

KWALIFIKOWANE CENTRUM CERTYFIKACJI „CENCERT”

POLITYKA CERTYFIKACJI DLA CERTYFIKATÓW KWALIFIKOWANYCH

Wersja: 2.2

Karta dokumentu:

Tytuł dokumentu	Polityka certyfikacji dla certyfikatów kwalifikowanych
Nazwa pliku	CenCert Polityka certyfikatów kwalifikowanych w. 2.2.docx
Właściciel dokumentu	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Wersja	2.2
Status dokumentu	Zatwierdzony
Data zatwierdzenia	27 czerwca 2016 r.
Liczba stron	51

zatwierdzone przez:

Wersja	zatwierdzający
2.2	Paweł A. Luksic - prezes zarządu ENIGMA SOI Sp. z o.o. Jacek Pokraśniewicz – prokurent

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 <i>CertificatePolicies</i> 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 <i>CertificatePolicies</i> 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.

Spis treści

1. WSTĘP	6
1.1. WPROWADZENIE.....	6
1.2. IDENTYFIKATOR POLITYKI CERTYFIKACJI.....	6
1.3. OPIS SYSTEMU CERTYFIKACJI I UCZESTNICZĄCYCH W NIM PODMIOTÓW.....	6
1.4. ZAKRES ZASTOSOWAŃ.....	8
1.5. ZASADY ADMINISTROWANIA POLITYKĄ CERTYFIKACJI.....	8
1.6. SŁOWNIK UŻYWANYCH TERMINÓW I AKRONIMÓW.....	9
2. ZASADY DYSTRYBUCJI I PUBLIKACJI INFORMACJI	11
3. IDENTYFIKACJA I UWIERZYTELNIENIE	12
3.1. STRUKTURA NAZW PRZYDZIELANYCH SUBSKRYBENTOM.....	12
3.2. UWIERZYTELNIENIE SUBSKRYBENTA PRZY WYSTAWIENIU PIERWSZEGO CERTYFIKATU.....	15
3.3. UWIERZYTELNIENIE SUBSKRYBENTA PRZY WYSTAWIANIU KOLEJNYCH CERTYFIKATÓW.....	16
3.4. SPOSOBY UWIERZYTELNIENIA SUBSKRYBENTA PRZY ZGŁASZANIU ŻĄDANIA UNIEWAŻNIENIA, ZAWIESZENIA I UCHYLENIA ZAWIESZENIA CERTYFIKATU.....	16
4. CYKL ŻYCIA CERTYFIKATU – WYMAGANIA OPERACYJNE	18
4.1. ZGŁOSZENIE CERTYFIKACYJNE.....	18
4.2. PRZETWARZANIE ZGŁOSZEŃ CERTYFIKACYJNYCH.....	19
4.3. WYSTAWIENIE CERTYFIKATU.....	19
4.4. AKCEPTACJA CERTYFIKATU.....	19
4.5. KORZYSTANIE Z PARY KLUCZY I CERTYFIKATU.....	20
4.5.1 Korzystanie z certyfikatu.....	20
4.5.2 Korzystanie z klucza prywatnego.....	21
4.6. WYMIANA CERTYFIKATU.....	22
4.7. WYMIANA CERTYFIKATU POŁĄCZONA Z WYMIANĄ PARY KLUCZY.....	23
4.8. ZMIANA TREŚCI CERTYFIKATU.....	23
4.9. UNIEWAŻNIENIE I ZAWIESZENIE CERTYFIKATU.....	24
4.10. USŁUGI INFORMOWANIA O STATUSIE CERTYFIKATÓW.....	25
4.11. ZAKOŃCZENIE UMOWY CERTYFIKACYJNEJ.....	26
4.12. POWIERZANIE I ODTWARZANIE KLUCZY PRYWATNYCH.....	26
5. ZABEZPIECZENIA ORGANIZACYJNE, OPERACYJNE I FIZYCZNE	27
5.1. ZABEZPIECZENIA FIZYCZNE.....	27
5.2. ZABEZPIECZENIA PROCEDURALNE.....	27
5.3. ZABEZPIECZENIA OSOBOWE.....	29
5.4. PROCEDURY TWORZENIA LOGÓW AUDYTOWYCH.....	30
5.5. ARCHIWIZACJA ZAPISÓW.....	31
5.6. WYMIANA PARY KLUCZY CENTRUM CERTYFIKACJI KLUCZY.....	32
5.7. UTRATA POUFNOŚCI KLUCZA PRYWATNEGO CCK I DZIAŁANIE CCK W PRZYPADKU KATASTROF.....	33
5.7.1 Utrata poufności klucza prywatnego CCK.....	33
5.7.2 Katastrofy.....	33
5.8. ZAKOŃCZENIE DZIAŁALNOŚCI CCK.....	34
6. ZABEZPIECZENIA TECHNICZNE	35
6.1. GENEROWANIE I INSTALOWANIE PAR KLUCZY.....	35
6.1.1 Generowanie par kluczy.....	35

Polityka certyfikacji dla certyfikatów kwalifikowanych

6.1.2	Dostarczenie klucza prywatnego Subskrybentowi	35
6.1.3	Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji	36
6.1.4	Dostarczenie klucza publicznego CCK.....	36
6.1.5	Rozmiary kluczy.....	36
6.1.6	Cel użycia klucza	36
6.2.	OCHRONA KLUCZY PRYWATNYCH	37
6.3.	INNE ASPEKTY ZARZĄDZANIA PARĄ KLUCZY	39
6.4.	DANE AKTYWUJĄCE	39
6.5.	ZABEZPIECZENIA KOMPUTERÓW	40
6.6.	ZABEZPIECZENIA ZWIĄZANE Z CYKLEM ŻYCIA SYSTEMU INFORMATYCZNEGO	40
6.7.	ZABEZPIECZENIA SIECI KOMPUTEROWEJ	40
6.8.	ZNAKOWANIE CZASEM	41
6.8.1	Oznaczenie czasem w procesie wystawiania certyfikatów	41
7.	PROFIL CERTYFIKATÓW I LIST CRL	42
7.1.	PROFIL CERTYFIKATÓW I ZAŚWIADCZEŃ.....	42
7.1.1	Identyfikatory DN.....	42
7.1.2	Profil certyfikatów	42
7.1.3	Profil zaświadczeń certyfikacyjnych.....	44
7.2.	PROFIL LIST CRL	44
8.	AUDYT.....	46
9.	INNE POSTANOWIENIA	47
9.1.	OPLATY	47
9.2.	ODPOWIEDZIALNOŚĆ FINANSOWA	47
9.3.	POUFNOŚĆ INFORMACJI	47
9.4.	OCHRONA DANYCH OSOBOWYCH	48
9.5.	ZABEZPIECZENIE WŁASNOŚCI INTELEKTUALNEJ	48
9.6.	UDZIELANE GWARANCJE	48
9.7.	ZWOLNIENIA Z DOMYŚLNIE UDZIELANYCH GWARANCJI	48
9.8.	OGRANICZENIA ODPOWIEDZIALNOŚCI	49
9.9.	PRZENOSZENIE ROSZCZEŃ ODSZKODOWAWCZYCH	49
9.10.	PRZEPISY PRZEJŚCIOWE I OKRES OBOWIĄZYWANIA POLITYKI CERTYFIKACJI.....	50
9.11.	OKREŚLANIE TRYBU I ADRESÓW DORECZANIA PISM	50
9.12.	ZMIANY W POLITYCE CERTYFIKACJI	50
9.13.	ROZSTRZYGANIE SPORÓW	50
9.14.	OBOWIĄZUJĄCE PRAWO.....	51
9.15.	PODSTAWY PRAWNE	51
9.16.	INNE POSTANOWIENIA	51

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 certyfikacyjnych polegających na wystawianiu kwalifikowanych certyfikatów.

Centrum Certyfikacji Kluczy realizujące niniejszą politykę stanowi kwalifikowany podmiot świadczący usługi certyfikacyjne, zgodnie z *Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym oraz eIDAS*.

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

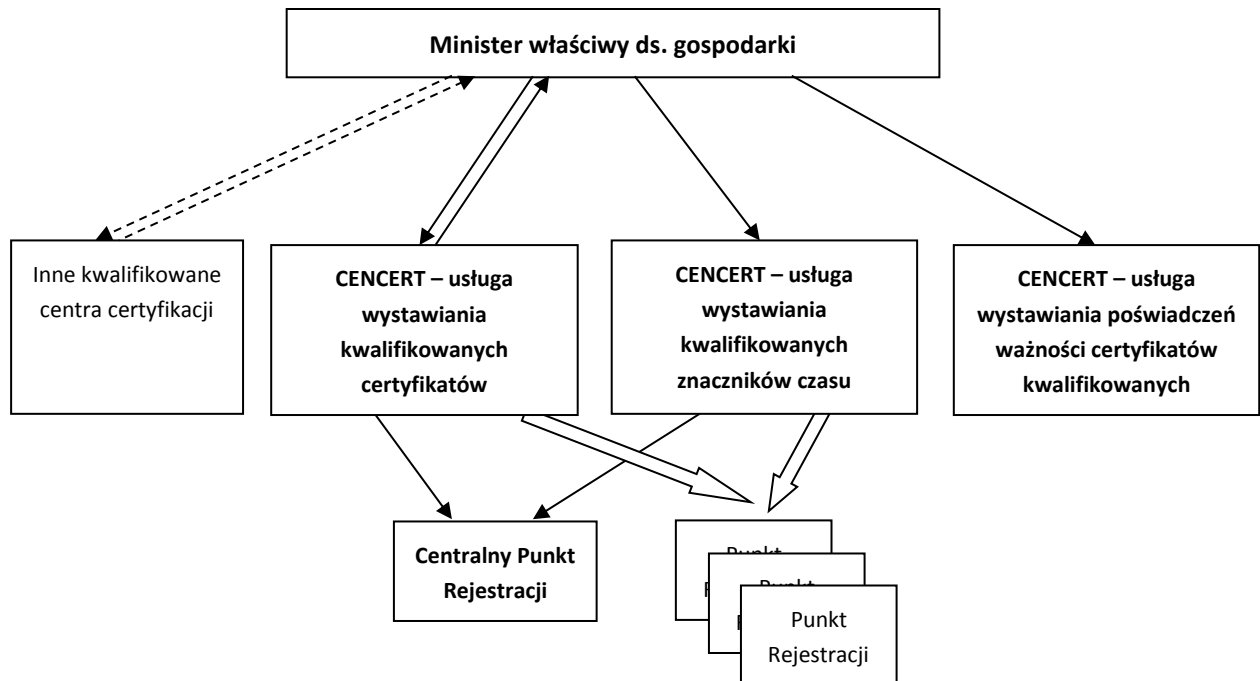
1.2. Identyfikator polityki certyfikacji

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	27 czerwca 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 krajowego systemu PKI obejmującego kwalifikowane podmioty certyfikacyjne. Rolę Nadrzędnego CCK (tzw. „*Root CA*”) pełni Minister właściwy do spraw gospodarki 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 zaświadczeń certyfikacyjnych 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 pełni swoje funkcje od momentu wejścia w życie Polityki certyfikacji, a zlikwidowany może być 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 bezpiecznego podpisu elektronicznego weryfikowanego przy użyciu kwalifikowanego certyfikatu wystawionego zgodnie z niniejszą polityką certyfikacji.

1.4. Zakres zastosowań

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

1.5. Zasady administrowania polityką certyfikacji

Podmiotem uprawnionym do administrowania polityką certyfikacji, w tym zatwierdzania, zatwierdzania zmian itd., jest firma ENIGMA Systemy Ochrony Informacji Sp. z o.o., reprezentowana przez przedstawicieli upoważnionych zgodnie z wpisem KRS lub na podstawie osobnego upoważnienia.

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

O ile Zarząd nie postanowi inaczej, wszystkie certyfikaty wystawione w okresie obowiązywania wcześniejszej wersji polityki certyfikacji i nadal ważne w chwili zatwierdzenia nowej wersji, zachowują swoją ważność i podlegają postanowieniom tej wersji polityki certyfikacji, zgodnie z którą zostały wystawione.

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 – jednostka organizacyjna, której zadaniem jest generowanie, dystrybucja i unieważnianie certyfikatów kluczy publicznych zgodnie z określoną polityką certyfikacji. Jeśli w jednym miejscu, przy wykorzystaniu wspólnych lub częściowo wspólnych zasobów technicznych i ludzkich, realizuje się kilka polityk certyfikacji, wystawiając certyfikaty podpisywane różnymi kluczami prywatnymi i certyfikaty te zawierają różne dane w polu <i>wystawca certyfikatu</i> (różne identyfikatory DN), mówimy o oddzielnych Centrach Certyfikacji Kluczy.
CRL	Lista unieważnionych certyfikatów. Jest wystawiana, poświadczana elektronicznie i publikowana przez CCK.
DN	Identyfikator DN – <i>Distinguished Name</i> – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500
HSM	<i>Hardware Security Module</i> – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego CCK do generowania podpisów/poświadczeń elektronicznych. Urządzenia HSM pozwalają na użycie klucza prywatnego przez uprawnioną osobę/osoby lecz nie pozwalają na pobranie klucza prywatnego z urządzenia lub skopiowanie go, nawet przez osobę mającą uprawnienia dostępu do klucza.

Termin/akronim	Opis
Klucz prywatny	Dane służące do składania podpisu kwalifikowanego przez Subskrybenta Dane służące do składania poświadczenia elektronicznego przez Centrum Certyfikacji Kluczy lub odpowiedniego ministra lub podmiot wskazany zgodnie z zapisami art. 23. Ust. 3 do 5 Ustawy
Klucz publiczny	Dane służące do weryfikacji podpisu elektronicznego, umieszczone w certyfikacie lub zaświadczeniu certyfikacyjnym
OCSP	<i>Online Certificate Status Protocol</i> - protokół i nazwa usługi PKI służącej do informowania o statusie konkretnych certyfikatów, o które pyta usługobiorca (czy certyfikat jest ważny, czy unieważniony)
PKI	<i>Public Key Infrastructure</i> – 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
Rozporządzenie	Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urzędów służących do składania i weryfikacji podpisu elektronicznego (Dz.U. z 2002r. nr 128 poz. 1094).
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 18 września 2001 r. o podpisie elektronicznym.
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

Znaczenie terminów użytych w niniejszej polityce certyfikacji, o ile nie są one zdefiniowane powyżej, są zgodne ze znaczeniem określonym w eIDAS lub Ustawie.

2. Zasady dystrybucji i publikacji informacji

CCK publikuje następujące informacje:

- Aktualny klucz publiczny CCK (w postaci samopodpisanego zaświadczenia certyfikacyjnego).
- Aktualną listę CRL.
- Aktualną politykę certyfikacji, materiały marketingowe, komunikaty bieżące itd.

CCK nie publikuje certyfikatów Subskrybentów.

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

Adres serwera www CCK CenCert to: www.cencert.pl

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 także dane osoby fizycznej, 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>

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 (na podst. Art. 20 ust. 2 Ustawy), 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: XXXXXXXXXXXXX” lub „NIP: XXXXXXXXXXXXX”.

Wariant II

Kraj (countryName) = PL

Imię (givenName) = <imiona Subskrybenta>

Nazwisko (sureName) = <nazwisko Subskrybenta>

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>

(opcjonalnie) **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 (na podst. Art. 20 ust. 2 Ustawy), 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: XXXXXXXXXXXXX” lub „NIP: XXXXXXXXXXXXX”.

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.

Wariant II budowy identyfikatora wyróżniającego Subskrybenta występuje jedynie wtedy, gdy certyfikat Subskrybenta zawiera informację, że występuje on „w imieniu” lub jako „członek organu”, lub jako „organ władzy publicznej”, o danych zawartych w atrybucie *Organizacja*.

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. Upoważnienie powinno dotyczyć konkretnego Subskrybenta.
- Jeśli dokumenty wymienione w pkt. 3) – 4) powyżej nie były podpisane przez osobę (lub osoby) uprawnione do reprezentowania danego podmiotu – upoważnienie do podpisania ww. dokumentów podpisane przez osoby uprawnione do reprezentowania danego podmiotu.

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.

Jeśli klucze Subskrybenta nie są generowane przez CCK, Subskrybent dostarcza zgłoszenie certyfikacyjne w formacie PKCS#10, zawierające podpis cyfrowy. Dowodem posiadania przez Subskrybenta klucza prywatnego odpowiadającego kluczowi publicznemu, który ma być umieszczony w certyfikacie, jest podpis cyfrowy zawarty w zgłoszeniu certyfikacyjnym.

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 bezpiecznego podpisu elektronicznego.

Uwierzytelnienie Subskrybenta może być zrealizowane na podstawie podpisu elektronicznego oraz umowa o świadczenie usług certyfikacyjnych może być podpisana elektronicznie jedynie wtedy, gdy zarówno certyfikat o który się ubiega Subskrybent, jak i certyfikat służący do jego uwierzytelnienia i weryfikacji podpisu pod umową, są kwalifikowanymi certyfikatami wystawianymi przez CenCert zgodnie z niniejszą polityką certyfikacji.

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 oryginału wniosku o unieważnienie certyfikatu, podpisanego odręcznie przez osobę (osoby) uprawnione do reprezentowania podmiotu lub

przez osobę upoważnioną. W przypadku gdy osoba podpisująca wniosek działa na podstawie upoważnienia, powinno ono być dołączone w oryginale i podpisane przez osoby uprawnione do reprezentowania podmiotu.

Subskrybent oraz podmiot, którego dane są umieszczone w certyfikacie Subskrybenta, może unieważnić certyfikat na następujące sposoby:

- 1) Poprzez osobistą wizytę w jednym z punktów rejestracji, w godzinach pracy danego punktu rejestracji
- 2) Poprzez zgłoszenie telefoniczne.

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

W przypadku zgłoszenia telefonicznego tożsamość Subskrybenta jest weryfikowana na podstawie hasła ustalonego przy wystawieniu certyfikatu lub na podstawie danych osobowych podawanych w procesie przy wystawianiu certyfikatu. W przypadku gdy weryfikacja tożsamości Subskrybenta nastąpiła z pominięciem hasła (na podstawie danych osobowych), certyfikat jest zawieszany.

Subskrybent może uchylić zawieszenie certyfikatu na następujące sposoby:

- 1) Poprzez osobistą wizytę w jednym z punktów rejestracji, w godzinach pracy danego punktu rejestracji
- 2) Poprzez zgłoszenie telefoniczne.

W przypadku wizyty osobistej tożsamość Subskrybenta jest weryfikowana na podstawie dowodu osobistego lub paszportu. W przypadku zgłoszenia telefonicznego tożsamość Subskrybenta jest weryfikowana na podstawie hasła ustalonego przy wystawieniu certyfikatu.

Uchylenie zawieszenia certyfikatu jest możliwe jedynie przed upływem 7 dni od daty 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 wystawieniu certyfikatu zawierającego dodatkowo dane innego podmiotu, zgodnie z art. 20 ust. 2. pkt. 2-4. Ustawy, Centrum Certyfikacji Kluczy powiadamia ten podmiot o treści certyfikatu oraz poucza o możliwości unieważnienia certyfikatu na wniosek podmiotu.

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.

Podmiot weryfikujący podpis elektroniczny złożony przez Subskrybenta powinien stosować „bezpieczne urządzenie do weryfikacji bezpiecznych podpisów elektronicznych weryfikowanych przy użyciu ważnego kwalifikowanego certyfikatu” znajdujące się na liście bezpiecznych urządzeń publikowanej przez Centrum Certyfikacji Kluczy.

Podmiot weryfikujący podpis elektroniczny złożony przez Subskrybenta powinien zastosować takie środki techniczne weryfikacji podpisu, aby posiadać dowód złożenia podpisu przez Subskrybenta „nie później niż w określonym momencie” i gwarantujące, aby ważność certyfikatu Subskrybenta oraz zaświadczenia certyfikacyjnego Centrum Certyfikacji Kluczy była potwierdzona na ten moment – zarówno pod względem „okresu ważności”, jak i ewentualnego unieważnienia bądź zawieszenia.

Jedynym sposobem potwierdzenia ważności certyfikatu Subskrybenta, na moment złożenia danego podpisu elektronicznego, pod kątem ewentualnego unieważnienia bądź zawieszenia, jest jeden z następujących, równoważnych, sposobów:

- Pobranie listy CRL poświadczonej przez Centrum Certyfikacji Kluczy CenCert, datowanej na moment przypadający po momencie złożenia podpisu, ale przed upłynięciem okresu ważności certyfikatu Subskrybenta, która:
 - Nie zawiera wpisu o unieważnieniu certyfikatu Subskrybenta wykorzystywanego do weryfikacji podpisu lub
 - Zawiera wpis o unieważnieniu lub zawieszeniu certyfikatu Subskrybenta wykorzystywanego do weryfikacji podpisu, ale moment unieważnienia lub zawieszenia przypada później niż moment złożenia podpisu.
- Pobranie odpowiedzi OCSP poświadczonej przez Centrum Certyfikacji Kluczy CenCert, spełniającej następujące warunki:
 - Odpowiedź zawiera status certyfikatu: Ważny,
 - Moment, na który odpowiedź jest ważna, zapisany i poświadczony przez CCK w odpowiedzi OCSP przypada po momencie złożenia podpisu elektronicznego, ale przed upłynięciem okresu ważności certyfikatu używanego do weryfikacji podpisu.

Z faktu nieukazania się w określonym czasie nowej listy CRL nie można wnioskować o braku unieważnień certyfikatów. Fakt posiadania odpowiedzi OCSP aktualnej na inny moment, niż określono powyżej, nie może stanowić podstawy do uznania certyfikatu za ważny.

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 kwalifikowanym znacznikiem czasu.

W celu zabezpieczenia wartości dowodowej podpisu po upływie ważności zaświadczenia certyfikacyjnego CCK CenCert związanego z kluczem służącym do generowania certyfikatów i list CRL lub z kluczem służącym do generowania odpowiedzi 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 pod podpisem, zaświadczenie certyfikacyjne, lista CRL lub odpowiedź OCSP ważna na moment znacznika czasu znajdującego się pod podpisem – i na oznaczeniu całej takiej paczki dodatkowym znacznikiem czasu.

W przypadku nieprzestrzegania przez podmiot weryfikujący certyfikat zasad weryfikacji certyfikatów określonych w niniejszej polityce, użycia innych niż wyżej określone narzędzi do weryfikacji podpisu lub przekroczenia w inny sposób postanowień niniejszej polityki certyfikacji lub obowiązującego prawa, Centrum Certyfikacji Kluczy nie odpowiada w żaden sposób za uzyskanie prawdziwego wyniku weryfikacji podpisu elektronicznego, weryfikowanego przy użyciu certyfikatu Subskrybenta.

4.5.2 Korzystanie z klucza prywatnego

Klucz prywatny związany z certyfikatem Subskrybenta służy do składania podpisów kwalifikowanych (stanowi „dane służące do składania bezpiecznych podpisów elektronicznych”) 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).

Klucz prywatny powinien być używany wyłącznie do składania Podpisów kwalifikowanych i powinien być przetwarzany wyłącznie przy użyciu Bezpiecznego urządzenia do składania bezpiecznych podpisów elektronicznych, znajdującego się w wykazie publikowanym przez Centrum Certyfikacji Kluczy. 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 bezpiecznym podpisem elektronicznym wytworzonym przy użyciu klucza prywatnego Subskrybenta związanego z ważnym kwalifikowanym certyfikatem, 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.

W przypadku wystawienia nowego certyfikatu zawierającego dane podmiotu, z którym związany jest Subskrybent, podmiot ten jest informowany przez CCK CenCert na takich zasadach, jak przy wystawieniu pierwszego certyfikatu.

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.

W przypadku wystawienia nowego certyfikatu zawierającego dane podmiotu, z którym związany jest Subskrybent, podmiot ten jest informowany przez CCK CenCert na takich zasadach, jak przy wystawieniu pierwszego certyfikatu.

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.
- Podmiot, którego dane są umieszczone w certyfikacie (o ile takie dane w certyfikacie zamieszczono).
- Centrum Certyfikacji Kluczy.

Subskrybent oraz podmiot, którego dane są umieszczone w certyfikacie Subskrybenta, 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.

Podmiot, z którym związany jest Subskrybent i którego dane zawarto w certyfikacie, jest zobowiązany 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 związku pomiędzy Subskrybentem a podmiotem, uzasadniającej zamieszczenie danych podmiotu w certyfikacie w danym charakterze (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.

Centrum Certyfikacji Kluczy prowadzi kwalifikowaną usługę OCSP, w ramach której udzielane są elektroniczne, poświadczane przez CCK odpowiedzi zawierające status danego certyfikatu. Odpowiedzi OCSP zawierają określenie momentu, na który dana odpowiedź jest ważna. Moment ten może być wcześniejszy niż moment dostarczenia odpowiedzi lub zadania pytania. Odpowiedź OCSP zawierająca status certyfikatu: „ważny” stanowi dowód ważności danego certyfikatu w określonym momencie, na równi z listą CRL, w tym sensie, że certyfikat nie został zawieszony ani unieważniony.

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. Powierzenie i odtwarzanie kluczy prywatnych

Centrum Certyfikacji Kluczy nie powierza swojego klucza prywatnego innym 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 w CCK	Nazwa funkcji według przepisów o podpisie elektronicznym	Rodzaj obowiązków
----------------------------	---	--------------------------

Nazwa funkcji w CCK	Nazwa funkcji według przepisów o podpisie elektronicznym	Rodzaj obowiązków
Administrator Systemu Informatycznego	Administrator Systemu	Instalowanie, konfigurowanie, zarządzanie systemem i siecią informatyczną
Operator Systemu	Operator Systemu	Stała obsługa systemu teleinformatycznego, w tym wykonywanie kopii zapasowych
Administrator CCK	Administrator Systemu	Konfigurowanie systemu CCK w zakresie polityki Centrum Certyfikacji Kluczy, nadawania uprawnień do systemu CCK. Zarządzanie kluczami CCK
Operator CCK	Inspektor ds. rejestracji	Nadawanie uprawnień Inspektorom ds. rejestracji w systemie CCK, możliwość unieważnienia certyfikatu, możliwość ręcznego spowodowania publikacji listy CRL
Inspektor ds. rejestracji	Inspektor ds. rejestracji	Weryfikacja tożsamości Subskrybentów, podpisywanie zgłoszeń certyfikacyjnych, unieważnianie, zawieszanie i uchylanie zawieszenia certyfikatów, tworzenie listy CRL
Inspektor ds. audytu	Inspektor ds. audytu	Analizowanie zapisy rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
Inspektor ds. bezpieczeństwa	Inspektor ds. bezpieczeństwa	Nadzór nad wdrożeniem i stosowaniem wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych

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 przez Inspektora ds. rejestracji, we wszystkie dni w roku, w zakresie unieważniania bądź zawieszania 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 lub przestępstwa określone w Ustawie o podpisie elektronicznym,
- 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 kończy się egzaminem, a do wykonywania obowiązków dopuszczane są tylko te osoby, które uzyskały wymaganą liczbę punktów.

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 o podpisie elektronicznym, do kary pozbawienia wolności do lat 5 włącznie.

5.4. Procedury tworzenia logów audytowych

Centrum Certyfikacji Kluczy zapewnia rejestrowanie wszelkich istotnych zdarzeń związanych z realizacją świadczonych przez CCK usług certyfikacyjnych. System informatyczny CCK zapewnia automatyczne tworzenie logów audytowych w 2 miejscach:

- Log systemu operacyjnego – rejestruje 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,
 - Log systemu CCK – rejestruje w szczególności następujące zdarzenia:
 - 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,

Polityka certyfikacji dla certyfikatów kwalifikowanych

- istotne zdarzenia związane ze zmianami w środowisku systemu CCK, w tym w podsystemie zarządzania kluczami i certyfikatami,
- rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia,
- zamykanie, otwieranie i ponowne uruchamianie po zamknięciu systemu,
- Log urządzenia HSM – rejestruje 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,
 - negatywne wyniki testów generatora pseudolosowego.

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;

Log systemu operacyjnego jest dostępny dla Administratora systemu i jest zabezpieczony przed modyfikacją przed osobami nieposiadającymi praw Administratora systemu za pomocą mechanizmów systemu operacyjnego.

Log systemu CCK jest dostępny dla Inspektora ds. Audytu i jest zabezpieczony przed modyfikacją przed osobami nieposiadającymi praw Administratora systemu za pomocą mechanizmów systemu operacyjnego.

Logi systemu operacyjnego oraz systemu CCK są przeglądane w każdym dniu roboczym odpowiednio przez Administratora systemu oraz Inspektora ds. audytu.

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 i zaświadczenia certyfikacyjne wystawione w poprzednim roku – okres przechowywania kopii archiwalnej wynosi 20 lat,
- wszystkie listy CRL wystawione w poprzednim roku – okres przechowywania kopii archiwalnej wynosi 20 lat,
- umowy o świadczenie usług certyfikacyjnych (w postaci elektronicznej) zawarte w ostatnim roku - okres przechowywania kopii archiwalnej wynosi 20 lat,
- rejestry zdarzeń – okres przechowywania kopii archiwalnej wynosi 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 otrzymaniu poprzedniego zaświadczenia certyfikacyjnego wystawionego w imieniu ministra właściwego ds. gospodarki.

Procedura wymiany pary kluczy polega na:

- Wygenerowaniu nowej pary kluczy.
- Zgłoszeniu nowego klucza publicznego w celu umieszczenia go w zaświadczeniu certyfikacyjnym wystawionym w imieniu ministra właściwego ds. gospodarki.
- Otrzymaniu nowego zaświadczenia certyfikacyjnego.
- Wykonaniu operacji „przełączenia” kluczy w oprogramowaniu CCK, co powoduje, że wszystkie nowe certyfikaty, listy CRL i zaświadczenia certyfikacyjne wystawiane są już przy użyciu nowego klucza CCK. Przy „przełączeniu” kluczy następuje także wygenerowanie zakładkowych zaświadczeń certyfikacyjnych kluczy CCK.
- Wygenerowaniu zaświadczenia certyfikacyjnego dla klucza ministra właściwego ds. gospodarki i przekazanie tego zaświadczenia ministrowi.

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 podejrzenia zajścia takiego zdarzenia.

Procedury te przewidują w szczególności:

1. Powiadomienie Subskrybentów oraz ministra ds. gospodarki o zaistniałej sytuacji oraz o planie dalszego działania.
2. Wytworzenie nowych kluczy CCK i zgłoszenie ich ministrowi ds. gospodarki, w celu wystawienia nowych zaświadczeń certyfikacyjnych.
3. Po unieważnieniu zaświadczenia certyfikacyjnego przez ministra gospodarki - unieważnienie wszystkich certyfikatów Subskrybentów.
4. 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 zaświadczenie certyfikacyjne, 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 Wylączenie Centralnego Punktu Rejestracji

W przypadku katastrofy powodującej wylączenie Centralnego Punktu Rejestracji, personel CCK niezwłocznie uruchamia Zastępczy Centralny Punkt Rejestracji, obsługujący Subskrybentów w zakresie unieważnienia, zawieszenia i uchylecia 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 wylączenia Centralnego Punktu Rejestracji.

5.7.2.3 Wylączenie repozytorium CCK i/lub serwera usług OCSP

W przypadku katastrofy polegającej na wylączeniu 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. gospodarki, z co najmniej 3-miesięcznym wyprzedzeniem.

O planowanym zakończeniu działalności informowani są także Subskrybenci.

Po zakończeniu działalności klucz prywatny CCK jest niszczoney.

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. gospodarki 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 Centrum Certyfikacji Kluczy zgodnie z udokumentowaną procedurą. W toku wykonywania procedury generowania kluczy wymagana jest obecność co najmniej osób pełniących następujące funkcje:

1. Administrator systemu informatycznego
2. Administrator CCK
3. Inspektor ds. bezpieczeństwa.

Wymagana jest nieprzerwana obecność Inspektora ds. bezpieczeństwa od momentu wywołania procedury generowania kluczy na urządzeniu HSM do momentu zapakowania kart elektronicznych zawierających fragmenty klucza oraz innych poufnych danych powstałych przy generowaniu kluczy (jak kody PIN) w sposób zgodny z procedurą.

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 określone w przepisach o podpisie elektronicznym.

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 tak technicznie zabezpieczona, że ma on możliwość stwierdzenia, że zapisany na niej klucz prywatny nie mógł być wcześniej wykorzystany do złożenia podpisu elektronicznego (konieczność jednorazowej, nieodwracalnej aktywacji karty przed jej użyciem).

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 zaświadczenia certyfikacyjnego poświadczonego przez ministra właściwego ds. gospodarki lub podmiot przez niego wskazany.

Klucz publiczny Centrum Certyfikacji Kluczy jest publikowany, w postaci samopodpisanego zaświadczenia certyfikacyjnego, w repozytorium CCK na stronie WWW, którego dane znajdują się w rozdziale 2.

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, zaświadczeń certyfikacyjnych i list CRL zgodnie z niniejszą polityką certyfikacji. Odpowiadający mu klucz publiczny służy wyłącznie do weryfikowania certyfikatów, zaświadczeń certyfikacyjnych i list CRL. Samopodpisane zaświadczenia

certyfikacyjne i zakładkowe zaświadczenia certyfikacyjne mają ustawione odpowiednie wartości (*cRLSign* i *keyCertSign*) w polu rozszerzenia *keyUsage*.

Klucze prywatne Subskrybentów mogą być używane wyłącznie do składania bezpiecznego podpisu elektronicznego weryfikowanego przy użyciu kwalifikowanego certyfikatu. Certyfikaty mają ustawione odpowiednie wartości (*nonRepudation*) w polu rozszerzenia *keyUsage*.

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, Inspektorów ds. rejestracji, Subskrybentów) nie są tworzone. Wyjątkiem mogą być kopie niektórych kluczy infrastruktury używanych wewnątrz 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, umożliwiającej 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, w tym osoby pełniącej rolę Inspektora ds. bezpieczeństwa. 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 (wchodzącego w skład *Bezpiecznego urządzenia do składania bezpiecznych podpisów elektronicznych*) i wprowadzenie na klawiaturze stacji roboczej 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 używa urządzeń HSM charakteryzujących się niskim poziomem emisji elektromagnetycznej, nie nakłada się jednak 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 archiwizowane 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 kluczy publicznych Subskrybentów i ich certyfikatów wynosi maksymalnie 2 lata.

Okres ważności par kluczy Inspektorów ds. rejestracji oraz certyfikatów tych kluczy 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, w tym Inspektora ds. bezpieczeństwa.
2. Administrator systemu informatycznego nie może posiadać żadnych danych aktywujących pozwalających na wykonywanie jakichkolwiek operacji w CCK.
3. Administrator CCK i Operator CCK nie mogą posiadać danych pozwalających na wykonywanie operacji w systemie operacyjnym lub w systemie baz danych z prawami administratora systemu lub bazy.
4. 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, w tym Inspektora ds. bezpieczeństwa, i zabezpieczona tak, jak przesyłki z materiałami niejawnymi. Tak zabezpieczona koperta jest przechowywana w metalowej szafie 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.
5. Jest prowadzony rejestr, w którym są odnotowywane przypadki składania danych aktywujących oraz fakt każdorazowego dostępu do tych danych.

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 w środowisku testowym. 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 i podlegają przeglądowi co najmniej w każdy dzień roboczy.

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 polityką certyfikacji są połączone za pomocą logicznie wydzielonej, dwusegmentowej sieci wewnętrznej. Sieć ta spełnia następujące wymagania:

- 1) dostęp z zewnątrz do wewnętrznego segmentu sieci odbywa się tylko za pośrednictwem serwerów (lub serwera) „proxy” zlokalizowanych w strefie DMZ (pomiędzy urządzeniami firewall), przy czym wszystkie urządzenia zlokalizowane w strefie DMZ mogą się kontaktować bez konieczności użycia urządzenia firewall tylko między sobą, natomiast w przypadku transmisji informacji z segmentem sieci wewnętrznej muszą korzystać z wewnętrznego urządzenia firewall, a w przypadku transmisji z zewnętrzną siecią teleinformatyczną muszą korzystać z pośrednictwa zewnętrznego urządzenia firewall;
- 2) wewnętrzny segment sieci, w którym znajdują się serwery dokonujące poświadczeń elektronicznych, jest oddzielony od segmentu podłączonego do strefy DMZ, za pomocą urządzenia firewall, rozpoznającego dane przychodzące spoza sieci wewnętrznej na podstawie adresu i portu docelowego i rozsyłającego je do odpowiednich adresów w sieci wewnętrznej;
- 3) urządzenia firewall (zewnętrzne i wewnętrzne) posiadają certyfikaty ITSEC klasy co najmniej E3 oraz są skonfigurowane w taki sposób, że pozwalają na realizację wyłącznie tych protokołów i usług, które są niezbędne do realizacji usług certyfikacyjnych.

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

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 ?
<i>Extensions</i>		
<i>AuthorityKeyIdentifier</i>		NIE

Polityka certyfikacji dla certyfikatów kwalifikowanych

Pole	Opis/wartość	krytyczne ?
<i>keyIdentifier</i>	skrót SHA-1 z klucza publicznego	
<i>SubjectKeyIdentifier</i>		NIE
<i>subjectkeyIdentifier</i>	skrót SHA-1 z klucza publicznego	
<i>KeyUsage</i>	nonRepudation	TAK
<i>CertificatePolicies</i>		TAK
<i>PolicyInformation</i>		
<i>CertPolicyId</i>	wartość {1.2.616.1.113681.1.1.10.1.1.2}	
<i>basicConstraints</i>	pusta sekwencja (określenie, że subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)	TAK
<i>crlDistributionPoints</i>	zawiera lokalizacje aktualnego CRL urzędu	NIE
<i>qcStatements</i>		NIE
<i>qcStatement</i>	Deklaracja, że certyfikat jest kwalifikowany	
<i>statementId</i>	id-etsi-qcs-QcCompliance {0 4 0 1862 1 1}	
<i>(opcja) qcStatement</i>	Limit transakcji	
<i>statementId</i>	id-etsi-qcs-QcLimitValue {0 4 0 1862 1 2}	
<i>statementInfo</i>	waluta i wartość limitu	
<i>(opcja) qcStatement</i>	Wskazanie charakteru działalności podmiotu	
<i>statementId</i>	id-gov-subjectSignatureType {1 2 616 1 101 3 1 1 2}	
<i>statementInfo</i>	weWłasnymImieniu (1), upowaznionyPrzedstawiciel (2), czlonekOrganu (3), organWladzyPuyblicznej (4)	

Certyfikaty mogą dodatkowo zawierać niekrytyczne rozszerzenie *AuthorityInfoAccess*, wskazujące na możliwość skorzystania z usługi potwierdzania ważności certyfikatu on-line (OCSP).

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.

7.1.3 Profil zaświadczeń certyfikacyjnych

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

Rozszerzenia

Pole	Opis/wartość	krytyczne ?
<i>extensions</i>		
<i>AuthorityKeyIdentifier</i>		NIE
<i>keyIdentifier</i>	skrót SHA-1 z klucza publicznego	
<i>SubjectKeyIdentifier</i>		NIE
<i>SubjectKeyIdentifier</i>		
<i>KeyUsage</i>	keyCertSign, cRLSign	TAK
<i>CertificatePolicies</i>		TAK
<i>PolicyInformation</i>		
<i>CertPolicyId</i>	{2 5 29 32 0}	
<i>basicConstraints</i>		TAK
<i>cA</i>	True	
<i>PathLenConstraint</i>	„0” dla samopodpisanych zaświadczeń certyfikacyjnych “2” dla zaświadczeń certyfikacyjnych wystawionych na klucz ministra	

7.2. Profil list CRL

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

Rozszerzenia

Polityka certyfikacji dla certyfikatów kwalifikowanych

Pole	Opis/wartość	krytyczne ?
<i>extensions</i>		
<i>AuthorityKeyIdentifier</i>		NIE
<i>keyIdentifier</i>	skrót SHA-1 z klucza publicznego	
<i>cRLNumber</i>	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.

Niezależnie od tego, w każdym dniu roboczym osoba pełniąca funkcję Inspektora ds. audytu przegląda rejestr zapisu zdarzeń w celu bieżącej kontroli działania CCK i punktów rejestracji.

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 podpisie elektronicznym, 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,
- Wystawione zaświadczenia certyfikacyjne,
- 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 użycia certyfikatu poza zakresem określonym w polityce certyfikacji, która została wskazana w certyfikacie, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została ujawniona w certyfikacie.

Centrum Certyfikacji Kluczy nie odpowiada za szkodę wynikłą z nieprawdziwości danych zawartych w certyfikacie, wpisanych na wniosek osoby składającej podpis elektroniczny.

Centrum Certyfikacji Kluczy w żaden sposób nie odpowiada za skutki wykorzystania klucza lub certyfikatu Subskrybenta niezgodnie z polityką certyfikacji, zgodnie z którą został wystawiony. W szczególności Centrum Certyfikacji Kluczy nie ponosi żadnej odpowiedzialności za skutki nieprawidłowej, niezgodnej z niniejszą polityką certyfikacji i/lub obowiązującymi przepisami weryfikacji jakiegokolwiek certyfikatu Subskrybenta, zaświadczenia certyfikacyjnego, odpowiedzi OCSP lub znacznika czasu.

Centrum Certyfikacji Kluczy w żaden sposób nie odpowiada za skutki, które mogą wynikać z użycia oprogramowania lub sprzętu, który nie był dostarczony przez CCK lub nie znajduje się na Liście bezpiecznych urządzeń opublikowanej przez CCK.

Centrum Certyfikacji Kluczy w żaden sposób nie odpowiada za to, czy Subskrybent użył do generowania swojego klucza prywatnego właściwego, dostarczonego lub rekomendowanego przez CCK Komponentu technicznego (karty elektronicznej). Centrum Certyfikacji Kluczy oferuje odpowiednie karty elektroniczne, jednak nie kontroluje, czy Subskrybent użył przy generowaniu kluczy właściwej karty. Odpowiedzialność za skutki wyboru i użycia danego Komponentu technicznego, w przypadku użycia komponentu niezgodnego ze specyfikacją spoczywa wyłącznie na Subskrybencie.

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 wydane 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 Rozporządzeniem ministra

finansów z dnia 16 grudnia 2003 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi certyfikacyjne ubezpieczenia cywilnego.

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

We wszelkich sprawach dotyczących spraw związanych z niniejszą polityką certyfikacji można się zwracać do firmy ENIGMA SOI Sp. z o.o. pod adresem biuro@enigma.com.pl.

Skargi na działalność Centrum Certyfikacji Kluczy można także, na zasadach określonych przez przepisy Kodeksu postępowania administracyjnego, do ministra właściwego do spraw gospodarki.

9.14. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu Rzeczypospolitej 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 18 września 2001 r. o podpisie elektronicznym.
- 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.