

KWALIFIKOWANE CENTRUM CERTYFIKACJI „CENCERT”

# **POLITYKA CERTYFIKACJI DLA POŚWIADCZANIA WAŻNOŚCI KWALIFIKOWANYCH CERTYFIKATÓW**

**Wersja: 2.0**

**Karta dokumentu:**

<b>Tytuł dokumentu</b>	Polityka certyfikacji dla poświadczania ważności kwalifikowanych certyfikatów
<b>Właściciel dokumentu</b>	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
<b>Wersja</b>	2.0
<b>Status dokumentu</b>	zatwierdzony
<b>Data zatwierdzenia</b>	19 stycznia 2011 r.
<b>Liczba stron</b>	38

zatwierdzone przez:

<b>Wersja</b>	<b>1. zatwierdzający</b>
2.0	Zarząd ENIGMA SOI Sp. z o.o.

**historia wersji**

<b>Wersja</b>	<b>Data</b>	<b>Komentarze</b>
1.0	2008-09-18	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	Poprawka identyfikatora OID polityki, poprawka identyfikatora DN CCK, inne drobne poprawki tekstu
2.0	2011-01-19	Zmiany wynikające z przejęcia firmy Safe Technologies S.A. przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o. Poprawki drobnych błędów.

## Spis treści

<b>1. WSTĘP</b> .....	<b>5</b>
1.1. WPROWADZENIE.....	5
1.2. IDENTYFIKATOR POLITYKI CERTYFIKACJI.....	5
1.3. OPIS SYSTEMU CERTYFIKACJI I UCZESTNICZĄCYCH W NIM PODMIOTÓW.....	5
1.4. ZAKRES ZASTOSOWAŃ.....	6
1.5. ZASADY ADMINISTROWANIA POLITYKĄ CERTYFIKACJI.....	7
1.6. SŁOWNIK UŻYWANYCH TERMINÓW I AKRONIMÓW.....	7
<b>2. ZASADY DYSTRYBUCJI I PUBLIKACJI INFORMACJI</b> .....	<b>10</b>
<b>3. IDENTYFIKACJA I UWIERZYTELIENIE</b> .....	<b>11</b>
3.1. STRUKTURA NAZW PRZYDZIELANYCH SUBSKRYBENTOM.....	11
3.2. UWIERZYTELIENIE SUBSKRYBENTA PRZY PIERWSZEJ REALIZACJI USŁUGI.....	11
3.3. UWIERZYTELIENIE SUBSKRYBENTA PRZY REALIZACJI USŁUGI KOLEJNY RAZ.....	11
3.4. SPOSOBY UWIERZYTELIENIA SUBSKRYBENTA PRZY ZGŁASZANIU ŻĄDANIA UNIEWAŻNIENIA, ZAWIESZENIA I UCHYLENIA ZAWIESZENIA CERTYFIKATU.....	11
<b>4. CYKL ŻYCIA POŚWIADCZENIA WAŻNOŚCI – WYMAGANIA OPERACYJNE</b> .....	<b>12</b>
4.1. ŻĄDANIE POŚWIADCZENIA WAŻNOŚCI CERTYFIKATU.....	12
4.2. PRZETWARZANIE ŻĄDAŃ POŚWIADCZENIA WAŻNOŚCI CERTYFIKATU.....	12
4.3. WYSTAWIENIE ODPOWIEDZI ZAWIERAJĄCEJ STATUS CERTYFIKATU.....	12
4.4. AKCEPTACJA POŚWIADCZEŃ WAŻNOŚCI CERTYFIKATÓW.....	13
4.5. KORZYSTANIE Z ODPOWIEDZI O STATUSIE CERTYFIKATU.....	13
4.6. WYMIANA.....	13
4.7. WYMIANA POŁĄCZONA Z WYMIANĄ PARY KLUCZY.....	13
4.8. ZMIANA TREŚCI ODPOWIEDZI.....	14
4.9. UNIEWAŻNIENIE I ZAWIESZENIE ODPOWIEDZI.....	14
4.10. USŁUGI INFORMOWANIA O STATUSIE ODPOWIEDZI.....	14
4.11. ZAKOŃCZENIE STOSUNKU PRAWNEGO.....	14
4.12. POWIERZANIE I ODTWARZANIE KLUCZY PRYWATNYCH.....	14
<b>5. ZABEZPIECZENIA ORGANIZACYJNE, OPERACYJNE I FIZYCZNE</b> .....	<b>15</b>
5.1. ZABEZPIECZENIA FIZYCZNE.....	15
5.2. ZABEZPIECZENIA PROCEDURALNE.....	16
5.3. ZABEZPIECZENIA OSOBOWE.....	17
5.4. PROCEDURY TWORZENIA LOGÓW AUDYTOWYCH.....	18
5.5. ARCHIWIZACJA ZAPISÓW.....	19
5.6. WYMIANA PARY KLUCZY CENTRUM CERTYFIKACJI KLUCZY.....	20
5.7. UTRATA POUFNOŚCI KLUCZA PRYWATNEGO CCK I DZIAŁANIE CCK W PRZYPADKU KATASTROF.....	21
5.7.1 Utrata poufności klucza prywatnego CCK.....	21
5.7.2 Katastrofy.....	22
5.8. ZAKOŃCZENIE DZIAŁALNOŚCI CCK.....	24
<b>6. ZABEZPIECZENIA TECHNICZNE</b> .....	<b>25</b>
6.1. GENEROWANIE I INSTALOWANIE PAR KLUCZY.....	25
6.1.1 Generowanie par kluczy.....	25
6.1.2 Dostarczenie klucza prywatnego Subskrybentowi.....	25
6.1.3 Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji.....	25

# Polityka certyfikacji dla poświadczania ważności kwalifikowanych certyfikatów

6.1.4	Dostarczenie klucza publicznego CCK.....	25
6.1.5	Rozmiary kluczy.....	26
6.1.6	Cel użycia klucza .....	26
6.2.	OCHRONA KLUCZY PRYWATNYCH .....	26
6.3.	INNE ASPEKTY ZARZĄDZANIA PARĄ KLUCZY .....	27
6.4.	DANE AKTYWUJĄCE .....	27
6.5.	ZABEZPIECZENIA KOMPUTERÓW.....	28
6.6.	ZABEZPIECZENIA ZWIĄZANE Z CYKLEM ŻYCIA SYSTEMU INFORMATYCZNEGO .....	28
6.7.	ZABEZPIECZENIA SIECI KOMPUTEROWEJ.....	29
6.8.	ZNAKOWANIE CZASEM .....	30
<b>7.</b>	<b>PROFIL POŚWIADCZENIA WAŻNOŚCI .....</b>	<b>31</b>
7.1.	IDENTYFIKATORY DN.....	31
7.2.	PROFIL ŻAŻAŻ POŚWIADCZENIA WAŻNOŚCI CERTYFIKATU .....	31
7.3.	PROFIL POŚWIADCZENIA WAŻNOŚCI CERTYFIKATÓW.....	31
<b>8.</b>	<b>AUDYT.....</b>	<b>33</b>
<b>9.</b>	<b>INNE POSTANOWIENIA .....</b>	<b>34</b>
9.1.	OPLATY .....	34
9.2.	ODPOWIEDZIALNOŚĆ FINANSOWA .....	34
9.3.	POUFNOŚĆ INFORMACJI .....	34
9.4.	OCHRONA DANYCH OSOBOWYCH .....	35
9.5.	ZABEZPIECZENIE WŁASNOŚCI INTELEKTUALNEJ .....	35
9.6.	UDZIELANE GWARANCJE .....	35
9.7.	ZWOLNIENIA Z DOMYŚLNIE UDZIELANYCH GWARANCJI .....	35
9.8.	OGRANICZENIA ODPOWIEDZIALNOŚCI .....	36
9.9.	PRZENOSZENIE ROSZCZEŃ ODSZKODOWAWCZYCH .....	36
9.10.	PRZEPISY PRZEJŚCIOWE I OKRES OBOWIĄŻYWANIA POLITYKI CERTYFIKACJI.....	36
9.11.	OKREŚLANIE TRYBU I ADRESÓW DORĘCZANIA PISM .....	36
9.12.	ZMIANY W POLITYCE CERTYFIKACJI .....	37
9.13.	ROZSTRZYGANIE SPORÓW .....	37
9.14.	OBOWIĄŻUJĄCE PRAWO.....	37
9.15.	PODSTAWY PRAWNE .....	37
9.16.	INNE POSTANOWIENIA .....	38

# 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 potwierdzaniu ważności kwalifikowanych certyfikatów wystawianych przez Centrum Certyfikacji Kluczy CenCERT . Centrum Certyfikacji Kluczy realizujące niniejszą politykę stanowi kwalifikowany podmiot świadczący usługi certyfikacyjne, zgodnie z *Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym*.

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

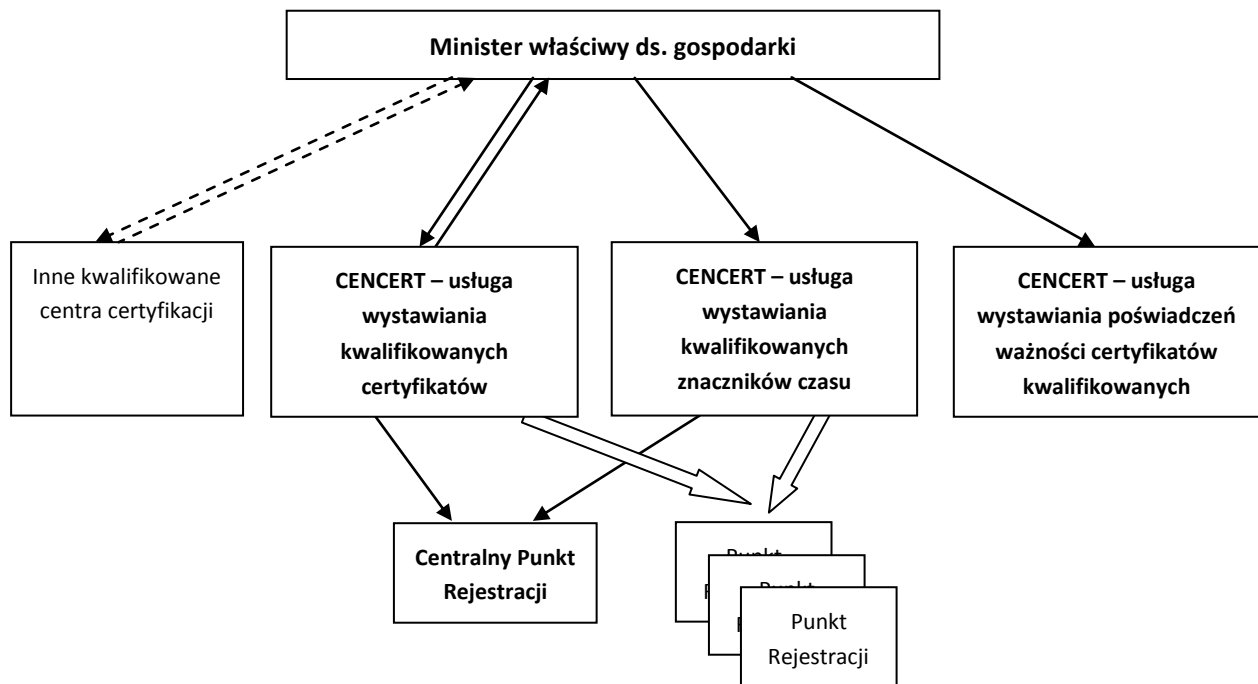
## 1.2. Identyfikator polityki certyfikacji

<b>Nazwa polityki</b>	Polityka certyfikacji dla poświadczania ważności kwalifikowanych certyfikatów
<b>Kwalifikator polityki</b>	Brak
<b>Numer OID (ang. Object Identifier)</b>	1.3.6.1.4.1.10214.99.1.1.1.3.2.0
<b>Data wprowadzenia</b>	21.04.2011
<b>Data wygaśnięcia</b>	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 obsługuje Subskrybentów poprzez:

- Centralny Punkt Rejestracji (CPR), którego dane znajdują się w rozdziale 1.5.

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

Subskrybentem usług certyfikacyjnych może być każda osoba fizyczna, prawna lub jednostka organizacyjna nieposiadająca osobowości prawnej.

## 1.4. Zakres zastosowań

Poświadczenia elektroniczne wystawiane zgodnie z niniejszą polityką certyfikacji określają status danego certyfikatu kwalifikowanego, wystawionego przez CCK CenCERT zgodnie z odpowiednią polityką certyfikacji, na moment określony w poświadczeniu. W szczególności poświadczenia elektroniczne potwierdzające status certyfikatu jako ‘ważny’ stanowią dowód, na równi z listą CRL, ważności danego certyfikatu w określonym momencie.

## **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.  
05-090 Raszyn  
Ul. Aleja Krakowska 20a

Telefon kontaktowy:

+48 22 720 79 55 – czynny całą dobę

Fax:

+48 22 720 79 55– czynny całą dobę

## **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
<b>CCK</b>	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 zawierającymi różne dane w polu <i>wystawca certyfikatu</i> (różne identyfikatory DN), mówimy o oddzielnych Centrach Certyfikacji Kluczy.
<b>CRL</b>	Lista unieważnionych certyfikatów. Jest wystawiana, poświadczana elektronicznie i publikowana przez CCK.
<b>DN</b>	Identyfikator DN – <i>Distinguished Name</i> – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500
<b>HSM</b>	<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.
<b>Klucz prywatny</b>	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
<b>Klucz publiczny</b>	Dane służące do weryfikacji podpisu elektronicznego, umieszczane w certyfikacie lub zaświadczeniu certyfikacyjnym
<b>OSCP</b>	<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)
<b>PKI</b>	<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
<b>Podpis kwalifikowany</b>	Bezpieczny podpis elektroniczny weryfikowany przy użyciu ważnego kwalifikowanego certyfikatu - zgodnie z definicją określoną w Ustawie

<b>Termin/akronim</b>	<b>Opis</b>
<b>Rozporządzenie</b>	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 urządzeń służących do składania i weryfikacji podpisu elektronicznego (Dz.U. z 2002r. nr 128 poz. 1094).
<b>Subskrybent</b>	Osoba korzystająca z kwalifikowanych usług certyfikacyjnych świadczonych przez CCK CenCERT
<b>Ustawa</b>	Ustawa z dnia 18 września 2001 r. o podpisie elektronicznym. (Dz. U. z 2001r. nr 130 poz. 1450)

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

## **2. Zasady dystrybucji i publikacji informacji**

CCK publikuje następujące informacje:

- Aktualną politykę certyfikacji, materiały marketingowe, komunikaty bieżące itd.

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](http://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**

Nie dotyczy.

#### **3.2. Uwierzytelnienie Subskrybenta przy pierwszej realizacji usługi**

Nie jest wymagane uwierzytelnienie Subskrybentów usługi potwierdzania ważności certyfikatów.

#### **3.3. Uwierzytelnienie Subskrybenta przy realizacji usługi kolejny raz**

Jak w rozdziale 3.2.

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

Nie dotyczy.

## **4. Cykl życia poświadczania ważności – wymagania operacyjne**

### **4.1. Żądanie poświadczania ważności certyfikatu**

Centrum Certyfikacji Kluczy wystawia poświadczenie określające status ważności danego certyfikatu jako odpowiedź na przesłane elektronicznie żądanie potwierdzenia statusu certyfikatu. Nie wymaga się aby żądanie było uwierzytelnione podpisem elektronicznym.

Centrum Certyfikacji Kluczy zastrzega sobie możliwość selektywnego odrzucania żądań bez ich przetwarzania w przypadku wykrycia lub podejrzenia ataku sieciowego z określonego adresu lub podsieci.

Żądanie potwierdzenia ważności certyfikatu może dotyczyć więcej niż jednego certyfikatu.

### **4.2. Przetwarzanie żądań poświadczania ważności certyfikatu**

System informatyczny Centrum Certyfikacji Kluczy niezwłocznie po odebraniu żądania potwierdzenia ważności certyfikatu weryfikuje poprawność żądania. Żądanie jest automatycznie odrzucane w przypadku niepoprawnej składni lub niemożności wykonania usługi (np. gdy zawarte w żądaniu parametry usługi nie są realizowane przez CCK).

### **4.3. Wystawienie odpowiedzi zawierającej status certyfikatu**

Po poprawnej weryfikacji żądania potwierdzenia ważności certyfikatu system informatyczny CCK niezwłocznie wystawia i odsyła Subskrybentowi (jako odpowiedź na żądanie, w ramach protokołu HTTP) poświadczoną elektronicznie przez CCK odpowiedź zawierającą informację o statusie kwalifikowanego certyfikatu (lub kwalifikowanych certyfikatów, jeśli żądanie dotyczyło więcej niż jednego certyfikatu).

Odpowiedź zawiera informację, czy certyfikat jest:

1. ważny (tzn. nie jest unieważniony lub zawieszony)
2. unieważniony bądź zawieszony
3. status certyfikatu nie jest znany.

#### **4.4. Akceptacja poświadczeń ważności certyfikatów**

Nie występuje.

#### **4.5. Korzystanie z odpowiedzi o statusie certyfikatu**

Odpowiedź o statusie kwalifikowanego certyfikatu stanowi mechanizm dostarczania Subskrybentom informacji o zawieszeniach i unieważnieniach certyfikatów alternatywnych w stosunku do list CRL.

Poświadczona elektronicznie odpowiedź o statusie certyfikatu, zawierająca status certyfikatu określony jako „ważny”, stanowi dowód, że w danym momencie (określonym w odpowiedzi) dany certyfikat nie był unieważniony ani zawieszony.

Odpowiedź ta nie informuje jednak, czy dany certyfikat w tym momencie był w okresie ważności ani czy w ogóle taki certyfikat był przez CCK kiedykolwiek wystawiony. Zweryfikowanie poprawności certyfikatu (w szczególności czy jest prawidłowo poświadczony przez CCK) oraz jego okresu ważności musi być wykonywane przy weryfikacji podpisu elektronicznego niezależnie od uzyskania informacji o statusie certyfikatu.

#### **4.6. Wymiana**

Nie dotyczy.

#### **4.7. Wymiana połączona z wymianą pary kluczy**

Nie dotyczy.

#### **4.8. Zmiana treści odpowiedzi**

Nie dotyczy.

#### **4.9. Unieważnienie i zawieszenie odpowiedzi**

Nie dotyczy.

#### **4.10. Usługi informowania o statusie odpowiedzi**

Nie dotyczy.

#### **4.11. Zakończenie stosunku prawnego**

Stosunek prawny pomiędzy Centrum Certyfikacji Kluczy a Subskrybentem, dotyczący realizacji usługi potwierdzania ważności kwalifikowanych certyfikatów kończy się wraz z zakończeniem ważności zaświadczenia certyfikacyjnego służącego do weryfikacji wystawionych odpowiedzi.

#### **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. Pomieszczenia te są chronione tak, jak serwerownia CCK, za wyjątkiem wymagania ochrony przed zanikami zasilania oraz klimatyzacji.

Niszczenie wszelkich danych niestanowiących informacji publicznej (w tym wszelkich haseł, kodów PIN, protokołów itd.) zapisanych na nośnikach papierowych lub podobnych są niszczone przy użyciu niszczarki do papieru klasy co najmniej DIN 4 (ścinki nie większe niż 2 mm x 15 mm).

## 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
<b>Administrator Systemu Informatycznego</b>	Administrator Systemu	Instalowanie, konfigurowanie, zarządzanie systemem i siecią informatyczną
<b>Operator Systemu</b>	Operator Systemu	Stała obsługa systemu teleinformatycznego, w tym wykonywanie kopii zapasowych
<b>Administrator CCK</b>	Administrator Systemu	Konfigurowanie systemu CCK w zakresie polityki. Zarządzanie kluczami CCK
<b>Inspektor ds. audytu</b>	Inspektor ds. audytu	Analizowanie zapisów rejestrów zdarzeń mających miejsce w systemach teleinformatycznych wykorzystywanych przy świadczeniu usług certyfikacyjnych
<b>Inspektor ds. bezpieczeństwa</b>	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.

Operacja tworzenia kopii zapasowych CCK jest każdorazowo wykonywana przez Operatora Systemu pod bezpośrednim nadzorem Inspektora ds. Bezpieczeństwa.

### **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 byli skazani 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 kierowani 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.

## 5.4. Procedury tworzenia logów audytowych

Centrum Certyfikacji Kluczy zapewni 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 Windows – 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,
  - istotne zdarzeń związanych 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 Windows jest dostępny dla Administratora systemu i jest zabezpieczony przed modyfikacją przed osobami nieposiadającymi praw Administratora systemu za pomocą mechanizmów systemu Windows.

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

Logi systemu Windows oraz systemu CCK są przeglądane w każdym dniu roboczym odpowiednio przez Administratora systemu oraz Inspektora ds. audytu. Log systemu Windows jest przeglądany przy użyciu oprogramowania systemu Windows, ewentualnie przy użyciu dodatkowych narzędzi pomagających wyszukiwać określone wzorce. Log systemu CCK jest przeglądany przy użyciu specjalizowanego oprogramowania dostarczanego w ramach systemu CCK.

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:

- 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.

Archiwizowane dane są podpisywane elektronicznie oraz oznaczane kwalifikowanym znacznikiem czasu i w tej postaci archiwizowane.

Archiwizacja zapisów jest wykonywana przez Operatora systemu, w obecności co najmniej Administratora CCK, pod bezpośrednim nadzorem Inspektora ds. bezpieczeństwa.

Archiwizacja zapisów jest wykonywana na nośnikach magnetoptycznych jednokrotnego zapisu. Nośniki oznaczane są w sposób jednoznacznie identyfikujący rodzaj i zakres

zapisanych informacji oraz są podpisywane i oznaczone datą przez osoby wykonujące i nadzorujące archiwizację.

W wyniku realizacji procedury archiwizacji powstają dwa identyczne nośniki. Jeden z nich jest przechowywany w centrum podstawowym CCK, drugi w centrum zapasowym. Nośniki są zapakowane w taki sposób, aby użycie nośnika pozostawiło widoczne ślady. Dostęp do nośnika mają Administratorzy systemu informatycznego, pod bezpośrednim nadzorem Inspektora ds. bezpieczeństwa. Każdorazowy dostęp do nośnika jest odnotowywany, wraz z zapisaniem powodu dostępu.

Każdy nośnik archiwalny jest sprawdzany przez Administratora systemu informatycznego, pod bezpośrednim nadzorem Inspektora ds. bezpieczeństwa, raz na 5 lat, pod kątem poprawności odczytu i integralności zapisanych danych – poprzez weryfikację podpisu elektronicznego. Wraz ze sprawdzeniem nośnika wykonywana jest przez Administratora systemu informatycznego, pod nadzorem Inspektora ds. bezpieczeństwa, analiza ryzyka pod kątem wystąpienia przypadków określonych poniżej:

- W przypadku, gdy istnieje zwiększone ryzyko uszkodzenia nośnika w ciągu następnych 5 lat (w szczególności z powodu upłynięcia deklarowanego okresu trwałości nośnika), dane są przenoszone na inny nośnik – przez osoby uprawnione do wykonywania archiwizacji.
- W przypadku, gdy istnieje istotne ryzyko braku możliwości odczytu archiwum w ciągu następnych 5 lat z powodu przestarzałej technologii archiwizacji, formatów danych itd., Administrator systemu informatycznego przedstawia kierownictwu CCK plan działań zmierzający do zachowania możliwości odczytu danych archiwalnych. W razie potrzeby dane są przenoszone na inny nośnik. W razie potrzeby format danych może zostać zmieniony – w takim przypadku nowy format jest ponownie podpisywany elektronicznie i znakowany czasem, jednak dane w oryginalnym formacie, z oryginalnym podpisem elektronicznym i znacznikiem czasu muszą być także przechowywane.

## **5.6. Wymiana pary kluczy Centrum Certyfikacji Kluczy**

Wygenerowanie i wymiana pary kluczy Centrum Certyfikacji Kluczy może następować w planowych terminach lub wcześniej na podstawie decyzji Dyrektora Pionu Usług Utrzymaniowych.

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 poświadczenia wystawiane są już przy użyciu nowego klucza CCK.

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

### **5.7.1 Utrata poufności klucza prywatnego CCK**

Procedury obowiązujące w wypadku utraty poufności klucza prywatnego CCK należy zastosować również wtedy, gdy istnieje uzasadnione podejrzenie zajścia takiego zdarzenia.

O utracie poufności klucza prywatnego Centrum Certyfikacji Kluczy lub uzasadnionego podejrzenia zajścia takiego zdarzenia, każda osoba należąca do personelu Centrum Certyfikacji Kluczy i posiadająca taką wiedzę jest zobowiązana niezwłocznie poinformować Pełnomocnika Ochrony. Powoduje to podjęcie w CCK następujących działań:

1. Zarząd firmy, po pozytywnym zweryfikowaniu zgłoszenia (tzn. że zdarzenie takie rzeczywiście zaszło), niezwłocznie informuje ministra właściwego ds. gospodarki, podając jednocześnie, o ile to możliwe, datę i czas ujawnienia klucza.
2. Najszybciej jak to jest możliwe (ale po powiadomieniu ministra ds. gospodarki), o zaistniałej sytuacji oraz o planie dalszego działania informowani są Subskrybenci.
3. Dyrektor Pionu Usług Utrzymaniowych podejmuje decyzje powodujące zabezpieczenie wszelkich śladów mogących prowadzić do wyjaśnienia przyczyny zdarzenia oraz ustalenie osób winnych. Personel CCK współpracuje z organami ścigania, w przypadku ewentualnego śledztwa, udostępniając na podstawie odpowiednich przepisów wymagane informacje. Udostępnieniu nie podlegają: klucz prywatny CCK oraz klucze prywatne Subskrybentów (przy czym klucze prywatnych Subskrybentów Centrum Certyfikacji Kluczy nie przetwarza).
4. Zarząd powołuje komisję, która ma zbadać przyczyny zaistnienia zdarzenia oraz zaproponować ewentualne działania korygujące.

5. Najszybciej, jak to jest możliwe, Centrum Certyfikacji Kluczy generuje nową parę kluczy CCK do poświadczania ważności certyfikatów – stosując procedury obowiązujące przy generowaniu klucza CCK - i zgłasza klucz publiczny ministrowi ds. gospodarki, w celu umieszczenia go w zaświadczeniu certyfikacyjnym.
6. Po otrzymaniu nowego zaświadczenia certyfikacyjnego CCK wznowia normalną działalność.

## **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 przechowywany jest klucz CCK do poświadczania odpowiedzi oraz klucze infrastruktury niezbędne do funkcjonowania CCK.

Oba centra są zabezpieczone przed zanikiem zasilania, utratą jednej linii komunikacyjnej, pożarem, zalaniem, awarią pojedynczego komputera, urządzenia lub dysku.

W przypadku awarii sprzętu lub infrastruktury przekraczającej możliwości wynikające z zabezpieczeń stosowanych w pojedynczej lokalizacji, CCK przełącza swoją działalność na Centrum Zapasowe.

CCK może być skonfigurowane do jednoczesnej pracy Centrum Podstawowego i Centrum Zapasowego. W takim przypadku przełączenie na realizację usług przez Centrum Zapasowe może nastąpić automatycznie, w sposób niezauważalny dla Subskrybentów. W takim przypadku po katastrofie skutkującej wyłączeniem Centrum Podstawowego działania kryzysowe ograniczają się do:

1. Zabezpieczenia materiałów poufnych przechowywanych w Centrum Podstawowym.
2. Bieżącej analizy sytuacji pod kątem zagrożeń dla pracy Centrum Zapasowego.

Jeśli systemy CCK nie są skonfigurowane do jednoczesnej pracy Centrum Podstawowego i Zapasowego, w przypadku wystąpienia wyłączenia Centrum Podstawowego praca jest przełączana na Centrum Zapasowe zgodnie z zasadami określonymi poniżej.

O ile to w danej sytuacji możliwe, przełączenie jest wykonywane w następujący sposób:

1. Działaniami CCK kieruje Kierownik CCK, pod nadzorem Dyrektora Pionu Usług Utrzymaniowych..
2. O planowanym czasie przełączenia powiadamia się Punkty Rejestracji pracujące w godzinach przełączenia.
3. Równolegle personel CCK, w razie potrzeby z pomocą pracowników firmy ochrony osób i mienia, zabezpiecza materiały poufne (w szczególności klucz prywatny CCK) znajdujące się w Centrum Podstawowym.
4. Niezbędny do uruchomienia Centrum Zapasowego personel CCK stawia się do pracy w Centrum Zapasowym. Obejmuje to osoby pełniące następujące funkcje:
  - a. Administratora CCK
  - b. Inspektora ds. audytu
  - c. Inne osoby, o ile ich obecność jest potrzebna do uaktywnienia klucza CCK
5. Powinna być także zapewniona obecność lub dyżur telefoniczny z możliwością szybkiego przyjazdu osoby pełniącej następującą funkcje:
  - a. Administratora systemu informatycznego
6. Uaktywniany jest klucz CCK w urządzeniu HSM w Centrum Zapasowym.
7. Personel CCK zamyka oprogramowanie w Centrum Podstawowym i wykonuje działania zapewniające, że baza danych CCK Centrum Zapasowego jest w pełni zsynchronizowana z Centrum Podstawowym (o ile takie działania są konieczne).
8. Personel CCK uruchamia oprogramowanie CCK w Centrum Zapasowym, kontroluje aktualność danych o statusie certyfikatów, wczytuje niezbędne klucze (w tym klucze infrastruktury) i wprowadza oprogramowanie w stan gotowości do przyjmowania żądań.
9. Żądania potwierdzania ważności certyfikatów są kierowane do Centrum Zapasowego.

W przypadku nagłej utraty dostępności i możliwości pracy Centrum Podstawowego podejmowane są następujące działania:

1. Działaniami CCK kieruje Kierownik CCK, pod nadzorem Dyrektora Pionu Usług Utrzymaniowych.
2. Niezbędny do uruchomienia Centrum Zapasowego personel CCK stawia się niezwłocznie do pracy w Centrum Zapasowym. Obejmuje to osoby pełniące następujące funkcje:
  - a. Administratora CCK
  - b. Inspektora ds. audytu
  - c. Inne osoby, o ile ich obecność jest potrzebna do uaktywnienia klucza CCK.
3. Równolegle personel CCK, w razie potrzeby z pomocą pracowników firmy ochrony osób i mienia, zabezpiecza materiały poufne (w szczególności klucz prywatny CCK) znajdujące się w Centrum Podstawowym.
4. Powinna być także zapewniona obecność lub dyżur telefoniczny z możliwością szybkiego przyjazdu osoby pełniącej następującą funkcje:
  - a. Administratora systemu informatycznego

5. Uaktywniany jest klucz CCK w urządzeniu HSM w Centrum Zapasowym.
6. Personel CCK uruchamia oprogramowanie CCK w Centrum Zapasowym, kontroluje aktualność danych o statusie certyfikatów, wczytuje niezbędne klucze (w tym klucze infrastruktury) i wprowadza oprogramowanie w stan gotowości do przyjmowania żądań.
7. Żądania potwierdzania ważności certyfikatów są kierowane do Centrum Zapasowego.

Wszystkie czynności związane z przełączeniem pracy Centrum Certyfikacji na Centrum Zapasowe powinny być wykonywane w taki sposób, aby zminimalizować czas niedostępności usług.

## **5.8. Zakończenie działalności CCK**

Decyzję o zakończeniu działalności CCK podejmuje Zarząd Spółki. O ile to w danej sytuacji możliwe, zakończenie działalności powinno nastąpić nie wcześniej niż z dniem upływu ważności zaświadczenia certyfikacyjnego służącego do weryfikacji ostatniego wydanego poświadczania. Nie oznacza to konieczności świadczenia nowych usług (to jest wydawania nowych poświadczeń ważności) do tego czasu.

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 niszczone.

O ile inny kwalifikowany podmiot certyfikacyjny nie 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.

Generowanie par kluczy Centrum Certyfikacji Kluczy odbywa się wewnątrz urządzenia HSM posiadającego co najmniej jeden z certyfikatów wymaganych przepisami o podpisie elektronicznym.

#### **6.1.2 Dostarczenie klucza prywatnego Subskrybentowi**

Nie dotyczy.

#### **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.

### **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.

### **6.1.6 Cel użycia klucza**

Klucz prywatny Centrum Certyfikacji Kluczy może być wykorzystywany tylko do poświadczania ważności certyfikatów.

## **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 CCK i przetwarzanych programowo – o ile takie klucze występują.

Klucze prywatne nie są archiwizowane.

Klucz prywatny CCK jest odczytywany z urządzenia HSM jedynie w postaci zaszyfrowanych fragmentów klucza, umożliwiającą 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 wyłączenia urządzenia HSM.

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.

Klucze infrastruktury służące do szyfrowania kluczy prywatnych CCK są przechowywane na indywidualnych modułach kluczowych, chronionych kodami PIN i przydzielonych upoważnionym osobom. Fragmenty kluczy infrastruktury zapisane są na modułach kluczowych z wykorzystaniem procedury podziału sekretu.

### **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.

### **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 testów nie mogą być używane klucze prywatne CCK służące do realizacji usług kwalifikowanych, chyba że zostaną wypełnione wszystkie zasady obowiązujące przy realizacji tych usług.

CCK wykorzystuje do realizacji swoich usług jedynie oprogramowanie firm posiadających wyrobioną renomę na rynku, zajmujących się produkcją oprogramowania związanego z bezpieczeństwem od co najmniej 10 lat.

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**

Do oznaczania czasem poświadczeń ważności certyfikatów oraz zapisów w logach 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 poświadczania ważności

### 7.1. Identyfikatory DN

#### Identyfikator DN Centrum Certyfikacji Kluczy

Kraj (countryName) = *PL*

Nazwa organizacji (organizationName) = *ENIGMA SOI Sp. z o.o.*

Nazwa powszechna (commonName) = *CenCert Poświadczania Ważności Certyfikatów*

Numer seryjny (serialNumber) = *Nr wpisu: 10*

### 7.2. Profil żądań poświadczania ważności certyfikatu

Akceptowane są żądania znakowania czasem zgodne z normą RFC 2560. Do przesłania treści żądania oraz pobrania odpowiedzi używany jest protokół HTTP.

### 7.3. Profil poświadczania ważności certyfikatów

Odpowiedź serwera poświadczeń jest zgodna z normą RFC 2560.

Atrybut *certStatus* zawierający wartość „good” oznacza jedynie to, że certyfikat nie jest w danym momencie unieważniony ani zawieszony. Nie oznacza to, że certyfikat jest ważny ze względu na określony w nim okres ważności. W szczególności certyfikat który został unieważniony lub zawieszony, w okresie ważności będzie określany jako „revoked”, natomiast po upływie jego okresu ważności może być oznaczony jako „good”.

Atrybut *thisUpdate* określa moment, na który jest ważna informacja o statusie certyfikatu.

Atrybut *producedAt* określa moment poświadczania odpowiedzi o statusie ważności certyfikatu. Nie jest to równoznaczne z momentem, na który jest określony status certyfikatu.

## **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.

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.

Centrum Certyfikacji Kluczy podlega także kontrolom, prowadzonym zgodnie z przepisami o podpisie elektronicznym przez ministra właściwego ds. gospodarki.

## **9. Inne postanowienia**

### **9.1. Opłaty**

CCK nie pobiera opłat za świadczenie usług poświadczania ważności kwalifikowanych 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.

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*. Suma ubezpieczenia wynosi nie mniej niż 250.000 euro na jedno zdarzenie i 1.000.000 euro na wszystkie zdarzenia.

### **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,

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

## **9.4. Ochrona danych osobowych**

Centrum Certyfikacji Kluczy nie przetwarza danych osobowych Subskrybentów usługi poświadczania ważności kwalifikowanych certyfikatów.

## **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 poświadczanych danych poza zakresem określonym w polityce certyfikacji.

## **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**

Polityka CenCert w wersji 1.21, zatwierdzona i opublikowana przez firmę Safe Technologies S.A., zachowuje ważność aż do momentu upłynięcia okresu ważności odpowiedniego zaświadczenia certyfikacyjnego wystawionego dla Safe Technologies S.A. przez Ministra Gospodarki.

Niniejsza polityka certyfikacji obowiązuje w stosunku do wystawionych zgodnie z nią poświadczeń ważności.

W stosunku do nowo wystawianych poświadczeń 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 Dyrektora Pionu Usług Utrzymaniowych lub Zarządu spółki ENIGMA SOI Sp. z o.o.

Skargi na działalność Centrum Certyfikacji Kluczy można także kierować, 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:

- Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym. (Dz. U nr 130 Poz. 1450, z późn. zm.).
- Ustawie z dnia 29 sierpnia 1997 o ochronie danych osobowych (tekst jednolity Dz. U. Nr 101/2002 poz. 926, z późn. zm.)
- Ustawie z dnia 6 czerwca 1997 Kodeks karny (Dz. U. Nr 88/1997 poz. 553, z późn. zm.)
- Ustawie z dnia 4 lutego 1994 Prawo autorskie (Dz. U. Nr 24/1994 poz. 83, z późn. zm.)

## **9.16. Inne postanowienia**

Nie występują.