CENTRUM CERTYFIKACJI „CENCERT”

Polityka certyfikacji dla certyfikatów niekwalifikowanych firmowych

Wersja: 1.2

Karta dokumentu:

Tytuł dokumentu	Polityka certyfikacji dla certyfikatów niekwalifikowanych firmowych
Nazwa pliku	Polityka certyfikatów firmowych
Właściciel dokumentu	ENIGMA Systemy Ochrony Informacji Sp. z o.o.
Wersja	1.2
Status dokumentu	zatwierdzony
Data zatwierdzenia	20 września 2017
Liczba stron	45

zatwierdzone przez:

Wersja	**zatwierdzający**
1.1	Jacek Pokraśniewicz, Dyrektor Pionu Utrzymania Usług CenCert

historia wersji

Wersja	**Data**	**Komentarze**
1.0	2012-12-19	Wersja początkowa
1.1	2016-08-24	Zmiana algorytmu wystawianych certyfikatów na SHA-256, dostosowanie terminologii do eIDAS, inne drobne zmiany
1.2	2017-09-20	Zmiana HSM oraz długości kluczy CA (do 4096)

Spis treści

1. Wstęp

1.1. Wprowadzenie

Niniejszy dokument stanowi politykę certyfikacji realizowaną przez Centrum Certyfikacji Kluczy *CenCert* prowadzone przez firmę ENIGMA Systemy Ochrony Informacji Sp. z o.o., w celu realizacji usług certyfikacyjnych polegających na wystawianiu certyfikatów kluczy publicznych dla osób fizycznych, osób prawnych, jednostek organizacyjnych nieposiadających osobowości prawnej oraz urządzeń.

Podstawową zasadą funkcjonowania niniejszej polityki jest to, że certyfikaty Subskrybentów są wystawiane w *Domenach*, z których każda jest przydzielona na podstawie umowy/zamówienia danej firmie lub innej jednostce organizacyjnej (tzw. *Zarządzający* domeną). Każdy certyfikat wystawiony w danej Domenie zawiera dane identyfikacyjne Zarządzającego. Wymaga się, aby dane Subskrybentów zamieszczane w certyfikatach były weryfikowane w sposób odpowiedni i skuteczny u danego Zarządzającego, odpowiedzialność za to ciąży na Zarządzającym każdej Domeny.

Centrum Certyfikacji Kluczy realizuje niniejszą politykę zgodnie z rozporządzeniem Parlamentu Europejskiego i Rady (UE) nr 910/2014 z dnia 23 lipca 2014 r. (eIDAS), rozporządzeniami wykonawczymi Komisji Europejskiej wydanymi na podstawie eIDAS oraz prawem krajowym obowiązującym w Polsce.

Struktura niniejszego 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 niekwalifikowanych firmowych
Kwalifikator polityki	Brak
Numer OID (ang. *Object Identifier*)	1.3.6.1.4.1.10214.99.1.2.2.1

Data wprowadzenia	24 sierpnia 2016 r.
Data wygaśnięcia	Do odwołania

1.3. Opis systemu certyfikacji i uczestniczących w nim podmiotów

CCK CenCert, realizując niniejszą politykę certyfikacji, wystawia certyfikaty dla „użytkowników końcowych", służące do realizacji usług informatycznych wymagających podpisu lub pieczęci elektronicznej, uwierzytelnienia lub szyfrowania. W ramach niniejszej polityki nie są wystawiane certyfikaty dla „podległych" (w sensie hierarchii X.509) centrów certyfikacji wystawiających certyfikaty.

CCK CenCert obsługuje Subskrybentów w zakresie unieważnień certyfikatów, poprzez Centralny Punkt Rejestracji (CPR), którego dane znajdują się w rozdziale 1.5. Centralny Punkt Rejestracji realizuje usługi unieważniania w dni robocze, w godzinach 8-18.

CCK CenCert może obsługiwać także Subskrybentów (w zależności od określonego pomiędzy stronami zakresu usług) także poprzez:

- Centralny Punkt Rejestracji (w pozostałym zakresie usług)
- Mobilnych Inspektorów rejestracji,
- Inne, określone w porozumieniu z Zarządzającym, punkty rejestracji.

Na podstawie porozumienia z Zarządzającym CCK Cencert może przyznać osobom wskazanym przez Zarządzającego uprawnienia Inspektorów rejestracji w zakresie Domeny certyfikatów zarządzanych przez danego Zarządzającego.

1.4. Zakres zastosowań

Certyfikaty wystawiane zgodnie z niniejszą polityką certyfikacji mogą służyć do realizacji usług zgodnych z profilem danego certyfikatu.

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

Telefon kontaktowy:
+48 22 720 79 55 – dni robocze, w godzinach 8-18
+48 666 028 044 – dni robocze, w godzinach 8-18

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
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 zawierającymi różne dane w polu *wystawca certyfikatu* (różne identyfikatory DN), mówimy o oddzielnych Centrach Certyfikacji Kluczy.
CRL	Lista unieważnionych certyfikatów. Jest wystawiana, poświadczana elektronicznie i publikowana przez CCK.
DN	Identyfikator DN – *Distinguished Name* – Identyfikator podmiotu PKI według składni zdefiniowanej w normach serii X.500
HSM	*Hardware Security Module* – Sprzętowy moduł kryptograficzny – urządzenie posiadające funkcjonalność generowania kluczy kryptograficznych i wykorzystywania klucza prywatnego 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.
Klucz prywatny	Dane służące do składania podpisu elektronicznego (w tym w celu uwierzytelnienia) lub odszyfrowania danych przez osobę posługującą się certyfikatem. Dane służące do składania poświadczenia elektronicznego przez Centrum Certyfikacji Kluczy.
Klucz publiczny	Dane służące do weryfikacji podpisu elektronicznego lub do zaszyfrowania danych, umieszczane w certyfikacie lub zaświadczeniu certyfikacyjnym

Termin/akronim	Opis
OCSP	*Online Certificate Status Protocol* - protokół i nazwa usługi PKI służącej do informowania o statusie konkretnych certyfikatów, o które pyta usługobiorca (czy certyfikat jest ważny, czy unieważniony)
PKI	*Public Key Infrastructure* – infrastruktura klucza publicznego – system obejmujący Centra Certyfikacji Kluczy, Punkty Rejestracji oraz użytkowników końcowych, służący do dystrybucji certyfikatów klucza publicznego oraz zapewnienia możliwości ich wiarygodnej weryfikacji
Domena	W niniejszej polityce certyfikacji – grupa Subskrybentów obsługiwana przez CCK CenCert w jednolity sposób, na podstawie porozumienia z konkretną firmą lub instytucją (Zarządzający). Każdy Subskrybent obsługiwany na podstawie niniejszej polityki należy do dokładnie jednej Domeny. Certyfikaty Subskrybentów wystawiane zgodnie z niniejszą polityką certyfikacji zawierają nazwę firmy/instytucji, w sposób jednoznaczny identyfikującą Zarządzającego.
Zarządzający	Firma lub instytucja dysponująca, na podstawie porozumienia z CenCert (umowy, zamówienia itd.) możliwością zarządzania certyfikatami należącymi do dedykowanej dla Zarządzającego Domeny. Przez zarządzanie należy rozumieć podejmowanie decyzji o możliwości wystawienia certyfikatu z określonymi danymi oraz decyzji o unieważnieniu certyfikatu.
Subskrybent	Osoba (fizyczna lub prawna) uprawniona do dysponowania i dysponująca rzeczywiście kluczem prywatnym związanym z ważnym certyfikatem wystawionym przez CCK CenCert.
Strona ufająca	Podmiot mający potrzebę weryfikacji certyfikatu wystawionego zgodnie z niniejszą polityką certyfikacji.
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

2. Zasady dystrybucji i publikacji informacji

CCK publikuje następujące informacje:

- Aktualne klucze publiczne CA (w postaci certyfikatów wystawionych przez rootCA).
- Aktualne listy 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. Identyfikatory wyróżniające

Podmioty certyfikatów identyfikowane są przy użyciu identyfikatorów wyróżniających (ang. Distinguished Names) zdefiniowanych w Zaleceniach ITU z serii X.500.

Dopuszcza się wystawianie certyfikatów zawierających identyfikatory „anonimowe" (nie wskazujące na żadną osobę, firmę/instytucję, stronę WWW itd.), z tym że anonimowość nie dotyczy danych Zarządzającego.

CCK nie zapewnia, że identyfikatory wyróżniające zawarte w certyfikatach zawierają „znaczące" dane, przy pomocy których można podmiot zidentyfikować Subskrybentów. Nie dotyczy to danych Zarządzającego.

Identyfikatory DN Subskrybentów maja następującą budowę:

1) Atrybuty identyfikatora DN wspólne dla całej Domeny (bez możliwości edycji przy wystawianiu konkretnych certyfikatów):
   a) *Kraj* (Country Name) – kod kraju, w którym ma siedzibę Zarządzający
   b) *Organizacja* (Organization Name) – oficjalna nazwa Zarządzającego, zgodna z dokumentami
   c) (opcja) *Jednostka organizacyjna* (Organizational Unit Name) – nazwa jednostki organizacyjnej Zarządzającego, wpisywana na życzenie Zarządzającego
   d) *(opcja) Adres* (Street Address) – pełen adres siedziby Zarządzającego lub adres wyodrębnionej jednostki organizacyjnej Zarządzającego, wymienionej w polu *Jednostka organizacyjna*, w postaci „ul. Zabużańska 101, 00-870 Konin"
   e) *(opcja) Numer seryjny* (Serial Number) – numer typu REGON, KRS lub NIP przysługujący Zarządzającemu, wpisywany w postaci „KRS: XXXXXXX", „NIP: XXXXXXX"
2) Atrybuty identyfikatora DN określające Subskrybenta, zgodne z X.500 (takie jak *nazwa własna, imię, nazwisko, email* itd.). CCK dokłada starań, aby struktura atrybutów określających Subskrybenta uniemożliwiała pomyłki dotyczące przyporządkowania poszczególnych danych do Zarządzającego czy Subskrybenta.

Szczegółowa struktura (lub struktury) atrybutów DN w zakresie danych Subskrybentów ustalana jest dla konkretnej Domeny niezależnie, w zależności od potrzeb Zarządzającego.

Pola DN „Adres" i/lub „Numer seryjny" można pominąć, jeśli identyfikacja Zarządzającego na podstawie samej nazwy nie budzi wątpliwości (np. dla jednostek administracji państwowej lub samorządowej).

CCK potwierdza prawa Zarządzającego do posługiwania się danymi Zarządzającego umieszczonymi w certyfikacie.

Potwierdzanie praw Subskrybentów do posługiwania się danymi zawartymi w certyfikacie leży po stronie Zarządzającego. Dane Subskrybentów umieszczone w certyfikacie nie mogą wprowadzać w błąd Strony ufającej.

CCK 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 Zarządzającego prawa do posługiwania się daną nazwą lub innym oznaczeniem zamieszczonym w certyfikacie, jest on zobowiązany do zgłoszenia tego faktu celem unieważnienia certyfikatu z powodu nieaktualności danych zawartych w certyfikacie.

3.2. Uwierzytelnienie Subskrybenta przy wystawieniu pierwszego certyfikatu

CCK uwierzytelnia Zarządzającego oraz osoby go reprezentujące, na podstawie dokumentów takich jak KRS, statut instytucji, wpis do działalności gospodarczej.

Uwierzytelnienie Subskrybentów certyfikatów wystawianych w danej Domenie leży po stronie Zarządzającego uprawnionego do danej Domeny. Obowiązkiem Zarządzającego jest wdrożenie takich procedur uwierzytelniania, które będą zapewniały rzetelną i skuteczną weryfikację tożsamości Subskrybentów.

3.3. Uwierzytelnienie Subskrybenta przy wystawianiu kolejnych certyfikatów

Patrz rozdz. 3.2.

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

Unieważnienie certyfikatu realizowane przez Centralny Punkt Rejestracji dokonywane jest:

- telefonicznie, na podstawie hasła ustalonego dla każdego Subskrybenta przy wystawianiu certyfikatu,
- na podstawie pisma przysłanego do CPR przez Zarządzającego, podpisanego przez osoby upoważnione.

W przypadku posiadania przez Zarządzającego uprawnień Inspektora ds. rejestracji w danej Domenie, sposoby uwierzytelniania osób upoważnionych do podejmowania decyzji o unieważnieniu, zawieszeniu, bądź uchyleniu zawieszenia certyfikatu są określone przez procedury obowiązujące u Zarządzającego.

4. Cykl życia certyfikatu – wymagania operacyjne

4.1. Zgłoszenie certyfikacyjne

Zgłoszenia certyfikacyjne występują jedynie w kontekście danej Domeny zarządzanej przez danego Zarządzającego na podstawie umowy pomiędzy Zarządzającym a CCK CenCert lub zamówienia zgodnego ze wzorem stanowiącym Załącznik nr 1. do niniejszej polityki (lub co najmniej zawierającym istotne elementy tego wzoru zamówienia). Umowa, jeśli występuje, powinna zawierać istotne elementy wzoru zamówienia zapisanego w Załączniku nr 1.

W zależności od ustaleń z Zarządzającym, Centrum Certyfikacji Kluczy generuje klucze Subskrybentów i/lub przyjmuje od Zarządzającego zgłoszenia certyfikacyjne w formacie zgodnym z PKCS#10, zawierające klucze publiczne oraz identyfikatory DN Subskrybentów.

W przypadku gdy klucze są generowane przez Centrum Certyfikacji Kluczy, zapewnia ono, że sposób wytworzenia i przetwarzania kluczy prywatnych po stronie CCK gwarantuje, że nie mogą być one kopiowane ani wykorzystane w sposób sprzeczny z niniejszą polityką i ustaleniami z Zarządzającym.

4.2. Przetwarzanie zgłoszeń certyfikacyjnych

Zgłoszenia certyfikacyjne PKCS#10 (wytworzone w CCK CenCert przez Inspektora ds. rejestracji lub przyjęte przez CCK CenCert od Zarządzającego) są wprowadzane do systemu informatycznego Centrum Certyfikacji Kluczy indywidualnie lub w systemie pracy wsadowej (automatycznej).

4.3. Wystawienie certyfikatu

System informatyczny Centrum Certyfikacji Kluczy niezwłocznie po wczytaniu zgłoszenia weryfikuje podpis elektroniczny oraz uprawnienia Inspektora ds. rejestracji, a następnie wystawia certyfikat.

4.4. Akceptacja certyfikatu

Do sprawdzenia i akceptacji certyfikatu zobowiązany jest Subskrybent niezwłocznie po otrzymaniu certyfikatu, a przed jego użyciem (w szczególności przed wykonaniem pierwszego podpisu elektronicznego weryfikowanego przy użyciu tego certyfikatu). W przypadku nieprawdziwości danych zawartych w certyfikacie (w szczególności danych identyfikacyjnych Subskrybenta) Subskrybent jest zobowiązany do niezwłocznego poinformowania CCK lub Zarządzającego, zgodnie z procedurami obowiązującymi przy unieważnianiu certyfikatów, w celu unieważnienia certyfikatu i otrzymania nowego, zawierającego poprawne dane. Nie jest dozwolone posługiwanie się certyfikatem zawierającym nieprawdziwe dane.

4.5. Korzystanie z pary kluczy i certyfikatu

4.5.1 Korzystanie z certyfikatu

Certyfikaty Subskrybentów mogą być wykorzystywane zgodnie z przeznaczeniem, dla jakiego zostały wydane.

Jedynymi sposobami potwierdzenia przez oprogramowanie Strony ufającej ważności certyfikatu Subskrybenta jest sprawdzenie okresu ważności certyfikatu oraz sprawdzenie ważności certyfikatu na aktualnej liście CRL poświadczonej przez Centrum Certyfikacji Kluczy.

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

4.5.2 Korzystanie z klucza prywatnego

Klucz prywatny związany z certyfikatem Subskrybenta służy do celów określonych w certyfikacie oraz niniejszej polityce certyfikacji. Klucz ten powinien podlegać odpowiedniej ochronie, której poziom powinien odpowiadać przeznaczeniu klucza i występującym przy tym zagrożeniom.

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

4.6. Wymiana certyfikatu

Dopuszcza się wymianę ważnego certyfikatu 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.

Nie ma możliwości wymiany certyfikatu unieważnionego. W takim przypadku należy postępować według zasad przewidzianych przy wydawaniu pierwszego certyfikatu.

Wymiana certyfikatu następuje z inicjatywy Zarządzającego.

4.7. Wymiana certyfikatu połączona z wymianą pary kluczy

Nie ma możliwości wymiany certyfikatu unieważnionego. W takim przypadku należy postępować według zasad przewidzianych przy wydawaniu pierwszego certyfikatu.

Wymiana certyfikatu następuje z inicjatywy Zarządzającego.

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, działający poprzez Zarządzającego.

4.9. Unieważnienie i zawieszenie certyfikatu

Podmiotem uprawnionym do unieważnienia certyfikatu jest:

- Subskrybent,
- Zarządzający,
- Centrum Certyfikacji Kluczy.

Subskrybent oraz Zarządzający 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 i Zarządzający są solidarnie zobowiązani do niezwłocznego unieważnienia certyfikatu w następujących przypadkach:

- Gdy dostęp do klucza prywatnego związanego z certyfikatem ma (lub istnieje istotne zagrożenie, że może mieć) nieuprawniona osoba,
- Gdy dane zawarte w certyfikacie są nieprawidłowe.
- W przypadku dezaktualizacji danych Subskrybenta lub podmiotu, z którym związany jest Subskrybent, zawartych w certyfikacie.

Centrum Certyfikacji Kluczy ma prawo do unieważnienia certyfikatu jedynie w uzasadnionych przypadkach. W szczególności, Centrum Certyfikacji Kluczy ma prawo do unieważnienia certyfikatów w domenie Zarządzającego w przypadku istotnego naruszania przez Zarządzającego obowiązku skutecznej kontroli tożsamości Subskrybentów, określonego w rozdz. 3.2 wyżej.

Usługa zawieszania/uchylania zawieszenia certyfikatów jest świadczona jedynie wtedy, gdy przewiduje to porozumienie CCK CenCert z Zarządzającym.

Zawieszone certyfikaty nie są automatycznie unieważniane.

4.10. Usługi informowania o statusie certyfikatów

Jedyną formą informowania przez Centrum Certyfikacji Kluczy o statusie certyfikatu jest lista unieważnionych i zawieszonych certyfikatów (lista CRL).

Lista CRL jest wystawiana 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.

4.11. Zakończenie umowy certyfikacyjnej

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

Subskrybent oraz Zarządzający mogą ponadto zakończyć umowę w każdym czasie, poprzez unieważnienie certyfikatu.

4.12. Powierzanie i odtwarzanie kluczy prywatnych

Centrum Certyfikacji Kluczy nie powierza swojego klucza prywatnego inny podmiotom.

5. Zabezpieczenia organizacyjne, operacyjne i fizyczne

5.1. Zabezpieczenia fizyczne

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

Serwery CCK znajdują się w klimatyzowanej serwerowni, wyposażonej w system ochrony przed zalaniem, pożarem oraz zanikami zasilania, a także system kontroli dostępu oraz system alarmowy włamania i napadu klasy SA3.
Dostęp do pomieszczenia serwerowni jest możliwy tylko dla upoważnionych osób, a każdorazowy fakt dostępu jest odnotowywany.

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

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

Nazwa funkcji w CCK	**Nazwa funkcji według przepisów o podpisie elektronicznym**	**Rodzaj obowiązków**
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 w Centralnym Punkcie Rejestracji, we wszystkie dni w roku, w zakresie unieważniania certyfikatów.

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

5.3. Zabezpieczenia osobowe

Poniższe postanowienia niniejszego rozdziału nie dotyczą delegowanych przez Zarządzających osób pełniących funkcje Inspektorów ds. rejestracji, posiadających uprawnienia wyłącznie w zakresie Domen delegowanych poszczególnym Zarządzającym. Osoby te podlegają przeszkoleniu przez osoby upoważnione przez CCK CenCert, a za określenie szczegółowych warunków zatrudniania i wymagań co do kwalifikacji takich osób odpowiedzialni są poszczególni Zarządzający.

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.

Odpowiedzialność personelu CCK 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 obowiązujących przepisach.

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 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;

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, pozwalającego na zaawansowane filtrowanie zapisów oraz wiązanie poszczególnych zapisów w logiczne powiązane ciągi zdarzeń (np. ciąg zdarzeń dotyczący wystawienia określonego certyfikatu).

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 certyfikaty i zaświadczenia certyfikacyjne wystawione w poprzednim roku,
- wszystkie listy CRL wystawione w poprzednim roku,
- rejestry zdarzeń.

Okres przechowywania kopii archiwalnych wynosi 11 lat.

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 elektroniczne 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 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 powodem dostępu.

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 Utrzymania Usług CenCert.

Planowa wymiana pary kluczy CCK następuje nie wcześniej niż po 5 latach i nie później niż po 6 latach od daty wygenerowania aktualnego zaświadczenia certyfikacyjnego.

Procedura wymiany pary kluczy polega na:

- Wygenerowaniu nowej pary kluczy CCK i samo-podpisanego 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.
- Umieszczeniu nowego samo-podpisanego zaświadczenia certyfikacyjnego oraz zakładkowych zaświadczeń certyfikacyjnych w repozytorium CCK.

Alternatywnie, wymiana kluczy może być zrealizowana poprzez utworzenie nowej struktury PKI (przydzielenie nowego DNa dla CA).

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) podejmuje decyzję o nadaniu sprawie biegu.
2. Skompromitowany klucz prywatny CCK, jak również wszelkie zaświadczenia certyfikacyjne zawierające odpowiadający mu klucz publiczny zostają wycofane z repozytorium CCK.
3. Najszybciej jak to jest możliwe o zaistniałej sytuacji oraz o planie dalszego działania informowani są Zarządzający.
4. 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.
5. Zarząd powołuje komisję, która ma zbadać przyczyny zaistnienia zdarzenia oraz zaproponować ewentualne działania korygujące.
6. Najszybciej, jak to jest możliwe, Centrum Certyfikacji Kluczy generuje nową parę kluczy CCK do poświadczania certyfikatów i list CRL – stosując procedury obowiązujące przy generowaniu klucza CCK. CCK generuje także niezbędne klucze infrastruktury, oraz certyfikaty Inspektorów ds. Rejestracji.
7. CCK wznawia normalną działalność. O ile identyfikator DN Centrum Certyfikacji Kluczy nie uległ zmianie, CCK generuje listy CRL w taki sposób, że lista unieważnień zawiera także numery wszystkich certyfikatów poświadczonych kluczem CCK, który utracił poufność – każdy certyfikat aż do następnej listy CRL po upłynięciu okresu ważności certyfikatu.
8. Jeśli integralność bazy danych certyfikatów nie budzi wątpliwości, Dyrektor Pionu Usług Utrzymaniowych, w konsultacji z Zarządzającymi, podejmuje decyzję o ponownym wystawieniu certyfikatów na te same klucze Subskrybentów i tym samym końcu okresu ważności (chyba że zapadną inne ustalenia co do okresu ważności), bez konieczności

ponownego generowania kluczy Subskrybentów. CCK CenCert ustali z Zarządzającymi sposób instalacji certyfikatów po stronie Subskrybentów.

9. Certyfikaty na okres ważności nie dłuższy niż okres ważności certyfikatów unieważnionych z powodu ujawnienia klucza CCK, wystawiane są nieodpłatnie.

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 certyfikatów i list CRL 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.

Oba centra są zabezpieczone przed zanikiem zasilania, pożarem, zalaniem. Centrum Podstawowe jest ponadto zabezpieczone przed utratą jednej linii telekomunikacyjnej oraz awarią pojedynczego komputera, urządzenia lub dysku.

CCK posiada udokumentowane oraz okresowo testowane procedury przewidujące działania na wypadek konieczności przełączenia przetwarzania na Centrum Zapasowe, zarówno w przypadku planowego, jak i nagłego przełączenia.

Wszystkie czynności związane z przełączeniem pracy Centrum Certyfikacji na Centrum Zapasowe powinny być wykonane w takim czasie, aby było możliwe opublikowanie następnej listy CRL w ciągu 1 godziny od ewentualnego unieważnienia certyfikatu, nie później jednak niż następnego dnia po opublikowaniu ostatniej wcześniejszej listy CRL.

5.7.2.2 Wyłączenie Centralnego Punktu Rejestracji

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

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

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

5.7.2.3 Wyłączenie repozytorium CCK i/lub serwera usług OCSP

W przypadku katastrofy polegającej na wyłączeniu działania repozytorium CCK, 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 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 informowani są Zarządzający z wyprzedzeniem co najmniej 6 miesięcy.

Po zakończeniu działalności klucz prywatny CCK jest niszczony.

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 zabezpieczenia wszystkich poufnych informacji..

Generowanie par kluczy Centrum Certyfikacji Kluczy odbywa się wewnątrz urządzenia HSM.

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, przez Centrum Certyfikacji Kluczy CenCert lub przez Zarządzającego daną Domeną – zależnie od ustaleń przyjętych pomiędzy CCK CenCert a Zarządzającym.

6.1.2 Dostarczenie klucza prywatnego Subskrybentowi

Jeśli klucze prywatne Subskrybentów są generowane przez CCK, sposób przekazania tych kluczy Subskrybentom jest określany w porozumieniu z danym Zarządzającym. Standardowo klucze są przekazywane, na nośnikach, za pośrednictwem Zarządzającego.

6.1.3 Dostarczenie klucza publicznego Subskrybenta do Punktów Rejestracji

Klucz publiczny Subskrybenta jest dostarczany do CCK w postaci zgłoszenia certyfikacyjnego zgodnego z normą PKCS#10 - na nośniku danych (CD/DVD lub Flash memory) lub w postaci załącznika do poczty elektronicznej wysłanej na adres CPR.

6.1.4 Dostarczenie klucza publicznego CCK

Klucz publiczny Centrum Certyfikacji Kluczy jest publikowany, w postaci certyfikatu wystawionego przez rootCA,, w repozytorium CCK na stronie WWW, którego dane znajdują się w rozdziale 2. Repozytorium jest dostępne także poprzez protokół HTTPS.

6.1.5 Rozmiary kluczy

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

Klucze Centrum Certyfikacji Kluczy mają długość 4096 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 co najmniej 1024 bity,
- 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*.

Zawartość rozszerzenia *keyUsage* w certyfikatach Subskrybentów jest odpowiednia do celu, dla którego dane certyfikaty są wystawiane.

6.2. Ochrona kluczy prywatnych

CA używa do przetwarzania klucza prywatnego używanego do wystawiania certyfikatów urządzeń HSM posiadających certyfikat FIPS PUB 140 dla poziomu 3.

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 wewnętrznie w CCK i przetwarzanych programowo – o ile takie klucze występują.

Klucze prywatne CCK nie są archiwizowane.

Klucze prywatne Subskrybentów mogą być archiwizowane przez CCK jedynie w przypadku, gdy takie wyraźne postanowienie zawarto w porozumieniu CCK CenCert z Zarządzającym daną Domeną. W takim przypadku archiwizowane klucze prywatne są dostępne w postaci zaszyfrowanej, możliwej do odczytania jedynie dla osób mających określone, specjalne uprawnienia.

Klucze prywatne Inspektorów ds. rejestracji 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. Aktywacja partycji z kluczami wymaga współdziałania co najmniej 2 upoważnionych osób.

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.

Niszczenie kluczy prywatnych 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. Z procedury niszczenia sporządza się protokół.

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

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

6.3. Inne aspekty zarządzania parą kluczy

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

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

Okres ważności certyfikatów kluczy publicznych Subskrybentów wynosi maksymalnie 2 lata dla kluczy RSA 1024 i 5 lat dla kluczy RSA 2048 i dłuższych.

Okres ważności par kluczy Inspektorów ds. rejestracji oraz certyfikatów tych kluczy jest nie dłuższy niż 5 lat.

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.

CA przeprowadza audyty, w tym testy penetracyjne, używanego systemu informatycznego. Wyniki audytów nie są publikowane.

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

6.6. Zabezpieczenia związane z cyklem życia systemu informatycznego

W Centrum Certyfikacji Kluczy przyjęto udokumentowaną procedurę dokonywania modyfikacji lub zmian w systemie teleinformatycznym. W szczególności dotyczy to testów nowych wersji oprogramowania i/lub wykorzystania do tego celu istniejących baz danych.

Zasady te gwarantują nieprzerwaną pracę systemu teleinformatycznego, integralność jego zasobów oraz zachowanie poufności danych.

W szczególności procedura gwarantuje testowanie nowych wersji oprogramowania w środowisku testowym. Gwarantuje także, że do realizacji jakichkolwiek prac w środowisku testowym nie mogą być używane kluczy prywatne CCK służące do podpisywania certyfikatów kwalifikowanych w środowisku produkcyjnym (w tym do podpisywania 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) 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 UTC(pl).

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 Firmowych 2017***

7.1.2 Profil certyfikatów

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

Podpisy pod certyfikatami są realizowane przy użyciu funkcji sha512.

Rozszerzenia certyfikatu

Pole	**Opis/wartość**	**krytyczne ?**
Extensions		
AuthorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
SubjectKeyIdentifier		NIE
subjectkeyIdentifier	skrót SHA-1 z klucza publicznego	
KeyUsage	Zgodnie z potrzebami	TAK
CertificatePolicies		NIE

Pole	Opis/wartość	krytyczne ?
PolicyInformation		
CertPolicyId	{1.3.6.1.4.1.10214.99.1.2.2.1}	
basicConstraints	pusta sekwencja (określenie, że subskrybent jest użytkownikiem końcowym i nie może wydawać certyfikatów)	TAK
crlDistributionPoints	http://crl.cencert.pl/nkw/firmowy_2017.crl	NIE

Mogą być także stosowane inne, krytyczne bądź niekrytyczne, rozszerzenia certyfikatów, w zależności od potrzeb.

Certyfikaty kluczy Inspektorów ds. Rejestracji posiadają krytyczne 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 krytyczne 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 ?
extensions		
AuthorityKeyIdentifier		NIE
keyIdentifier	skrót SHA-1 z klucza publicznego	
SubjectKeyIdentifier		NIE
SubjectKeyIdentifier		
KeyUsage	keyCertSign, cRLSign	TAK
CertificatePolicies		TAK
PolicyInformation		

Pole	**Opis/wartość**	**krytyczne ?**
CertPolicyId	{1.3.6.1.4.1.10214.99.1.2.2.1}	
basicConstraints		TAK
cA	True	
PathLenConstraint	*„0”* dla samopodpisanych zaświadczeń certyfikacyjnych	

7.2. Profil list CRL

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

Rozszerzenia

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

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

8. Audyt

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

9. Inne postanowienia

9.1. Opłaty

CCK pobiera opłaty za świadczenie swoich usług zgodnie z porozumieniem z Zarządzającym.

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 CenCert odpowiada wyłącznie za szkody wynikające z przyczyn zawinionych przez CCK CenCert.

Centrum Certyfikacji Kluczy CenCert nie odpowiada za utracone korzyści.

Maksymalna odpowiedzialność finansowa CCK CenCert, niezależnie od przyczyny powstania szkody, jest ograniczona w stosunku rocznym do wysokości równej wysokości opłat uiszczonych przez danego Zarządzającego na rzecz CCK CenCert w roku poprzedzającym zaistnienie szkody.

9.3. Poufność informacji

Zasady ochrony poufności informacji związanych ze świadczeniem usług certyfikacyjnych określone są w eIDAS i innych przepisach o podpisie elektronicznym, a także w Ustawie o ochronie danych osobowych.

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

- Polityka certyfikacji w wersjach aktualnie obowiązujących,
- Klucz publiczny CCK,
- Lista unieważnionych certyfikatów,
- Wystawione certyfikaty centrum certyfikacji (samo podpisane, zakładkowe),

- Informacje bieżące, przeznaczone do publikacji (takie jak bieżące komunikaty, dane kontaktowe CCK).

9.4. Ochrona danych osobowych

Centrum Certyfikacji Kluczy przetwarza dane osobowe Subskrybentów w takim zakresie, w jakim dane te są umieszczane w certyfikacie.

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

Dane osobowe Subskrybentów nie są przekazywane innym podmiotom i są wykorzystywane przez CCK jedynie do realizacji usług certyfikacyjnych, w tym ewentualnie do przypominania o kończącym się okresie ważności certyfikatu.

Subskrybenci są poinformowani o przysługujących im prawach w związku z przetwarzaniem przez CCK ich danych osobowych poprzez zapisy strony WWW Centrum Certyfikacji Kluczy.

Dane osobowe są zbierane przez CCK od samych Subskrybentów lub są przekazywane CCK przez firmy/instytucje reprezentujące Subskrybentów (Zarządzających). W przypadku przekazywania danych osobowych przez Zarządzających, są oni odpowiedzialni za pozyskanie zgody Subskrybentów na przekazanie CCK danych osobowych w celu wystawienia certyfikatu (o ile dane takie występują w certyfikacie), a także za poinformowanie Subskrybentów, że ich dane będą przetwarzane przez CCK CenCert zgodnie z niniejszą Polityką certyfikacji.

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 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 wyniknąć z użycia oprogramowania lub sprzętu, który nie był dostarczony przez CCK.

Centrum Certyfikacji Kluczy w żaden sposób nie odpowiada za to, czy Subskrybent użył do generowania i/lub przetwarzania swojego klucza prywatnego właściwego, zabezpieczonego odpowiedniego dla danego zastosowania urządzenia.

Centrum Certyfikacji Kluczy nie odpowiada za ewentualne szkody mogące wyniknąć z niewłaściwego wypełniania przez Zarządzających poszczególnymi Domenami obowiązków weryfikacji tożsamości Subskrybentów, otrzymujących certyfikaty w ich Domenach.

9.9. Przenoszenie roszczeń odszkodowawczych

CCK może ubezpieczać swoją działalność na zasadach ogólnych stosowanych w prowadzeniu działalności gospodarczej.

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.

Certyfikaty wystawione wcześniej, na podstawie niezatwierdzonej wersji polityki certyfikacji, pozostają ważne do momentu unieważnienia lub upłynięcia okresu ich ważności.

Do kluczy CA utworzonych w okresie obowiązywania polityki w wersji 1.1 lub wcześniejszych (klucze wciąż używane do wystawiania list CRL) mają zastosowanie postanowienia rozdziałów: 6.1.5, 6.2, 7.1 polityki w wersji 1.1. (zamiast analogicznych rozdziałów niniejszej wersji).

Postanowienia rozdziałów 1.3, 1.5 (godziny pracy Centralnego Punktu Rejestracji) dotyczą także wszystkich wystawionych wcześniej certyfikatów.

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 Utrzymania Usług CenCert lub Zarządu spółki ENIGMA SOI Sp. z o.o.

9.14. Obowiązujące prawo

Działanie podsystemu certyfikacji podlega prawu europejskiemu oraz prawu Rzeczpospolitej Polskiej.

9.15. Podstawy prawne

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

- Rozporządzeniu eIDAS i wydanych na jego podstawie rozporządzeniach wykonawczych.
- Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym – do dnia uchylenia ustawy przez ustawę o usługach zaufania.
- 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

Załącznik 1 zawiera wzór zamówienia stanowiącego podstawę do wystawienia certyfikatów wdanej Domenie. Zamówienia powinny być składane na formularzu według tego wzoru lub na formularzach zawierających istotne postanowienia zapisane w tym wzorze.

Jeśli certyfikaty są wystawiane na podstawie umowy z Zarządzającym, umowa powinna zawierać zapisy oddające istotne postanowienia zapisane w Załączniku nr 1.