie uprawnieniami inspektorów ds. rejestracji
Inspektor ds. rejestracji	Weryfikacja tożsamości Subskrybentów, podpisywanie zgłoszeń certyfikacyjnych, zmiana statusu certyfikatów subskrybentów, tworzenie list CRL
Inspektor ds. audytu	Analizowanie zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
Inspektor ds. bezpieczeństwa	Nadzór nad wdrożeniem i stosowaniem wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych

Co do zasady – każdy Inspektor ds. rejestracji jest również Inspektorem ds. unieważniania (rola wymagana przez standard NPR-CEN/TS 419261).

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 bądź zawieszania certyfikatów.

CCK zapewnia możliwość całodobowej obsługi Subskrybentów w zakresie unieważniania certyfikatów, poprzez dane kontaktowe Centralnego Punktu Rejestracji.

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,
- nie były skazane prawomocnym wyrokiem za przestępstwo przeciwko wiarygodności dokumentów, obrotowi gospodarczemu, obrotowi pieniędzmi i papierami

wartościowymi, przestępstwo skarbowe, przestępstwa określone w ustawie o podpisie elektronicznym lub ustawie o usługach zaufania oraz identyfikacji elektronicznej,

- posiadają niezbędną dla pracy na danym stanowisku wiedzę i umiejętności w zakresie technologii realizacji usług certyfikacyjnych świadczonych przez Centrum Certyfikacji Kluczy.

Wszystkie osoby pełniące wymienione funkcje, przed dopuszczeniem do wykonywania obowiązków, są kierowane na szkolenie obejmujące swoim zakresem podstawy systemów PKI oraz materiał odpowiedni dla określonego stanowiska pracy, w tym procedury i regulaminy pracy obowiązujące w CCK CenCert oraz omówienie możliwej odpowiedzialności karnej w zakresie związanym z świadczeniem usług certyfikacyjnych. Szkolenie każdej osoby pełniącej co najmniej jedną z wymienionych funkcji powtarzane jest co 5 lat lub, w razie potrzeby, częściej.

W przypadku gdy określoną funkcję pełni osoba niezatrudniona w firmie prowadzącej CCK na podstawie umowy o pracę, CCK zawiera w umowie z tą osobą lub z firmą, w której jest ona zatrudniona, możliwość dochodzenia przez CCK wszelkich strat, które ewentualnie może ponieść Centrum Certyfikacji Kluczy w wyniku nienależytego wykonywania przez daną osobę obowiązków wynikających z realizowanej przez nią funkcji lub w wyniku nieprzestrzegania obowiązujących przepisów prawa, jak też zasad i regulaminów obowiązujących w CCK.

W przypadku gdy określoną funkcję pełni osoba zatrudniona w firmie prowadzącej CCK 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 podpisie elektronicznym (w szczególności wymagań o poufności, wymagań w zakresie wystawiania i unieważniania certyfikatów) podlegają sankcjom karnym określonym w Ustawie.

5.4. Procedury tworzenia logów audytowych

Centrum Certyfikacji Kluczy zapewnia rejestrowanie wszelkich istotnych zdarzeń związanych z realizacją świadczonych przez CCK usług certyfikacyjnych, a w szczególności następujące zdarzenia:

- rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,

- istotne zdarzenia związane ze zmianami w środowisku systemu, w szczególności tworzenia kont i rodzaju przydzielanych uprawnień,
- zmiany w konfiguracji funkcji rejestrujących zdarzenia, w tym w szczególności każdą modyfikację czasu systemowego,
- czas tworzenia kopii zapasowych,
- czas archiwizowania rejestrów zdarzeń,
- zamykanie, otwieranie i ponowne uruchamianie po zamknięciu systemu,
- żądanie świadczenia usług certyfikacyjnych normalnie udostępnianych przez system lub usług niewykonywanych przez system, informacji o wykonaniu lub niewykonaniu usługi oraz o przyczynie jej niewykonania – w szczególności kompletny, podpisany przez Inspektora ds. rejestracji formularz zawierający polecenie wystawienia bądź unieważnienia certyfikatu,
- istotne zdarzenia związane ze zmianami w środowisku systemu CCK, w tym w podsystemie zarządzania kluczami i certyfikatami,

Poza systemem automatycznego generowania logów przechowywane są następujące zapisy:

- zapisy o instalacji nowego oprogramowania lub o aktualizacjach,
- wszystkie zgłoszenia unieważnienia kwalifikowanego certyfikatu oraz wszystkich wiadomości z tym związanych, a w szczególności wysłane i odebrane komunikaty o zgłoszeniach przesyłane w relacjach posiadacza kwalifikowanego certyfikatu z kwalifikowanym podmiotem świadczącym usługi certyfikacyjne;

Logi są zabezpieczone przed modyfikacją, Logi podlegają procedurom tworzenia kopii zapasowych oraz – w razie potrzeby – są archiwizowane.

Logi są przechowywane przez 3 lata od ostatniego wpisu.

5.5. Archiwizacja zapisów

Procedury archiwizacyjne wykonywane są raz w roku (na początku roku) i obejmują:

- wszystkie kwalifikowane certyfikaty wystawione w poprzednim roku,
- wszystkie listy CRL wystawione w poprzednim roku,
- umowy o świadczenie usług certyfikacyjnych (w postaci elektronicznej) zawarte w ostatnim roku,
- rejestry zdarzeń.

Wszystkie wymienione powyżej informacje przechowywane są przez 20 lat od ich wytworzenia, z wyjątkiem kopii archiwalnych rejestrów zdarzeń, które są przechowywane przez 3 lata.

Zarchiwizowane informacje są usuwane z systemu CCK, o ile były przechowywane w plikach (nie w bazie danych CCK). Zarchiwizowane informacje mogą być usunięte z bazy danych CCK, o ile jest to konieczne i nie zakłóci bieżącej pracy CCK.

5.6. Wymiana pary kluczy Centrum Certyfikacji Kluczy

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

Planowa wymiana pary kluczy CCK następuje nie wcześniej niż w 2 lata i nie później niż w 3 lata po utworzeniu poprzedniej (aktualnej) pary kluczy.

Procedura wymiany pary kluczy polega na:

- Wygenerowaniu nowej pary kluczy.
- Zgłoszeniu nowego klucza publicznego w celu umieszczenia go w certyfikacie wystawionym przez NCCert oraz na liście TSL.
- Otrzymaniu certyfikatu NCCert oraz wydaniu przez NCCert nowej listy TSL.
- Po upływie pewnego czasu, niezbędnego na wczytanie nowych list TSL do programów weryfikujących podpisy - wykonaniu operacji „przełączenia" kluczy w oprogramowaniu CCK, co powoduje, że wszystkie pieczęcie elektroniczne (pod certyfikatami, listami CRL itd.) wystawiane są już przy użyciu nowego klucza CCK. Przy „przełączeniu" kluczy następuje także wygenerowanie zakładkowych certyfikatów kluczy CCK.

5.7. Utrata poufności klucza prywatnego CCK i działanie CCK w przypadku katastrof

5.7.1 Utrata poufności klucza prywatnego CCK

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

Procedury te przewidują w szczególności:

1. Powiadomienie zgłoszenie incydentu zgodnie z eIDAS, poinformowanie Subskrybentów o zaistniałej sytuacji oraz o planie dalszego działania.
2. Wytworzenie nowych kluczy CCK i zgłoszenie ich ministrowi ds. informatyzacji, w celu wystawienia nowego certyfikatu NCCert oraz umieszczeniu 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.

5.7.2 Katastrofy

5.7.2.1 Wyłączenie Centrum Podstawowego

Centrum Certyfikacji Kluczy posiada dwie lokalizacje: Centrum Podstawowe i Centrum Zapasowe, w miejscach oddalonych od siebie.

W obu lokalizacjach przechowywane są klucze CCK do świadczenia usług oraz klucze infrastruktury niezbędne do funkcjonowania CCK.

Zawartość baz danych CCK jest na bieżąco uaktualniana w Centrum Zapasowym, na podstawie zawartości bazy w Centrum Podstawowym.

Centrum podstawowe jest zabezpieczone przed zanikiem zasilania, utratą jednej linii komunikacyjnej, pożarem, zalaniem, awarią pojedynczego komputera, urządzenia lub dysku. Centrum zapasowe jest zabezpieczone przed zanikiem zasilania, pożarem, zalaniem lub awarią pojedynczego dysku.

W przypadku katastrofy, awarii sprzętu lub infrastruktury przekraczającej możliwości wynikające z zabezpieczeń stosowanych w centrum podstawowym, CCK przełącza swoją działalność na centrum zapasowe, zgodnie z posiadanymi procedurami.

5.7.2.2 Wyłączenie Centralnego Punktu Rejestracji

W przypadku katastrofy powodującej wyłączenie Centralnego Punktu Rejestracji, personel CCK niezwłocznie uruchamia Zastępczy Centralny Punkt Rejestracji, obsługujący Subskrybentów w zakresie unieważnienia, zawieszenia i uchylenia zawieszenia certyfikatu.

Centrum Certyfikacji Kluczy niezwłocznie informuje Subskrybentów, za pośrednictwem stron WWW o zaistniałej sytuacji, przekazując w razie potrzeby nowe numery telefonów i faksu.

Uruchomienie Zastępczego Centralnego Punktu Rejestracji powinno nastąpić najpóźniej w ciągu 1 godziny od wyłączenia Centralnego Punktu Rejestracji.

5.7.2.3 Wyłączenie repozytorium CCK i/lub serwera usług OCSP

W przypadku katastrofy polegającej na wyłączeniu działania repozytorium CCK i/lub serwera usług OCSP, o ile analogiczna usługa nie jest świadczona przez Centrum Zapasowe, personel CCK podejmuje wysiłki w celu jak najszybszego przywrócenia działania tych usług.

Brak możliwości pobrania nowej listy CRL z jakiegokolwiek powodu, i/lub brak możliwości skorzystania z usługi OCSP, nie może być w żadnym wypadku interpretowany jako potwierdzenie ważności jakiegokolwiek certyfikatu.

5.8. Zakończenie działalności CCK

Decyzję o zakończeniu działalności CCK podejmuje Zarząd Spółki.

O planowanym zakończeniu działalności niezwłocznie informowany jest minister właściwy ds. informatyzacji, z co najmniej 3-miesięcznym wyprzedzeniem.

O planowanym zakończeniu działalności informowani są także Subskrybenci.

Po zakończeniu działalności klucz prywatny CCK jest niszczony.

O ile inny kwalifikowany podmiot certyfikacyjny nie będzie przejmie działalności CCK, dokumenty i zapisy, co do których jest wymagana archiwizacja, są przekazywane po zakończeniu działalności ministrowi ds. informatyzacji lub podmiotowi przez niego wskazanemu.

6. Zabezpieczenia techniczne

6.1. Generowanie i instalowanie par kluczy

6.1.1 Generowanie par kluczy

Pary kluczy Centrum Certyfikacji Kluczy 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 są generowane samodzielnie przez inspektorów, na karcie elektronicznej na której są następnie przechowywane i przetwarzane.

Klucze Subskrybentów są generowane samodzielnie przez Subskrybentów lub Inspektora ds. rejestracji, na urządzeniu (typowo: karcie elektronicznej) spełniającym wymagania SSCD/QSCD.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

W przypadku wygenerowania klucza prywatnego Subskrybenta przez Inspektora ds. Rejestracji na podstawie pisemnego zamówienia/umowy (zgodnie z rozdz. 4.2 polityki), od momentu wytworzenia jest on zabezpieczony w sposób gwarantujący brak możliwości powielenia go lub wykorzystania do realizacji podpisu elektronicznego.

Wytworzony klucz i certyfikat Subskrybenta jest mu niezwłocznie przekazywany zgodnie z zasadami rozdz. 4.2 polityki.

Karta elektroniczna, na której jest zapisany klucz prywatny Subskrybenta jest technicznie zabezpieczona w sposób umożliwiający potwierdzenie, że klucz prywatny nie był wykorzystany do złożenia podpisu elektronicznego przed przekazaniem karty Subskrybentowi (konieczność jednorazowej, nieodwracalnej aktywacji karty przez Subskrybenta, przed jej użyciem do złożenia podpisu).

6.1.3 Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji

Nie dotyczy.

6.1.4 Dostarczenie klucza publicznego CCK

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

6.1.5 Rozmiary kluczy

Wszystkie klucze, o których mowa w niniejszym rozdziale, są kluczami algorytmu RSA.

Klucze Centrum Certyfikacji Kluczy mają długość 2048 bitów.

Klucze Subskrybentów mają standardowo długość 2048 bitów. W przypadku szczególnych wymagań Subskrybenta (np. wysokowydajne aplikacje podpisujące), klucze mogą być krótsze, jednak nie krótsze niż 1024 bity.

Klucze infrastruktury:

- klucze do ochrony komunikacji pomiędzy CCK a punktami rejestracji mają długość 1024 bity lub większą,
- klucze Inspektorów ds. rejestracji mają długość 2048 bitów.

6.1.6 Cel użycia klucza

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

Klucz prywatny Centrum Certyfikacji Kluczy może być wykorzystywany tylko do podpisywania certyfikatów list CRL i tokenów OCSP zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów, list CRLi i tokenów OCSP.

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

6.2. Ochrona kluczy prywatnych

Urządzenia służące do generowania kluczy kryptograficznych oraz do generowania podpisów (przez Subskrybentów) lub poświadczeń elektronicznych (przez Centrum Certyfikacji Kluczy) muszą posiadać jeden z następujących certyfikatów:

1) ITSEC dla poziomu E3 z minimalną siłą mechanizmów zabezpieczających, określoną jako "wysoka", albo poziomu bezpieczniejszego lub

2) FIPS PUB 140 dla poziomu 3 albo bezpieczniejszego, lub

3) Common Criteria (norma ISO/IEC 15408) dla poziomu EAL4 albo bezpieczniejszego.

Klucz prywatny Centrum Certyfikacji Kluczy jest wytworzony i zapisany z użyciem mechanizmu podziału sekretów „*2 z m*", przy czym *m* wynosi co najmniej 6 i nie więcej niż 8 (do użycia klucza CCK jest potrzebne posiadanie dowolnych 2 fragmentów klucza, wszystkich fragmentów jest *m*).

Klucz prywatny CCK nie jest przekazywany (w tym powierzany) innym podmiotom.

Kopie zapasowe kluczy prywatnych CCK mogą być tworzone, przy zachowaniu takich samych wymagań bezpieczeństwa, jak dla kluczy w lokalizacji oryginalnej.

Kopie zapasowe kluczy prywatnych Inspektorów ds. rejestracji i Subskrybentów nie są tworzone. Wyjątkiem mogą być kopie niektórych kluczy infrastruktury używanych wewnętrznie w CCK i przetwarzanych programowo – o ile takie klucze występują.

Klucze prywatne nie są archiwizowane.

Klucze prywatne Inspektorów ds. rejestracji i Subskrybentów nie są nigdy odczytywane z urządzeń w którym zostały wygenerowane. Klucz prywatny CCK jest odczytywany z urządzenia HSM jedynie w postaci zaszyfrowanych fragmentów klucza, umożliwiających wykorzystanie fragmentu jedynie wewnątrz urządzenia HSM, z zachowaniem wszystkich przewidzianych zabezpieczeń.

Klucze prywatne Centrum Certyfikacji Kluczy są uaktywniane przez personel Centrum Certyfikacji Kluczy zgodnie z procedurami operacyjnymi. Uaktywnienie klucza wymaga obecności co najmniej dwóch uprawnionych osób. Klucz jest aktywny do momentu wyjęcia karty z urządzenia HSM (karta zabezpieczona zamkiem mechanicznym) lub wyłączenia urządzenia HSM.

Klucze prywatne Inspektorów ds. rejestracji są aktywowane przez włożenie karty elektronicznej do czytnika, uruchomienie oprogramowania Centaur PR odwołującego się do karty w celu uwierzytelniania operacji przed CCK i wprowadzenie na klawiaturze stacji roboczej kodu PIN. Klucz jest aktywny do momenty wyjęcia karty z czytnika lub zakończenia działania oprogramowania Centaur PR.

Klucze prywatne Subskrybentów są aktywowane przez włożenie karty elektronicznej do czytnika, uruchomienie oprogramowania podpisującego i wprowadzenie kodu PIN. Klucz jest

aktywny do momenty wyjęcia karty z czytnika lub zgodnie z ustawionymi w aplikacji parametrami (określona liczba podpisów lub określony czas aktywności karty).

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.

Niszczenie kluczy prywatnych CCK wykonywane jest komisyjnie przez personel CCK zgodnie z udokumentowaną procedurą. Wymagana jest obecność co najmniej dwóch osób, w tym osoby pełniącej rolę Inspektora ds. bezpieczeństwa. Wymagana jest identyfikacja kart przed zniszczeniem. Z procedury niszczenia sporządza się protokół.

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

W systemie PKI którego dotyczy niniejsza polityka certyfikacji nie występują klucze infrastruktury służące do szyfrowania podpisywanych danych przez Subskrybentów, nie występują również klucze infrastruktury służące do szyfrowania kluczy prywatnych CCK.

6.3. Inne aspekty zarządzania parą kluczy

Klucze publiczne Centrum Certyfikacji Kluczy prowadzi długoterminową archiwizację swoich kluczy publicznych, na takich zasadach, jakim podlegają inne archiwowane dane.

Okres ważności kluczy prywatnych Subskrybentów nie jest ograniczony. Zaleca się, aby klucze prywatne Subskrybentów, o długości 2048 bitów nie były używane dłużej niż przez 11 lat. Zaleca się, aby klucze prywatne Subskrybentów, o długości 1024 bitów nie były używane dłużej niż przez 2 lata.

Okres ważności certyfikatów Subskrybentów wynosi maksymalnie 2 lata.

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

6.4. Dane aktywujące

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

1. Uaktywnienie klucza CCK wymaga obecności co najmniej dwóch osób pełniących funkcje związane ze świadczeniem usług zaufania.
2. Wszelkie dane aktywujące powinny być zapamiętane przez osoby rutynowo je używające. Kopie tych danych oraz dane używane rzadko są zapisywane przez uprawnioną osobę, a następnie pakowane w nieprzezroczyste koperty. Koperta jest podpisywana i opisywana (zawartość koperty, kto i kiedy pakował) przez osoby pakujące, i zabezpieczona tak, jak przesyłki z materiałami niejawnymi. Tak zabezpieczona koperta jest przechowywana w Centrum Podstawowym i/lub Zapasowym, w pomieszczeniu o kontrolowanym dostępie. Dane aktywujące potrzebne – choćby potencjalnie – w obu lokalizacjach, są zapisywane w dwóch kopiach i przechowywane w obu lokalizacjach.

6.5. Zabezpieczenia komputerów

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

CCK może przeprowadzać audyty, w tym testy penetracyjne, używanego systemu informatycznego. Wyniki audytów nie są publikowane.

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

6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

W Centrum Certyfikacji Kluczy 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.

W szczególności procedura gwarantuje testowanie nowych wersji oprogramowania w środowisku testowym. Gwarantuje także, że do realizacji jakichkolwiek prac w środowisku testowym nie mogą być używane kluczy prywatne CCK służące do poświadczania certyfikatów kwalifikowanych.

Oprogramowanie urządzenia HSM i oprogramowanie używane do obsługi CCK kontroluje swoją integralność przy każdym uruchomieniu. W przypadku błędu integralności urządzenie lub oprogramowanie odmawia dalszej pracy.

6.7. Zabezpieczenia sieci komputerowej

Serwery wykorzystywane przez CenCert do świadczenia usług certyfikacyjnych zgodnie z niniejszą polityka certyfikacji są połączone za pomocą logicznie wydzielonej, dwusegmentowej sieci wewnętrznej.

6.8. Znakowanie czasem

6.8.1 Oznaczanie czasem w procesie wystawiania certyfikatów

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

Zegary stacji roboczych są synchronizowane protokołem NTP z czasem uniwersalnym za pośrednictwem znajdującego się w strukturze CCK, w strefie DMZ, atomowego zegara czasu UTC, synchronizowanego drogą satelitarną.

Zapewnia się synchronizację z czasem UTC zegarów stacji roboczych, służących do znakowania czasem, z dokładnością nie mniejszą niż 1s.

7. Profil certyfikatów i list CRL

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

7.1. Profil certyfikatów i zaświadczeń

7.1.1 Identyfikatory DN

Identyfikator DN Centrum Certyfikacji Kluczy

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**

7.1.2 Profil certyfikatów subskrybentów

Centrum Certyfikacji Kluczy wystawia certyfikaty w formacie zgodnym z Zaleceniem X.509:2000, wersja 3. formatu.

Stosowane są następujące identyfikatory algorytmów kryptograficznych:

Nazwa	**Identyfikator**
Sha-1WithRSAEncryption	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 5 }
RsaEncryption:	{ iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }

Rozszerzenia certyfikatu

Pole	**Opis/wartość**	**krytyczne ?**
Extensions		
AuthorityKeyIdentifier		NIE

Pole	Opis/wartość	krytyczne ?
keyIdentifier	skrót SHA-1 z klucza publicznego	
SubjectKeyIdentifier		NIE
subjectkeyIdentifier	skrót SHA-1 z klucza publicznego	
KeyUsage	nonRepudation	TAK
CertificatePolicies		TAK
PolicyInformation		
CertPolicyId	wartość {1.2.616.1.113681.1.1.10.1.1.2}	
basicConstraints	pusta sekwencja (określenie, że subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)	TAK
crlDistributionPoints	zawiera lokalizacje aktualnego CRL urzędu	NIE
qcStatements		NIE
qcStatement	Deklaracja, że certyfikat jest kwalifikowany	
statementId	id-etsi-qcs-QcCompliance {0.4.0.1862.1.1}	
(opcja) qcStatement	Limit transakcji	
statementId	id-etsi-qcs-QcLimitValue {0.4.0.1862.1.2}	
statementInfo	waluta i wartość limitu	
(opcja) qcStatement	Wskazanie charakteru działalnia podmiotu	
statementId	id-gov-subjectSignatureType {1.2.616.1.101.3.1.1.2}	
statementInfo	weWlasnymImieniu (1), upowaznionyPrzedstawiciel (2), czlonekOrganu (3), organWladzyPuyblicznej (4)	

Certyfikaty mogą zawierać dodatkowe deklaracje QCStatement:

- id-etsi-qcs-QcSSCD {0.4.0.1862.1.4} – deklaracja, że klucz prywatny związany z certyfikatem znajduje się w urządzeniu SSCD/QSCD. Należy zauważyć, że wszystkie klucze prywatne związane z kwalifikowanymi certyfikatami wystawionymi zgodnie z niniejszą polityką certyfikacji znajdują się w urządzeniach SSCD/QSCD, więc brak tego rozszerzenia nie oznacza, że nie zostało użyte urządzenie SSCD/QSCD.

- id-etsi-qct-esign {0.4.0.1862.1.6.1} - deklaracja oznaczająca certyfikat do podpisu elektronicznego zgodny z eIDAS. Brak rozszerzenia nie oznacza braku zgodności z eIDAS
- id-etsi-qcs-QcRetentionPeriod {0.4.0.1862.1.3} – określenie, przez ile lat po upływie ważności certyfikatu będą dostępne fizyczne dokumenty związane z używaniem i wiarygodnością certyfikatu.
- id-etsi-qcs-QcPDS {0.4.0.1862.1.5} – wskazanie (URL) na stronę WWW z oświadczeniami (PDS - *PKI Disclosure Statements*) CCK.

Certyfikaty mogą dodatkowo zawierać niekrytyczne rozszerzenia:

- *AuthorityInfoAccess*, wskazujące na usługę OCSP.
- id-etsi-qcs-semanticsId-Natural {0.4.0.194121.1} – wskazuje zgodność budowy atrybutu serialNumber identyfikatora DN ze składnią i semantyką zdefiniowaną w ETSI EN 319 412-1.

Certyfikaty kluczy Inspektorów ds. Rejestracji posiadają rozszerzenie ExtKeyUsage {1.3.6.1.4.1.10214.2.1.1.2} świadczące o tym, że są to certyfikaty infrastruktury używane wyłącznie w ramach systemu CCK i nie mogą być używane poza tym systemem.
Certyfikaty kluczy do ochrony komunikacji posiadają rozszerzenie ExtKeyUsage {1.3.6.1.4.1.10214.2.1.1.3} świadczące o tym, że są to certyfikaty infrastruktury używane wyłącznie w ramach systemu CCK i nie mogą być używane poza tym systemem.

7.2. Profil list CRL

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

Rozszerzenia

Pole	**Opis/wartość**	**krytyczne ?**
extensions		
AuthorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
cRLNumber	numer kolejny listy CRL wystawionej w CCK	NIE

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

8. Audyt

Centrum Certyfikacji Kluczy podlega regularnym audytom w ramach funkcjonującego w firmie Zintegrowanego Systemu Zarządzania, zgodnego z normami ISO 9001:2008 oraz ISO 27001.

Centrum Certyfikacji Kluczy podlega także audytom zgodnie z eIDAS.

9. Inne postanowienia

9.1. Opłaty

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

CCK nie pobiera opłat za unieważnienie, zawieszenie bądź uchylenie zawieszenia certyfikatu, a także za dostęp do klucza publicznego CCK oraz aktualnej listy unieważnionych certyfikatów.

9.2. Odpowiedzialność finansowa

Centrum Certyfikacji Kluczy odpowiada za wszelkie szkody spowodowane niewykonaniem lub nienależytym wykonaniem swych obowiązków w zakresie świadczonych usług, chyba że niewykonanie lub nienależyte wykonanie tych obowiązków jest następstwem okoliczności, za które podmiot świadczący usługi certyfikacyjne nie ponosi odpowiedzialności i którym nie mógł zapobiec mimo dołożenia należytej staranności, z uwzględnieniem ograniczeń odpowiedzialności CCK określonych w rozdziale 9.8 poniżej.

9.3. Poufność informacji

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

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

- Polityka certyfikacji w wersjach aktualnie obowiązujących,
- Klucz publiczny CCK,
- Lista unieważnionych certyfikatów,
- Certyfikaty infrastruktury,
- Informacje bieżące, przeznaczone do publikacji (takie jak cennik usług, oferta handlowa, bieżące komunikaty, dane kontaktowe).

9.4. Ochrona danych osobowych

Centrum Certyfikacji Kluczy przetwarza dane osobowe Subskrybentów. Centrum Certyfikacji Kluczy zgłosiło zbiór danych osobowych zgodnie z obowiązującymi przepisami, a także wdrożyło i realizuje odpowiednie regulaminy zapewniające ochronę danych osobowych.

Subskrybenci są informowani przy podpisywaniu umowy o przetwarzaniu ich danych osobowych przez CCK 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, odpowiedzi OCSP i znaczników czasu wystawianych przez CCK.

9.6. Udzielane gwarancje

Nie dotyczy

9.7. Zwolnienia z domyślnie udzielanych gwarancji

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

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

9.8. Ograniczenia odpowiedzialności

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

1) użycia certyfikatu niezgodnie z zakresem określonym w polityce wskazanej w certyfikacie, w tym za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została wskazana w certyfikacie;

2) nieprawdziwości danych zawartych w certyfikacie, podanych przez odbiorcę usług zaufania używającego tego certyfikatu, chyba że szkoda była wynikiem niedołożenia należytej staranności przez dostawcę usług zaufania;

3) przechowywania lub używania przez odbiorców usług zaufania danych do składania podpisu elektronicznego, pieczęci elektronicznej lub uwierzytelniania witryn internetowych w sposób niezapewniający ich ochrony przed nieuprawnionym wykorzystaniem.

Centrum Certyfikacji Kluczy nie odpowiada za skutki, które mogą wyniknąć z użycia oprogramowania lub sprzętu, który nie był dostarczony przez CCK.

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

9.9. Przenoszenie roszczeń odszkodowawczych

Centrum Certyfikacji Kluczy zawarło umowę ubezpieczenia odpowiedzialności cywilnej za szkody wyrządzone odbiorcom usług certyfikacyjnych, zgodnie z przepisami o podpisie elektronicznym.

9.10. Przepisy przejściowe i okres obowiązywania polityki certyfikacji

Niniejsza polityka certyfikacji obowiązuje w stosunku do certyfikatów wystawionych zgodnie z nią do utraty ważności tych certyfikatów (z powodu zakończenia okresu ważności lub unieważnienia). Certyfikaty wykorzystywane w celach dochodzeniowych lub dowodowych

po okresie ich ważności powinny być wykorzystywane zgodnie z polityką certyfikacji, w ramach której zostały wystawione.

W stosunku do nowo wystawianych certyfikatów stosuje się najnowszą obowiązującą politykę certyfikacji.

9.11. Określanie trybu i adresów doręczania pism

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

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.

9.15. Podstawy prawne

Zasady działania Centrum Certyfikacji Kluczy 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.
- Ustawie z dnia 29 sierpnia 1997 o ochronie danych osobowych.
- Ustawie z dnia 6 czerwca 1997 Kodeks karny.
- Ustawa z dnia 6 sierpnia 2010 r. o dowodach osobistych.
- Ustawa z dnia 13 lipca 2006 r. o dokumentach paszportowych.
- Ustawa z dnia 12 grudnia 2013 r. o cudzoziemcach.
- Ustawie z dnia 4 lutego 1994 Prawo autorskie.

9.16. Inne postanowienia

Nie występują.