Kodeks Postępowania Certyfikacyjnego Unizeto CERTUM - CCP

Wersja 2.0

Data: 15 lipca 2002

Status: poprzedni

UNIZETO Sp. z o.o.
„Centrum Certyfikacji Unizeto CERTUM”
ul. Królowej Korony Polskiej 21
70-486 Szczecin
Polska
http://www.certum.pl

Klauzula: Prawa Autorskie

Wszelkie pytania związane z prawami autorskimi należy adresować do Unizeto Sp. z o.o., ul. Królowej Korony Polskiej 21, 70-486 Szczecin, Polska, tel. +48 91 4801 201, fax +48 91 4801 220, email: info@certum.pl.

Spis treści

1. Wstęp

Kodeks Postępowania Certyfikacyjnego[1] **Unizeto CERTUM - Centrum Certyfikacji Powszechne** (nazywany dalej dla uproszczenia **Kodeksem Postępowania Certyfikacyjnego** lub w skrócie **KPC**) opisuje proces certyfikacji klucza publicznego oraz określa obszary zastosowań uzyskanych w jego wyniku certyfikatów. Znajomość natury, celu oraz roli Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **subskrybenta**[2] oraz **strony ufającej**[3].

Kodeks Postępowania Certyfikacyjnego jest uszczegółowieniem ogólnych zasad postępowania certyfikacyjnego, opisanego w **Polityce Certyfikacji Unizeto CERTUM - Centrum Certyfikacji Powszechne** (nazywanej dalej dla uproszczenia **Polityką Certyfikacji** lub w skrócie **PC**). Polityka Certyfikacji określa, jaki stopień zaufania można związać z określonym typem certyfikatu wydanego przez **Unizeto CERTUM - Centrum Certyfikacji Powszechne** (nazywango dalej dla uproszczenia **Unizeto CERTUM - CCP**). Z kolei Kodeks Postępowania Certyfikacyjnego pokazuje, w jaki sposób Unizeto CERTUM – CCP zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania.

Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego zostały zdefiniowane przez Unizeto CERTUM - CCP, które jest jednocześnie dostawcą usług certyfikacyjnych świadczonych na ich podstawie. Procedura definiowania i aktualizowania zarówno Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest zgodna z regułami opisanymi w rozdz.8.

Polityka Certyfikacji określa ogólne zasady stosowane w Unizeto CERTUM - CCP podczas procesu certyfikacji kluczy publicznych, definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Szczegółowy opis wspomnianych zasad przedstawiony jest w niniejszym **Kodeksie Postępowania Certyfikacyjnego**.

Kodeks Postępowania Certyfikacyjnego opisuje zbiór czterech polityk certyfikacji, według których Unizeto CERTUM - CCP wydaje certyfikaty urzędom i użytkownikom końcowym. Polityki te reprezentują cztery różne poziomy wiarygodności[4] (**Certum Level I**, **Certum Level II**, **Certum Level III** i **Certum Level IV**) przypisane certyfikatom klucza publicznego. Obszary zastosowań certyfikatów wystawianych zgodnie z tymi politykami mogą się pokrywać, inna jest jednak odpowiedzialność (w tym prawna) urzędu certyfikacji oraz użytkowników certyfikatu.

Struktura i merytoryczna zawartość Kodeksu Postępowania Certyfikacyjnego są zgodne z zaleceniem RFC 2527 *Certificate Policy and Certification Practice Statement Framework*.

---

[1] Określenia wprowadzane po raz pierwszy będą wyróżniane w tekście tlustym drukiem; ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym na końcu dokumentu.

[2] Osoba będąca podmiotem wydanego certyfikatu, która jest inicjatorem wiadomości oraz podpisuje ją używając do tego celu klucza prywatnego, który odpowiada kluczowi publicznemu zawartemu w certyfikacie.

[3] Odbiorca, który działa na podstawie zaufania do certyfikatu i podpisu cyfrowego.

[4] Pojęcie *wiarygodności* odnosi się do tego, jak bardzo strona ufająca może być pewna jednoznaczności powiązania pomiędzy kluczem publicznym a osobą (fizyczną lub prawną) lub urządzeniem (ogólnie podmiotem certyfikatu), których dane umieszczone zostały w certyfikacie. Dodatkowo wiarygodność odzwierciedla: (a) wiarę strony ufającej, że podmiot certyfikatu kontroluje użycie klucza prywatnego, powiązanego z kluczem publicznym umieszczonym w certyfikacie, oraz (b) poziom zabezpieczeń towarzyszących procedurze dostarczenia podmiotowi klucza prywatnego w przypadkach, gdy jest on generowany także przez system tworzący certyfikaty klucza publicznego.

Kodeks Postępowania Certyfikacyjnego pisany jest przy założeniu, że czytelnik jest ogólnie zaznajomiony z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz Infrastruktury Klucza Publicznego (**PKI**). Jeśli nie, zaleca się aby przyszły użytkownik i subskrybent usług Unizeto CERTUM - CCP przeszedł odpowiednie szkolenie z zakresu technik klucza publicznego oraz zasad elektronicznej wymiany dokumentów. Tematy szkoleń, ich terminy oraz materiały dostępne są w repozytorium Unizeto CERTUM - CCP pod adresem:

http://www.certum.pl/repozytorium

Z Kodeksem Postępowania Certyfikacyjnego związanych jest wiele dodatkowych dokumentów, które wykorzystywane są w systemie Unizeto CERTUM - CCP i regulują jego funkcjonowanie (patrz Tab.1.1). Dokumenty te mają różny status. Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane.

Tab.1.1 Ważniejsze dokumenty towarzyszące Kodeksowi Postępowania Certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Polityka Certyfikacji Unizeto CERTUM - Centrum Certyfikacji Powszechne	Jawny	http://www.certum.pl/repozytorium
2.	Dokumentacja systemu Certum CA	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
3.	Procedura generowania kluczy urzędu certyfikacji Unizeto CERTUM	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
4.	Procedura archiwizacji i niszczenia kluczy urzędu certyfikacji Unizeto CERTUM	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
5.	Księga nośników	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
6.	Dokumentacja techniczna baz danych	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
7.	Księga Urzędu Rejestracji	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
8.	Księga serwerów	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
9.	Księga Wymiany Oprogramowania Serwerów	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
10.	Księga Tworzenia Kopii Zapasowych i Awaryjnego Odtwarzania Serwerów	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy
11.	Księga Uruchamiania i Zatrzymywania Serwerów	Niejawny	lokalnie - tylko uprawnione osoby oraz audytorzy

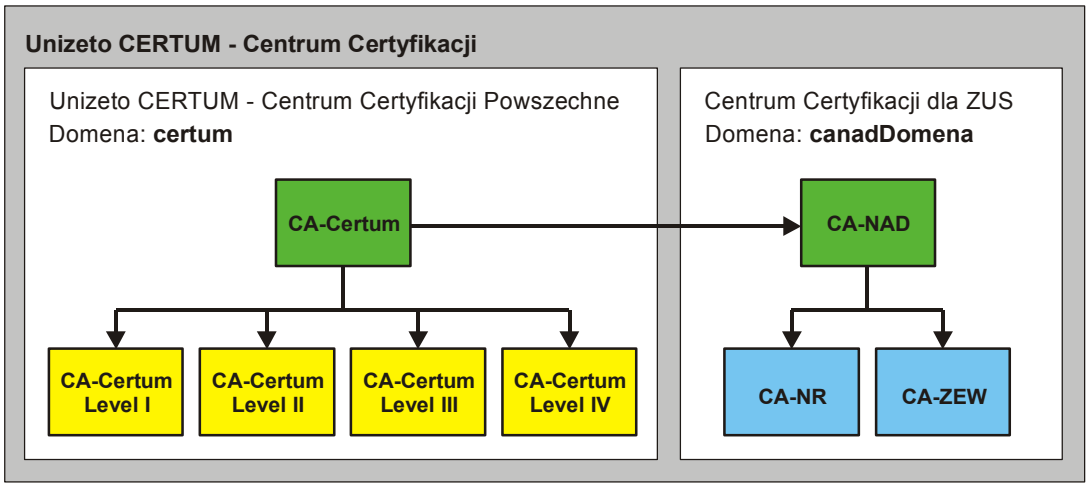
Dodatkowe informacje oraz pomoc serwisową można uzyskać za pośrednictwem poczty elektronicznej: info@certum.pl.

1.1. Wprowadzenie

Kodeks Postępowania Certyfikacyjnego opisuje i stanowi podstawę działania Unizeto CERTUM - CCP oraz wszystkich związanych z nim **urzędów certyfikacji**, **urzędów rejestracji**, **subskrybentów**, jak również **stron ufających**. Określa także zasady świadczenia usług

certyfikacyjnych, począwszy od rejestracji subskrybentów, certyfikacji kluczy publicznych, aktualizacji kluczy i certyfikatów, a na unieważnianiu certyfikatów kończąc.

Unizeto CERTUM - Centrum Certyfikacji Powszechne wchodzi w skład jednostki usługowej Unizeto CERTUM - Centrum Certyfikacji, tworząc w jego obrębie oddzielną domenę certyfikacji **certum** (patrz rys.1.1), z wydzielonym głównym urzędem certyfikacji CA-Certum. Główny urząd certyfikacji **CA-Certum** jest niezależny od domeny **canadDomena** i sam sobie wystawia tzw. autocertyfikat[5].



Rys.1.1 Hierarchiczne powiązania organów wydających certyfikaty, działających w ramach Unizeto CERTUM - Centrum Certyfikacji

Hierarchicznie poniżej głównego urzędu certyfikacji **CA-Certum** znajdują się podległe mu cztery inne urzędy certyfikacji. Są to: **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** oraz **CA-Certum Level IV**, wydające certyfikaty o różnym poziomie wiarygodności (patrz rozdz.1.4).

Niniejszy Kodeks Postępowania Certyfikacyjnego odnosi się do wszystkich urzędów certyfikacji i rejestracji, subskrybentów oraz stron ufających, korzystających z usług lub wymieniających jakiekolwiek wiadomości w obrębie domeny **certum**.

Polityka Certyfikacji Unizeto CERTUM - Centrum Certyfikacji Powszechne dopuszcza mechanizm wzajemnego poświadczenia certyfikatów (certyfikacja wzajemna) **CA-Certum** i dowolnego spośród urzędów certyfikacji, należącego do domeny **canadDomena**. Możliwe jest także funkcjonalne podporządkowanie **CA-NAD** głównemu urzędowi wydającemu certyfikaty **CA-Certum**.

W chwili obecnej Unizeto CERTUM nie jest związany z innymi organami wydającymi certyfikaty żadnymi umowami o certyfikacji wzajemnej. Sytuacja ta może jednak ulec zmianie, o czym użytkownicy zostaną poinformowani w stosownej wersji Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego.

Certyfikaty wydawane przez Unizeto CERTUM - CCP zawierają identyfikatory polityk certyfikacji[6], które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie

[5] **Autocertyfikatem** jest dowolny certyfikat klucza publicznego przeznaczony do weryfikacji podpisu złożonego na certyfikacie, w którym podpis da się zweryfikować przy pomocy klucza publicznego zwartego w polu **subjectKeyInfo**, zawartości pól **issuer** oraz **subject** są takie same, zaś pole **cA** rozszerzenia **BasicConstraints** ustawione jest na **true** (patrz rozdz.7.1.1.2).

[6] Identyfikatory polityk certyfikacji Unizeto Certum – Centrum Certyfikacji Powszechne budowane są w oparciu o identyfikator obiektu Unizeto Sp. z o.o. w Szczecinie zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów (KRIO, http://www.krio.pl). Identyfikator ten ma wartość:

```
id-unizeto  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616) organization(1) 113527)
```

certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Deklarowane przeznaczenie certyfikatu można określić na podstawie wpisów umieszczanych w strukturze **PolicyInformation** rozszerzenia **certificatesPolicies** (patrz rozdz.7.1.1.2) każdego certyfikatu wydawanego przez Unizeto CERTUM - CCP.

Unizeto CERTUM - CCP działa zgodnie z prawem obowiązującym na terytorium Rzeczypospolitej Polskiej oraz zasadami wynikającymi z przestrzegania, konstrukcji, interpretacji oraz ważności Polityki Certyfikacji.

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Kodeksu Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci**: KPC Unizeto CERTUM - CCP** lub **Kodeks Postępowania Certyfikacyjnego Unizeto CERTUM - CCP**. Jakiekolwiek cytowanie odnoszące się do tego dokumentu powinno używać jednej z dwóch dozwolonych form.

Dokument **KPC Unizeto CERTUM - CCP** jest dostępny:

- w postaci elektronicznej z repozytorium o adresie http://www.certum.pl/repozytorium lub na żądanie wysłane na adres email: info@certum.pl,
- w postaci kopii papierowej na żądanie wysłane na adres Unizeto CERTUM - Centrum Certyfikacji (patrz rozdz.1.5).

Z dokumentem polityki certyfikacji związany jest następujący zarejestrowany identyfikator obiektu (OID):

```
id-ccert-kpc-v3  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
           organization(1) id-unizeto(113527) id-ccert(2) id-certum(2)
           id-certPolicy-doc(0) id-ccert-kpc(1) 3}
```

w którym ostatnia wartość liczbowa odnosi się do aktualnej wersji tego dokumentu.

Identyfikator Kodeksu Postępowania Certyfikacyjnego nie jest umieszczany w treści wystawianych certyfikatów. W certyfikatach wydawanych przez Unizeto CERTUM - CCP umieszczane są jedynie identyfikatory polityk certyfikacji, które należą do zbioru polityk certyfikacji wspieranych przez niniejszy Kodeks Postępowania Certyfikacyjnego. Zbiór ten zawiera identyfikatory polityk certyfikacji, opisanych w rozdz.7.1.1.2.

1.3. Strony Kodeksu Postępowania Certyfikacyjnego

Kodeks Postępowania Certyfikacyjnego reguluje wszystkie najważniejsze relacje zachodzące pomiędzy podmiotami wchodzącymi w skład Unizeto CERTUM - CCP, jego zespołami doradczymi (w tym audytorami) oraz klientami (użytkownikami dostarczanych usług). W szczególności regulacje te dotyczą:

- urzędów certyfikacji **CA-Certum**, **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** oraz każdego innego urzędu, który zostanie utworzony zgodnie z zasadami określonymi w niniejszym Kodeksie Postępowania Certyfikacyjnego,
- Głównego Urzędu Rejestracji (GUR),
- lokalnych urzędów rejestracji (LUR),
- repozytorium,
- serwera weryfikacji statusu certyfikatów w trybie on-line (OCSP),

subskrybentów,

stron ufających.

Unizeto CERTUM - CCP jest otwartą jednostką usługową świadczącą usługi certyfikacyjne wszystkim osobom fizycznym i prawnym, akceptującym postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego. Postanowienia te (m.in. procedury generowania kluczy i wystawiania certyfikatów, zastosowane mechanizmy zabezpieczeń systemu informatycznego) mają na celu przekonanie użytkowników usług Unizeto CERTUM - CCP, że deklarowane poziomy wiarygodności wydawanych certyfikatów są praktycznym odzwierciedleniem postępowania urzędów certyfikacji.

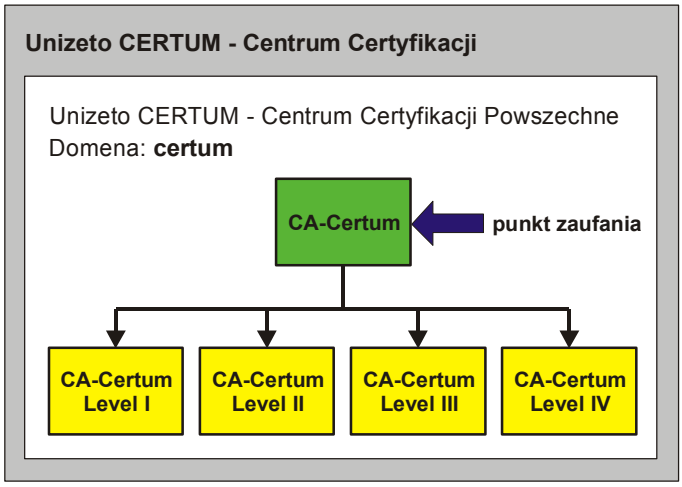
Postanowienia Kodeksu Postępowania Certyfikacyjnego są zgodne z Polityką Certyfikacji i zaleceniami Zespołu ds. Rozwoju Usług PKI (patrz rozdz.8).

1.3.1. Urzędy certyfikacji

W skład Unizeto CERTUM - CCP wchodzą urzędy certyfikacji, tworzące wspólną domenę urzędów certyfikacji o nazwie **certum** (rys.1.2).

Urząd certyfikacji **CA-Certum** jest głównym urzędem certyfikacji domeny certum, któremu podlegają wszystkie urzędy certyfikacji z tej domeny.

Aktualnie **CA-Certum** podlegają następujące cztery urzędy certyfikacji: **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV**.



Rys.1.2 Struktura domeny certyfikacji **certum** oraz jej punkt zaufania (**CA-Certum**)

1.3.1.1. Główny urząd certyfikacji CA-Certum

Główny urząd rejestracji CA-Certum może rejestrować i wydawać certyfikaty tylko urzędom certyfikacji oraz urzędom wystawiającym elektroniczne poświadczenia niezaprzeczalności, należącym do domeny **certum**. Każdy podległy urząd certyfikacji przed rozpoczęciem działalności musi złożyć wniosek w Głównym Urzędzie Rejestracji (GUR) o zarejestrowanie i wydanie certyfikatu klucza publicznego (patrz procedura opisana w dokumencie *„Procedura rejestrowania i certyfikowania nowych urzędów certyfikacji”*[7]).

Urząd **CA-Certum** działa w oparciu o wystawiony przez siebie autocertyfikat. W autocertyfikacie nie umieszcza się rozszerzenia **certificatePolicies** (patrz rozdz.7.1.1), co należy

[7] Procedurze tej nie podlegają cztery podstawowe urzędy certyfikacji **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** oraz inne podmioty świadczące usługi niezaprzeczalności.

interpretować jako brak ograniczeń na zbiór **ścieżek certyfikacji**[8], do których można dołączać certyfikat **CA-Certum**.

*Urząd certyfikacji **CA-Certum** musi być **punktem zaufania**[8] wszystkich subskrybentów Unizeto CERTUM - CCP. Oznacza to, że każda budowana przez nich ścieżka certyfikacji musi rozpoczynać się od certyfikatu urzędu **CA-Certum**.*

Urząd certyfikacji CA-Certum świadczy usługi certyfikacyjne dla:

samego siebie (wystawia i aktualizuje autocertyfikaty),

urzędów **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** oraz innym urzędom certyfikacji zarejestrowanym w domenie certyfikacji **certum**,

podmiotów świadczących usługi weryfikacji statusu certyfikatu w trybie on-line (OCSP) oraz innym podmiotom świadczącym usługi niezaprzeczalności (m.in. usługi znacznika czasu).

*W certyfikatach wystawianych urzędom **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** oraz certyfikatach innych urzędów i podmiotów, którym certyfikaty wystawia urząd **CA-Certum** nie umieszcza się rozszerzenia **certificatePolicies**.*

1.3.1.2. Zależne urzędy certyfikacji

Zależne urzędy certyfikacji **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** wystawiają certyfikaty subskrybentom zgodnie z politykami, których identyfikatory podane są w Tab.1.2.

Tab.1.2 Nazwy urzędów certyfikacji i nazwy polityk certyfikacji wg których działają

Nazwa urzędu certyfikacji	Nazwa polityki certyfikacji
CA-Certum Level I	Certum Level I
CA-Certum Level II	Certum Level II
CA-Certum Level III	Certum Level III
CA-Certum Level IV	Certum Level IV

Urzędy te nie umieszczają żadnych innych identyfikatorów polityk certyfikacji w wystawianych certyfikatach.

*Certyfikaty innym urzędom certyfikacji mogą wystawiać tylko dwa urzędy: **CA-Certum Level I** (testowe urzędy certyfikacji) oraz **CA-Certum Level IV** (komercyjne urzędy certyfikacji).*

Z zależnymi urzędami certyfikacji ściśle współpracują Główny Urząd Rejestracji oraz lokalne urzędy rejestracji. Urzędy rejestracji reprezentują zależne urzędy certyfikacji w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez urzędy certyfikacji uprawnień w zakresie identyfikacji i rejestracji subskrybentów. Sposób funkcjonowania oraz zakres obowiązków urzędów rejestracji zależy od wiarygodności certyfikatu wydawanego subskrybentom.

[8] Patrz **Słownik pojęć**

Zależne urzędy certyfikacji przystosowane są do wydawania certyfikatów dla:

użytkowników certyfikatów, którzy dzięki certyfikatom chcą zapewnić bezpieczeństwo swojej poczcie elektronicznej, zapewnić bezpieczeństwo i wiarygodność serwerom usługowym (np. witrynom sklepowym, bibliotekom informacji i oprogramowania, itp.),

podmiotów świadczących usługi niezaprzeczalności, np. urzędom znaczników czasu (TSA) lub urzędom notarialnym,

dostawców usług związanych z telefonią komórkową,

urządzeń sieciowych realizujących połączenia szyfrowane VPN,

operatorów urzędów rejestracji (GUR i Lokalnych Urzędów Rejestracji),

pracowników Unizeto CERTUM - CCP,

urządzeń (fizycznych i logicznych) będących pod opieką osób fizycznych lub prawnych; usługi certyfikacyjne dla urządzeń umożliwiają budowanie na bazie certyfikatu klucza publicznego innych usług, np. usług weryfikacji statusu certyfikatu (OCSP),

innym urzędom certyfikacji (dotyczy to tylko urzędów **CA-Certum Level I** i **CA-Certum Level IV**).

1.3.2. Urzędy rejestracji

Urzędy rejestracji przyjmują, weryfikują i następnie aprobują lub odrzucają - otrzymywane od wnioskodawców - wnioski o zarejestrowanie i wydanie certyfikatu oraz aktualizację, odnowienie lub unieważnienie certyfikatu. Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dostarczonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Urzędy rejestracji mogą występować także z wnioskami do właściwego urzędu certyfikacji o wyrejestrowanie subskrybenta i tym samym o pozbawienie go certyfikatu.

Stopień dokładności identyfikacji tożsamości subskrybenta wynika z potrzeb samego subskrybenta, a także narzucany jest przez klasę certyfikatu o wydanie którego stara się subskrybent (patrz rozdz.3). W przypadku najprostszej identyfikacji subskrybenta urząd rejestracji sprawdza tylko prawidłowość podanego adresu email. Najdokładniejsza identyfikacja wymaga z kolei osobistego stawienia się subskrybenta w urzędzie rejestracji i przedłożenia dokumentów potwierdzających jego tożsamość. Wymogi te oznaczają, że tego typu identyfikacja może być realizowana albo całkowicie automatycznie, albo ręcznie przez operatora urzędu rejestracji.

Urzędy rejestracji działają z upoważnienia odpowiedniego urzędu certyfikacji należącego do domeny **certum** w zakresie identyfikacji tożsamości aktualnego lub przyszłego subskrybenta oraz weryfikacji dowodu posiadania klucza prywatnego. Szczegółowy zakres obowiązków urzędów rejestracji i jego operatorów określony jest przez umowę zawartą z Unizeto CERTUM - CCP, niniejszy Kodeks oraz procedury funkcjonowania urzędu rejestracji, które są integralną częścią tej umowy.

Dowolna instytucja (osoba prawna) może pełnić rolę lokalnego urzędu rejestracji oraz uzyskać akredytację przy Unizeto CERTUM - CCP, o ile wystąpi z właściwym wnioskiem do Głównego Urzędu Rejestracji oraz spełni inne warunki określone w Kodeksie Postępowania Certyfikacyjnego (patrz rozdz.2).

Lista aktualnie akredytowanych przez GUR lokalnych urzędów rejestracji dostępna jest w repozytorium Unizeto CERTUM - CCP dostępnym pod adresem:

http://www.certum.pl/repozytorium.

Wyróżnia się dwa typy urzędów rejestracji, którym urzędy certyfikacji działające w ramach Unizeto CERTUM - CCP mogą przekazać część swoich uprawnień:

lokalne urzędy rejestracji, nazywane dalej lokalnymi urzędami rejestracji (LUR),

Główny Urząd Rejestracji (GUR).

Podstawowa różnica pomiędzy wymienionymi dwoma typami urzędów rejestracji polega na tym, że lokalne urzędy rejestracji nie mogą – w przeciwieństwie do Głównego Urzędu Rejestracji – akredytować innych lokalnych urzędów rejestracji oraz rejestrować nowych urzędów certyfikacji. Dodatkowo lokalne urzędy rejestracji nie posiadają uprawnień do poświadczania wszystkich żądań subskrybentów. Uprawnienia te mogą być ograniczone tylko do niektórych spośród wszystkich dostępnych typów[9] certyfikatów. Stąd:

LUR rejestrują subskrybentów końcowych (osoby fizyczne i prawne), którzy ubiegają się o certyfikaty o wiarygodności do poziomu Certum Level III włącznie,

GUR rejestruje lokalne urzędy rejestracji (LUR), nowe urzędy certyfikacji oraz subskrybentów końcowych (osoby fizyczne i prawne, urządzenia); nie nakłada się żadnych ograniczeń (poza tymi, które wynikają z roli pełnionych w infrastrukturze klucza publicznego Unizeto CERTUM - CCP) na typy certyfikatów wydawanych subskrybentom zarejestrowanym w GUR; dodatkowo GUR zatwierdza także nazwy wyróżnione aktualnych i tworzonych w przyszłości urzędów rejestracji.

Główny Urząd Rejestracji zlokalizowany jest w siedzibie Unizeto CERTUM - CCP. Adresy kontaktowe z Głównym Urzędem Rejestracji podane są w rozdz.1.5

1.3.3. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych baz danych zawierających certyfikaty:

wszystkich urzędów certyfikacji, należących do domeny certum lub z nią związanych (np. certyfikaty nowych urzędów certyfikacji zarejestrowane w Głównym Urzędzie Rejestracji),

operatorów urzędów rejestracji (lokalnych i GUR),

subskrybentów końcowych (osób prawnych i fizycznych, w tym także pracowników Unizeto CERTUM - CCP oraz urządzeń pod ich opieką, niezbędnych do funkcjonowania usług PKI), którzy wyrazili na to zgodę.

Dodatkowo w repozytorium znajdują się informacje ściśle związane z funkcjonowaniem certyfikatów, m.in.:

listy certyfikatów unieważnionych (CRL),

aktualna i poprzednia wersja Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego, oraz

inne na bieżąco modyfikowane informacje.

W domenie ***certum*** *funkcjonuje tylko jedno repozytorium, wspólne dla wszystkich urzędów certyfikacji działających w jej obrębie lub z nią powiązanych.*

[9] Typy certyfikatów omówione są w rozdz.1.4

Zawartość repozytorium dostępna jest za pośrednictwem protokołu HTTP pod adresem:

http://www.certum.pl/repozytorium

1.3.4. Użytkownicy końcowi

Pośród użytkowników końcowych wyróżnia się subskrybentów oraz strony ufające. Subskrybent jest tym podmiotem, którego identyfikator umieszczany jest w polu **podmiot** (*ang. subject*) certyfikatu i który sam dalej nie wydaje certyfikatów innym. Strona ufająca jest z kolei podmiotem, który posługuje się certyfikatem innego podmiotu w celu zweryfikowania jego podpisu cyfrowego lub zapewnienia poufności przesyłanej informacji.

1.3.4.1. Subskrybenci

Subskrybentami Unizeto CERTUM - Centrum Certyfikacji są dowolne osoby fizyczne i prawne oraz urządzenia będące pod ich kontrolą, o ile tylko spełniają warunki definicji subskrybenta podanej w rozdz.1.3.4. W szczególności subskrybentami są operatorzy urzędów rejestracji, pracownicy Unizeto CERTUM - CCP oraz te elementy sprzętowe, np. firewalle, routery, serwery uwierzytelniające, które niezbędne są do ochrony infrastruktury Unizeto CERTUM - CCP.

Organizacje pragnące uzyskać certyfikaty dla swoich pracowników wydane przez Unizeto CERTUM - CCP powinny uczynić to poprzez swoich przedstawicieli. Z kolei subskrybent indywidualny występuje o certyfikat w swoim imieniu.

Unizeto CERTUM - CCP oferuje certyfikaty o różnych poziomach wiarygodności oraz różnych typów. Subskrybent powinien zdecydować, jaki typ certyfikatu jest najodpowiedniejszy do jego potrzeb (patrz rozdz.1.4).

1.3.4.2. Strony ufające

Stroną ufającą, korzystającą z usług Unizeto CERTUM - CCP jest dowolny podmiot, którego podjęcie decyzji jest w jakikolwiek sposób uzależnione od ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym przez jeden z urzędów certyfikacji podległych **CA-Certum**.

Strona ufająca jest odpowiedzialna za to czy lub jak zweryfikować aktualny status certyfikatu subskrybenta. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu cyfrowego, zidentyfikowania źródła lub twórcy wiadomości lub utworzenia sekretnego kanału komunikacyjnego z właścicielem certyfikatu. Informacje zawarte w certyfikacie (m.in. identyfikatory i kwalifikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.4. Zakres stosowalności certyfikatów

Zakres stosowalności certyfikatów określa obszary tzw. dozwolonego użycia certyfikatu. Obszar ten definiowany jest przez dwa elementy. Pierwszy element określa naturę (charakter) zastosowania certyfikatu (np. podpis cyfrowy lub poufność, identyfikator polityki certyfikacji), drugi z kolei jest listą lub opisem zatwierdzonych lub zabronionych aplikacji.

Certyfikaty wystawiane przez Unizeto CERTUM - CCP mogą być stosowane do przetwarzania i ochrony informacji (także uwierzytelniania) o różnym poziomie wrażliwości.

Poziom wrażliwości informacji oraz jej podatność na **naruszenie**[10] powinny zostać oszacowane przez subskrybenta. W Polityce Certyfikacji oraz niniejszym Kodeksie Postępowania Certyfikacyjnego wprowadza się cztery poziomy wrażliwości: poziom I, określany także jako testowy, poziom II lub podstawowy, poziom III lub średni oraz poziom IV lub wysoki. Wymienione poziomy powiązane są relacją jeden do jeden z poziomami wiarygodności certyfikatów, które wymienione są w Tab.1.3[11].

Tab.1.3 Poziomy wrażliwości informacji a nazwy polityk certyfikacji

Poziom wrażliwości informacji	Nazwa polityki certyfikacji	Zakres stosowalności
Poziom I/testowy	Certum Level I	Najniższy poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty tego poziomu powinny być stosowane jedynie do testowania kompatybilności usług Unizeto CERTUM - CCP z usługami świadczonymi przez innych dostawców usług PKI oraz funkcjonalności certyfikatów we współpracy z testowanymi aplikacjami. Można używać ich także do innych celów, o ile nie jest istotne zapewnienie wiarygodności wysyłanej/otrzymywanej informacji.
Poziom II/podstawowy	Certum Level II	Ten poziom zapewnia podstawową ochronę informacji w środowisku, w którym występuje małe ryzyko naruszenia[12] danych, nie pociągające za sobą dalszych istotnych następstw. Dotyczyć to może dostępu do prywatnych informacji w przypadkach, gdy prawdopodobieństwo nieuprawnionego dostępu nie jest zbyt wysokie. Certyfikatów tego poziomu można używać do uwierzytelniania, kontroli integralności informacji która została podpisana oraz zapewnienia poufności informacji, w tym w szczególności poczty elektronicznej.
Poziom III/średni	Certum Level III	Poziom dotyczy ochrony informacji w środowisku, w którym występuje ryzyko naruszenia danych informacji oraz skutki tego naruszenia są średnie. Certyfikatów tego poziomu można używać w transakcjach finansowych lub transakcjach o znacznym poziomie ryzyka wystąpienia oszustw, a także w tych przypadkach dostępu do prywatnych informacji, w których prawdopodobieństwo nieuprawnionego dostępu jest istotne.
Poziom IV/wysoki	Certum Level IV	Ten poziom jest odpowiedni w przypadkach, gdy zagrożenie naruszenia danych jest wysokie lub bardzo istotne mogą być następstwa awarii usług zabezpieczających. Certyfikatów tego poziomu można używać w transakcjach o nieograniczonej wartości finansowej (chyba że inaczej zaznaczono w certyfikacie) lub o wysokim poziomie ryzyka wystąpienia oszustw.

Za określenie poziomu wiarygodności certyfikatu, przydatnego do określonego zastosowania, odpowiada strona ufająca. Strona ta na podstawie różnych istotnych czynników ryzyka powinna określić, które z wystawianych przez Unizeto CERTUM - CCP certyfikatów spełniają sformułowane wymagania. Wymagania strony ufającej powinny być znane (np. opublikowane w postaci **polityki podpisu** lub szerzej polityki zabezpieczeń systemu

[10] Patrz **Słownik pojęć**

[11] Patrz także *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

[12] Patrz **Słownik pojęć**

informatycznego) subskrybentom, którzy na ich podstawie mogą wystąpić do Unizeto CERTUM - Centrum Certyfikacji Powszechne o wydanie odpowiedniego certyfikatu, spełniającego te wymagania.

Wymagania określone przez stronę ufającą muszą być skonfrontowane przez subskrybenta z zakresami stosowalności (Tab.1.3) oraz typami certyfikatów (Tab.1.4), wydawanymi przez Unizeto CERTUM - CCP.

1.4.1. Typy certyfikatów i zalecane obszary ich zastosowań

Unizeto CERTUM - Centrum Certyfikacji Powszechne wydaje dziewięć podstawowych typów certyfikatów, określających jednocześnie obszary ich zastosowania. Są to:

1) **certyfikaty urzędów certyfikacji** – ich użycia nie ogranicza się do z góry określonych obszarów, ale obszar taki może wynikać z przyjętych w certyfikacie zastosowań klucza prywatnego (patrz pole **keyUsage**, rozdz.7) lub pełnionych ról (subskrybenta, urzędu certyfikacji lub innego urzędu świadczącego usługi w ramach PKI); do tego typu certyfikatów należą także certyfikaty operacyjne[13] urzędów certyfikacji,
2) **certyfikaty do poświadczania autentyczności serwera** – stosowane przez globalne oraz ekstranetowe serwisy usługowe pracujące w osłonie protokołu SSL/TLS/WTLS,
3) **certyfikaty do uwierzytelniania subskrybentów** (osób prawnych i fizycznych, urządzeń) - stosowane m.in. w protokołach SSL/TLS/WTLS,
4) **certyfikaty osobiste** – umożliwiają szyfrowanie i podpisywanie poczty elektronicznej oraz znajdują zastosowanie w zabezpieczaniu dokumentów elektronicznych (poczta elektroniczna wg standardu S/MIME lub PGP),
5) **certyfikaty do poświadczania statusu certyfikatów** – wydawane są na serwery działające zgodnie z protokołem OCSP i wystawiające tokeny aktualnego statusu weryfikowanego certyfikatu,
6) **certyfikaty urzędów znacznika czasu** – wydawane są na serwery, które w odpowiedzi na żądanie wystawiają tokeny znacznika czasu wiążące dowolne dane (dokumenty, wiadomości, podpisy cyfrowe, itd.) ze znacznikami czasu umożliwiającymi (w szczególnych przypadkach jednoznaczne) uporządkowanie danych,
7) **certyfikaty urzędów notarialnych** – wykorzystywane są przez serwer DVCS (*ang. Data Validation and Certification Server*), potwierdzający i certyfikujący dane,
8) **certyfikaty do szyfrowania** – umożliwiają zabezpieczanie plików, katalogów oraz systemów plików.
9) **certyfikaty do zabezpieczania kodu** – certyfikaty przeznaczone dla programistów przeznaczone do zabezpieczania oprogramowania przed sfałszowaniem.

Szczegółowe nazwy komercyjne oraz zastosowania wymienionych powyżej typów certyfikatów zależą od ich poziomu wiarygodności i nazwy polityki certyfikacji, w ramach której są wydawane (patrz Tab.1.4).

---

[13] **Certyfikaty operacyjne** są to certyfikaty uniwersalne wydane urzędom certyfikacji. Certyfikaty te umożliwiają funkcjonowanie urzędów certyfikacji i obejmują certyfikaty służące do: weryfikacji podpisu pod wiadomościami, szyfrowania danych, weryfikacji podpisów na wystawianych certyfikatach i listach CRL, wymiany kluczy, uzgadniania kluczy, świadczenia usług niezaprzeczalności (patrz rozszerzenie certyfikatu **keyUsage**)

Tab.1.4 Typy certyfikatów oraz ich zastosowania

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
Certum Level I	Private Email	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Private WEB Server	Zabezpieczanie transmisji danych dla serwerów WWW
	Private Microsoft Authenticode	Zabezpieczanie oprogramowania przed sfałszowaniem, dystrybucja oprogramowania w sieci globalnej zgodnie z Microsoft Authenticode™
	Private Microsoft VBS	Zabezpieczanie skryptów VB w Office 2000 przed sfałszowaniem, zabezpieczanie oprogramowania zgodnie z technologią Microsoft Visual Basic for Applications
	Private Netscape Object Signing	Podpisywanie wtyczek (ang. plugin), modułów i apletów Java zgodnie z technologią Netscape®
	Private Java Code Signing	Zabezpieczanie oprogramowania zgodnie z technologią Sun Microsystems® Java
	Private Software Publisher	Zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633, UNIX® Code Signing (uniwersalny certyfikat programisty)
	Private VPN	Zabezpieczanie transmisji danych – protokół Ipsec. Dla urządzeń sieciowych, serwerów i kanałów VPN
	Private WAP Server	Zabezpieczanie bezprzewodowej transmisji danych - WTLS
	Private Time Stamp	Oznaczanie czasem obiektów i transakcji elektronicznych
	Private Netscape Form Signing	Podpisywanie formularzy zgodnie z technologią Netscape®
	Private Strong Internet	Uwierzytelnianie klienta do zasobów sieci, serwera usługowego, stacji roboczej, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	Private CA	Testowy urząd certyfikacyjny
	Private EDI	Dedykowane rozwiązania i systemy, np. Netscape EXpert, Softshare EDI, itp.
	Private SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.
	Private Apple Code Signing	Zabezpieczanie oprogramowania zgodnie z technologią Apple® na platformie Macintosh
	Private Biometric Data	Zabezpieczanie finansowych transmisji danych, głównie między bankiem i jego klientem, z informacjami biometrycznymi podmiotu
	Private Castanet Signing	Szyfrowanie i podpisywanie kanałów dystrybucji oprogramowania zgodnie z Marimba® Castanet
	Private IPsec Client	Klient szyfrowanej transmisji danych wg protokołu IPsec
	Private Data Encryption	Szyfrowanie danych dla osób indywidualnych, kryptograficzne systemy plików

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
	Private OCSP	Wystawianie poświadczeń statusu certyfikatów dla serwisów OCSP
	Private Notary Service	Serwisy usług notarialnych, certyfikat dla urzędu NA (ang. Notary Authority)
Certum Level II	Certum Silver	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Commercial VPN	Zabezpieczanie transmisji danych – protokół IPsec Dla urządzeń sieciowych, serwerów i kanałów VPN
	Commercial Strong Internet	Uwierzytelnianie klienta do zasobów sieci, serwera usługowego, stacji roboczej, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	Commercial SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.
	Commercial IPsec Client	Klient szyfrowanej transmisji danych wg protokołu Ipsec
	Commercial Data Encryption	Szyfrowanie danych, zabezpieczenia kryptograficznych systemów plików
Certum Level III	Certum Gold	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Enterprise Web Server	Zabezpieczanie transmisji danych dla serwerów WWW
	Microsoft Authenticode	Zabezpieczanie oprogramowania przed sfałszowaniem, dystrybucja oprogramowania w sieci globalnej zgodnie z Microsoft Authenticode™
	Microsoft VBS	Zabezpieczanie skryptów VB w Office 2000 przed sfałszowaniem, zabezpieczanie oprogramowania zgodnie z technologią Microsoft Visual Basic for Applications
	Netscape Object Signing	Podpisywanie wtyczek (ang. plugin), modułów i apletów Java zgodnie z technologią Netscape®
	Java Code Signing	Zabezpieczanie oprogramowania zgodnie z technologią Sun Microsystems® Java
	Software Publisher	Zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633, UNIX® Code Signing (uniwersalny certyfikat programisty)
	Enterprise VPN	Zabezpieczanie transmisji danych – protokół IPsec Dla urządzeń sieciowych, serwerów i kanałów VPN
	Enterprise WAP Server	Zabezpieczanie bezprzewodowej transmisji danych - WTLS
	Netscape Form Signing	Podpisywanie formularzy zgodnie z technologią Netscape®
	Enterprise EDI	Dedykowane rozwiązania i systemy, np. Netscape EXpert, Softshare EDI, itp.
	Enterprise SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.
	Apple Code Signing	Zabezpieczanie oprogramowania zgodnie z technologią Apple® na platformie Macintosh

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
	Castanet Signing	Szyfrowanie i podpisywanie kanałów dystrybucji oprogramowania zgodnie z Marimba® Castanet
Certum Level IV	Certum Platinum	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, wymagane jest stosowanie mikroprocesorowej karty kryptograficznej
	Trusted WEB Server	Zabezpieczanie transmisji danych dla serwerów WWW, w szczególności serwisów bankowości elektronicznej i płatności on-line
	Trusted VPN	Zabezpieczanie transmisji danych – protokół IPsec Dla urządzeń sieciowych, serwerów i kanałów VPN, w szczególności routerów bankowości elektronicznej
	Trusted Time Stamp	Oznaczanie czasem obiektów oraz transakcji elektronicznych o dużej wartości
	Trusted Strong Internet	Uwierzytelnianie klienta do zasobów sieci, serwera usługowego, stacji roboczej, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	Trusted CA	Świadczenie usług certyfikacyjnych
	Trusted EDI	Dedykowane rozwiązania i systemy finansowe EDI, np. Netscape EXpert, Softshare EDI, itp.
	Trusted Biometric Data	Klient usług bankowości elektronicznej
	Trusted IPsec Client	Klient szyfrowanej transmisji danych wg protokołu IPsec, stosowany do transmisji danych o szczególnym znaczeniu
	Trusted Data Encryption	Szyfrowanie danych dla osób indywidualnych, kryptograficzne systemy plików, stosowany w systemach handlu elektronicznego i bankowości
	Trusted OCSP	Serwis OCSP poświadczający statusy certyfikatów
	Trusted Notary Service	Urząd notariatu elektronicznego

1.4.2. Rekomendowane aplikacje

Certyfikaty wystawione zgodnie z jedną z czterech polityk certyfikacji mogą być stosowane z aplikacjami, które spełniają przynajmniej następujące wymagania:

prawidłowo zarządzają kluczami publicznymi i prywatnymi, ich przesyłaniem oraz używaniem,

certyfikaty oraz związane z nimi klucze prywatne używane są zgodnie z ich deklarowanym przeznaczeniem, potwierdzonym przez Unizeto CERTUM - CCP,

posiadają wbudowane mechanizmy weryfikacji statusu certyfikatu, budowania ścieżek certyfikacji oraz sprawdzania jego ważności (ważności podpisu, okresu ważności, itp.),

przekazuje użytkownikowi prawidłowe informacje o stanie aplikacji, certyfikatów, itp.

Lista aplikacji zalecanych i aprobowanych przez Unizeto CERTUM - CCP przedstawiona jest w Tab.1.5. Najbardziej aktualna wersja tej listy opublikowana jest w repozytorium pod adresem:

http://www.certum.pl/repozytorium.

Aplikacje umieszczane są na liście aplikacji rekomendowanych na podstawie pisemnych oświadczeń producentów i/lub testów wykonanych przez Unizeto CERTUM - CCP. Unizeto CERTUM wymaga, aby każdy subskrybent sam generował klucze kryptograficzne, podlegające procesowi certyfikacji przy pomocy rekomendowanych narzędzi (patrz tab.1.5). Unizeto CERTUM pozostawia wybór algorytmu i przeznaczenie kluczy kryptograficznych subskrybentowi. Istnieje też możliwość wygenerowania kluczy przez urząd na karcie kryptograficznej lub w sprzętowym module kryptograficznym i przekazania subskrybentowi wraz z ww. kluczami. W takim wypadku Unizeto CERTUM używa kart mikroprocesorowych lub modułów spełniających wymogi minimum FIPS PUB 140-1.

Tab.1.5 Lista rekomendowanych aplikacji

Nazwa aplikacji/wersja/producent	Komercyjna nazwa typu certyfikatu	Krótki opis aplikacji
Wszystkie aplikacje wspierające certyfikaty klucza publicznego X.509	Wszystkie certyfikaty wydawane przez CA Certum	Różne zastosowania

1.4.3. Nierekomendowane aplikacje

Zabrania się używania certyfikatów Unizeto CERTUM - CCP niezgodnie z ich deklarowanym przeznaczeniem oraz w aplikacjach, które nie spełniają minimalnych wymagań określonych w rozdz.1.4.2.

Lista aplikacji, których nie rekomenduje się lub zabronione jest w nich używanie certyfikatów (może to być uzależnione od poziomu wiarygodności certyfikatu) wydanych przez Unizeto CERTUM - CCP przedstawiona jest w Tab.1.6. Najbardziej aktualna wersja tej listy opublikowana jest w repozytorium pod adresem:

http://www.certum.pl/repozytorium.

Lista aplikacji nierekomendowanych zawiera aplikacje, które nie przeszły testów (wykonanych przez Unizeto CERTUM - CCP) na zgodność z oświadczeniami producentów.

Tab.1.6 Lista aplikacji nierekomendowanych

Nazwa aplikacji/wersja/producent	Komercyjna nazwa typu certyfikatu	Krótki opis aplikacji
–	Wszystkie certyfikaty wydawane przez CA Certum	Nie ma przeciwwskazań odnośnie istniejących aplikacji

1.5. Kontakt

Dane kontaktowe dotyczą podmiotu który zarządza niniejszym Kodeksem Postępowania Certyfikacyjnego, adresu pod który można przesyłać uwagi dotyczące Kodeksu i Polityki Certyfikacji oraz adresu Zespołu, który weryfikuje zgodność Kodeksu z Polityką Certyfikacji.

1.5.1. Dane jednostki administrującej Kodeksem

Niniejszym Kodeksem Postępowania Certyfikacyjnego, Polityką Certyfikacji oraz innymi dokumentami dotyczącymi usług PKI, świadczonymi przez Unizeto CERTUM - CCP bezpośrednio administruje **Zespół ds. Rozwoju Usług PKI**, działający w ramach struktury Unizeto Sp. z o.o. Wszelkie zapytania i uwagi związane z zawartością wymienionych

dokumentów powinny być kierowane do Zespołu ds. Rozwoju Usług PKI pod następującym adresem:

Unizeto Sp. z o.o.

70-486 Szczecin, ul. Królowej Korony Polskiej 21

Unizeto CERTUM – Zespół ds. Rozwoju Usług PKI

E-mail: info@certum.pl

1.5.2. Adres kontaktowy

Osoby które są zainteresowane uzyskaniem kopii Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji lub innych informacji związanych z tymi dokumentami lub chcące zadać pytanie związane wymienionych dokumentów lub tych informacji, powinny skorzystać z następujących adresów:

UNIZETO Spółka z o.o.

70-486 Szczecin, ul. Królowej Korony Polskiej 21

Unizeto CERTUM – Zespół ds. Rozwoju Usług PKI

E-mail: info@certum.pl

Numer telefonu: (+48 91) 48 01 297

Numer faksu: (+48 91) 48 01 220

1.5.3. Jednostka oceniająca zgodność Kodeksu z Polityką Certyfikacji

Oceny zgodności Kodeksu Postępowania Certyfikacyjnego z Polityką Certyfikacji dokonuje Zespół ds. Rozwoju Usług PKI. Zespół ten zatwierdza także kodeksy postępowania certyfikacyjnego urzędów certyfikacji, które zostały zarejestrowane przy Unizeto CERTUM - Centrum Certyfikacji i którym zostały wydane certyfikaty, pozwalające na świadczenie usług certyfikacyjnych. Sposób kontaktowania się z Zespołem podany jest w rozdz.1.5.2.

1.6. Skróty i oznaczenia

CRL lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów

DN nazwa wyróżniona (*ang. Distinguished Name*)

GUR Główny Urząd Rejestracji

KPC Kodeks Postępowania Certyfikacyjnego Unizeto CERTUM - Centrum Certyfikacji Powszechne

KRIO Krajowy Rejestr Identyfikatorów Obiektów

LUR Lokalny Urząd Rejestracji

OCSP protokół serwera weryfikacji statusu certyfikatów, pracującego w trybie *on-line* (*ang. On-line Certificate Status Protocol*)

PC Polityka Certyfikacji

PKI Infrastruktura Klucza Publicznego

PSE osobiste bezpieczne środowisko (*ang. personal security environment*) jest to lokalny bezpieczny nośnik klucza prywatnego podmiotu, klucza publicznego (zwykle w postaci autocertyfikatu); w zależności od polityki bezpieczeństwa nośnik ten może mieć postać kryptograficznie zabezpieczonego pliku (np. zgodnie z PKCS#12) lub odpornego na penetrację sprzętowego tokena (np. identyfikacyjna karta elektroniczna).

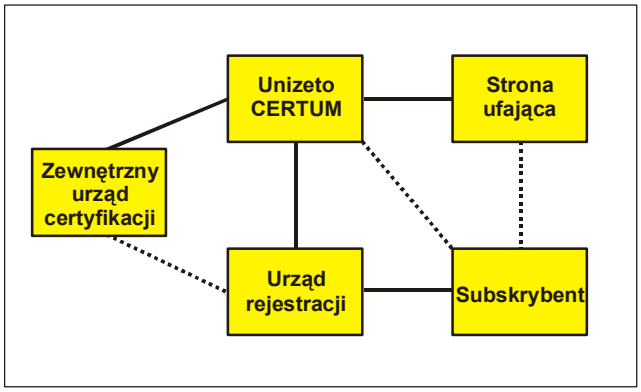
RSA kryptograficzny algorytm asymetryczny (nazwa pochodzi od pierwszych liter jego twórców Rivesta, Shamira i Adlemana), w których jedno przekształcenie prywatne wystarcza zarówno do podpisywania jak i deszyfrowania wiadomości, zaś jedno przekształcenie publiczne wystarcza zarówno do weryfikacji jak i szyfrowania wiadomości

TTP zaufana trzecia strona, instytucja lub jej przedstawiciel mający zaufanie innych podmiotów w zakresie działań związanych z zabezpieczeniem, działań związanych z uwierzytelnianiem, mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego (wg PN 2000)

UC urząd certyfikacji (*ang. certification authority*)

2.Postanowienia ogólne

W rozdziale tym przedstawione są zobowiązania/gwarancje i odpowiedzialność Unizeto CERTUM - CCP, urzędów rejestracji, subskrybentów oraz użytkowników certyfikatów (stron ufających). Zobowiązania te oraz odpowiedzialność regulowane są przez wzajemne umowy zawierane pomiędzy wymienionymi stronami (patrz rys.2.1).



Rys.2.1 Umowy zawierane pomiędzy stronami

Umowy Unizeto CERTUM ze stronami ufającymi oraz subskrybentami opisują typy usług, które udostępniane są przez Unizeto CERTUM - CCP, wzajemne zobowiązania oraz odpowiedzialności, w tym finansowe Unizeto Sp. z o.o.

Umowa pomiędzy Unizeto CERTUM a lokalnymi urzędami zawierana jest w przypadkach, gdy urząd ten pełni rolę agenta dowolnego urzędu certyfikacji działającego w domenie **certum**. Na podstawie takiej umowy urząd rejestracji może zawierać w imieniu Unizeto CERTUM umowy z subskrybentami. Tam gdzie jest to uzasadnione urzędy rejestracji mogą zawierać także oddzielne umowy z subskrybentami na świadczone przez siebie usługi i określające ich wzajemne relacje.

Jeśli Unizeto CERTUM - Centrum Certyfikacji zarejestruje i wyda certyfikat dowolnemu zewnętrznemu podmiotowi, pełniącemu rolę podległego urzędu certyfikacji, to musi to nastąpić na podstawie umowy zawartej pomiędzy tymi dwiema stronami.

Kodeks Postępowania Certyfikacyjnego i Polityka Certyfikacji są integralną częścią umów zawieranych pomiędzy Unizeto CERTUM - CCP a subskrybentami, stronami ufającymi, zewnętrznymi urzędami rejestracji lub innymi podmiotami, które są dostawcami usług infrastruktury klucza publicznego typu znacznik czasu, weryfikacja statusu certyfikatów, itd.

Umowy zawierane pomiędzy zewnętrznymi urzędami certyfikacji a lokalnymi urzędami certyfikacji powinny być zawierane na podstawie tych samych zasad, które regulują relacje urzędów rejestracji z Unizeto CERTUM.

Niniejszy Kodeks Postępowania Certyfikacyjnego nie nakłada żadnych ograniczeń na treść umowy pomiędzy strona ufającą i subskrybentem o ile nie narusza ona zobowiązań i odpowiedzialności tych stron określonych w tym Kodeksie.

2.1. Zobowiązania

2.1.1. Zobowiązania Unizeto CERTUM - CCP

Unizeto CERTUM - CCP gwarantuje, że:

swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie tworzące system, który spełnia wymagania określone w CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*,

jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,

świadczone usługi są zgodne z powszechnie akceptowanymi normami:

- usługi certyfikacyjne z zaleceniami normy X.509, PKCS#10, PKCS#7 i PKCS#12,
- usługi znacznika czasu z zaleceniem RFC 3161,
- weryfikacja statusu certyfikatu (OCSP) z zaleceniem RFC 2560,
- usługi notarialne (DVCS) z zaleceniem RFC 3029,

przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym Kodeksie Postępowania Certyfikacyjnego, w szczególności w zakresie:

- weryfikacji informacji identyfikującej tożsamość subskrybenta, któremu wydawany jest certyfikat w ramach domeny **certum**; przyjęte procedury weryfikujące tożsamość subskrybenta zależą od informacji zawartej w certyfikacie i zmieniają się w zależności od wysokości opłaty za certyfikat, natury i tożsamości subskrybenta certyfikatu oraz obszaru zastosowań, w obrębie którego wydany certyfikat jest wiarygodny (szczegóły patrz rozdz.3 i 4),
- certyfikatów, które są zawsze unieważniane, jeśli tylko istnieje przekonanie lub pewność, iż zawartość certyfikatu zdezaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.),
- powiadamiania subskrybenta oraz innych podmiotów zainteresowanych zajściem tego zdarzenia w przypadku, gdy subskrybent jest podmiotem wydawanego, unieważnianego lub zawieszanego certyfikatu,
- publikowania list certyfikatów unieważnionych i zawieszonych informacji w miejscach określonych w niniejszym Kodeksie,
- generowania i stosowania kluczy prywatnych wyłącznie do celów, które określono w niniejszym Kodeksem Postępowania Certyfikacyjnego oraz takiej ich ochrony, która nie pozwala na ich użycie niezgodne z tymi celami,
- personalizacji i wydawania elektronicznych kart identyfikacyjnych, na których zapisywane są certyfikaty oraz para kluczy (w przypadku wygenerowania jej przez urząd certyfikacji),
- okresowego i terminowego publikowania informacji, które niezbędne są do prawidłowego pozyskiwania, posługiwania się oraz unieważniania certyfikatów.

wystawiane certyfikaty nie zawierają żadnych sfałszowanych danych, które byłyby znane lub które pochodziłyby od osób zatwierdzających wnioski o wystawienie certyfikatów lub wystawiających te certyfikaty,

wystawiane certyfikaty nie zawierają żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty,

nazwy wyróżnione (DN) subskrybentów umieszczane w certyfikatach są unikalne w domenie **certum**,

zapewnienia ochrony danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* oraz *Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*,

w przypadku generowania pary kluczy z upoważnienia subskrybenta klucze te zostaną w sposób poufny przekazane subskrybentowi, a następnie zniszczone, zaraz po przekazaniu kluczy subskrybentowi, z nośnika pierwotnego, chyba że subskrybent zażąda zarchiwizowania tych kluczy.

Ponadto Unizeto CERTUM - CCP zobowiązuje się do:

rejestrowania i wydawania certyfikatów tylko tym urzędom certyfikacji, których polityka certyfikacji oraz kodeks postępowania certyfikacyjnego uzyskają aprobatę Zespołu ds. Rozwoju Usług PKI; Zespół musi każdorazowo wskazać przynajmniej jedną z czterech polityk certyfikacji (określonych w Tab.1.2 i rozdz.7.1.1.2), na którą odwzorowuje się polityka rejestrowanego urzędu certyfikacji,

zawierania umów z subskrybentami, stronami ufającymi, urzędami certyfikacji oraz urzędami rejestracji; usługi certyfikacyjne świadczone są tylko na podstawie zawartych umów i zawsze na wniosek subskrybenta, strony ufającej, urzędu certyfikacji lub urzędu rejestracji,

prowadzenia listy zarejestrowanych urzędów rejestracji, z którymi posiada umowy o współpracy oraz rekomendowania wykorzystywanego przez te urzędy sprzętu i oprogramowania,

prowadzenia listy rekomendowanego oprogramowania i sprzętu do generowania par kluczy asymetrycznych,

prowadzenia listy rekomendowanych i nierekomendowanych aplikacji, spełniających lub niespełniających wymagania określone w rozdz. 1.4.2,

przeprowadzania zgodnych z harmonogramem audytów w urzędach certyfikacji i rejestracji należących do lub powiązanych z domeną **certum**,

zlecania planowanych audytów domeny **certum** niezależnym audytorom, udostępniania im wszystkich niezbędnych informacji i dokumentów oraz stosowania się do ich zaleceń pokontrolnych.

2.1.2. Zobowiązania urzędów rejestracji

Każdy urząd rejestracji, który funkcjonuje w domenie **certum** lub z którym Unizeto CERTUM - CCP jest związane umowami gwarantuje, że:

swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie, które posiadają rekomendację Unizeto CERTUM - CCP,

jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,

dołożył wszelkich starań, aby dane identyfikacyjne każdego z subskrybentów, umieszczane w bazach danych Unizeto CERTUM - CCP, były zgodne z prawdą oraz, że informacja ta była aktualna w momencie ich potwierdzania,

potwierdzane informacje subskrybenta, przesyłane następnie do urzędu certyfikacji w celu ich umieszczenia w certyfikacie są dokładne,

nie przyczynił się w sposób zamierzony lub niezamierzony do powstania błędów lub niedokładności w informacji umieszczanej w certyfikacie,

świadczone usługi są zgodne z powszechnie akceptowanymi normami (de jure i de facto): X.509, PKCS#10, PKCS#7 i PKCS#12,

świadczone usługi realizowane są na podstawie procedur, które są dostosowane do zaleceń niniejszego Kodeksu Postępowania Certyfikacyjnego; w szczególności dotyczy to:

- procedur weryfikacji tożsamości subskrybentów,
- przeprowadzania **dowodu posiadania klucza prywatnego**[14], powiązanego z przedstawionym do certyfikacji kluczem publicznym,
- procedur przyjmowania od klientów, rozpatrywania i potwierdzania lub odrzucania wniosków o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie,
- procedur występowania do urzędu certyfikacji, na podstawie wcześniej zaakceptowanego wniosku subskrybenta, o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie; procedury te określają także okoliczności, w których urząd certyfikacji może samodzielnie występować z takimi wnioskami,
- procedur rejestrowania innych urzędów rejestracji, z którymi Unizeto CERTUM - CCP zawarło umowy (procedury te nie dotyczą Głównego Urzędu Rejestracji),
- archiwizowania wniosków i informacji otrzymywanych od subskrybentów, wydanych decyzji oraz informacji przekazanych do urzędów certyfikacji,
- procedur generowania kluczy subskrybentom, o ile dopuszcza to umowa zawarta z urzędem certyfikacji oraz subskrybentem; klucze te nie mogą być archiwizowane przez urząd rejestracji, chyba że inaczej stanowi umowa zawarta z subskrybentem,
- procedur personalizacji i wydawania elektronicznych kart identyfikacyjnych, na których zapisywane są certyfikaty oraz para kluczy (w przypadku wygenerowania jej przez urząd rejestracji),

poddaje się planowym audytom wewnętrznym i zewnętrznym, w szczególności tym, które są prowadzone przez jednostkę usługową Unizeto CERTUM - CCP lub przez nią zlecane.

[14] Patrz **Słownik pojęć**

Urząd rejestracji zobowiązuje się ponadto do:

podporządkowania się zaleceniom Unizeto CERTUM - CCP, zwłaszcza tym, które są wynikiem przeprowadzonego audytu,

zapewnienia ochrony danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* oraz *Rozporządzeniem Ministra Spraw Wewnętrznych i Administracji z dnia 3 czerwca 1998 r. w sprawie określenia podstawowych warunków technicznych i organizacyjnych, jakim powinny odpowiadać urządzenia i systemy informatyczne służące do przetwarzania danych osobowych*,

ochrony kluczy prywatnych operatorów zgodnie z wymogami bezpieczeństwa nakreślonymi szczegółowo w Kodeksie Postępowania Certyfikacyjnego;

nieużywania kluczy prywatnych operatorów do innych celów niż te, które określono w niniejszym Kodeksie Postępowania Certyfikacyjnego, chyba że uzyska na to specjalną zgodę Unizeto CERTUM - CCP,

pozyskania **aktywnych**[15] certyfikatów kluczy publicznych i list CRL urzędów certyfikacji Unizeto CERTUM - CCP z wiarygodnych źródeł oraz ich rzetelnej weryfikacji.

2.1.3. Zobowiązania subskrybenta końcowego

Kodeks Postępowania Certyfikacyjnego wraz z Polityką Certyfikacji jest integralną częścią każdej umowy zawartej pomiędzy subskrybentem końcowym a Unizeto CERTUM - CCP. Poprzez złożenie w urzędzie rejestracji wniosku o rejestrację oraz ręczne podpisanie potwierdzenia rejestracji lub zaakceptowanie certyfikatu (patrz rozdz.4.3) subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w wymienionych dokumentach.

W zależności od wzajemnych relacji pomiędzy Unizeto CERTUM - CCP a subskrybentem, a także od poziomu wiarygodności certyfikatu o który występuje subskrybent, zobowiązania mogą być wyrażone w postaci formalnej umowy lub mogą mieć charakter nieformalnego porozumienia pomiędzy subskrybentem a Unizeto CERTUM - CCP.

Niezależnie od charakteru umowy subskrybent końcowy zobowiązany jest do:

wyrażenia zgody na warunki określone w formalnej lub nieformalnej umowie pomiędzy subskrybentem a Unizeto CERTUM - CCP; zgoda ta powinna mieć charakter podpisu odręcznego w przypadku umowy formalnej oraz oświadczenia woli (umowa nieformalna) w chwili akceptacji wydanego certyfikatu; treść oświadczenia woli subskrybenta opublikowana jest w repozytorium,

zaakceptowania każdego wydanego mu certyfikatu; gwarancje oraz odpowiedzialność Unizeto CERTUM - CCP związane z danym certyfikatem rozpoczynają się z chwilą jego akceptacji,

podjęcia takich środków ostrożności, które pozwolą mu na prawidłowe wygenerowanie (samodzielnie, urzędowi rejestracji lub urzędowi certyfikacji) i bezpieczne przechowywanie klucza prywatnego z certyfikowanej pary kluczy, tzn. jego ochronę przed zgubieniem, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem; w przypadku samodzielnego generowania kluczy subskrybent powinien używać oprogramowania i sprzętu, które posiadają rekomendację Unizeto CERTUM - CCP,

[15] Patrz **Słownik pojęć**

podawania prawdziwych danych we wnioskach przekazywanych do urzędu rejestracji lub urzędu certyfikacji i umieszczanych następnie w bazach danych jednostki usługowej Unizeto CERTUM - CCP oraz w wydawanych przez tę jednostkę certyfikatach klucza publicznego; jednocześnie subskrybent musi być świadom odpowiedzialności za szkody (bezpośrednie lub pośrednie) będące konsekwencją sfałszowania danych,

uznania, że każdy podpis cyfrowy złożony przy pomocy należącego do niego klucza prywatnego, związanego z zaakceptowanym certyfikatem klucza publicznego jest jego podpisem i że certyfikat ten nie był przeterminowany (nie minął jego okres ważności) ani też unieważniony lub zawieszony w momencie składania podpisu,

subskrybent zobowiązany jest do przynajmniej ogólnego zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz infrastruktury klucza publicznego (PKI).

Subskrybent końcowy zobowiązuje się ponadto:

stosować się do zasad niniejszego Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji,

do generowania kluczy kryptograficznych, zarządzania hasłami, kluczami publicznymi i prywatnymi oraz wymiany informacji z urzędami certyfikacji oraz urzędami rejestracji używać tylko i wyłącznie oprogramowania rekomendowanego przez Unizeto CERTUM - CCP; dostęp do tego oprogramowania oraz do nośników lub urządzeń na których przechowywane są klucze lub hasła powinien być należycie kontrolowany,

traktować utratę lub ujawnienie (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,

nie udostępniać osobom nieuprawnionym swoich kluczy prywatnych,

nigdy jako subskrybent końcowy nie używać klucza prywatnego, powiązanego z certyfikatem wystawionym przez Unizeto CERTUM - CCP do podpisywania jakichkolwiek certyfikatów lub list CRL,

dostarczać do urzędu rejestracji lub urzędu certyfikacji dowód posiadania klucza prywatnego lub w inny sposób dowieść fakt jego posiadania,

nie przekazywać używanych przez siebie haseł osobom nieuprawnionym,

okazywać w urzędzie rejestracji wymagane dokumenty, potwierdzające informacje zawarte w składanym wniosku oraz tożsamość wnioskodawcy lub podmiotu działającego z jego upoważnienia,

w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie zawiadamiać o tym fakcie wystawcę certyfikatu lub dowolny urząd rejestracji, zarejestrowany przy Unizeto CERTUM - CCP,

wykorzystywać certyfikaty klucza publicznego oraz odpowiadające im klucze prywatne tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w Kodeksie Postępowania Certyfikacyjnego (patrz rozdz.1.4)

pozyskiwać certyfikaty kluczy publicznych urzędów certyfikacji i urzędów rejestracji oraz innych jednostek usługowych Unizeto CERTUM - CCP.

2.1.4. Zobowiązania stron ufających

Kodeks Postępowania Certyfikacyjnego wraz z Polityką Certyfikacji jest integralną częścią każdej umowy zawartej przez stronę ufającą z Unizeto CERTUM - CCP lub subskrybentem. W szczególności przedmiotem takiej umowy:

z Unizeto CERTUM - CCP może być świadczenie przez tę jednostkę usług repozytoryjnych, usług znacznika czasu oraz usług weryfikacji statusu certyfikatów (OCSP),

z subskrybentem jest określenie warunków które musi spełnić podpis cyfrowy, aby być uznanym przez stronę ufającą za ważny.

W zależności od wzajemnych relacji pomiędzy stroną ufającą a Unizeto CERTUM - CCP lub subskrybentem, a także od poziomów certyfikatów które są przez stronę ufającą akceptowane, zobowiązania strony ufającej mogą być wyrażone w postaci formalnej umowy lub mogą mieć charakter nieformalnego porozumienia z Unizeto CERTUM - CCP lub subskrybentem.

Niezależnie od charakteru umowy strona ufająca zobowiązana jest do:

wyrażenia zgody na warunki określone w formalnej lub nieformalnej umowie pomiędzy stroną ufającą a Unizeto CERTUM - CCP lub subskrybentem; zgoda ta powinna mieć charakter podpisu odręcznego w przypadku umowy formalnej oraz oświadczenia woli (umowa nieformalna) w chwili pierwszego odwołania się do dowolnej usługi świadczonej przez Unizeto CERTUM - CCP lub pierwszego zaakceptowania podpisu subskrybenta; gwarancje oraz odpowiedzialność Unizeto CERTUM - CCP lub subskrybenta obowiązują od momentu zawarcia umowy,

rzetelnej weryfikacji[16] każdego podpisu cyfrowego umieszczonego na dokumencie lub certyfikacie, który do niej dotrze; w celu zweryfikowania podpisu strona ufająca powinna:

- określić **ścieżkę certyfikacji**[17], zawierającą wszystkie certyfikaty innych urzędów certyfikacji, które umożliwią wiarygodne przeprowadzenie weryfikacji podpisu na certyfikacie wystawcy podpisu,
- upewnić się, że wybrana ścieżka certyfikacji jest najlepsza z punktu widzenia realizacji podpisu; istnieje bowiem możliwość, że od danego certyfikatu (przy pomocy którego zrealizowano podpis) do urzędu certyfikacji, któremu ufa weryfikujący podpis wiedzie więcej niż jedna ścieżka,
- sprawdzić, czy certyfikaty tworzące ścieżkę certyfikacji nie występują w repozytorium Unizeto CERTUM - CCP na liście certyfikatów unieważnionych lub zawieszonych; unieważnienie lub zawieszenie któregokolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony,
- sprawdzić, czy wszystkie certyfikaty należące do ścieżki certyfikacji należą do urzędów certyfikacji oraz czy nadano im prawo podpisywania innych certyfikatów,

---

[16] Weryfikacja podpisu cyfrowego ma na celu określenie, czy (1) podpis cyfrowy został zrealizowany przy pomocy klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez Unizeto CERTUM - Centrum Certyfikacji Powszechne certyfikacie subskrybenta, oraz (2) podpisana wiadomość (dokument) nie został zmodyfikowany już po złożeniu na nim podpisu.

[17] Patrz **Słownik pojęć**

- opcjonalnie określić datę oraz czas złożenia podpisu na wiadomości lub dokumencie. Jest to możliwe tylko w przypadku, gdy wiadomość lub dokument zostały przed podpisaniem opatrzone znacznikiem czasu, uzyskanym z organu znacznika czasu (TSA) lub też znacznik czasu został związany z podpisem cyfrowym już po jego umieszczeniu na dokumencie; tego typu weryfikacja umożliwi świadczenie usług typu niezaprzeczalność i rozstrzyganie ewentualnych sporów,
- korzystając ze zdefiniowanej ścieżki certyfikacji zweryfikować prawdziwość certyfikatu wystawcy podpisu na wiadomości lub dokumencie, a następnie oryginalność samego podpisu na wiadomości lub dokumencie.

właściwie i poprawnie realizować operacje kryptograficzne przy użyciu oprogramowania i sprzętu, których poziom bezpieczeństwa jest zgodny z poziomem wrażliwości przetwarzanej informacji i poziomu wiarygodności stosowanych certyfikatów,

uznania podpisu cyfrowego za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis cyfrowy jest ważny lub uzyskany wynik weryfikacji jest negatywny,

zaufania tylko tym certyfikatom klucza publicznego:

- które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca, np. w formie polityki podpisu (patrz rozdz. 1.4),
- których status został zweryfikowany w oparciu o aktualne listy certyfikatów unieważnionych lub przy wykorzystaniu usługi OCSP, udostępnianej przez Unizeto CERTUM - CCP,

określenia warunków, jakie musi spełniać certyfikat klucza publicznego oraz podpis cyfrowy, aby został uznany przez tą stronę za ważny; warunki te mogą zostać sformułowane np. w postaci odpowiedniej polityki podpisu i opublikowane.

Każdy dokument z wykrytą wadą w podpisie cyfrowym lub wynikłymi z niego wątpliwościami powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność. Każdy, kto taki dokument zaakceptuje ponosi wszelkie związane z tym konsekwencje, niezależnie od szeroko akceptowanych cech podpisu cyfrowego, określających go jako skuteczny mechanizm weryfikacji tożsamości subskrybenta składającego podpis. Strona ufająca zobowiązana jest do zapoznania się z KPC lub PC (**gwarancje** i **odpowiedzialność**).

2.1.5. Zobowiązania repozytorium Unizeto CERTUM - CCP

Repozytorium jest zarządzane i kontrolowane przez Unizeto CERTUM - CCP. Wynikające z tego faktu zobowiązania Unizeto CERTUM - CCP dotyczą:

zagwarantowania, że wszystkie certyfikaty opublikowane w repozytorium należą do subskrybentów wskazanych w certyfikacie oraz że subskrybenci ci zaakceptowali certyfikat zgodnie z wymaganiami przedstawionymi w rozdz.2.1.3 i rozdz.4.3,

terminowego publikowania i archiwizowania certyfikatów urzędów certyfikacji, urzędów rejestracji, należących do domeny **certum** oraz certyfikatów subskrybentów, po uprzednim uzyskaniu na to ich zgody,

publikowania i archiwizowania Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego, wzorów umów zawieranych z subskrybentami i stronami ufającymi oraz list rekomendowanych i nierekomendowanych aplikacji,

udostępniania informacji o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL), serwer OCSP lub zapytania kierowane za pośrednictwem protokołu HTTP,

zagwarantowania urzędom certyfikacji, urzędom rejestracji, subskrybentom oraz stronom ufającym gwarancji, ciągłego dostępu do informacji zgromadzonej w repozytorium,

szybkiego i zgodnego z okresami określonymi w Polityce Certyfikacji publikowania list CRL oraz innej informacji,

gwarancji bezpiecznego i kontrolowanego dostępu do informacji zawartych w repozytorium.

Wszyscy użytkownicy, poza stronami ufającymi, mają nieograniczony dostęp do wszystkich informacji zgromadzonych w repozytorium. Ograniczenia w dostępie stron ufających do repozytorium dotyczą zwykle certyfikatów subskrybentów i regulowane są przez umowy zawierane pomiędzy stroną ufającą a Unizeto CERTUM - CCP.

2.2. Odpowiedzialność

Odpowiedzialność stron świadczących usługi lub korzystających z tych usług w domenie zarządzanej przez Unizeto CERTUM - CCP regulowana jest przez odpowiednie umowy dwustronne. W tym kontekście odpowiedzialność kontraktowa stron wynika z naruszenia warunków określonych w umowie lub w innych dokumentach związanych z tą umową. W szczególnych przypadkach, jeśli tak stanowi umowa, część odpowiedzialności jednej ze stron może być przekazywana lub przejmowana przez inne strony. Taka sytuacja może wystąpić np. w przypadku oddelegowania przez urząd certyfikacji swoich uprawnień w zakresie weryfikacji tożsamości subskrybenta dowolnemu urzędowi rejestracji. Urząd rejestracji może przejąć wtedy odpowiedzialność za swoje zobowiązania, określone w rozdz.2.1.2.

Unizeto CERTUM - CCP ponosi odpowiedzialność za skutki działań urzędów certyfikacji ***CA-Certum****,* ***CA-Certum Level I****,* ***CA-Certum Level II****,* ***CA-Certum Level III*** *i* ***CA-Certum Level IV****, Głównego Urzędu Rejestracji, repozytorium oraz jeśli tak określono w zawartych umowach, innych urzędów certyfikacji i urzędów rejestracji.*

Przedstawione poniżej zapisy o odpowiedzialności stron nie eliminują lub nie zastępują odpowiedzialności określonej w umowach zawieranych pomiędzy stronami lub wynikającej z odrębnych przepisów prawa.

2.2.1. Odpowiedzialność urzędów certyfikacji Unizeto CERTUM - CCP

Urzędy certyfikacji Unizeto CERTUM - CCP ponoszą odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą:

powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,

są wynikiem udowodnionych błędów popełnionych przez Unizeto CERTUM - CCP, zawłaszcza w zakresie niezgodności procesu weryfikacji tożsamości z deklarowanymi procedurami, niewłaściwej ochrony klucza prywatnego urzędów certyfikacji lub braku dostępu do świadczonych usług, np. do list certyfikatów unieważnionych,

powstały wskutek naruszenia innych gwarancji Unizeto CERTUM - CCP, określonych w rozdz.2.1.1, 2.1.5 i 2.1.2.

Jeśli Unizeto CERTUM - CCP zawarło umowy z innymi urzędami rejestracji na świadczenie usług w zakresie weryfikacji tożsamości subskrybentów, to odpowiedzialność z tytułu gwarancji określonych w rozdz.2.1.2 ponosi tylko w przypadku, gdy w umowie zawartej pomiędzy Unizeto CERTUM - CCP a subskrybentem ten ostatni oświadczy, że:

dane i dokumenty, które podał w urzędzie są prawdziwe i dokładne,

zgadza się, że akceptacja certyfikatu jest równoznaczna z faktem, iż certyfikat nie zawiera żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty.

Unizeto CERTUM - CCP nie zawiera umów z subskrybentami, którzy w opisanym przypadku nie złożą tego typu oświadczenia.

Jednocześnie Unizeto CERTUM - CCP nie ponosi żadnej odpowiedzialności za działania stron trzecich, subskrybentów oraz innych stron nie związanych z Unizeto CERTUM - CCP. W szczególności Unizeto CERTUM - CCP nie odpowiada:

za szkody powstałe na skutek sytuacji anormalnych: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,

za szkody powstałe na skutek instalacji i użytkowania aplikacji oraz sprzętu stosowanego do generowania kluczy kryptograficznych, zarządzania nimi, szyfrowania oraz realizacji podpisu cyfrowego, które znajduje się na liście aplikacji nieakredytowanych (zastrzeżenie to dotyczy stron ufających) lub nie znajduje się na liście aplikacji akredytowanych (zastrzeżenie to dotyczy subskrybentów),

za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonego oraz używanie niezgodnie z deklarowanym przeznaczeniem wynikającym z typu certyfikatu, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego,

w przypadku braku potwierdzonej przez subskrybenta akceptacji certyfikatu; całą odpowiedzialność ponosi subskrybent i powinna ona być ona określona w umowie pomiędzy subskrybentem a stroną ufającą,

w przypadku podania przez subskrybenta fałszywych danych i umieszczenie ich na jego wniosek zarówno w bazach Unizeto CERTUM - CCP, jak też w wydanym mu certyfikacie klucza publicznego.

2.2.2. Odpowiedzialność urzędów rejestracji

Odpowiedzialność Głównego Urzędu Rejestracji przenosi się automatycznie na Unizeto CERTUM - CCP i wynika łącznie z gwarancji określonych w rozdz.2.1.1, 2.1.2 i 2.1.5. Warunki

tej odpowiedzialności regulują umowy zawarte przez Unizeto CERTUM - CCP z subskrybentami oraz stronami ufającymi.

Odpowiedzialność innych urzędów rejestracji, działających w imieniu i z upoważnienia Unizeto CERTUM – CCP, określana jest na podstawie umów zawartych pomiędzy tymi stronami. Umowy te szczegółowo określają sankcje, które wynikają z naruszenia gwarancji określonych w rozdz.2.1.2 oraz regulują odpowiedzialność obu stron w stosunku do subskrybentów i stron ufających.

W szczególności, jeśli urząd rejestracji nie dopilnuje złożenia przez subskrybenta oświadczenia o treści określonej w rozdz.2.2.1, to cała odpowiedzialność z tytułu naruszenia gwarancji z rozdz.2.1.2 spada na urząd rejestracji, chyba że inaczej stanowi umowa zawarta pomiędzy urzędem rejestracji a subskrybentem.

2.2.3. Odpowiedzialność subskrybentów

Odpowiedzialność subskrybenta wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.3. Warunki tej odpowiedzialności reguluje umowa zawarta z Unizeto CERTUM - CCP lub urzędem rejestracji.

2.2.4. Odpowiedzialność stron ufających

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.4. Warunki tej odpowiedzialności reguluje umowa zawarta z subskrybentem oraz z Unizeto CERTUM - CCP.

Umowy z subskrybentami lub Unizeto CERTUM - CCP wymagają aby strony ufające potwierdziły, że dysponują wystarczającą ilością informacji umożliwiającą im podjęcie świadomej decyzji o akceptacji lub odrzuceniu podpisu cyfrowego w momencie jego przedłożenia.

W umowie strony ufające powinny określić wysokość kwot transakcji, które będą przez nie akceptowane jedynie na podstawie informacji zawartych w certyfikacie oraz złożyć oświadczenie, że znane są im prawne konsekwencje wynikające z zaniedbania swoich obowiązków, określonych w (patrz rozdz.2.1.4).

2.2.5. Odpowiedzialność repozytorium

Pełną odpowiedzialność za funkcjonowanie repozytorium i wynikłe z tego skutki ponosi Unizeto CERTUM - CCP (patrz rozdz. 2.2.1).

2.3. Odpowiedzialność finansowa

Odpowiedzialność jednostki usługowej Unizeto CERTUM - CCP oraz stron powiązanych poprzez usługi świadczone przez tę jednostkę wynika z rutynowych czynności wykonywanych przez te podmioty lub z czynności stron trzecich.

Odpowiedzialność każdego z podmiotów jest określona w umowach dwustronnych lub wynika ze złożonych oświadczeń woli.

Jeśli szkody wystąpią z winy Unizeto CERTUM - CCP lub z winy stron z którymi Unizeto CERTUM - CCP ma tak zawarte umowy, że wina ta przenosi się na Unizeto CERTUM, to wówczas łączne gwarancje finansowe Unizeto CERTUM - CCP w stosunku do wszystkich stron (w tym także stron ufających) nie mogą przekroczyć jednorazowo sumy kwot dla wyszczególnionych w Tab.2.1 poziomów wiarygodności certyfikatów, osób lub urządzeń.

Tab.2.1 Maksymalne gwarancje finansowe

Nazwa polityki certyfikacji	Typ podmiotu			
	Osoba fizyczna	Osoba prawna	Urządzenie	
			Osoby fizycznej	Osoby prawnej
Certum Level I	0 zł	0 zł	0 zł	0 zł
Certum Level II	400 zł	400 zł	400 zł	400 zł
Certum Level III	20 000 zł	20 000 zł	20 000 zł	20 000 zł
Certum Level IV	100 000 zł	100 000 zł	100 000 zł	100 000 zł

Wspólna łączna odpowiedzialność Unizeto CERTUM - CCP w stosunku do określonej osoby lub wszystkich osób (prawnych i fizycznych) lub urządzenia pod opieką tej osoby lub osób, wynikająca z posługiwania się przy realizacji podpisu cyfrowego lub innych operacji kryptograficznych certyfikatem określonego poziomu wiarygodności, ograniczona jest do kwot nie przekraczających podanych w Tab.2.1.

2.4. Interpretacja i egzekwowanie aktów prawnych

2.4.1. Obowiązujące akty prawne

Funkcjonowanie Unizeto CERTUM - CCP oparte jest na ogólnych zasadach zawartych w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz jest zgodne z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi.

2.4.2. Postanowienia dodatkowe

2.4.2.1. Rozłączność postanowień

W przypadku uznania części zapisów niniejszego Kodeksu Postępowania Certyfikacyjnego lub umów zawieranych na jego podstawie za naruszające obowiązujące przepisy prawa lub z nimi niezgodne, sąd może nakazać poszanowanie pozostałej części zapisów Kodeksu lub podpisanych umów, o ile kwestionowane zapisy nie są istotne z punktu widzenia uzgodnionej pomiędzy stronami wymiany (np. transakcji handlowej).

Rozłączność postanowień jest istotna zwłaszcza w przypadku umów o których jest mowa w rozdz.2.1. Nieumieszczenie w umowie klauzuli o rozłączności postanowień może uczynić całą umowę za niezgodną z prawem, nawet jeśli nie jest to intencją stron.

2.4.2.2. Ciągłość postanowień

Postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego obowiązują od daty zaakceptowania przez Zespół ds. Rozwoju PKI aż do momentu ich unieważnienia lub zastąpienia innymi. Modyfikacja starych postanowień lub wprowadzenie nowych odbywa się zgodnie z procedurą przedstawioną w rozdz.8. W przypadku, gdy nowe postanowienia nie naruszają w istotny sposób postanowień poprzednich, obowiązujące umowy należy uznać za ważne, chyba że inaczej uznają strony tych umów lub sąd, do którego zwróci się jedna ze stron.

Jeśli umowa zawarta na podstawie niniejszego Kodeksu Postępowania Certyfikacyjnego zawiera klauzulę o poufności jej zapisów lub poufności informacji, w posiadanie której weszły strony w trakcie trwania umowy lub klauzulę o przestrzeganiu praw autorskich i intelektualnych stron, to postanowienia tych klauzul uważa się za obowiązujące również po ustaniu ważności umowy przez okres, który powinien być integralną częścią tej umowy lub Kodeksu Postępowania Certyfikacyjnego.

Postanowienia umów lub Kodeksu Postępowania Certyfikacyjnego nie mogą być przenoszone na osoby trzecie, poza przypadkami określonymi w umowie oraz w rozdz.4.1.4.

2.4.2.3. Łączenie postanowień

Niniejszy Kodeks Postępowania Certyfikacyjnego oraz zawierane umowy mogą zawierać odwołania do innych postanowień o ile:

zostało to wyrażone w formie klauzuli w Kodeksie lub umowie,

postanowienia, do których odwołuje się Kodeks lub umowa mają formę pisemną.

2.4.2.4. Powiadamianie

Strony wymienione w niniejszym Kodeksie Postępowania Certyfikacyjnego mogą w drodze umów określić metody komunikowania się ze sobą. Jeśli tego nie zrobiono, to niniejszy Kodeks dopuszcza stosowanie wymiany informacji za pośrednictwem poczty fizycznej lub poczty elektronicznej, faksu i telefonu oraz protokołów sieciowych (m.in. TCP/IP, HTTP), itp.

Wybór środka komunikowania się może być jednak wymuszony przez rodzaj przekazywanej informacji. Na przykład większość usług świadczonych przez Unizeto CERTUM - CCP wymaga zastosowania jednego lub kilku dozwolonych protokołów sieciowych.

Niektóre komunikaty i informacje muszą być przekazywane stronom zgodnie z wcześniej uzgodnionym harmonogramem lub odstępstwami od tego harmonogramu. Dotyczy to w szczególności publikowania list certyfikatów unieważnionych, publikowania nowych certyfikatów urzędów rejestracji i urzędów certyfikacji, rozsyłania powiadomień o tym fakcie do subskrybentów oraz stron ufających (jeśli tak stanowi umowa) oraz informowania o naruszeniu klucza prywatnego dowolnego urzędu certyfikacji.

2.4.3. Rozstrzyganie sporów

Przedmiotem rozstrzygania sporów mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami powiązanymi ze sobą wzajemnymi formalnymi lub nieformalnymi umowami, odwołującymi się w jakikolwiek sposób do niniejszego Kodeksu Postępowania Certyfikacyjnego.

W przypadku wystąpienia sporów lub zażaleń będących konsekwencją użycia certyfikatu wydanego lub innych usług świadczonych przez Unizeto CERTUM - CCP, skarżący zobowiązuje się pisemnie (w formie listu poleconego) poinformować Unizeto CERTUM - CCP o dokładnej przyczynie sporu lub zażalenia. Jednocześnie skarżący zobowiązuje się dać Unizeto CERTUM - CCP uzgodniony okres czasu na podjęcie próby rozwiązania sporu przed uruchomieniem innych mechanizmów rozstrzygania sporów.

Jeśli minie uzgodniony okres czasu skarżący może przekazać sprawę do rozstrzygnięcia przez niezależnego, uzgodnionego mediatora. Zaakceptowane przez obie strony postanowienie mediatora powinno być ostateczne i wiążące obie strony.

Jeżeli na drodze mediacji problem nie zostanie rozstrzygnięty w sposób satysfakcjonujący, to spór powinien być rozstrzygnięty na drodze sądowej, zgodnie z obowiązującymi w Polsce przepisami Kodeksu Cywilnego oraz innymi obowiązującymi przepisami prawa.

Unizeto CERTUM - CCP rozstrzyga tylko spory z klientami (subskrybentami, urzędami rejestracji, urzędami certyfikacji, stronami ufającymi, itp.) wynikłe zawartych zawartych umów. Ich integralną częścią są zasady wymienione powyżej. Podobne zasady rozstrzygania sporów powinny obowiązywać także w przypadku umów, których stroną nie jest Unizeto CERTUM - CCP.

2.5. Opłaty

Za świadczone usługi Unizeto CERTUM - CCP pobiera opłaty. Wysokości opłat oraz rodzaje usług objętych opłatami są opublikowane w cenniku, dostępnym w repozytorium Unizeto CERTUM - CCP pod adresem:

http://www.certum.pl/repozytorium

Unizeto CERTUM - CCP stosuje cztery modele pobierania opłat za świadczone usługi:

sprzedaż detaliczną – opłaty pobierane są oddzielnie za każdą jednostkę usługową, np. za każdy pojedynczy certyfikat lub mały pakiet certyfikatów,

sprzedaż hurtową – opłaty pobierane są za pakiet usług, np. dużą liczbę certyfikatów sprzedanych jednorazowo osobie prawnej.

sprzedaż abonamentową – opłaty są pobierane raz w miesiącu; wysokość opłaty abonamentowej uzależniona jest od rodzaju i liczby jednostek usługowych i jest stosowana zwłaszcza w przypadku usługi znacznika czasu oraz weryfikacji statusu certyfikatu przy wykorzystaniu protokołu OCSP,

sprzedaż pośrednią – opłata jest pobierana za każdą jednostkę usługową od klienta, który świadczy usługi zbudowane na bazie infrastruktury Unizeto CERTUM - CCP; np. jeśli nowy komercyjny urząd certyfikacji otrzyma certyfikat od Unizeto CERTUM - CCP, to Unizeto CERTUM - CCP pobiera opłatę za każdy certyfikat wydany przez ten urząd.

Opłaty mogą być wnoszone przy pomocy karty kredytowej lub przelewów bankowych na podstawie faktury lub zamówienia.

2.5.1. Opłaty za wydanie lub recertyfikację

Unizeto CERTUM - CCP pobiera opłaty za wydanie i recertyfikację[18] (patrz punkt 2.5).

Ze względu na odmienność procedur wydawania certyfikatu i recertyfikacji opłaty realizowane według jednego z czterech modeli wymienionych w rozdz.2.5.1 można podzielić na trzy składowe: koszty identyfikacji i uwierzytelnienia lub szerzej koszty obsługi w urzędzie rejestracji, koszty wytworzenia certyfikatu oraz koszty personalizacji i wydania identyfikacyjnej karty elektronicznej (tokena). Składniki te mogą tworzyć oddzielne pozycje w cenniku i być przydatne zwłaszcza w przypadku recertyfikacji (można pominąć koszty identyfikacji i uwierzytelnienia subskrybenta oraz wydania tokena).

[18] Patrz **Słownik pojęć**

2.5.2. Opłaty za dostęp do certyfikatów

Opłaty za dostęp do certyfikatów mogą dotyczyć tylko stron ufających. Przy pobieraniu opłat stosowany jest model sprzedaży abonamentowej lub pośredniej. W tym ostatnim przypadku opłaty mogą być pobierane w zależności od liczby aplikacji (np. punktów sprzedaży), posiadanych przez stronę ufającą.

Unizeto CERTUM - CCP przyjmuje jako zasadę, że opłaty za dostęp do certyfikatów są regulowane przy pomocy umów zawieranych ze stronami ufającymi. Wysokość tych opłat uzależniona jest od wiarygodności certyfikatów.

Unizeto CERTUM - CCP nie pobiera żadnych opłat za udostępnienie stronom ufającym certyfikatów o poziomie wiarygodności Certum Level I.

2.5.3. Opłaty za unieważnienie i informacje o statusie certyfikatu

Unizeto CERTUM - CCP nie pobiera żadnych opłat za unieważnianie certyfikatów, umieszczanie ich na listach CRL oraz udostępnianie stronom ufającym list CRL opublikowanych w repozytorium lub w innych miejscach.

Unizeto CERTUM - CCP może jednak pobierać opłaty za usługi weryfikacji statusu certyfikatu świadczone w oparciu o protokół OCSP lub inne udostępnione mechanizmy. Przy pobieraniu opłat stosowany jest model sprzedaży detalicznej lub abonamentowej.

Jednocześnie bez pisemnej zgody, Unizeto CERTUM - CCP nie zezwala na dostęp do informacji o unieważnionych certyfikatach (list CRL) lub informacji o statusie certyfikatu stronom trzecim, które świadczą usługi weryfikacji statusu certyfikatu. Może to nastąpić tylko po uprzednim zawarciu umowy z Unizeto CERTUM - CCP. Przy pobieraniu opłat stosowany jest w tym przypadku model sprzedaży pośredniej, tzn. pobierana jest opłata od każdego poświadczenia statusu certyfikatu wydanego przez stronę trzecią.

2.5.4. Inne opłaty

Unizeto CERTUM - CCP może pobierać opłaty za inne usługi (patrz punkt 2.5). Usługi te mogą dotyczyć m.in.:

generowania kluczy urzędom certyfikacji lub subskrybentom,

testowania aplikacji i umieszczania jej na liście aplikacji rekomendowanych,

sprzedaży licencji,

realizacji prac projektowych, wdrożeniowych i instalacyjnych,

sprzedaży Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji, podręczników, przewodników itp., wydanych w formie drukowanej,

szkoleń.

2.5.5. Zwrot opłat

Unizeto CERTUM - CCP dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. Jeśli jednak subskrybent lub strona ufająca nie są zadowoleni ze świadczonych usług, to mogą w ciągu 30 dni od wydania certyfikatu zażądać unieważnienia certyfikatu i zwrotu wniesionej opłaty. Po upływie 30 dni subskrybent może zażądać unieważnienia certyfikatu i zwrotu wniesionej opłaty jedynie w przypadku, gdy Unizeto

CERTUM - CCP nie wywiązuje się ze swoich zobowiązań oraz obowiązków określonych w niniejszym Kodeksie Postępowania Certyfikacyjnego.

Żądania o zwrot opłat należy kierować pod adres podany w rozdz.1.5.2.

2.6. Repozytorium i publikacje

2.6.1. Informacje publikowane przez Unizeto CERTUM - CCP

Wszystkie informacje publikowane przez Unizeto CERTUM - CCP dostępne są w repozytorium pod następującym ogólnym adresem:

http://www.certum.pl/repozytorium

Informacje te to:

Polityka Certyfikacji,

Kodeks Postępowania Certyfikacyjnego,

wzory umów z subskrybentami i stronami ufającymi,

oświadczenie Unizeto CERTUM - CCP o poufności otrzymywanej i przetwarzanej informacji,

certyfikaty: urzędów certyfikacji **CA-Certum**, **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**, innych urzędów certyfikacji, urzędów rejestracji, certyfikaty subskrybentów,

listy certyfikatów unieważnionych (CRL); listy certyfikatów unieważnionych dostępne są w tzw. punktach dystrybucji CRL, których adresy umieszczane są w każdym certyfikacie wydanym przez Unizeto CERTUM - CCP; podstawowym punktem dystrybucji list CRL jest repozytorium http://crl.certum.pl,

raporty z audytu dokonywanego przez upoważnioną instytucję (w możliwie szczegółowej postaci);

informacje pomocnicze, np. ogłoszenia.

Certyfikaty urzędów certyfikacji, urzędów rejestracji oraz certyfikaty subskrybentów udostępniane są także na każde żądanie wysłane do serwera WWW na adres:

http://www.certum.pl/search

Oprócz okresowego publikowania list certyfikatów unieważnionych repozytorium umożliwia także dostęp do najbardziej aktualnej informacji o statusie certyfikatu w trybie on-line. Odbywa się to albo za pośrednictwem strony WWW (adres http://www.certum.pl) lub usługi OCSP (adres: http://ocsp.certum.pl).

2.6.2. Częstotliwość publikacji Unizeto CERTUM - CCP

Wymienione poniżej publikacje Unizeto CERTUM - CCP są ogłaszane z następującą częstotliwością:

Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego – patrz rozdz.8;

certyfikaty urzędów certyfikacji funkcjonujących w ramach Unizeto CERTUM - CCP – każdorazowo, gdy nastąpi emisja nowych certyfikatów;

certyfikaty urzędów rejestracji – każdorazowo, gdy nastąpi emisja nowych certyfikatów;

certyfikaty subskrybentów – za ich zgodą każdorazowo, gdy nastąpi emisja nowych certyfikatów;

listy certyfikatów unieważnionych – patrz rozdz.4.9.4 i 4.9.9;

raporty z audytu dokonywanego przez upoważnioną instytucję – każdorazowo, po otrzymaniu go przez Unizeto CERTUM - CCP;

informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.6.3. Dostęp do publikacji Unizeto CERTUM - CCP

Wszystkie informacje publikowane przez Unizeto CERTUM - CCP w jego repozytorium pod adresem: http://www.certum.pl/repozytorium są dostępne publicznie. Mogą być jednak odczytywane bez ograniczeń dopiero po uzyskaniu od strony ufającej zgody na warunki określone w umowie zawartej z Unizeto CERTUM - CCP.

Jednostka usługowa Unizeto CERTUM - CCP zaimplementowała i wdrożyła logiczne oraz fizyczne mechanizmy zabezpieczające przed nieautoryzowanym dodawaniem, usuwaniem lub modyfikowaniem wpisów w repozytorium.

W przypadku gdy zostanie wykryte naruszenie integralności wpisów w repozytorium, zostaną podjęte odpowiednie działania mające na celu przywrócenie integralności wpisom, wyciągnięcie sankcji prawnych w stosunku do sprawców tego nadużycia, a także poinformowanie i skompensowanie poszkodowanym ewentualnych strat.

2.7. Audyt

Celem audytu jest określenie stopnia zgodności postępowania jednostki usługowej Unizeto CERTUM - CCP lub wskazanych przez nią elementów z deklaracjami i procedurami (włączając w to Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego).

Audyt Unizeto CERTUM - CCP dotyczy przede wszystkim ośrodka przetwarzania danych oraz procedur zarządzania kluczami. Przeglądom poddawane są także wszystkie urzędy certyfikacji, które znajdują się w drzewie certyfikacji głównego urzędu certyfikacji **CA-Certum**, urzędy rejestracji oraz inne elementy infrastruktury klucza publicznego, m.in. serwer OCSP.

Audyt Unizeto CERTUM - CCP może być prowadzony przez komórki wewnętrzne Unizeto Sp z o.o. (audyt wewnętrzny) oraz przez jednostki organizacyjne niezależne Unizeto Sp z o.o. (audyt zewnętrzny). W obu przypadkach audyt jest prowadzony na wniosek i pod nadzorem **administratora bezpieczeństwa** (patrz rozdz.5.2.1).

2.7.1. Częstotliwość audytu

Audyt zewnętrzny sprawdzający prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) jest wykonywany przynajmniej raz na dwa lata. Z kolei audyt wewnętrzny przeprowadzany jest przynajmniej raz w roku.

2.7.2. Tożsamość/kwalifikacje audytora

Audyt zewnętrzny wykonywany jest przez upoważnioną do tego rodzaju działalności i niezależną od Unizeto CERTUM - CCP instytucję krajową lub posiadającą przedstawicielstwo na terytorium Polski. Instytucja ta powinna:

zatrudniać pracowników, którzy posiadają odpowiednie udokumentowane przygotowanie techniczne w zakresie infrastruktury klucza publicznego (PKI), technik i narzędzi zabezpieczania informacji oraz prowadzenia audytów bezpieczeństwa,

być zarejestrowaną organizacją lub stowarzyszeniem, dobrze znaną i posiadającą wysoką renomę pośród tego typu instytucji.

Aktualnym zewnętrznym audytorem Unizeto CERTUM - CCP jest firma Ernst&Young.

Audyt wewnętrzny realizowany jest przez Biuro Zarządzania i Ochrony Informacji, funkcjonujące w strukturze Unizeto Sp. z o.o.

2.7.3. Związek audytora z audytowaną jednostką

Patrz punkt 2.7.2

2.7.4. Zagadnienia obejmowane przez audyt

Audyt wewnętrzny i zewnętrzny prowadzony jest zgodnie z zasadami określonymi przez American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA*) WebTrust Principles and Criteria for Certification Authorities*, nazywanymi dalej w skrócie *WebTrust*.

Audytem wg *WebTrust* objęte są m.in. następujące zagadnienia:

zabezpieczenia fizyczne Unizeto CERTUM - CCP,

procedury weryfikacji tożsamości subskrybentów,

usługi certyfikacyjne i procedury ich świadczenia,

zabezpieczenia oprogramowania i dostępu do sieci,

ochrona personelu Unizeto CERTUM - CCP;

dzienniki systemowe i procedury monitorowania systemu,

procedury sporządzania kopii zapasowych oraz ich odtwarzania.

realizacja procedur archiwizacji,

dokumentowanie zmian parametrów konfiguracyjnych Unizeto CERTUM - CCP,

dokumentowanie przeglądów i serwisu sprzętu oraz oprogramowania.

2.7.5. Podejmowane działania w celu usunięcia usterek wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są **administratorowi bezpieczeństwa** Unizeto CERTUM - CCP. Administrator bezpieczeństwa zobowiązany jest w ciągu 14 dni od daty otrzymania raportów do przygotowania pisemnego stanowiska wobec wszelkich uchybień wskazanych w raportach. Odpowiedź musi określić także sposoby i terminy usunięcia usterek. Informacja o usunięciu usterek przekazywana jest instytucji audytującej.

W przypadku wykrycia usterek, które zagrażają bezpieczeństwu procedur certyfikacji realizowanych przez urzędy certyfikacji ***CA-Certum Level III*** *i* ***CA-Certum Level IV****, administrator bezpieczeństwa może podjąć decyzję o czasowym zawieszeniu ich działalności. O zawieszeniu funkcjonowania urzędów certyfikacji oraz przewidywanym terminie wznowienia ich działalności zostaną poinformowani wszyscy klienci Unizeto CERTUM - Centrum Certyfikacji. Informacja ta zostanie umieszczona w repozytorium, przesłana pocztą elektroniczną oraz w uzasadnionych przypadkach opublikowana w prasie.*

2.7.6. Informowanie o wynikach audytu

Raport z audytu w możliwie szczegółowej postaci wraz z ogólną opinią instytucji audytującej o zgodności funkcjonowania Unizeto CERTUM - CCP z wymaganiami określonymi w *WebTrust*, a także stanowisko administratora bezpieczeństwa po każdym audycie są publikowane w repozytorium.

2.8. Niejawność informacji

Unizeto CERTUM - CCP gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującym w tym zakresie prawem, a w szczególności *Ustawą z dnia 22 stycznia 1999 r. o ochronie informacji niejawnych* i towarzyszących jej aktów wykonawczych oraz *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.*

Wzajemne relacje pomiędzy subskrybentem i stroną ufającą a Unizeto CERTUM - CCP opierają się na zaufaniu. Unizeto CERTUM - CCP gwarantuje, że stronom trzecim udostępniane są tylko te informacje, które publicznie dostępne są w certyfikacie. Pozostałe dane spośród tych, które dostarczane są we wnioskach kierowanych do Unizeto CERTUM - CCP nie zostaną nigdy, w żadnych okolicznościach, dobrowolnie lub świadomie ujawnione innym podmiotom, z wyjątkiem żądania ze strony władz sądowych, mającego umocowanie w obowiązującym prawie.

Unizeto CERTUM - CCP może posiadać dostęp do kluczy prywatnych subskrybentów tylko w dwóch przypadkach:

1) zlecenia wygenerowania kluczy i ich zarchiwizowania,
2) przysłania do zarchiwizowania lokalnie wygenerowanych kluczy prywatnych.

Archiwizacja kluczy w obu przypadkach odbywa się na wyraźne żądanie subskrybenta.

Certyfikaty emitowane przez Unizeto CERTUM - CCP uwierzytelniają przesyłanie informacji pomiędzy subskrybentem a stroną ufającą, która może posiadać status *informacji niejawnej.*

2.8.1. Informacje które muszą być traktowane jako niejawne

Unizeto CERTUM - CCP i osoby w nim zatrudnione, jak również podmioty za których pośrednictwem wykonywane są czynności certyfikacyjne, są obowiązane zachować w tajemnicy rozumianej jako tajemnica przedsiębiorstwa[19], w trakcie zatrudnienia oraz po jego zakończeniu. Informacje stanowiące tajemnicą przedsiębiorstwa regulowane są przez wewnętrzne zarządzenia firmy i dotyczą one w szczególności:

informacji otrzymywanej od subskrybentów, z wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych; we wszystkich pozostałych

[19] Przez tajemnicę przedsiębiorstwa rozumie się nie ujawnione do wiadomości publicznej informacje techniczne, technologiczne, handlowe lub organizacyjne przedsiębiorstwa, co do których przedsiębiorca podjął niezbędne działania w celu zachowania ich poufności.

przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub prawomocnego nakazu sądowego;

informacji wpływającej od/do subskrybentów (m.in. treści umów z subskrybentami i stronami ufającymi, rozliczenia, wnioski o zarejestrowanie, wydanie, odnowienie lub unieważnienie certyfikatów; z wyjątkiem informacji umieszczonych w certyfikatach lub repozytorium, zgodnie z postanowieniami niniejszego Kodeksu Postępowania Certyfikacyjnego); część z powyższych informacji może być udostępniana wyłącznie za zgodą i w zakresie pisemnie określonym przez jej właściciela (subskrybenta),

zapisów transakcji systemowych (zarówno w całości, jak też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. logi transakcji systemowych);

zapisów informacji o zdarzeniach (logi) związanych z usługami certyfikacyjnym i zachowywanymi przez Unizeto CERTUM - CCP oraz urzędy rejestracji;

raportów kontroli wewnętrznej oraz zewnętrznej, o ile stanowić to może zagrożenie bezpieczeństwa Unizeto CERTUM - CCP (zgodnie z rozdz.2.7 większa część tych informacji powinna być publicznie dostępna);

plany działań awaryjnych,

informacje o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie, informacje o administrowaniu usługami certyfikacyjnymi oraz projektowanymi zasadami rejestrowania.

Unizeto CERTUM - CCP nie obowiązuje zachowanie tajemnicy wobec strony umowy o świadczenie usług certyfikacyjnych. Osoby odpowiedzialne za zachowanie tajemnicy i zasad postępowania z informacjami ponoszą odpowiedzialność karną zgodnie z przepisami prawa.

2.8.2. Informacje które mogą być traktowane jako jawne

Wszystkie informacje, które niezbędne są w procesie prawidłowego funkcjonowania usług certyfikacyjnych uważane są za informacje jawne. W szczególności za informacje jawne uważa się te informacje, które umieszczane są w certyfikacie przez organy wydające certyfikaty zgodnie z opisem przedstawionym w rozdz.7. Przyjmuje się w tym przypadku zasadę, że subskrybent występując z wnioskiem o wydanie certyfikatu jest świadom jaka informacja umieszczana jest w certyfikacie i wyraża zgodę na jej upublicznienie.

Część informacji wpływających i przekazywanych od/do subskrybentów może być udostępniana innym podmiotom wyłącznie za zgodą subskrybenta, i w zakresie określonym przy procesie rejestracji.

Wymienione poniżej informacje, przekazane urzędom certyfikacji i urzędom rejestracji, traktowane są jako ogólnie dostępne za pośrednictwem repozytorium:

Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego,

wzorce umów Unizeto CERTUM - CCP z subskrybentami oraz stronami ufającymi;

cennik usług,

poradniki dla użytkowników,

certyfikaty urzędów certyfikacji, urzędów rejestracji;

certyfikaty subskrybentów, którzy wyrazili na to zgodę

listy certyfikatów unieważnionych (CRL),

informacje o szkoleniach prowadzonych przez Centrum,

wyciągi z raportów pokontrolnych, dokonywanych przez upoważnioną instytucję (w możliwie szczegółowej postaci).

Publikowane przez Unizeto CERTUM - CCP wyciągi z raportów pokontrolnych dotyczą:

zagadnień, jakie obejmował audyt,

ogólnej oceny wystawionej przez instytucję wykonującą audyt,

stopień realizacji zaleceń.

2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu

W przypadku gdy unieważnienie certyfikatu następuje na podstawie wniosku uprawnionej strony – innej niż strona, której certyfikat jest unieważniany, informacja o fakcie unieważnienia i szczegółowych przyczynach unieważnienia jest przekazywana obu stronom.

2.8.4. Udostępnianie informacji niejawnej w przypadku nakazów sądowych

Informacja niejawna może zostać udostępniona na żądanie organów sądowych, ale tylko i wyłącznie po spełnieniu wszystkich wymagań stawianych przez obowiązujące na terenie Rzeczypospolitej Polskiej akty prawne.

2.8.5. Udostępnianie informacji niejawnej w celach naukowych

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych warunków w tym zakresie.

2.8.6. Udostępnianie informacji niejawnej na żądanie właściciela

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych warunków w tym zakresie.

2.8.7. Inne okoliczności udostępniania informacji niejawnej

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych warunków w tym zakresie.

2.9. Prawo do własności intelektualnej

Wszystkie używane przez Unizeto CERTUM - CCP znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli. Unizeto CERTUM - CCP zobowiązuje się do umieszczania odpowiednich (wymaganych przez właścicieli) uwag w tej dziedzinie.

Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez Unizeto CERTUM - CCP jest własnością podmiotu tego certyfikatu, określonego w polu subject certyfikatu (patrz rozdz.7.1).

Unizeto CERTUM - Centrum Certyfikacji Powszechne posiada wyłączne prawa do dowolnego produktu lub informacji projektowanej, implementowanej i wdrażanej na podstawie lub zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego.

3.Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się Unizeto CERTUM - CCP podczas wydawania certyfikatów. Zasady te oparte na określonych typach informacji które umieszczane są w treści certyfikatu definiują środki, jakie są niezbędne do uzyskania pewności iż informacje te są dokładne i wiarygodne w momencie wydawania certyfikatu.

Procedura weryfikacji przeprowadzana jest **obligatoryjnie** zawsze w fazie rejestracji subskrybenta i modyfikacji jego danych oraz **na żądanie** Unizeto CERTUM - CCP w przypadku każdej innej usługi certyfikacyjnej.

3.1. Rejestracja początkowa

Akt rejestracji subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składający wniosek o rejestrację nie posiada żadnego **ważnego certyfikatu**[20] wydanego przez dowolny z urzędów wydających certyfikaty, afiliowanych przy Unizeto CERTUM - CCP.

Rejestracja obejmuje szereg procedur, które jeszcze przed wydaniem certyfikatu subskrybentowi umożliwiają urzędowi certyfikacji zgromadzenie uwiarygodnionych danych o podmiocie lub danych identyfikujących go.

Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po pomyślnym zweryfikowaniu dostarczonych danych subskrybent zostaje wpisany na listę uprawnionych użytkowników usług Unizeto CERTUM - CCP i zaopatrzony w żądany certyfikat klucza publicznego. Wydany certyfikat na żądanie subskrybenta jest publikowany w repozytorium.

Każdy subskrybent przystępujący do usług infrastruktury klucza publicznego i ubiegający się o wydanie certyfikatu musi wykonać następujące podstawowe czynności, poprzedzające wydanie certyfikatu:

zdalnie, na stronie WWW Unizeto CERTUM - CCP wypełnić formularz rejestracyjny,

wygenerować parę kluczy asymetrycznych RSA lub DSA i dostarczyć urzędowi rejestracji dowód posiadania klucza prywatnego; opcjonalnie subskrybent może zlecić wygenerowanie pary kluczy urzędowi certyfikacji lub urzędowi rejestracji,

zaproponować nazwę wyróżniającą (**DN**, patrz rozdz.3.1.1);

wypełnić i złożyć wniosek o rejestrację z kluczem publicznym i dowodem posiadania spójnego z nim klucza prywatnego;

opcjonalnie stawić się (jeśli jest to wymagane przez daną politykę certyfikacji, według której wydawany jest certyfikat będący przedmiotem wniosku) wraz z wymaganymi dokumentami we wskazanym urzędzie rejestracji,

z agentem urzędu rejestracji podpisać umowę na świadczenie usług przez Unizeto CERTUM - CCP; integralną częścią tej umowy jest niniejszy Kodeks Postępowania Certyfikacyjnego.

[20] Patrz **Słownik pojęć**

Rejestracja może wymagać osobistego stawienia się subskrybenta lub uprawomocnionego przez niego reprezentanta w urzędzie rejestracji. Unizeto CERTUM - CCP dopuszcza jednak takie procedury rejestracji, w których wnioski o rejestrację mogą być przesyłane za pośrednictwem zwykłej poczty, poczty elektronicznej, witryny stron typu WWW itp., zaś ich rozpatrywanie nie wymaga fizycznego kontaktu z wnioskodawcą.

3.1.1. Typy nazw

Certyfikaty wydawane przez Unizeto CERTUM - CCP są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wydawca certyfikatu, jak też działający w jego imieniu urząd rejestracji akceptują tylko takie nazwy subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenia serii X.500). Podstawowe nazwy subskrybentów oraz nazwy wystawców certyfikatów, umieszczane w certyfikatach Unizeto CERTUM - CCP są zgodne z nazwami wyróżnionymi DN (określanymi także mianem nazw katalogowych), budowanymi według rekomendacji X.500 i X.520. W ramach nazwy DN dopuszcza się także możliwość definiowania atrybutów systemu nazw domenowych (DNS, *ang. Domain Nameserver System*), określonych w RFC 2247. Pozwoli to subskrybentom na posługiwanie się równolegle dwoma typami nazw: DN i DNS, co może być istotne zwłaszcza w przypadku wydawania certyfikatów serwerom będącym pod kontrolą subskrybenta.

W celu łatwiejszej komunikacji elektronicznej z subskrybentem w certyfikatach Unizeto CERTUM - CCP używa się także alternatywnej nazwy subskrybenta. Nazwa ta może zawierać także adres poczty elektronicznej subskrybenta, zgodny z zaleceniem RFC 822.

Nazwy katalogów, w których przechowywane są certyfikaty, listy certyfikatów unieważnionych (CRL), Polityka Certyfikacji, itp., jak również nazwy punktów dystrybucji CRL zgodne są z zaleceniem RFC 1738 oraz schematami nazewniczymi stosowanymi przez protokół LDAP (patrz RFC 1778).

W Tab.3.1 przedstawiono minimalne wymagania nakładane na nazwy subskrybentów w ramach każdej z czterech zdefiniowanych w rozdz.1 polityk certyfikacji.

Tab.3.1 Wymagania nakładane na nazwę podmiotu certyfikatu

Nazwa polityki certyfikacji	Wymagania
Certum Level I	Niepusta wartość pola subject lub pusta w przypadku, gdy występuje pole alternatywnej nazwy podmiotu (SubjectAltName) i jest zaznaczone jako krytyczne[21].
Certum Level II	Niepusta wartość pola subject i opcjonalnie pole alternatywnej nazwy podmiotu (SubjectAltName) w przypadku, gdy jest zaznaczone jako niekrytyczne.
Certum Level III	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.
Certum Level IV	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.

[21] Zdefiniowane nazwy mogą zawierać atrybuty, które nie są atrybutami w dokumentach serii X.500; w szczególności w polach tych może wystąpić atrybut, który określa adres poczty elektronicznej.

Wszystkie przekazane przez subskrybenta we wniosku o rejestrację informacje, które zostaną umieszczone przez organ wydający certyfikaty w certyfikacie wydanym subskrybentowi są jawne. Szczegółowa lista danych umieszczonych w certyfikacie jest zgodna z zaleceniem x.509 v.3 i podana jest w rozdz.7 (patrz także rozdz.3.1.2)

3.1.2. Konieczność używania nazw znaczących

Nazwy wchodzące w skład nazwy wyróżnionej DN subskrybenta posiadają swoje znaczenie w języku polskim lub innym języku kongresowym.

Struktura nazwy wyróżnionej (DN), akceptowana/przydzielana i weryfikowana w urzędzie rejestracji, uzależniona jest od typu subskrybenta.

W przypadku **osób fizycznych** (osób indywidualnych lub pracowników firm) nazwa DN składa się obligatoryjnych następujących, nie obligatoryjnych pól (opis pola poprzedzano jego skróconą nazwą przyjętą za zaleceniem RFC 2459 i X.520):

pola C – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),

pola ST – region/województwo, na którego terenie działa lub mieszka subskrybent,

pola L – miasto, w którym ma siedzibę lub mieszka subskrybent,

pola CN – nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje subskrybent, jeśli w nazwie DN wystąpiły pola O lub OU (patrz niżej); w polu tym może być podana także nazwa produktu lub urządzenia,

pola O[22] – nazwa instytucji, w której pracuje subskrybent,

pola OU[22] – nazwa jednostki organizacyjnej, zatrudniającej subskrybenta

oraz pięciu pól opcjonalnych[23] (umieszczane są na żądanie subskrybenta, po uzgodnieniu z wystawcą certyfikatów):

pola S – nazwisko subskrybenta (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),

pola G – imię (imiona) subskrybenta,

pola P – pseudonim subskrybenta, którego używa w swoim środowisku lub którym chce się posługiwać bez ujawnienia swojego prawdziwego imienia i nazwiska,

pola T – numer telefonu,

pola F – numer faksu.

W przypadku **osób prawnych** nazwa DN składa się następujących, nie obligatoryjnych pól (opis pola poprzedzano jego skróconą nazwą przyjętą za zaleceniem X.520)

pola C – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**);

pola O – nazwa instytucji;

pola OU – nazwa jednostki organizacyjnej instytucji;

pola ST – region/województwo, na którego terenie działa instytucja;

---

22 Argument ten umieszczany jest w nazwie DN tylko w przypadku, gdy osoba fizyczna jest pracownikiem firmy

23 Pola te nie powinny mieć wpływu na unikalność nazwy DN subskrybenta.

pola L – miasto, w którym ma siedzibę lub mieszka subskrybent;

pola CN – nazwa zwyczajowa instytucji,

oraz dwóch pól opcjonalnych[24] (umieszczane są na żądanie osoby prawnej w porozumieniu z wystawcą certyfikatów)

pola T – numer telefonu,

pola F – numer faksu.

Dodatkowo w przypadku **urządzeń**, będących pod opieką osób fizycznych/prawnych nazwa DN zawiera oprócz tych samych elementów, które występują w nazwie osoby fizycznej/prawnej także nie obligatoryjne pole:

pola SN – numer seryjny lub identyfikator urządzenia.

Nazwa subskrybenta DN musi być zatwierdzona przez operatora urzędu rejestracji oraz zaakceptowana przez urząd certyfikacji. Unizeto CERTUM - CCP gwarantuje (w ramach swojej domeny) unikalność nazw DN.

3.1.3. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez Unizeto CERTUM - CCP w wydawanych przez siebie certyfikatach jest zgodna z profilem certyfikatów opisanym w dokumencie *Profil certyfikatu PKC i listy CRL*[25]. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz.3.1.2.

3.1.4. Unikalność nazw

Identyfikacja każdego z subskrybentów certyfikatów wydawanych przez Unizeto CERTUM - CCP realizowana jest w oparciu o nazwę wyróżnioną DN.

Unizeto CERTUM - CCP gwarantuje unikalność przydzielonej subskrybentowi nazwy wyróżnionej (DN).

Nazwa DN subskrybenta jest proponowana we wniosku przez samego subskrybenta. Jeśli nazwa ta jest zgodna z ogólnymi wymaganiami określonymi w rozdz.3.1.1 i 3.1.2, to operator urzędu rejestracji wstępnie akceptuje zgłoszoną propozycję. W przypadku, gdy operator urzędu rejestracji posiada dostęp do bazy nadanych nazw DN[26], wtedy sprawdza dodatkowo unikalność nazwy subskrybenta w domenie Unizeto CERTUM - CCP. Jeśli test ten zakończy się sukcesem, to nazwa DN subskrybenta jest ostatecznie akceptowana. W przypadku braku dostępu do bazy Unizeto CERTUM ostateczną decyzję o akceptacji lub odrzuceniu nazwy podejmuje operator Głównego Urzędu Certyfikacji.

Jeśli proponowana przez subskrybenta nazwa DN nie narusza praw innych podmiotów do nazwy (patrz rozdz.3.1.5), to Unizeto CERTUM - CCP może dodać dodatkowe atrybuty do nazwy DN (np. kwalifikator domeny lub numer seryjny) i zagwarantować w ten sposób unikalność nazwy w swojej domenie. Subskrybent ma prawo w trybie przewidzianym w rozdz.4.4 odrzucić proponowaną nazwę DN.

Format globalnie unikalnej nazwy subskrybenta ma postać:

---

[24] Pola te nie powinny mieć wpływu na unikalność nazwy DN subskrybenta.

[25] *Profil certyfikatu PKC i listy CRL*, Publikacja Centrum Certyfikacji, Unizeto Sp. z o.o.

[26] Dostęp taki posiada zawsze operator Głównego Urzędu Rejestracji

certum.pl/ nazwa wystawcy/ nazwa subskrybenta

gdzie **certum.pl** jest nazwą domeny Unizeto CERTUM - CCP, **nazwa wystawcy** jest nazwą DN jednego z urzędów certyfikacji, zaś nazwa subskrybenta – nazwą DN podmiotu certyfikatu. Wartości dwóch ostatnich elementów pobierane są z certyfikatu subskrybenta.

Jeśli dowolny subskrybent zrezygnuje z usług świadczonych przez Unizeto CERTUM - CCP, to żądanie rejestracji takiej samej nazwy DN przypisanej innemu subskrybentowi musi być odrzucone.

Unizeto CERTUM - CCP może zarejestrować subskrybenta pod nazwą DN używaną kiedyś przez innego subskrybenta tylko na podstawie pisemnej zgody tego ostatniego.

W ramach domeny Unizeto CERTUM - CCP gwarantowana jest także unikalność nazw katalogów, obsługiwanych w obrębie repozytorium. Oznacza to, że aplikacje które bazują na tej własności nazw katalogów Centrum i świadczonych w ich ramach usług mają zagwarantowaną ciągłość usług, bez ryzyka ich przerwania lub podmiany przez inną usługę.

3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

Zabrania się używania we wnioskach nazw, które nie są własnością subskrybenta. Unizeto CERTUM - CCP nie sprawdza czy subskrybent ma prawo do posługiwania się nazwą umieszczoną we wniosku o rejestrację, ani też nie zamierza odgrywać roli arbitra rozstrzygającego spory dotyczące praw własności do nazwy DN, nazwy handlowej lub znaku handlowego.

W przypadku powstania sporu na tle reklamacji nazw Unizeto CERTUM - CCP rezerwuje sobie prawo do odrzucenia wniosku subskrybenta lub jego zawieszenia, bez ponoszenia jakiejkolwiek odpowiedzialności z tego tytułu.

Unizeto CERTUM - CCP rezerwuje sobie także prawo do podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta i przydzielania mu wynikłych z tego nazw.

3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaku towarowego

Unizeto CERTUM - CCP posiada własny zastrzeżony znak towarowy składający się ze znaku graficznego oraz napisu stanowiących łącznie logo o następującej postaci:

Rys.3.1. Logo Unizeto CERTUM

Znak ten oraz napis tworzą łącznie logo Unizeto CERTUM. Logo to jest zastrzeżonym znakiem towarowym Unizeto CERTUM i nie może być używane przez żadną inną stronę bez uprzedniej pisemnej zgody Unizeto CERTUM.

Znak Unizeto CERTUM jest dodatkowym elementem logo każdego urzędu rejestracji działającego z upoważnienia Centrum Certyfikacji. Zgoda na używanie logo Centrum wydawana jest automatycznie w momencie rejestracji przez Centrum nowego urzędu rejestracji.

3.1.7. Dowód posiadania klucza prywatnego

Jeśli podmiot w momencie składania wniosku o wydanie certyfikatu jest w posiadaniu klucza prywatnego, to urzędy certyfikacji działające w ramach Unizeto CERTUM - CCP oraz urzędy rejestracji (w przypadku powierzenia im przez wystawcę certyfikatów uprawnień w zakresie weryfikacji tożsamości) muszą uzyskać pewność, że podmiot ten posiada klucz prywatny pasujący do przesłanego klucza publicznego.

Weryfikacja faktu posiadania klucza prywatnego realizowana jest w oparciu o tzw. dowód posiadania klucza prywatnego. Dowód ten powinien być poświadczeniem, że poddawany procedurze certyfikacji klucz publiczny jest do pary z kluczem prywatnym, będącym w wyłącznym posiadaniu subskrybenta.

Postać dowodu zależy od typu certyfikowanej pary kluczy (para kluczy do realizacji podpisu cyfrowego, szyfrowania lub uzgadniania kluczy).

Podstawowy dowód posiadania klucza prywatnego ma postać podpisu cyfrowego składanego (przez aplikację subskrybenta):

> na żądaniach rejestracji i modyfikacji danych oraz okresowo na żądaniach aktualizacji kluczy/certyfikatu i unieważnienia certyfikatu (w przypadku zgubienia klucza prywatnego oraz sekretu unieważniania certyfikatu), dostarczanych do urzędu rejestracji,
>
> odpowiednio na żądaniach certyfikacji, aktualizacji kluczy/certyfikatu i unieważnienia certyfikatu, przesyłanych bezpośrednio do urzędu certyfikacji.

W przypadku kluczy do szyfrowania dowód posiadania klucza prywatnego przeprowadzany jest pośrednio. Polega on na wystawieniu żądanego przez subskrybenta certyfikatu i zaszyfrowaniu go kluczem publicznym, znajdującym się w certyfikacie. Subskrybent musi rozszyfrować przy pomocy posiadanego klucza prywatnego otrzymany certyfikat i przysłać go zwrotnie do urzędu certyfikacji.

Weryfikacja dowodu posiadania przez subskrybenta klucza prywatnego do uzgadniania kluczy polega na ustanowieniu przez urząd certyfikacji oraz subskrybenta wspólnego sekretu, a następnie na wykorzystaniu go przez urząd certyfikacji do zaszyfrowania wystawionego certyfikatu. Subskrybent musi rozszyfrować przy pomocy posiadanego klucza prywatnego otrzymany certyfikat i przysłać go zwrotnie do urzędu certyfikacji.

Wymóg przedstawienia dowodu posiadania klucza prywatnego nie znajduje zastosowania w przypadku, gdy na żądanie subskrybenta para kluczy jest generowana przez urząd certyfikacji lub urząd rejestracji.

Klucze prywatne powinny być generowane wewnątrz tokena (np. identyfikacyjnej karcie elektronicznej) lub po ich utworzeniu na zewnątrz przy użyciu sprzętowego lub programowego generatora kluczy zapisane w tokenie. Dowolny podmiot może być w posiadaniu tokena już w momencie generowania, jak również zapisywania na nim kluczy lub też token ten jest mu

dostarczony dopiero po wygenerowaniu kluczy[27]. W ostatnim przypadku Unizeto CERTUM - CCP musi zagwarantować bezpieczne dostarczenie tokena wraz z kluczem do podmiotu dla którego jest przeznaczony (patrz rozdz.6.1.2).

3.1.8. Uwierzytelnienie tożsamości osób prawnych

Uwierzytelnienie tożsamości osoby prawnej musi spełniać dwa cele. Po pierwsze należy wykazać, że w momencie rozpatrywania wniosku podana we wniosku osoba prawna istniała i prowadziła działalność gospodarczą, po drugie, należy dowieść, że osoba fizyczna, która wystąpiła z wnioskiem o wydanie certyfikatu lub go odbiera jest upoważniona przez tę osobę prawną do reprezentowania jej interesów.

Procedury uwierzytelniania tożsamości osób prawnych stosowane są w przypadkach, gdy osoba ta:

- występuje w roli subskrybenta i zleca urzędowi certyfikacji wykonanie dowolnej usługi certyfikacji,
- żąda wydania certyfikatu na urządzenie lub aplikację (oprogramowanie), znajdujące się pod opieką tej osoby,
- występuje w roli podmiotu, który składa wniosek o wpisanie na listę akredytowanych urzędów rejestracji lub urzędów certyfikacji, podporządkowanych Unizeto CERTUM - CCP,
- chce świadczyć dodatkowe usługi certyfikacyjne, np. jako urząd znacznika czasu, OCSP.

Wyróżnia się dwa podstawowe sposoby uwierzytelniania tożsamości osób prawnych. Pierwszy sposób wymaga osobistego stawienia się upoważnionego przedstawiciela osoby prawnej w siedzibie urzędu rejestracji lub też przedstawiciela urzędu rejestracji w miejscu wskazanym we wniosku jako siedziba osoby prawnej. Z kolei w przypadku drugim potwierdzenie tożsamości może przebiegać w trybie *on-line*, za pośrednictwem wiadomości wymienianych bezpośrednio z urzędem certyfikacji.

Pierwszy sposób uwierzytelniania jest obligatoryjny zawsze wtedy, gdy składany wniosek wiąże się z zarejestrowaniem i wydaniem osobie prawnej certyfikatów o poziomie wiarygodności **Certum Level III** i **Certum Level IV**. Obejmuje to także niektóre szczególne przypadki, gdy wnioski te dotyczą certyfikacji, aktualizacji certyfikatów i kluczy lub unieważnienia certyfikatów tych samych poziomów.

Urząd rejestracji zobowiązany jest do zażądania od wnioskodawcy przedstawienia odpowiednich dokumentów, które w sposób niebudzący wątpliwości potwierdzą tożsamość instytucji składającej wniosek oraz osoby, która ją reprezentuje.

Dla potrzeb niniejszego Kodeksu Postępowania Certyfikacyjnego przyjmuje się, że upoważnieni przedstawiciele instytucji, niezależnie od typu certyfikatu o który się ubiegają, zobowiązani są do okazania na żądanie przedstawiciela urzędu rejestracji:

- aktualnego wypisu z Krajowego Rejestru Sądowego lub potwierdzoną za zgodność z oryginałem kopię wpisu do ewidencji działalności gospodarczej,
- dokumentu potwierdzającego przydzielone posiadane numeru NIP lub REGON,

[27] Może to zrobić przez urząd certyfikacji lub urząd rejestracji.

dokumentów potwierdzających tożsamość osoby składającej wniosek (dowód osobisty lub paszport) oraz upoważnienia do reprezentowania interesów instytucji.

Ten ostatni wymóg jest istotny zwłaszcza w przypadku ubiegania się o certyfikaty wydawane operatorom urzędów certyfikacji oraz pracownikom instytucji.

Procedura weryfikacji tożsamości osoby prawnej oraz upoważnionego przez nią reprezentanta polega na (patrz także Tab.3.2):

weryfikacji oryginalności dokumentów okazanych przez subskrybenta; weryfikacja ta powinna być szczegółowa, włącznie z wykorzystaniem informacji zawartych w bazach danych organu wydającego certyfikaty (z upoważnienia którego działa punkt rejestracji) lub innych instytucji z nim związanych,

weryfikacji autentyczności dostarczonego wniosku; polegająca na:

- sprawdzeniu zgodności danych umieszczonych we wniosku z dostarczonymi dokumentami,
- bądź opcjonalnie na zweryfikowaniu dowodu posiadania klucza prywatnego (jeśli wniosek dotyczy pary kluczy do realizacji podpisu) oraz poprawności nazwy **DN**,

weryfikacji informacji zawartych w złożonym wniosku z informacjami dostępnymi z innych źródeł (np. Rejestru Sądowego, Głównego Urzędu Statystycznego, Urzędu Skarbowego, Panoramy Firm), mających na celu potwierdzenie faktu istnienia osoby prawnej wymienionej we wniosku,

weryfikacji upoważnień oraz tożsamości przedstawiciela osoby prawnej, który w imieniu tej osoby złożył wniosek, w tym wniosek o akredytację jako urzędu rejestracji lub urzędu certyfikacji.

Urząd rejestracji zobligowany jest do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku (patrz Tab.3.2, rozdz.3.1.9).

Jeśli procedura weryfikacji tożsamości zakończyła się pozytywnie, to upoważniony do tego operator urzędu rejestracji:

przydziela osobie prawnej nazwę wyróżnioną DN lub akceptuje jej postać zaproponowaną w złożonym wniosku,

wystawia **token**, który poświadcza prawdziwość danych zawartych w rozpatrywanym wniosku i wysyła go do urzędu certyfikacji,

tworzy kopie wszystkich dokumentów i zaświadczeń, na podstawie których operator weryfikował tożsamość osoby prawnej oraz działającego w jego imieniu uprawnionego przedstawiciela,

w imieniu urzędu certyfikacji podpisuje z osobą prawną umowę na świadczenie usług certyfikacyjnych; umowa taka zawierana jest zarówno w przypadku występowania osoby prawnej w charakterze subskrybenta, urzędu rejestracji, urzędu certyfikacji, jak też podmiotu charakterze podmiotu świadczącego dodatkowe usługi certyfikacyjne.

Po przesłaniu potwierdzenia (tokena) do urzędu certyfikacji, urząd ten sprawdza czy token został wystawiony przez uprawniony do tego urząd rejestracji.

Proces uwierzytelniania jest dokumentowany. Rodzaj dokumentowanych informacji i czynności jest uzależniony od poziomu wiarygodności certyfikatu będącego przedmiotem wniosku i w szczególności dotyczy:

tożsamości operatora urzędu rejestracji, weryfikującego tożsamość subskrybenta,

złożenia przez operatora odręcznie podpisanego oświadczenia, że tożsamość wnioskodawcy zweryfikował zgodnie z wymaganiami niniejszego Kodeksu Postępowania Certyfikacyjnego,

daty weryfikacji,

identyfikatora operatora oraz wnioskodawcy w przypadku jego osobistego pobytu w urzędzie rejestracji i wcześniejszego przypisania mu takiego identyfikatora,

odręcznie podpisanego przez wnioskodawcę oświadczenia o prawdziwości danych umieszczonych we wniosku; oświadczenie to może być podpisane po przysłaniu go na adres wnioskodawcy (przypadek, gdy nie jest wymagana fizyczna obecność wnioskodawcy w urzędzie rejestracji) lub w obecności operatora urzędu rejestracji.

Unizeto CERTUM - CCP zawsze odrzuca wniosek subskrybenta o rejestrację w przypadku stwierdzenia, że osoba prawna jest już zarejestrowana.

Drugi ze sposobów weryfikacji tożsamości (weryfikacja w trybie *on-line*) realizowany jest w przypadku, gdy wnioski przesyłane są bezpośrednio do urzędu certyfikacji. Dotyczy to:

wniosków o certyfikację, które dotyczą dodatkowych certyfikatów w ramach tej samej polityki certyfikacji,

wniosków o recertyfikację oraz aktualizację kluczy,

wniosek o unieważnienie certyfikatu,

wniosek o udostępnienie certyfikatu,

wniosek o weryfikację certyfikatu lub listy CRL.

Jeśli osoba prawna nie jest w stanie w dostateczny sposób uwierzytelnić swojego wniosku (nie posiada aktualnie ważnego klucza prywatnego do realizacji podpisu lub klucza do uwierzytelniania wiadomości) lub zażąda tego urząd certyfikacji, to wtedy upoważniony przedstawiciel tej osoby musi osobiście stawić się w urzędzie rejestracji i uzyskać potwierdzenie wniosku.

Uwierzytelnianie subskrybenta (instytucji) składającego wnioski bezpośrednio do urzędu certyfikacji realizowane jest w oparciu o informacje zawarte w bazach danych Unizeto CERTUM - CCP i przebiega następująco:

weryfikowane jest uwierzytelnienie wniosku (np. podpis cyfrowy złożony pod przesłanym wnioskiem),

w przypadku, gdy wniosek jest podpisany cyfrowo, to weryfikowana jest autentyczność dołączonego do wniosku certyfikatu, związanego z prywatnym kluczem podpisującym (w oparciu o tzw. ścieżkę certyfikacji),

w bazie wystawcy certyfikatu poszukuje się subskrybenta o nazwie wyróżnionej (DN), zapisanej w certyfikacie, pobiera jego certyfikat lub klucz uwierzytelniania wiadomości i porównuje z certyfikatem lub uwierzytelnieniem dołączonym do wniosku,

porównywany jest identyfikator podmiotu zawarty we wniosku, opcjonalnie w certyfikacie oraz bazach danych wystawcy certyfikatu.

Jeśli wszystkie testy dadzą wynik pozytywny przyjmuje się, że tożsamość instytucji została potwierdzona.

Szczegółowy opis postępowania operatora urzędu rejestracji przedstawiony jest w dokumencie „Księga Urzędu Rejestracji". Dokument ma status „niejawny" i udostępniany jest tylko personelowi urzędów rejestracji oraz wybranym kancelariom notarialnym Rzeczypospolitej Polskiej.

3.1.9. Uwierzytelnienie tożsamości osób fizycznych

Uwierzytelnienie tożsamości osoby fizycznej musi spełniać dwa cele. Po pierwsze musi wykazać, że podane we wniosku dane odnoszą się do istniejącej osoby fizycznej i po drugie, że wnioskodawca jest rzeczywiście tą osobą fizyczną, która została wymieniona we wniosku.

Uwierzytelnianie osób fizycznych, podobnie jak osób prawnych, może być realizowane w dwóch trybach: z udziałem i bez udziału urzędu rejestracji.

Uwierzytelnianie osób fizycznych bez udziału urzędu rejestracji realizowane jest w sposób opisany w rozdz.3.1.8. Z kolei potwierdzenie tożsamości subskrybenta jako osoby fizycznej z udziałem urzędu rejestracji realizowane jest w oparciu o:

dokumenty potwierdzające tożsamość osoby składającej wniosek o zarejestrowanie (dowód osobisty lub paszport);

dokument potwierdzający przydzielone numery PESEL lub NIP,

oraz dodatkowo w przypadku, gdy subskrybent jest pracownikiem instytucji (osoby prawnej), której dane chce umieścić w certyfikacie:

pisemne upoważnienie zawierające wyraźną zgodę tej instytucji na umieszczenie jej danych w certyfikacie osoby fizycznej.

aktualny wypis z Krajowego Rejestru Sądowego lub potwierdzoną za zgodność z oryginałem kopię wpisu do ewidencji działalności gospodarczej

dokumenty potwierdzające przydzielone numery NIP lub REGON.

Dopuszcza się możliwość reprezentowania interesów subskrybenta przez upoważnione w tym celu osoby trzecie. Osoby te muszą się okazać odpowiednimi uprawomocnionymi upoważnieniami, wystawionymi przez subskrybenta.

Procedura weryfikacji tożsamości osoby fizycznej przeprowadzana przez operatora urzędu rejestracji jest podobna do procedury stosowanej w przypadku osób prawnych i polega na:

weryfikacji oryginalności dokumentów okazanych przez subskrybenta; weryfikacja ta powinna być szczegółowa, włącznie z wykorzystaniem informacji zawartych w bazach danych urzędu certyfikacji (z upoważnienia którego działa punkt rejestracji) lub innych instytucji z nim związanych,

weryfikacji autentyczności dostarczonego wniosku; weryfikacja ta polega

- na sprawdzeniu zgodności danych umieszczonych we wniosku z dostarczonymi dokumentami,

- opcjonalnie na zweryfikowaniu dowodu posiadania klucza prywatnego (jeśli wniosek dotyczy pary kluczy do realizacji podpisu) oraz poprawności nazwy **DN**,

weryfikacji informacji zawartych w złożonym wniosku z informacjami dostępnymi z innych źródeł (np. Rejestru Sądowego, Głównego Urzędu Statystycznego, Urzędu Skarbowego, Panoramy Firm), mających na celu potwierdzenie faktu istnienia osoby prawnej wymienionej we wniosku,

po pozytywnym zakończeniu procedury weryfikacji operator urzędu wykonuje czynności opisane w rozdz.3.1.8. Proces uwierzytelniania jest dokumentowany tak samo jak w rozdz.3.1.8.

Wymagania nakładane na procedurę weryfikacji tożsamości osoby fizycznej, uzależnione od poziomu wiarygodności certyfikatu, podane są w Tab.3.2.

Tab.3.2 Wymagania nakładane na proces weryfikacji tożsamości osoby fizycznej

Nazwa polityki certyfikacji	Wymagania
Certum Level I	A. W przypadku certyfikatów na pocztę elektroniczną: weryfikowana jest autentyczność skrzynki pocztowej, poprzez odesłanie informacji zawierającej instrukcję instalacji certyfikatu na adres skrzynki pocztowej podanej we wniosku. B. W przypadku innych certyfikatów testowych porównywane są dane otrzymane: faksem (zalecana forma), listem zwykłym (opcja), listem poleconym (opcja), podczas osobistego pobytu w urzędzie rejestracji (opcja), pocztą elektroniczną z załącznikiem typu: gif, tif, jpg, bmp (opcja) z danymi, jakie subskrybent przekazał elektronicznie do urzędu certyfikacji.

Nazwa polityki certyfikacji	Wymagania
Certum Level II	A. Operatorzy urzędu rejestracji porównują dane subskrybenta otrzymane: faksem (zalecana forma), listem zwykłym (opcja), listem poleconym (opcja), przy osobistym stawiennictwie (opcja), pocztą elektroniczną z załącznikiem typu: gif, tif, jpg, bmp (opcja) z danymi, które subskrybent przekazał elektronicznie do urzędu rejestracji/certyfikacji. B. W przypadku klientów indywidualnych operator potwierdza: adres skrzynki pocztowej, nr telefonu lub faksu. C. W przypadku zamówień zbiorowych potwierdzane są następujące dane: wiarygodność firmy, adres skrzynki osoby odpowiedzialnej za proces certyfikacji, nr telefonu lub faksu, adres do korespondencji.
Certum Level III	A. Operatorzy urzędu rejestracji weryfikują dane klienta otrzymane: listem poleconym (zalecana forma), w trakcie pobytu w urzędzie rejestracji (opcja) z danymi, jakie subskrybent przekazał elektronicznie do urzędu rejestracji. List polecony powinien zawierać kopie oryginalnych dokumentów, potwierdzone własnoręcznym czytelnym podpisem (opcjonalnie pieczątką osoby tworzącej kopię dokumentu) lub notarialnie. B. W przypadku zamówień zbiorowych oraz indywidualnych, sprawdzany jest: adres skrzynki pocztowej osoby odpowiedzialnej za proces certyfikacji, nr telefonu lub faksu, adres do korespondencji, dokument, który potwierdza, że osoba występująca o certyfikat X.509, jest pracownikiem lub reprezentantem firmy (w przypadku firm, a nie osób fizycznych).

Nazwa polityki certyfikacji	Wymagania
Certum Level IV	A. Operatorzy weryfikują dane subskrybenta otrzymane: podczas jego pobytu w urzędzie rejestracji (zalecana forma), listem poleconym, zawierającym dane potwierdzone notarialnie (opcja) z danymi, jakie podmiot przekazał elektronicznie do urzędu certyfikacji. List powinien zawierać kopie dokumentu potwierdzone notarialnie. B. W przypadku zamówień zbiorowych oraz indywidualnych, sprawdzane są: adres skrzynki pocztowej osoby odpowiedzialnej za proces certyfikacji, nr telefonu lub faksu, adres do korespondencji, poświadczenia, że osoba występująca o certyfikat X.509, jest pracownikiem lub reprezentantem firmy (w przypadku firm, a nie osób prywatnych). W przypadku osobistego stawiennictwa operator wykonuje kopie przedkładanych dokumentów, może umieścić na tych dokumentach datę i podpis odręczny. Kopie te mogą również zostać opatrzone własnoręcznym podpisem osoby starającej się o certyfikat klucza publicznego, wraz z dopiskiem: *Dokumenty przedłożyłem osobiście.*

Szczegółowy opis postępowania operatora urzędu rejestracji przedstawiony jest w dokumencie „Księga Urzędu Rejestracji". Dokument ma status „niejawny" i udostępniany jest tylko personelowi urzędów rejestracji oraz wybranym kancelariom notarialnym Rzeczypospolitej Polskiej.

3.1.10. Uwierzytelnienie pochodzenia urządzeń

W wielu przypadkach certyfikat klucza publicznego wydawany jest na urządzenie, np. router, firewall, serwery. W takich przypadkach przyjmuje się, że każde urządzenie musi znajdować się pod opieką osoby prawnej lub fizycznej (musi posiadać swojego sponsora). Sponsor jest odpowiedzialny za dostarczenie następujących danych, związanych z urządzeniem:

identyfikator urządzenia,

klucz publiczny urządzenia,

atrybuty i uprawnienia urządzenia (w przypadku, gdy powinny być umieszczone w certyfikacie),

dane kontaktowe sponsora, w razie konieczności pozwalające urzędowi rejestracji lub certyfikacji na szybkie przekazanie mu informacji.

Weryfikacja rejestrowanej informacji jest uzależniona od poziomu wiarygodności żądanego certyfikatu. Stosowane są dwie następujące metody uwierzytelniania źródła pochodzenia urządzenia oraz integralności przedłożonych danych:

weryfikacja cyfrowo podpisanego wniosku przysłanego przez sponsora (wniosek musi być podpisany przy użyciu klucza prywatnego związanego z certyfikatem o poziomie wiarygodności równym lub wyższym od żądanego),

podczas osobistej rejestracji urządzenia przez sponsora, przy czym tożsamość sponsora potwierdzana jest zgodnie z wymaganiami określonymi w rozdz.3.1.9.

3.1.11. Uwierzytelnienie pełnomocnictw i innych atrybutów

Urzędy rejestracji i urzędy certyfikacji Unizeto CERTUM potwierdzać pełnomocnictwa osób fizycznych do podejmowania działań w imieniu innych podmiotów, zwykle osób prawnych. Takie pełnomocnictwa związane są najczęściej z określoną rolą w instytucji, np. prezes firmy może upoważnić dowolną zaufaną osobę do podpisywania w jego imieniu poleceń przelewów.

Uwierzytelnienie pełnomocnictw jest częścią procesu przetwarzania przez urząd rejestracji lub urząd certyfikacji wniosku o wydanie certyfikatu osobie prawnej lub certyfikatu na urządzenie będące pod opieką osoby prawnej lub fizycznej. Wydany certyfikat jest w obu przypadkach zaświadczeniem, że osoba prawna lub urządzenie mogą posługiwać się kluczem prywatnym w imieniu osoby prawnej.

Pełnomocnictwa są przekazywane przez podmiot prawny albo swoim pracownikom albo agentom (np. biur rozrachunkowych). Procedura uwierzytelniania pełnomocnictw stosowana przez Unizeto CERTUM - Centrum Certyfikacji oprócz weryfikacji samych pełnomocnictw obejmuje także uwierzytelnienie osoby fizycznej, której te pełnomocnictwa zostały przekazane. Z tego ostatniego wymogu można zrezygnować jedynie w przypadku, gdy osoba ta jest już subskrybentem Unizeto CERTUM - Centrum Certyfikacji. Uwierzytelnianie tożsamości osoby fizycznej przebiega zgodnie z procedurami opisanymi w rozdz.3.1.9.

Sama procedura potwierdzania pełnomocnictw polega na:

weryfikacji autentyczności dostarczonego wniosku,

na sprawdzeniu zgodności danych podmiotu prawnego umieszczonych we wniosku z dostarczonymi dokumentami,

opcjonalnie na zweryfikowaniu dowodu posiadania klucza prywatnego (jeśli wniosek dotyczy pary kluczy do realizacji podpisu) oraz poprawności nazwy DN podmiotu prawnego oraz osoby fizycznej, która może podejmować działania w imieniu tego podmiotu,

zażądaniu dostarczenia dokumentu, wystawionego przez przynajmniej jednego członka zarządu, potwierdzającego pełnomocnictwa osoby fizycznej; dokument musi być poświadczony notarialnie,

kontakcie z bezpośrednim przełożonym osoby fizycznej i uzyskaniu potwierdzenia prawdziwości przekazanych jej pełnomocnictw.

3.2. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy, recertyfikacji lub modyfikacji certyfikatu

Uwierzytelnienie tożsamości subskrybentów, którzy złożyli wniosek o aktualizację kluczy, recertyfikację lub modyfikację certyfikatu musi być realizowane przez operatora urzędu rejestracji w następujących przypadkach:

wniosek został uwierzytelniony jedynie przy pomocy hasła,

modyfikacji uległy dane zawarte w wystawionym certyfikacie,

na każde żądanie operatora urzędu certyfikacji,

dotyczy certyfikacji kluczy, której wynikiem ma być certyfikat wydany po raz pierwszy danemu subskrybentowi według nowej polityki certyfikacji.

Subskrybenci przesyłający wnioski bezpośrednio do urzędu certyfikacji są uwierzytelniani przez ten urząd jedynie na podstawie autentyczności podpisu cyfrowego i związanego z nim certyfikatu klucza publicznego.

3.2.1. Aktualizacja kluczy

Aktualizacja kluczy może być realizowana przez subskrybenta okresowo, w oparciu o parametry wskazanego certyfikatu, będącego już w posiadaniu subskrybenta. W efekcie aktualizacji kluczy tworzony jest nowy certyfikat, którego parametry są takie same jak wskazanego we wniosku certyfikatu, poza zawartym w nim nowym kluczem publicznym, numerem seryjnym certyfikatu i innym okresem jego ważności (szczegóły patrz rozdz.4.7).

Weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest zgodnie z wymaganiami określonymi w Tab.3.3.

Tab.3.3 Wymagania nakładane na weryfikację tożsamości subskrybenta w przypadku aktualizacji kluczy podpisujących i szyfrujących

Nazwa polityki certyfikacji	Opis wymagania
Certum Level I	Subskrybent może potwierdzić swoją tożsamość uwierzytelniając się wzajemnie bezpośrednio z urzędem certyfikacji, np. przy użyciu protokołu TLS/SSL. W tym przypadku musi posiadać ważny certyfikat i klucz prywatny komplementarny z zawartym w certyfikacie kluczem publicznym.
Certum Level II	Uwierzytelnianie może przebiegać podobnie, jak w przypadku certyfikatów Certum Level I, z tym jednak zastrzeżeniem, że tożsamość subskrybenta musi być zweryfikowana zgodnie z procedurą stosowaną podczas rejestracji początkowej (patrz rozdz.3.1) przynajmniej raz na 5 lat od daty poprzedniego uwierzytelnienia realizowanego wg tej procedury.
Certum Level III	Uwierzytelnianie może przebiegać podobnie, jak w przypadku certyfikatów Certum Level I, z tym jednak zastrzeżeniem, że tożsamość subskrybenta musi być zweryfikowana zgodnie z procedurą stosowaną podczas rejestracji początkowej (patrz rozdz.3.1) przynajmniej raz na 5 lat od daty poprzedniego uwierzytelnienia realizowanego wg tej procedury.
Certum Level IV	Uwierzytelnianie może przebiegać podobnie, jak w przypadku certyfikatów Certum Level I, z tym jednak zastrzeżeniem, że tożsamość subskrybenta musi być zweryfikowana zgodnie z procedurą stosowaną podczas rejestracji początkowej (patrz rozdz.3.1) przynajmniej raz na 4 lata od daty poprzedniego uwierzytelnienia realizowanego wg tej procedury.

3.2.2. Recertyfikacja

Subskrybenci lub urzędy certyfikacji korzystają z recertyfikacji w przypadku, gdy posiadają już certyfikat i komplementarny z nim klucz prywatny, i chcą nadal korzystać z tej samej pary kluczy. Nowy certyfikat utworzony w wyniku recertyfikacji posiada ten sam klucz publiczny, tą

samą nazwę podmiotu certyfikatu oraz inne informacje z poprzedniego certyfikatu, ale nowy okres ważności, numer seryjny i nowy podpis wystawcy certyfikatu (szczegóły patrz rozdz.4.6).

Recertyfikacji podlegają tylko te certyfikaty, których okres ważności jeszcze nie minął, nie zostały unieważnione oraz zmianie nie uległa nazwa i inne atrybuty podmiotu certyfikatu.

Każde żądanie recertyfikacji klucza obsługiwane jest w trybie *off-line*, tzn. wymaga ręcznego zaakceptowania przez operatora urzędu certyfikacji.

Aktualnie, w celu zapewnienia unikalności podpisu cyfrowego i maksimum bezpieczeństwa Unizeto CERTUM - CPP nie recertyfikuje drugi raz tej samej pary kluczy, należącej do subskrybenta. Ograniczenie to nie dotyczy recertyfikowania kluczy urzędów certyfikacji (patrz rozdz.6.1.1.4).

3.2.3. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza utworzenie nowego certyfikatu na podstawie certyfikatu, który jest aktualnie w posiadaniu subskrybenta. Nowy certyfikat posiada inny klucz publiczny, nowy numer seryjny, ale w porównaniu z certyfikatem na podstawie którego jest wystawiany, różni się przynajmniej jednym polem (jego zawartością lub wystąpieniem całkiem nowego pola).

Potrzeba modyfikacji może wystąpić np. w przypadku zmiany stanowiska w pracy lub zmiany nazwiska pod warunkiem, że dane te zostały poprzednio umieszczone w certyfikacie lub powinny zostać dodane. Jeśli zmianie uległy dane, które zgodnie z procedurami uwierzytelniania subskrybneta są weryfikowane na podstawie odpowiednich dokumentów, np. zaświadczenia z pracy o zajmowanym stanowisku, to każdy taki wniosek musi być potwierdzony w urzędzie rejestracji (szczegóły patrz rozdz.4.8).

Modyfikacji podlegają tylko te certyfikaty, których okres ważności jeszcze nie minął, nie zostały unieważnione oraz zmianie nie uległa nazwa i inne atrybuty subskrybenta.

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy po unieważnieniu

Jeśli subskrybent w wyniku unieważnienia certyfikatu nie posiada aktywnego w ramach danej polityki certyfikacji klucza podpisującego, a następnie złoży wniosek o aktualizację, to wniosek ten musi uzyskać potwierdzenie wystawione przez operatora urzędu rejestracji. Identyfikacja i uwierzytelnienie subskrybenta przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz.3.1).

Każdy następny wniosek o recertyfikację, modyfikację lub aktualizację kluczy obsługiwany jest standardowo (patrz rozdz.4.7).

3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie mogą być składane drogą elektroniczną bezpośrednio do właściwego wystawcy certyfikatu lub pośrednio za pośrednictwem urzędu rejestracji. Możliwe jest także posłużenie się wnioskiem nieelektronicznym.

W przypadku pierwszej z dróg postępowania subskrybent musi złożyć uwierzytelniony wniosek o unieważnienie certyfikatu. Uwierzytelnienie wniosku przez subskrybenta polega na złożeniu pod nim podpisu cyfrowego.

Procedurze postępowania zgodnej z przypadkiem drugim powinien poddać się subskrybent, który jednocześnie zgubił (został mu skradziony, itp.) aktywny klucz prywatny oraz sekret unieważniania certyfikatów. Wniosek o unieważnienie musi zostać poświadczony przez urząd rejestracji. Poświadczenie to nie musi mieć postaci elektronicznej.

W obu powyższych przypadkach składany wniosek musi umożliwić jednoznaczną identyfikację tożsamości subskrybenta. Wniosek o unieważnienie może dotyczyć więcej niż jednego certyfikatu.

Identyfikacja i uwierzytelnienie subskrybenta w urzędzie rejestracji przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz.3.1). Uwierzytelnienie subskrybenta w urzędzie certyfikacji polega na zweryfikowaniu autentyczności uwierzytelnienia wniosku.

Dokładny opis procedury unieważniania certyfikatów został zawarty w pkt. 4.9.3.

4.Wymagania funkcjonalne

Poniżej przedstawiono podstawowe procedury certyfikacji. Każda z procedur rozpoczyna się od złożenia przez subskrybenta stosownego wniosku pośrednio (po ewentualnym potwierdzeniu go przez urząd rejestracji) lub bezpośrednio w urzędzie certyfikacji. Na jego podstawie urząd certyfikacji podejmuje odpowiednią decyzję, realizując żądaną usługę lub odmawiając jej realizacji. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania subskrybenta.

Unizeto CERTUM - CCP udostępnia następujące podstawowe usługi: rejestracja, certyfikacja, recertyfikacja, aktualizacja kluczy, modyfikacja certyfikatu oraz unieważnienie lub zawieszenie certyfikatu.

Jeśli składany wniosek zawiera klucz publiczny, to musi być on przygotowany w sposób, który - niezależnie od stosowanej polityki certyfikacji – wiąże kryptograficznie klucz publiczny z innymi danymi zawartymi we wniosku, w tym w szczególności z danymi identyfikacyjnymi subskrybenta.

Wniosek w miejsce klucza publicznego może zawierać żądanie subskrybenta wygenerowania w jego imieniu klucza asymetrycznego. Może to być realizowane w urzędzie rejestracji lub urzędzie certyfikacji. Po wygenerowaniu klucze są w sposób bezpieczny przekazywane subskrybentowi przy zachowaniu zasady, że klucze te nie mogą być uaktywnione przez nieuprawnioną do tego osobę.

4.1. Składanie wniosków

Wnioski kierowane do jednego z urzędów certyfikacji mogą być składane zarówno przez subskrybenta, jak też operatora urzędu rejestracji.

Wnioski subskrybenta są składane bezpośrednio do urzędu certyfikacji lub pośrednio przy udziale urzędu rejestracji. Wnioski składane bezpośrednio mogą dotyczyć: certyfikacji, recertyfikacji, aktualizacji kluczy oraz unieważnienia lub zawieszenia certyfikatu. Z kolei pośrednio mogą być składane przede wszystkim wnioski o rejestrację i modyfikację certyfikatu, chociaż nie zabrania się w tym przypadku także innych wniosków związanych z pozostałymi usługami certyfikacyjnymi, świadczonymi przez określony urząd certyfikacji.

Operator urzędu rejestracji występuje w podwójnej roli: roli subskrybenta oraz osoby upoważnionej do reprezentowania urzędu certyfikacji. W tej pierwszej roli operator może składać takie same wnioski jak każdy inny subskrybent. Z kolei w roli drugiej może składać w urzędzie certyfikacji potwierdzone przez siebie wnioski innych subskrybentów oraz w uzasadnionych przypadkach wnioski o unieważnienie lub zawieszenie certyfikatów subskrybentów, którzy w rażący sposób naruszają niniejszy Kodeks Postępowania Certyfikacyjnego.

Wnioski dostarczane są za pośrednictwem protokołów sieciowych takich HTTP, S/MIME lub TCP/IP.

Unizeto CERTUM - CCP wydaje certyfikaty jedynie na podstawie złożonego wniosku o rejestrację, recertyfikację, aktualizację kluczy lub modyfikację certyfikatu.

Wnioski mogą być składane przez różne podmioty i na certyfikaty, których zastosowanie jest uzależnione od potrzeb tych pomiotów:

certyfikaty osób fizycznych – wydawane po uprzednim złożeniu wniosku,

certyfikaty osób fizycznych – wydawane przed złożeniem wniosku w przypadku, gdy urząd certyfikacji lub urząd rejestracji generuje parę kluczy i certyfikat, a następnie dostarcza je osobie fizycznej na identyfikacyjnej karcie elektronicznej lub innym tokenie,

certyfikaty osób fizycznych – wydawane na wniosek składany przez pośrednika w imieniu osób fizycznych,

certyfikaty osób fizycznych – wydawane na wniosek składany przez pośredników lub pracowników w imieniu organizacji, która przekazała im odpowiednie uprawnienia w tym zakresie,

certyfikaty osób prawnych – podmiotem certyfikatu jest osoba prawna, np. organizacja, przy ograniczeniu, że klucz prywatny jest pod ochroną i może być używany tylko przez uprawnionego przedstawiciela,

certyfikaty urządzeń (np. serwerów) lub aplikacji pod opieką osób fizycznych, będących osobami prywatnymi, pośrednikami lub pracownikami organizacji i uprawnionymi do korzystania z tego urządzenia lub aplikacji.

4.1.1. Wniosek o rejestrację

Wniosek o rejestrację składany jest przez subskrybenta pośrednio w urzędzie rejestracji lub bezpośrednio w urzędzie certyfikacji i zawiera jako minimum informacje przedstawione poniżej:

nazwa pełna instytucji lub nazwisko, pierwsze imię, drugie imię subskrybenta,

nazwę wyróżnioną DN, której struktura zależy od kategorii subskrybenta (patrz rozdz.3.1.2),

identyfikatory NIP lub REGON/PESEL,

adres siedziby lub adres zamieszkania subskrybenta (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu),

wnioskowany typ certyfikatu,

identyfikator polityki certyfikacji, według której ma zostać wystawiony certyfikat,

adres poczty elektronicznej (e-mail),

klucz publiczny, który ma być poddany certyfikacji.

W przypadku gdy zawarty we wniosku klucz publiczny jest kluczem do weryfikacji podpisu, wniosek musi zawierać także dowód posiadania klucza prywatnego.

Po uwierzytelnieniu tożsamości subskrybenta (patrz rozdz.3.1.8 i rozdz.3.1.9), składającego wniosek o rejestrację oraz otrzymaniu potwierdzenia wystawionego przez urząd rejestracji wniosek jest przesyłany przez ten urząd do urzędu certyfikacji.

4.1.2. Wniosek o recertyfikację, aktualizację kluczy lub modyfikację certyfikatu

Wniosek należący do tej grupy wniosków składany jest przez subskrybenta w urzędzie rejestracji lub bezpośrednio w urzędzie certyfikacji. W urzędzie rejestracji wniosek składany jest w następujących przypadkach:

bezpośrednio po unieważnieniu jakiegokolwiek certyfikatu,

ubieganiu się o certyfikat, który ma być wystawiany zgodnie z inną polityką certyfikacji niż certyfikaty będące aktualnie w posiadaniu subskrybenta,

braku aktualnie ważnego klucza prywatnego do realizacji podpisu cyfrowego,

na wyraźne żądanie operatora urzędu certyfikacji.

W przypadku gdy nie jest spełniony żaden z powyższych warunków, subskrybent może przekazać wniosek bezpośrednio do urzędu certyfikacji. Nie jest jednak zabronione przekazanie wniosku do urzędu rejestracji.

Wniosek o certyfikację, aktualizację kluczy lub certyfikatu musi zawierać przynajmniej:

nazwę wyróżnioną DN wnioskodawcy (subskrybenta),

wnioskowany typ certyfikatu,

identyfikator polityki certyfikacji według której ma zostać wystawiony certyfikat,

klucz publiczny (poprzednio używany w przypadku recertyfikacji i modyfikacji certyfikatu lub nowy w przypadku aktualizacji kluczy), który ma być poddany certyfikacji.

Część lub całość danych zawartych w powyższym wniosku musi być uwierzytelniona przy zastosowaniu podpisu cyfrowego, jeśli tylko subskrybent posiada aktualnie ważny klucz prywatny do realizacji podpisu. W przypadku gdy zawarty we wniosku klucz publiczny jest kluczem do weryfikacji podpisu, wniosek musi zawierać także dowód posiadania klucza prywatnego.

4.1.3. Wniosek o unieważnienie lub zawieszenie

Wniosek o unieważnienie certyfikatu składany jest przez subskrybenta w urzędzie rejestracji lub bezpośrednio w urzędzie certyfikacji. W urzędzie rejestracji wniosek składany jest w następujących przypadkach:

braku aktualnie ważnego klucza prywatnego do realizacji podpisu cyfrowego,

na wyraźne żądanie operatora urzędu certyfikacji.

W przypadku, gdy nie jest spełniony żaden z powyższych warunków, subskrybent może przekazać wniosek bezpośrednio do urzędu certyfikacji. Nie jest jednak zabronione przekazanie wniosku do urzędu rejestracji.

Informacje podawane we wniosku o unieważnienie lub zawieszenie certyfikatu:

nazwa wyróżniona DN wnioskodawcy (subskrybenta),

lista certyfikatów do unieważnienia lub zawieszenia, zawierająca pary: numer seryjny certyfikatu, przyczyna unieważnienia.

Część lub całość danych zawartych w powyższym wniosku musi być uwierzytelniona przy zastosowaniu podpisu cyfrowego, jeśli tylko subskrybent posiada aktualnie ważny klucz prywatny do realizacji podpisu.

Wniosek o unieważnienie może być przekazany w postaci elektronicznej z uwierzytelnieniem, w postaci papierowej (faks, list, itp.) lub ustnej (telefon). W dwóch ostatnich przypadkach certyfikat jest zawieszany do momentu zweryfikowania zgłoszonego żądania. Unizeto CERTUM - CCP nie zawiesza certyfikatów w systemach otwartych. Zawieszenia certyfikatów można dokonywać jedynie w zamkniętych systemach korporacyjnych afiliowanych przy Unizeto CERTUM - CCP.

W momencie unieważnienia certyfikatu, automatycznie o tym fakcie są informowani operatorzy urzędów rejestracji oraz zainteresowani subskrybenci (via Email).

4.2. Przetwarzanie wniosków

Unizeto CERTUM - CCP przyjmuje wnioski certyfikacyjne składane zarówno indywidualne jak i hurtowo. Wnioski mogą być składane w trybie *on-line* lub trybie *off-line*.

Tryb *on-line* realizowany jest za pośrednictwem stron WWW serwera Unizeto CERTUM - CCP o adresie https://www.certum.pl. Subskrybent po odwiedzeniu odpowiedniej strony wypełnia – zgodnie z zawartymi tam instrukcjami – właściwy formularz wniosku certyfikacyjnego i wysyła go do urzędu certyfikacji. W przypadku wniosków dotyczących certyfikatów Certum Level I wniosek przetwarzany jest najczęściej automatycznie, zaś w pozostałych przypadkach ręcznie, jeśli wniosek wymaga porównania zawartych w nim danych z dokumentami zawarcia umowy na świadczenie usług certyfikacyjnych (dotyczy tylko wniosków o rejestrację) – lub automatycznie, jeśli wystarczy porównanie z bazami danych Unizeto CERTUM - CCP.

Złożenie wniosku w trybie *off-line* wymaga:

osobistego stawienia się subskrybenta lub uprawnionego przedstawiciela organizacji w urzędzie rejestracji lub urzędzie certyfikacji, wypełnienia i odręcznego podpisania wniosku, podpisania umowy na świadczenie usług certyfikacyjnych oraz wygenerowania identyfikatora i hasła, przy pomocy którego wnioskodawca będzie mógł pobrać certyfikat za pośrednictwem strony WWW (dwie ostatnie czynności dotyczą tylko wniosków o rejestrację) lub wygenerowania numeru PIN, który chroni dostęp do karty elektronicznej zawierającej klucze i certyfikat,

przysłania wniosku papierowego pocztą wraz kopiami dokumentów (w tym także potwierdzonych notarialnie), niezbędnych do weryfikacji tożsamości wnioskodawcy; po pozytywnej weryfikacji generowany jest identyfikator i hasło, przy pomocy którego wnioskodawca będzie mógł pobrać certyfikat za pośrednictwem strony WWW (dotyczy tylko wniosków o rejestrację) lub wygenerowania numeru PIN, który chroni dostęp do karty elektronicznej zawierającej klucze i certyfikat; identyfikator i hasło lub karta odsyłane są zwrotnie do wnioskodawcy (PIN przekazywany jest oddzielnie).

W trybie *off-line* mogą być składane także wnioski hurtowe. Wnioski takie są potwierdzane przez operatora urzędu certyfikacji lub urzędu rejestracji i przetwarzane grupowo.

Każdy wniosek certyfikacyjny w trybie *on-line* przesyłany jest do:

skrzynki poświadczania żądań, jeśli wniosek wymaga wystawienia potwierdzenia przez urząd rejestracji,

skrzynki żądań, jeśli wniosek nie wymaga wystawienia potwierdzenia przez urząd rejestracji.

Obie skrzynki są pod pełną kontrolą urzędu certyfikacji. Co więcej, jeśli operator urzędu certyfikacji uzna, że złożony w skrzynce żądań wniosek wymaga uzyskania przez subskrybenta potwierdzenia w urzędzie rejestracji, to wniosek ten zostanie przesunięty do skrzynki poświadczania żądań. O fakcie tym subskrybent zostanie poinformowany przy pomocy poczty elektronicznej.

Wnioski zgłaszane w trybie *off-line*, po ich pozytywnym zweryfikowaniu przez operatora urzędu rejestracji lub operatora certyfikacji, przekazywane są zawsze do **skrzynki żądań**.

4.2.1.1. Przetwarzanie wniosków w urzędzie rejestracji

Każdy wniosek, który został skierowany do skrzynki poświadczania żądań lub złożony w urzędzie rejestracji w postaci papierowej przetwarzany jest (jeśli jest to wymagane przez politykę certyfikacji, to w obecności wnioskodawcy) następująco:

operator urzędu pobiera wniosek subskrybenta (papierowy lub elektroniczny ze skrzynki poświadczania żądań),

weryfikuje zawarte w nim dane, m.in. dane osobowe subskrybenta (patrz procedura identyfikacji i uwierzytelnienia subskrybenta opisana w rozdz.3.1.8) oraz jeśli występuje, to sprawdza także dowód posiadania klucza prywatnego (rozdz.3.1.9),

jeśli weryfikacja wniosku przebiegnie pozytywnie, to operator poświadcza (podpisuje) żądanie; jeśli oryginalny wniosek zawiera błędne dane, to wniosek jest odrzucany,

poświadczony wniosek przesyłany jest do skrzynki żądań urzędu certyfikacji,

w urzędzie rejestracji weryfikowane są także inne dane, które nie wchodzą w skład wniosku, a które wymagane są przez Unizeto CERTUM - CCP do prowadzenia działalności biznesowej.

4.2.1.2. Przetwarzanie wniosków w urzędzie certyfikacji

Urząd certyfikacji pobiera wnioski ze skrzynki żądań. Wnioski te mogą zawierać poświadczenia wystawione przez urząd rejestracji. Jeśli wniosek nie zawiera poświadczenia, to urząd certyfikacji:

wiąże wniosek z bazą danych zarejestrowanych subskrybentów,

weryfikuje uwierzytelnienia wniosku (podpis cyfrowy lub kod uwierzytelniający),

weryfikuje formalną poprawność wniosku (składni i zawartości),

sprawdza czy subskrybent jest uprawniony do wystawienia przysłanego typu wniosku oraz zawartej w nim treści,

wszystkie czynności odnotowuje w bazie danych i dziennikach czynności.

Jeśli wniosek zawiera poświadczenie, to urząd certyfikacji w pierwszej kolejności sprawdza czy poświadczenie zostało wystawione przez uprawniony do tego urząd rejestracji. Jeśli tak, to dalsze przetwarzanie przebiega podobnie jak w przypadku przetwarzania wniosku bez poświadczenia. Dodatkowo, jeśli wniosek zawiera żądanie wystawienia certyfikatu do weryfikacji podpisów, to urząd certyfikacji sprawdza przedstawiony przez subskrybenta dowód posiadania klucza prywatnego.

4.3. Wydanie certyfikatu

Urząd certyfikacji, po otrzymaniu odpowiedniego wniosku oraz po pomyślnym przetworzeniu go (patrz rozdz.4.1.4.2), **wydaje certyfikat**. Certyfikat uważa się za ważny (o statusie aktywny lub gotowy) od momentu zaakceptowania go przez subskrybenta (patrz rozdz.4.3). Okresy ważności wydawanego certyfikatu zależą od typu certyfikatu oraz kategorii subskrybenta i są zgodne z okresami podanymi w Tab.6.6.

Każdy certyfikat wystawiany jest w trybie on-line. Procedura wystawiania przebiega następująco:

przetworzony wniosek subskrybenta przesyłany jest na serwer wystawiania certyfikatów,

jeśli wniosek zawiera żądanie wygenerowania pary kluczy, to serwer zleca to zadanie sprzętowemu generatorowi kluczy spełniającemu wymagania minimum FIPS-140 Level 2,

testowana jest jakość dostarczonych lub wygenerowanych przez urząd certyfikacji kluczy publicznych,

w przypadku pomyślnego zakończenia wszystkich procedur, serwer wystawia certyfikat i zleca jego podpisanie sprzętowemu modułowi kryptograficznemu; certyfikat zapisywany jest bazach danych urzędu certyfikacji,

urząd certyfikacji przygotowuje odpowiedź, zawierającą wydany certyfikat (jeśli został wystawiony) i wysyła go subskrybentowi; certyfikat nie jest publikowany w repozytorium (nawet jeśli subskrybent wyraził na to zgodę) do czasu otrzymania od subskrybenta potwierdzenia akceptacji certyfikatu (rozdz.4.4).

Serwer, na żądanie operatora urzędu certyfikacji, może wysłać wezwanie potwierdzenia rozpatrywanego wniosku. W takim przypadku:

przekierowuje wniosek do skrzynki poświadczania żądań,

wysyła do wnioskodawcy (via e-mail) informację o konieczności uzyskania potwierdzenia wniosku w jednym ze wskazanych urzędów rejestracji.

Urząd certyfikacji Unizeto CERTUM - CCP stosuje dwa podstawowe mechanizmy informowania subskrybenta o wydaniu mu certyfikatu. Pierwszy wykorzystuje pocztę elektroniczną lub pocztę zwykłą i polega na wysłaniu pod wskazany adres (e-mail lub korespondencyjny) informacji, która umożliwi subskrybentowi pobranie certyfikatu. Mechanizm ten wykorzystywany jest także w przypadku konieczności poinformowania wszystkich subskrybentów danego urzędu certyfikacji o wydaniu temu urzędowi nowego certyfikatu lub części subskrybentów w przypadku wydania nowego certyfikatu np. na serwer organizacji, której są pracownikami.

Drugi z mechanizmów polega na wydaniu certyfikatu i po zapisaniu go (zwykle razem, gdzie znajduje się klucz prywatny) na identyfikacyjnej karcie elektronicznej i przesłaniu zwykłą pocztą na adres subskrybenta (PIN przesyłany jest w oddzielnej kopercie). Fakt wydania identyfikacyjnej karty elektronicznej subskrybentowi jest odnotowywany w bazie danych urzędu certyfikacji.

Szczegółowe procedury zarządzania identyfikacyjnymi kartami elektronicznymi opisane są w dokumencie „Księga Urzędu Rejestracji". Dokument ma status „niejawny" i udostępniany jest tylko upoważnionemu do tego personelowi oraz audytorom.

Każdy wydany certyfikat publikowany jest w repozytorium Unizeto CERTUM - CCP. Opublikowanie certyfikatu jest równoważne zawiadomieniu innych stron ufających, że urząd wydał certyfikat subskrybentowi, który jako właściciel tego certyfikatu może być od tej chwili autoryzowany w roli strony ufającej.

Unizeto CERTUM - CCP publikuje certyfikat w repozytorium dopiero po zaakceptowaniu certyfikatu przez subskrybenta (patrz rozdz.4.3).

4.3.1. Okres oczekiwania na wydanie certyfikatu

Urząd certyfikacji powinien dołożyć wszelkich starań, aby od momentu otrzymania wniosku o rejestrację i certyfikację, certyfikację lub aktualizację (kluczy lub certyfikatu) przeprowadzić jego weryfikację oraz wydać certyfikat w czasie nie dłuższym niż ten, który podano w Tab.4.1.

Tab.4.1 Maksymalne okresy oczekiwania na wydanie certyfikatu

Poziom wiarygodności certyfikatu	Okres oczekiwania
Certum Level I	7 dni
Certum Level II	7 dni
Certum Level III	7 dni
Certum Level IV	7 dni

Podane okresy zależą głównie od dokładności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy Unizeto CERTUM - CCP a wnioskodawcą.

4.3.2. Odmowa wydania certyfikatu

Unizeto CERTUM - CCP może odmówić wydania certyfikatu dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą wskutek poniesionych przez wnioskodawcę (w wyniku odmowy) strat lub kosztów. Urząd certyfikacji powinien niezwłocznie zwrócić wnioskodawcy wniesioną przez niego opłatę za wydanie certyfikatu (jeśli dokonał stosownej przedpłaty), chyba że wnioskodawca we wniosku o wydanie certyfikatu dostarczył do urzędu rejestracji/certyfikacji sfałszowane lub nieprawdziwe dane.

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

identyfikator subskrybenta (nazwa **DN**) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,

istnieje podejrzenie lub pewność, że subskrybent sfałszował lub podał nieprawdziwe dane,

subskrybent w sposób szczególnie uciążliwy dla Unizeto CERTUM - CCP angażuje jego zasoby oraz moce obliczeniowe, np. wysyłając zbyt dużą jak na jego potrzeby liczbę wniosków,

z innych nie wymienionych powyżej przyczyn.

Informacja o odmowie wydania certyfikatu przesyłana jest wnioskodawcy w postaci odpowiedniej decyzji z krótkim uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do Unizeto CERTUM - CCP w terminie 14 dni od daty otrzymania decyzji.

4.4. Akceptacja certyfikatu

Po otrzymaniu certyfikatu subskrybent zobowiązany jest do sprawdzenia jego zawartości, w tym w szczególności poprawności zawartych w nim danych oraz komplementarności klucza publicznego z posiadanym kluczem prywatnym. Jeśli certyfikat zawiera jakiekolwiek wady, które nie mogą być zaakceptowane przez subskrybenta, to certyfikat powinien być natychmiast

unieważniony (jest to równoznaczne z jawnie wyrażonym przez subskrybenta brakiem akceptacji certyfikatu).

Akceptacja certyfikatu oznacza wystąpienie w ciągu 7 dniu od daty otrzymania certyfikatu jednego z poniższych zdarzeń:

- podanie PIN-u, dzięki któremu następuje instalacja certyfikatu za pośrednictwem strony WWW (https://www.certum.pl/install),
- odebranie przesyłki poleconej zawierającej certyfikat i wysłanej przez Unizeto CERTUM,
- brak pisemnej odmowy, potwierdzonej notarialnie, akceptacji certyfikatu po otrzymaniu go przez subskrybenta w ciągu 7 dni od daty otrzymania certyfikatu lub PIN-u umożliwiającego jego instalację.

Jeśli certyfikat nie zostanie w sposób jawny odrzucony w ciągu 7 dni od daty jego otrzymania, to uznawany jest za zaakceptowany.

Każdy zaakceptowany certyfikat jest publikowany w repozytorium Unizeto CERTUM - CCP i publicznie dostępny.

Akceptacja certyfikatu jest także jednoznaczna z oświadczeniem subskrybenta, że zanim użył certyfikatu w dowolnej operacji kryptograficznej, dokładnie zapoznał się z treścią umowy z Unizeto CERTUM - CCP zawartej w trakcie procedury rejestracji w urzędzie rejestracji. W przypadku składania wniosku elektronicznie, subskrybent automatycznie akceptuje przyszły certyfikat klucza publicznego w momencie złożenia wniosku o jego wydanie.

Akceptując certyfikat subskrybent zgadza się na zasady zawarte w Kodeksie Postępowania Certyfikacyjnego jak i Polityce Certyfikacji oraz przestrzeganie treści umowy zawartej z Unizeto CERTUM - CCP.

Strona ufająca może zawsze zweryfikować, czy certyfikat komplementarny z kluczem prywatnym przy pomocy którego został podpisany dokument został zaakceptowany przez wystawcę tego dokumentu (patrz rozdz.4.9.11).

4.5. Stosowanie kluczy oraz certyfikatów

Subskrybenci, w tym operatorzy urzędów rejestracji muszą używać kluczy prywatnych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.4.3),
- zgodnie z treścią umowy zawartej pomiędzy subskrybentem a Unizeto CERTUM - CCP,
- tylko w okresie ich ważności (nie dotyczy to certyfikatów do weryfikacji podpisów cyfrowych),
- tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego, w tym w szczególności do realizacji podpisu.

Z kolei strony ufające, w tym operatorzy urzędów rejestracji muszą używać kluczy publicznych i certyfikatów:

zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.4.3),

zgodnie z treścią umowy zawartej pomiędzy stroną ufającą a Unizeto CERTUM - CCP,

tylko po zweryfikowaniu ich statusu (patrz rozdz.4.9) oraz wiarygodności podpisu urzędu certyfikacji, który wystawił certyfikat,

w przypadku klucza publicznego do wymiany kluczy, szyfrowania danych lub uzgadniania kluczy tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu strona ufająca także nie może używać tego typu kluczy publicznych.

4.6. Recertyfikacja

Unizeto CERTUM - CCP świadczy usługę recertyfikacji tej samej pary kluczy kryptograficznych tylko w przypadku urzędów certyfikacji. Jeśli procedura recertyfikacji zakończy się pomyślnie, to certyfikat, który był przedmiotem aktualizacji nie jest unieważniany.

4.7. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy ma miejsce zawsze wtedy, gdy subskrybent (już zarejestrowany) wygeneruje nową parę kluczy (lub zleci to urzędowi certyfikacji) i zażąda wystawienia nowego certyfikatu potwierdzającego przynależność do niego nowego klucza publicznego. Certyfikację i aktualizację kluczy należy interpretować następująco:

certyfikacja kluczy nie jest związana z żadnym ważnym certyfikatem i jest stosowna przez subskrybentów wtedy, gdy zachodzi potrzeba uzyskania jednego lub więcej (zwykle dodatkowych) certyfikatów dowolnego typu, niekoniecznie wystawionych w ramach tej samej polityki certyfikacji,

aktualizacja kluczy dotyczy zawsze ściśle określonego, wskazanego we wniosku certyfikatu; z tego powodu nowy certyfikat posiada identyczną treść jak związany z nim certyfikat; jedyne różnice to: nowy klucz publiczny, nowy numer seryjny certyfikatu, nowy okres ważności certyfikatu oraz nowy podpis urzędu certyfikacji.

Wniosek o aktualizację kluczy złożony przez subskrybenta może dotyczyć tylko:

certyfikatu który nie został wcześniej unieważniony,

przypadku, gdy subskrybent posiada aktualny i ważny klucz prywatny do realizacji podpisów.

Z kolei certyfikacja kluczy może dotyczyć także sytuacji, gdy subskrybent:

nie posiada aktualnego i ważnego klucza prywatnego do realizacji podpisów;

chce uzyskać dodatkowy certyfikat tego samego lub innego typu, ale tylko w ramach polityki certyfikacji, zgodnie z którą został mu wydany przynajmniej jeden certyfikat i który jest nadal ważny;

subskrybent nie posiada żadnego ważnego certyfikatu wystawionego według jednej z polityk zdefiniowanych w niniejszym Kodeksie Postępowania Certyfikacyjnego.

Certyfikacja lub aktualizacja kluczy odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem odpowiedniego wniosku.

Wniosek o aktualizację kluczy nie musi być potwierdzany przez urząd rejestracji – subskrybent może go przesłać bezpośrednio do skrzynki żądań. Jednak w przypadkach, gdy:

zażąda tego operator urzędu certyfikacji,

subskrybent nie posiada aktualnego i ważnego klucza prywatnego do podpisania wniosku,

wówczas wniosek o aktualizację musi być potwierdzony przez urząd rejestracji. Wymaga to wizyty subskrybenta w urzędzie rejestracji i poddania się procedurze identyfikacji i uwierzytelnienia (rozdz.3.1).

Wniosek o certyfikację kluczy musi być zawsze potwierdzany w przypadkach, gdy:

zażąda tego operator urzędu certyfikacji,

subskrybent nie posiada aktualnego i ważnego klucza prywatnego do podpisania wniosku,

wniosek został uwierzytelniony przy pomocy klucza uwierzytelniającego (sekretu),

dotyczy polityki certyfikacji, w ramach której subskrybent nie posiada żadnego ważnego certyfikatu.

W pozostałych przypadkach wniosek o certyfikację kluczy, po podpisaniu przez subskrybenta, może być bezpośrednio przesłany do urzędu certyfikacji.

Procedura przetwarzania wniosku o aktualizację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.1, zaś procedura wydawania certyfikatu taka jak w rozdz.4.2. W wyniku realizacji tej ostatniej procedury:

subskrybent jest powiadamiany o wystawieniu nowego certyfikatu o nowym numerze seryjnym,

subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,

nowy certyfikat jest publikowany w repozytorium.

Unizeto CERTUM - Centrum Certyfikacji Powszechne informuje zawsze subskrybenta (co najmniej 7 dni wcześniej) o zbliżaniu się daty utraty ważności certyfikatu.

Procedurze certyfikacji i aktualizacji klucza mogą podlegać także certyfikaty urzędów certyfikacji. W tym jednak przypadku o zajściu takiego faktu muszą zostać poinformowani wszyscy klienci urzędu certyfikacji.

Unizeto CERTUM - Centrum Certyfikacji Powszechne informuje zawsze subskrybenta (co najmniej 7 dni wcześniej) o zbliżaniu się daty utraty ważności certyfikatu. Informacja taka przesyłana jest także w przypadku certyfikatów urzędów certyfikacji.

4.8. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza zastąpienie używanego (**aktualnie ważnego**) certyfikatu nowym certyfikatem, w którym - w stosunku do zastępowanego certyfikatu - zmianie mogą ulec niektóre zawarte w nim informacje, poza zmianą klucza publicznego.

Modyfikacja certyfikatu:

odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o modyfikację certyfikatu;

może dotyczyć certyfikat, którego okres ważności nie minął i nie został wcześniej unieważniony.

Modyfikacji mogą podlegać jedynie następujące informacje:

klucz publiczny w powiązaniu ze zmianą przynajmniej jednej z przedstawionych poniżej informacji,

nazwisko subskrybenta, np. z powodu wyjścia za mąż, rozwodu lub sądowej zmiany nazwiska,

zmiany stanowiska pracy lub jednostki organizacyjnej,

zmiana adresu poczty elektronicznej,

zapisane w certyfikacie uprawnienia lub pełnione role,

dodanie lub usunięcie rozszerzenia certyfikatu lub zmiana jego zawartości,

zdefiniowanie i dodanie nowych identyfikatorów obiektów, np. identyfikatorów polityk certyfikacji,

zmiana rodzaju zobowiązań lub ich wysokości, które może podejmować subskrybent posługujący się certyfikatem.

Procedura modyfikacji certyfikatu wymaga uwierzytelnienia wniosku przez subskrybenta przy pomocy podpisu cyfrowego. Subskrybent musi więc posiadać aktualnie ważny klucz prywatny do realizacji podpisu. Jeśli subskrybent nie posiada takiego klucza, to musi poddać się procedurze certyfikacji opisanej w rozdz.4.7.

Wniosek o modyfikację certyfikatu musi być potwierdzany przez urząd rejestracji. Wymaga to kontaktu subskrybenta z urzędem rejestracji i poddanie się procedurze identyfikacji i uwierzytelnienia (rozdz.3.18).

Procedura przetwarzania wniosku o modyfikację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.1., zaś procedura wydawania certyfikatu taka jak w rozdz.4.2. W wyniku realizacji tej ostatniej procedury:

subskrybent jest powiadamiany o wystawieniu nowego certyfikatu o nowym numerze seryjnym,

subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,

nowy certyfikat jest publikowany w repozytorium.

Jeśli procedura modyfikacji certyfikatu zakończy się pomyślnie, to certyfikat który był przedmiotem modyfikacji jest unieważniany i umieszczany na liście CRL. Jako przyczynę unieważnienia podaje się określenie ***modyfikacja***[28] *(ang. affiliationChanged) oznaczające, że (1) unieważniony certyfikat został zastąpiony innym, w którym zostały zmodyfikowane niektóre dane, np. nazwa subskrybenta, oraz (2) informujące strony ufające, że nie ma powodów aby uważać, iż klucz prywatny związany z certyfikatem został ujawniony.*

Procedurze modyfikacji mogą podlegać także certyfikaty urzędów certyfikacji. W tym jednak przypadku o zajściu takiego faktu muszą zostać poinformowani wszyscy klienci urzędu certyfikacji.

4.9. Unieważnienie i zawieszenie certyfikatu

Unieważnienie lub zawieszenie ma ściśle określony wpływ na certyfikaty oraz obowiązki posługującego się nim subskrybenta.

Zawieszenie certyfikatów praktykowane jest jedynie w zamkniętych systemach korporacyjnych afiliowanych przy Unizeto CERTUM - CCP.

W trakcie trwania zawieszenia lub natychmiast po unieważnieniu certyfikatu subskrybenta należy uznać, że certyfikat stracił ważność (jest w stanie unieważnienia). Podobnie w przypadku certyfikatów urzędów certyfikacji, anulowanie ważności tego rodzaju certyfikatu oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność certyfikatów wydanych przez tenże urząd certyfikacji w okresie, gdy jego certyfikat był ważny.

Unieważnienie lub zawieszenie certyfikatów nie ma wpływu na wcześniej zaciągnięte zobowiązania lub obowiązki wynikłe z przestrzegania niniejszego Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji.

Niniejszy rozdział określa warunki, które muszą być spełnione lub zaistnieć, aby urząd certyfikacji miał podstawy do unieważnienia lub zawieszenia certyfikatu. Mimo, iż zawieszenie certyfikatu jest szczególną formą unieważnienia, dalej będziemy rozróżniać te dwa pojęcia dla podkreślenia istotnej różnicy pomiędzy nimi: zawieszenie certyfikatu można anulować, unieważnienie - nie (tam jednak gdzie wyraźnie nie zostanie to podkreślone słowo, unieważnienie obejmować będzie także zawieszenie certyfikatu).

Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia). Na przykład, jeśli subskrybent straci kontrolę nad nośnikiem, na którym zapisana była para kluczy chronionych hasłem lub numerem PIN, to fakt taki powinien natychmiast zgłosić do urzędu certyfikacji z żądaniem zawieszenia certyfikatu. W przypadku szybkiego odnalezienia nośnika oraz pewności, że nie została naruszona ochrona klucza prywatnego, certyfikat można (na wniosek subskrybenta) odwiesić przywracając mu stan aktywności.

Jeśli klucz prywatny, odpowiadający kluczowi publicznemu, zawartemu w unieważnianym certyfikacie pozostaje w dalszym ciągu pod kontrolą subskrybenta, to powinien być przez niego nadal chroniony w sposób, który gwarantuje jego wiarygodność przez cały okres zawieszenia certyfikatu oraz przechowywania go po unieważnieniu, aż do momentu fizycznego zniszczenia.

[28] W tym przypadku domyślnie chodzi o zastąpienie certyfikatu

4.9.1. Okoliczności unieważnienia certyfikatu

Podstawową przyczyną unieważnienia certyfikatu jest fakt utraty (lub samo podejrzenie takiej utraty) kontroli nad kluczem prywatnym, będącym w posiadaniu subskrybenta certyfikatu lub też rażące naruszanie przez subskrybenta zasad Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego.

Unieważnianie certyfikatu ma miejsce w następujących okolicznościach:

zawsze wtedy, gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się,

ilekroć klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub nośnik na którym jest przechowywany jest lub istnieje uzasadnione podejrzenie, że będzie ujawniony[29]; procedura unieważniania certyfikatu jest wówczas przeprowadzana na wniosek subskrybenta,

subskrybent rezygnuje z umowy zawartej z Unizeto CERTUM - CCP (wówczas operacja ta jest ściśle związana z unieważnieniem rejestracji subskrybenta w urzędzie rejestracji); jeśli subskrybent nie wystąpi z takim wnioskiem sam, prawo takie przysługuje urzędowi certyfikacji lub przedstawicielowi instytucji, której pracownikiem jest subskrybent,

na każde żądanie subskrybenta, właściciela scertyfikowanego klucza publicznego,

przez wystawcę certyfikatu, tzn. przez Unizeto CERTUM - CCP, np. wskutek nieprzestrzegania przez subskrybenta Polityki Certyfikacji lub postanowień innych dokumentów sygnowanych przez urząd certyfikacji,

w przypadku zakończenia działalności przez urząd certyfikacji unieważnionia się wszystkie certyfikaty wydane przez ten urząd przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego urzędu certyfikacji,

subskrybent zwleka lub ignoruje płatności za usługi świadczone przez urząd certyfikacji,

klucz prywatny lub bezpieczeństwo systemu komputerowego urzędu certyfikacji zostały ujawnione w sposób, który bezpośrednio zagraża wiarygodności certyfikatów,

subskrybent, będący pracownikiem organizacji, po rozwiązaniu z nim umowy o pracę nie oddał identyfikacyjnej karty elektronicznej, na której przechowywany był certyfikat i komplementarny z nim klucz prywatny,

inne przyczyny opóźniających lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

Dodatkowo urząd certyfikacji unieważnia te zawieszone certyfikaty, których nie reaktywowano lub nie unieważniono w okresie 1 miesiąca od daty zawieszenia.

Z wnioskiem o unieważnienie można występować (patrz rozdz.3.4) za pośrednictwem urzędu rejestracji (wymaga to skontaktowania się subskrybenta z urzędem rejestracji) lub bezpośrednio do urzędu certyfikacji (wniosek może być uwierzytelniony przy pomocy podpisu).

[29] Ujawnienie klucza prywatnego oznacza: (1) nieuprawniony dostęp lub podejrzenie nieuprawnionego dostępu do klucza prywatnego, (2) zagubienie lub podejrzenie zagubienia klucza prywatnego, (3) kradzież lub podejrzenie kradzieży klucza prywatnego, (4) przypadkowe zniszczenie klucza prywatnego.

W pierwszym przypadku podpisany przez urząd rejestracji wniosek o unieważnienie certyfikatu lub dokument papierowy odsyłany jest do urzędu certyfikacji, w drugim zaś – subskrybent sam uwierzytelnia wniosek o unieważnienie i bezpośrednio wysyła go do urzędu certyfikacji.

Wniosek o unieważnienie certyfikatu powinien zawierać informacje, które umożliwią uwierzytelnienie subskrybenta w urzędzie rejestracji zgodnie z procedurą przedstawioną w rozdz.3.1.8 lub urzędzie certyfikacji na podstawie uwierzytelnienia wniosku.

Jeśli uwierzytelnienie tożsamości subskrybenta składającego wniosek nie zakończy się pomyślnie, urząd wydający certyfikaty odmawia unieważnienia certyfikatu i jedynie zawiesza go do czasu wyjaśnienia przyczyn odmowy.

4.9.2. Kto może żądać unieważnienia certyfikatu

Następujące podmioty mogą zgłaszać żądanie unieważnienia certyfikatu subskrybenta:

subskrybent będący podmiotem unieważnianego certyfikatu,

autoryzowany przedstawiciel urzędu certyfikacji (w przypadku Unizeto CERTUM - CCP rolę taką pełni administrator bezpieczeństwa),

sponsor subskrybenta[30], np. pracodawca subskrybenta; subskrybent musi być o tym fakcie niezwłocznie poinformowany,

urząd rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej unieważnienie certyfikatu.

Urzędy certyfikacji zachowują szczególną ostrożność przy rozpatrywaniu wniosków o unieważnienie certyfikatu, których autorem nie jest subskrybent i honorują tylko te, które obejmują przypadki wymienione w rozdz.4.9.1 oraz gdy ryzyko utraty zaufania do kwestionowanego certyfikatu przewyższa niedogodności oraz potencjalne straty subskrybenta, powstałe w wyniku unieważnienia.

Jeśli podmiot wnioskujący o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu (subskrybentem), to urząd certyfikacji:

musi określić i prowadzić listę podmiotów, które mogą występować z takimi wnioskami,

musi wysłać powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

Każdy wniosek może być przekazany:

bezpośrednio do urzędu certyfikacji w postaci wniosku elektronicznego z potwierdzeniem lub bez potwierdzenia urzędu rejestracji,

bezpośrednio lub pośrednio (za pośrednictwem innych urzędów rejestracji) do głównego urzędu rejestracji w postaci wniosku nieelektronicznego (dokument papierowy, faks, telefon, itp.).

4.9.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na trzy sposoby:

[30] Patrz **Słownik pojęć**

pierwszy sposób polega na przesłaniu do urzędu certyfikacji elektronicznego wniosku o unieważnienie, podpisanego aktualnym kluczem prywatnym lub autoryzowanego przy pomocy hasła; unieważnienia tego typu można dokonać jedynie na wniosek subskrybenta (dowolny podmiot, posiadacz unieważnianego certyfikatu),

drugi sposób wymaga przesłania do urzędu certyfikacji elektronicznego wniosku o unieważnienie, potwierdzonego przy pomocy podpisu cyfrowego przez urząd rejestracji; dotyczy to przypadków, gdy (a) subskrybent zgubił, został mu skradziony klucz prywatny lub nie posiada hasła, (b) unieważnienia zażądał sponsor subskrybenta, autoryzowany przedstawiciel urzędu certyfikacji lub urzędu rejestracji, jeśli tylko istnieją podstawy do zażądania unieważnienia certyfikatu subskrybenta,

trzeci sposób polega na tym, że uwierzytelniony wniosek nieelektroniczny (dokument papierowy, faks lub telefon) można przekazać do Głównego Urzędu Rejestracji; uwierzytelnienie wniosku papierowego (w tym faksu) może polegać na poświadczeniu go w dowolnym urzędzie rejestracji, np. przy pomocy stempla i podpisu odręcznego złożonego przez osobę znaną Głównemu Urzędowi Rejestracji lub umieszczeniem w dokumencie frazy, na którą odpowiedź musi znać wnioskodawca; wniosek w postaci telefonicznej zostanie przyjęty dopiero po uprzednim podaniu frazy; po zweryfikowaniu wniosku Główny Urząd Rejestracji przygotowuje elektronicznie potwierdzone żądanie unieważnienia certyfikatu i przekazuje go do urzędu certyfikacji.

W przypadku dwóch pierwszych sposobów urząd certyfikacji – po pozytywnej weryfikacji wniosku – **unieważnia** certyfikat, zaś w przypadku trzecim tylko **zawiesza** certyfikat. Informacja o unieważnionym lub zawieszonym certyfikacie umieszczana jest na liście **CRL** (patrz rozdz.7.2), wydawanej przez urząd certyfikacji.

Urząd certyfikacji przekazuje stronie ubiegającej się o unieważnienie certyfikatu potwierdzenie unieważnienia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy.

Każdy wniosek o unieważnienie certyfikatu musi pozwolić na jednoznaczną identyfikację unieważnianego certyfikatu, zawierać przyczynę unieważnienia oraz być uwierzytelniony (podpisany cyfrowo lub odręcznie).

Procedura unieważnienia certyfikatu przebiega następująco:

urząd certyfikacji po otrzymaniu wniosku o unieważnienie certyfikatu sprawdza jego wiarygodność; jeśli jest to wniosek w postaci elektronicznej, weryfikowana jest poprawność certyfikatu przedstawionego do unieważnienia oraz ewentualnie dołączonego do wniosku **tokena** wydanego przez urząd rejestracji; wniosek w postaci papierowej (patrz wyżej - trzeci sposób unieważnienia lub zawieszenia certyfikatu) wymaga potwierdzenia przez źródło nadania wniosku; potwierdzenie to można uzyskać telefonicznie, faksem lub w trakcie osobistej wizyty wnioskodawcy u upoważnionego przedstawiciela urzędu certyfikacji (lub odwrotnie);

jeśli wniosek jest wiarygodny, to urząd certyfikacji umieszcza informację o unieważnionym lub zawieszonym certyfikacie na liście certyfikatów unieważnionych (CRL) wraz z informacją o przyczynie unieważnienia lub informacją o zawieszeniu certyfikatu (patrz rozdz.7.2.1);

przekazuje, drogą elektroniczną lub zwykłą pocztą, stronie ubiegającej się o unieważnienie certyfikatu potwierdzenie unieważnienia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy,

dodatkowo, w przypadku gdy strona wnioskująca o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu, to urząd certyfikacji musi wysłać powiadomienie do tego podmiotu o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

Wymaga się, aby wnioski o unieważnienie pochodzące od autoryzowanego przedstawiciela urzędu certyfikacji lub sponsora subskrybenta potwierdzane były przez upoważniony do tego urząd rejestracji.

Jeśli unieważniany certyfikat lub komplementarny z nim klucz prywatny były przechowywane na identyfikacyjnej karcie elektronicznej, to po unieważnieniu certyfikatu należy fizycznie zniszczyć nośnik kluczy lub w sposób nieodwracalny usunąć klucze z tego nośnika. Operacji tej dokonuje właściciel karty - osoba prywatna lub osoba prawna (dokładniej, działający z jej upoważnienia przedstawiciel). Właściciel karty musi ją tak przechowywać do momentu zniszczenia lub usunięcia kluczy, aby nie było możliwości jej nieuprawnionego i złośliwego użycia.

4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Unizeto CERTUM - CCP gwarantuje, że maksymalne okresy zwłoki[31] w przetwarzaniu wniosków o unieważnienie certyfikatów:

przesyłane w postaci elektronicznej (i we właściwym formacie) lub przekazywane telefonicznie,

przesyłane w formie papierowej,

są zgodne z okresami podanymi w Tab.4.2.

Tab.4.2 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

Nazwa polityki certyfikacji	Dopuszczalny okres zwłoki
Certum Level I	Nie ma obowiązu unieważniania
Certum Level II	W ciągu 48 godzin
Certum Level III	W ciągu 48 godzin
Certum Level IV	W ciągu 48 godzin

Wnioski o unieważnienie certyfikatów zgłaszane przez urzędy certyfikacji do wystawców tych certyfikatów rozpatrywane są w ciągu 30 minut od otrzymania wniosku, niezależnie od polityk certyfikacji, według których były wystawione.

Fakt unieważnienia certyfikatu odnotowywany jest w bazach danych Unizeto CERTUM - CCP. Na liście certyfikatów unieważnionych (CRL) unieważniony certyfikat zostanie umieszczony zgodnie z przyjętym w Unizeto CERTUM - CCP cyklem publikowania takich list (patrz rozdz.4.9.9).

W momencie unieważnienia certyfikatu automatycznie o tym fakcie są informowani operatorzy urzędów rejestracji oraz zainteresowani subskrybenci.

---

[31] Przez dopuszczalny okres zwłoki należy rozumieć maksymalny dozwolony okres czasu jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a momentem zakończenia jego rozpatrywania, odnotowania w bazach urzędu certyfikacji i odesłania decyzji wnioskodawcy. Okresu tego nie należy mylić z okresem publikowania list CRL (patrz rozdz.4.9.9).

Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem usługi weryfikacji statusu certyfikatu (patrz rozdz.4.9.11), natychmiast po deklarowanym okresie zwłoki w unieważnieniu certyfikatu. Z żądaniem takiej usługi może wystąpić np. strona ufająca weryfikująca wiarygodność podpisu cyfrowego pod dokumentem otrzymanym od subskrybenta.

4.9.5. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

na każde żądanie subskrybenta, właściciela scertyfikowanego klucza publicznego, np. wskutek czasowej nieobecności pracownika w firmie (do miesiąca czasu),

jeśli urząd certyfikacji otrzyma wniosek unieważnienia certyfikatu i na jego podstawie nie jest w stanie potwierdzić tożsamości instytucji żądającej unieważnienia (dotyczy to wniosków przesyłanych pocztą elektroniczną, które przeszły test na dowód posiadania klucza prywatnego),

dane zawarte w papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,

wniosek o unieważnienie został przekazany telefonicznie,

urząd certyfikacji może niezwłocznie zawiesić certyfikat w przypadku uzasadnionego podejrzenia, że certyfikat wydano bez przestrzegania postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego; certyfikat może pozostać zawieszony do czasu aż urząd certyfikacji znajdzie podstawy do unieważnienia certyfikatu,

innych okoliczności wymagających wyjaśnień ze strony subskrybenta.

Z wnioskiem o zawieszenie można występować za pośrednictwem urzędu rejestracji (wymaga to osobistego stawienia się subskrybenta) lub bezpośrednio do właściwego urzędu certyfikacji. W pierwszym z przypadków podpisany przez urząd rejestracji wniosek o zawieszenie certyfikatu lub dokument papierowy odsyłany jest przez operatora urzędu rejestracji do urzędu certyfikacji, w drugim zaś – subskrybent sam podpisuje wniosek o zawieszenie i bezpośrednio wysyła go w postaci elektronicznej do urzędu certyfikacji.

Wniosek o zawieszenie certyfikatu zawiera podobne informacje jak w przypadku wniosku o unieważnienie.

Zaleca się, aby wszystkie wnioski o zawieszenie (w formie elektronicznej oraz papierowej) zgłaszane były za pośrednictwem urzędów rejestracji. Takie postępowanie pozwoli głębiej poznać rzeczywiste przyczyny leżące u podstaw zgłaszanego wniosku oraz ocenić ryzyko, jakie może zaistnieć po przeprowadzeniu tylko operacji zawieszenia certyfikatu.

4.9.6. Kto może żądać zawieszenia certyfikatu

Następujące podmioty mogą zgłaszać żądanie zawieszenia certyfikatu subskrybenta:

subskrybent, będący podmiotem zawieszanego certyfikatu,

autoryzowany przedstawiciel urzędu certyfikacji (w przypadku Unizeto CERTUM - CCP rolę taką pełni administrator bezpieczeństwa), jeśli w oparciu o otrzymany wniosek o unieważnienie, nie można potwierdzić tożsamości subskrybenta lub istnieją inne uzasadnione powody do zawieszenia,

sponsor subskrybenta[32] zawsze wtedy, gdy istnieje podejrzenie, że subskrybent w sposób uciążliwy wykorzystuje udostępniane mu zasoby, np. wysyłając innym podmiotom informacje o znacznych objętościach,

urząd rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej zawieszenie certyfikatu.

Zawieszenie certyfikatu na żądanie subskrybenta wymaga dokładnego zweryfikowania czy podmiot zgłaszający wniosek o zawieszenie jest rzeczywiście subskrybentem zawieszanego certyfikatu.

Subskrybent, niezależnie od tego czy był inicjatorem zawieszenia certyfikatu, czy też uczynił to inny upoważniony do tego organ, musi być o fakcie zawieszenia niezwłocznie poinformowany.

Każdy wniosek może być przekazany:

bezpośrednio do urzędu certyfikacji w postaci wniosku elektronicznego z potwierdzeniem lub bez potwierdzenia urzędu rejestracji,

bezpośrednio lub pośrednio (za pośrednictwem innych urzędów rejestracji) do głównego urzędu rejestracji w postaci wniosku nieelektronicznego (dokument papierowy, faks, telefon, itp.).

4.9.7. Procedura zawieszenia i odwieszania certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu (patrz rozdz.4.9.3). Po poprawnej weryfikacji wniosku urząd certyfikacji zmienia status certyfikatu na unieważniony i umieszcza go na liście certyfikatów unieważnionych (z przyczyną unieważnienia **certificateHold** (patrz rozdz.7.2.1).

Urząd certyfikacji może anulować zawieszenie certyfikatu (poprzez przywrócenie go do normalnego stanu), jeśli tylko spełnione zostaną wszystkie wymienione poniżej okoliczności:

żądający odwieszenia certyfikatu subskrybent oraz urząd certyfikacji nawzajem potwierdzą swoją tożsamość,

urząd certyfikacji stwierdzi, że wniosek o zawieszenie został złożony bez odpowiedniej autoryzacji ze strony zgłaszającego taki wniosek, np. nie został podpisany przez wnioskodawcę lub nie był potwierdzony przez urząd rejestracji,

urząd certyfikacji stwierdzi, że ustąpiły lub nie potwierdziły się przyczyny z powodu których certyfikat zawieszono.

Odwieszenie certyfikatu odbywa się tylko i wyłącznie z inicjatywy subskrybenta, po uprzednim uwierzytelnionym potwierdzeniu wniosku o odwieszenie certyfikatu. Żądanie takie musi poprzedzić przedłożenie dowodu, że klucz prywatny odpowiadający zawieszonemu certyfikatowi jest bezpieczny oraz nie wystąpiły lub nie wystąpią przypadki nieautoryzowanego użycia klucza.

Wniosek o odwieszenie może być przesłany do urzędu certyfikacji faksem lub listownie (po uprzednim potwierdzeniu przez urząd rejestracji) lub złożony osobiście.

[32] Patrz **Słownik pojęć**

Urząd certyfikacji rezerwuje sobie prawo odrzucenia wniosku subskrybenta o odwieszenie, jeśli tylko może to w jakikolwiek naruszyć wiarygodność urzędu certyfikacji.

Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, urząd certyfikacji usuwa certyfikat z listy CRL i staje się on pełnowartościowym certyfikatem, jakim był przed zawieszeniem. Jeśli przyczyny zawieszenia potwierdzą się lub certyfikat pozostaje w stanie zawieszenia dłużej niż 1 miesiąc, to certyfikat jest unieważniany bez możliwości anulowania tej operacji.

4.9.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu

Gwarantowane przez urząd certyfikacji czasy zwłoki w rozpatrzeniu wniosków o zawieszenie certyfikatu, jak również dostępność statusu certyfikatu po jego zawieszeniu są takie same jak w przypadku unieważnienia certyfikatu (patrz rozdz.4.9.4).

Okresy te nie obejmują czasu otrzymania potwierdzenia oraz umieszczenia zawieszonego certyfikatu na liście CRL (patrz rozdz.4.9.9).

Informacja o zawieszeniu (szerzej, statusie certyfikatu) jest dostępna za pośrednictwem usługi weryfikacji certyfikatu, natychmiast po deklarowanym okresie zwłoki zawieszenia. Z żądaniem takiej usługi może wystąpić strona zawieszająca certyfikat, a także strona ufająca weryfikująca wiarygodność podpisu cyfrowego pod dokumentem otrzymanym od subskrybenta.

4.9.9. Częstotliwość publikowania list CRL

Każdy z urzędów certyfikacji funkcjonujący w ramach Unizeto CERTUM - CCP emituje oddzielną listę certyfikatów unieważnionych.

Wszystkie listy uaktualniane są nie rzadziej niż raz w miesiącu[33], jeśli w tym czasie nie został unieważniony żaden nowy certyfikat. Nowa lista CRL publikowana jest jednak w repozytorium po każdym unieważnieniu certyfikatu. W przypadku gdy przyczyną unieważnienia certyfikatu jest ujawnienie klucza prywatnego, nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie (patrz rozdz.4.9.4). Lista CRL urzędu CA-Certum publikowana jest nie rzadziej niż raz na 25 lat, chyba, że w tym czasie nastąpi odwołanie certyfikatu jednego z urzędów afiliowanych przy CA-Certum.

W przypadku unieważnienia certyfikatu urzędu certyfikacji afiliowanego przy Unizeto CERTUM - CCP jest on natychmiast umieszczany na liście CRL.

4.9.10. Możliwości sprawdzania listy CRL

Strona ufająca otrzymująca podpisany przez subskrybenta dokument elektroniczny, zobowiązana jest do sprawdzenia czy certyfikat klucza publicznego odpowiadający kluczowi prywatnemu, przy pomocy którego subskrybent zrealizował podpis, nie znajduje się na liście certyfikatów unieważnionych CRL. Strona ufająca powinna posiadać zawsze aktualną listę CRL.

Weryfikację stanu certyfikatów strona ufająca może oprzeć na listach CRL tylko w tych przypadkach, gdy proponowane przez Unizeto CERTUM - CCP okresy odnowienia list CRL nie niosą ryzyka znaczących strat w działalności prowadzonej przez stronę ufającą. W przypadkach przeciwnych, strona ufająca powinna skontaktować się (telefonicznie, faksem) z organem

---

[33] Zapowiedź terminu następnej publikacji może być także umieszczana w treści aktualnie wydanej listy CRL (patrz pole **NextUpdate**, rozdz.7.2). Wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy, co oznacza, że publikacja ta może nastąpić także przez upływem deklarowanego terminu. W przypadku Unizeto CERTUM - Centrum Certyfikacji Powszechne standardowa wartość tego pola (zapowiedź publikacji) wynosi jeden miesiąc poza urzędem **CA-Certum**.

wydającym certyfikaty lub skorzystać z elektronicznej usługi weryfikacji stanu certyfikatu w trybie *on-line* (rozdz.4.9.11).

Jeśli weryfikowany certyfikat znajduje się na liście CRL, ufająca strona zobowiązana jest do odrzucenia dokumentu z którym związany jest weryfikowany certyfikat w przypadkach, gdy certyfikat unieważniono z powodu jednej z poniższych przyczyn:

```
unspecified          - nieokreślona (nieznana)
keyCompromise        - naruszenie ochrony klucza
cACompromise         - naruszenie ochrony klucza urzędu certyfikacji
cessationOfOperation - zaprzestanie operacji z wykorzystaniem klucza
certificateHold      - certyfikat zawieszony (wstrzymany)
```

W przypadkach, gdy certyfikat unieważniono lub odwieszono, podając jako przyczynę:

```
affiliationChanged   - zamiana danych (afiliacji) subskrybenta
superseded           - zastąpienie (odnowienie) klucza
removeFromCRL[34]    - certyfikat wycofany z listy CRL (odwieszony)
```

Ostateczna decyzja o zaufaniu (lub nie) do weryfikowanego certyfikatu należy do strony ufającej. Przy podejmowaniu takiej decyzji należy wziąć pod uwagę, że z powodu wyżej wymienionych przyczyn nie istnieje żadne uzasadnione podejrzenie lub pewność, że klucz prywatny subskrybenta został ujawniony.

4.9.11. Dostępność weryfikacji unieważnienia/statusu certyfikatu w trybie on-line

Unizeto CERTUM - CCP udostępnia usługę weryfikacji certyfikatu w czasie rzeczywistym. Usługa tego typu realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 2560[35]. Protokół OCSP umożliwia uzyskiwanie częstszych informacji o unieważnieniu certyfikatu w porównaniu z przypadkiem posługiwania się jedynie listami certyfikatów unieważnionych (CRL).

Protokół OCSP działa w oparciu o model **żądanie – odpowiedź**. W odpowiedzi na każde żądanie serwer OCSP, świadczący usługi na rzecz Unizeto CERTUM, zwraca następujące standardowe informacje o statusie certyfikatu:

poprawny (*ang. good*) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny[36],

unieważniony (*ang. revoked*) – oznacza, że certyfikat został unieważniony,

nieznany (*ang. unknown*) – oznacza, że weryfikowany certyfikat nie został wydany przez jeden z urzędów afiliowanych przy CA-Certum.

Usługa OCSP udostępniana jest wszystkim subskrybentom oraz innym stronom ufającym, którzy zawarli umowę z Unizeto CERTUM - CCP na świadczenie tego typu usługi.

Status certyfikatu zawsze podawany jest w czasie rzeczywistym (tzn. natychmiast po unieważnieniu certyfikatu), w oparciu o bazy danych Unizeto CERTUM i zawiera informacje bardziej aktualne niż te zawarte na listach CRL.

---

[34] Przyczyna wycofania certyfikatu z listy CRL (**removeFromCRL**) umieszczana jest jedynie w tzw. listach **deltaCRL** (patrz *Profil certyfikatu PKC i listy CRL*, Publikacja Centrum Certyfikacji, Unizeto Sp z o.o, 22 października 2001 r.)

[35] RFC 2560 *Internet X.509 Public Key Infrastructure: On-line Certificate Status Protocol – OCSP*

[36] Patrz **Słownik pojęć**.

4.9.12. Obowiązek sprawdzania unieważnień w trybie on-line

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie *on-line*, realizowanej w oparciu o usługi i mechanizmy przedstawione w rozdz.4.9.11. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy ryzyko sfałszowania dokumentów elektronicznych opartych na podpisach cyfrowych jest znaczne lub wymuszone jest przez inne obowiązujące w tym zakresie przepisy.

4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów

W przypadku naruszenia ochrony (ujawnienia) kluczy prywatnych urzędów certyfikacji funkcjonujących w ramach Unizeto CERTUM - CCP informacja o tym jest umieszczana natychmiast na listach CRL oraz obligatoryjnie przesłana za pośrednictwem poczty elektronicznej do wszystkich subskrybentów tego urzędu certyfikacji, którego klucz został ujawniony. Informowani są wszyscy subskrybenci, których interesy mogą być jakikolwiek sposób (bezpośredni lub pośredni) zagrożone.

4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów

Subskrybenci powinni obligatoryjnie odbierać i zapoznawać się z treścią poczty elektronicznej o statusie **pilna**, nadawanej przez jakikolwiek urząd certyfikacji afiliowany przy Unizeto CERTUM.

4.9.15. Specjalne obowiązki w przypadku naruszenia ochrony klucza

Niniejszy Kodeks Postępowania Certyfikacyjnego nie określa żadnych wymagań w tym zakresie.

4.9.16. Unieważnienie lub zawieszenie certyfikatu urzędu certyfikacji

Certyfikat urzędu certyfikacji może zostać unieważniony lub zawieszony przez urząd, który ten certyfikat wystawił. Może to zrobić w przypadku wystąpienia jednej z poniższych sytuacji:

urząd certyfikacji jest przekonany, że dane zawarte w certyfikacie urzędu któremu wystawił certyfikat są fałszywe,

klucz prywatny urzędu certyfikacji lub jego system komputerowy zostały ujawnione w sposób mający wpływ na pewność wydawanych przez niego certyfikatów,

urząd certyfikacji naruszył zasady niniejszego Kodeksu Postępowania Certyfikacyjnego.

4.10. Rejestrowanie zdarzeń oraz procedury audytu

W celu nadzoru nad sprawnym działaniem systemu Unizeto CERTUM - CCP, rozliczania użytkowników oraz personelu Unizeto CERTUM - CCP ze swoich działań, rejestrowane są wszystkie zdarzenia występujące w systemie.

Wymaga się, aby każda ze stron – w jakikolwiek sposób związana z procedurami certyfikowania kluczy subskrybenta – dokonywała rejestracji informacji i zarządzała nią adekwatnie do pełnionych obowiązków. Zapisy zarejestrowanej informacji tworzą tzw. dziennik zdarzeń i muszą być tak przechowywane, aby umożliwiały stronom dostęp do odpowiedniej i

niezbędnej w danej chwili informacji, a także towarzyszyły przy rozstrzyganiu sporów pomiędzy stronami oraz pozwalały na wykrywanie prób włamań do systemu Unizeto CERTUM - CCP. Rejestrowane zdarzenia podlegają procedurom kopiowania. Kopie przechowywane są poza siedzibą Unizeto CERTUM - CCP.

Tam gdzie jest to możliwe wpisy do dziennika zdarzeń są realizowane automatycznie. Z kolei tam, gdzie jest to niemożliwe stosowany jest papierowy dziennik raportów. Wszystkie wpisy do dzienników zarówno elektroniczne jak i odręczne są przechowywane i udostępniane w czasie prowadzenia audytów (patrz rozdz.4.6.2).

Wymagania przedstawione w rozdz.2.7, związane z zagwarantowaniem jakości systemu poprzez preaudyt, licencje rządowe, gwarancje kontraktowe lub inne, nie powinny być mylone ze słowem audyt w znaczeniu, o którym jest mowa w tym rozdziale. Niemniej jednak mogą mieć wpływ na typy rejestrowanych zdarzeń, jeśli tak wynika z umów pomiędzy stronami.

W systemie Unizeto CERTUM - CCP administrator bezpieczeństwa zobowiązany jest do regularnego audytu zgodności wdrożonych mechanizmów z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego, a także do oceny efektywności istniejących procedur bezpieczeństwa.

4.10.1. Typy rejestrowanych zdarzeń

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa Unizeto CERTUM - CCP rejestrowane są w dziennikach zdarzeń oraz archiwizowane. Archiwa są szyfrowane i w celu zapobieżenia modyfikacjom zapisywane na nośnikach jednokrotnego zapisu.

Dzienniki zdarzeń Unizeto CERTUM - CCP przechowują zapisy o wszystkich zdarzeniach generowanych przez dowolny komponent programowy wchodzący w skład systemu. Zdarzenia te dzieli się na trzy oddzielne typy wpisów:

systemowe – rekord wpisu zawiera informacje o żądaniu klienta i odpowiedzi serwera (lub odwrotnie) na poziomie protokołu sieciowego (np. http, https, tcp, itp.); rejestracji podlega adres IP hosta lub serwera, wykonywana operacja (np. wyszukiwanie, edycja, zapis, itp.) oraz jej wynik (np. liczba wpisów do bazy),

błędy – w rekordzie zapisywane są informacje o błędach na poziomie protokołów sieciowych oraz na poziomie modułów oprogramowania,

audyt – rekord wpisu zawiera wszystkie wiadomości związane z usługami certyfikacyjnymi, np. żądanie rejestracji i certyfikacji, żądanie aktualizacji kluczy, potwierdzenia akceptacji certyfikatów, publikowanie certyfikatów i list CRL, itp.

Dzienniki te są wspólne dla wszystkich komponentów zainstalowanych na danym serwerze lub stacji roboczej i mają z góry określoną pojemność. Po jej przekroczeniu automatycznie tworzona jest nowa wersja dziennika. Stary dziennik po zarchiwizowaniu jest usuwany z dysku.

Rekordy zdarzeń rejestrowane automatycznie lub ręcznie w dzienniku zdarzeń zawierają:

typ zdarzenia,

identyfikator zdarzenia,

datę i czas wystąpienia zdarzenia,

identyfikator lub inne dane pozwalające na określenie osoby odpowiedzialnej za zaistniałe zdarzenia,

określenie czy zdarzenie dotyczy operacji zakończonej sukcesem, czy błędem,

Rejestrowane zdarzenia obejmują:

alarmy generowane przez firewall i IDS,

czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów oraz innymi usługami świadczonymi przez organ wydający certyfikaty,

wszelkie modyfikacje struktury sprzętowej i programowej,

modyfikacje sieci i połączeń,

fizyczne wejścia do obszarów zastrzeżonych oraz ich naruszenia,

zmiany haseł, PIN-ów, uprawnień oraz ról personelu,

udane i nieudane próby dostępu do oprogramowania serwerów Unizeto CERTUM - CCP oraz jego baz danych,

generowanie kluczy dla potrzeb urzędu certyfikacji, jak również innych stron, np. urzędów rejestracji,

wszystkie otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej; obowiązek rejestrowania tego typu zdarzeń spoczywa nie tylko na urzędzie certyfikacji, ale także na urzędach rejestracji,

historia tworzenia kopii bezpieczeństwa oraz archiwizowania rekordów informacyjnych oraz baz danych.

Szczegółowa lista rejestrowanych zdarzeń zależna jest od poziomu wiarygodności (nazwy polityki certyfikacji) certyfikatów wystawianych lub potwierdzanych przez określony urząd certyfikacji lub urząd rejestracji (patrz Tab.4.3.)[37].

Tab.4.3 Lista zdarzeń rejestrowanych w systemie Unizeto CERTUM - Centrum Certyfikacji Powszechne

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
AUDYT ZABEZPIECZEŃ						
Dowolne zmiany parametrów audytu, m.in. częstotliwość rejestrowania zdarzeń, typy rejestrowanych zdarzeń.	X	X	X	X	X	X
Dowolna próba usunięcia lub modyfikacji systemu rejestracji zdarzeń.	X	X	X	X	X	X
Dowolne zdarzenie związane z procesem realizacji podpisu (np. podpis cyfrowy, funkcja skrótu z kluczem lub uwierzytelnianie podmiotu, wiadomości, etc.)	X	X	X	X	X	X

[37] Opracowano na podstawie *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Pobranie znacznika czasu od zaufanej trzeciej strony	X	X	X	X	X	X
Rozpoczęcie i przerwanie funkcji rejestrujących zdarzenia	X	X	X	X	X	X
Data i czas archiwizowania dziennika zdarzeń	X	X	X	X	X	X
Przekroczenie pojemności dziennika nośników, na których rejestrowane są wpisy do dziennika zdarzeń	X	X	X	X	X	X
Zabezpieczenie (podpis cyfrowy, kontrola dostępu) bieżącego lub zarchiwizowanego dziennika przed nieautoryzowaną modyfikacją, zniszczeniem lub podmianą	X	X	X	X	X	X
Okresowa archiwizacja dziennika zdarzeń	X	X	X	X	X	X
Każdy zaplanowany okresowy i uprawniony przegląd aktualnych lub zarchiwizowanych dzienników, obejmujący także potwierdzenie integralności dzienników.	X	X	X	X	X	X
IDENTYFIKACJA I UWIERZYTELNIANIE						
Zakończone powodzeniem lub niepowodzeniem próby wejścia w określoną rolę w systemie	X		X	X	X	X
Zmiana maksymalnej liczby prób uwierzytelnienia w systemie	X		X	X	X	X
Maksymalna liczba prób uwierzytelnienia zakończonych niepowodzeniem, które mogą wystąpić podczas rejestrowania (logowania) się użytkownika w systemie	X		X	X	X	X
Administrator systemowy zmienił metodę uwierzytelniania się, np. z uwierzytelniania przy pomocy hasła na uwierzytelnianie z wykorzystaniem tokenów wyzwanie/odpowiedź	X	X	X	X	X	X
LOKALNE WPISY DANYCH						
Wszystkie dane związane z zabezpieczeniami, które zostały wprowadzone do systemu (np. tożsamość podmiotu dokonującego wpisu danych, który musi być zaakceptowany przez ten podmiot).	X	X	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
ZDALNE WPISY DANYCH						
Wszystkie wiadomości związane z zabezpieczeniami, które zostały przysłane i odebrane przez system	X	X	X	X	X	X
DANE WYJŚCIOWE I DANE EKSPORTOWANE						
Wszystkie zakończone powodzeniem lub niepowodzeniem żądania dostępu do informacji poufnej lub związanej z zabezpieczeniami	X	X	X	X	X	X
GENEROWANIE KLUCZA						
Każde wygenerowanie klucza dla potrzeb urzędu certyfikacji, urzędu rejestracji lub subskrybenta (wpis do dziennika nie jest obowiązkowy w przypadku generowania symetrycznego klucza sesji lub klucza jednokrotnego użytku)	X	X	X	X	X	X
ŁADOWANIE I PRZECHOWYWANIE KLUCZA						
Ładowanie składowych klucza prywatnego do sprzętowego modułu kryptograficznego (HSM)	X	X	X	X	X	X
Archiwizacja klucza prywatnego urzędu certyfikacji, urzędu rejestracji lub użytkownika końcowego	X	X	X	X	X	X
Każdy dostęp do klucza prywatnego przechowywanego w archiwum urzędu certyfikacji na żądanie podmiotu certyfikatu, z którym klucz prywatny jest do pary	X	X	X	X	X	X
Każde użycie dowolnego z pary kluczy asymetrycznych, z którymi związany jest certyfikat klucza publicznego w operacjach kryptograficznych	X	X	X	X	X	X
Każde anulowanie materiału kluczowego, np. publicznie dostępnych parametrów klucza Diffie-Hellmana	X	X	X	X	X	X
Każde zniszczenie klucza urzędu rejestracji lub urzędu certyfikacji	X	X	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Tożsamość podmiotu autoryzującego operacje zarządzania kluczami	X	X	X	X	X	X
Tożsamość dowolnego podmiotu mającego pod kontrolą jakikolwiek materiał kluczowy (np. składowe klucza lub kluczy, przechowywane na przenośnych nośnikach, np. kartach elektronicznych)	X	X	X	X	X	X
Administrowanie kluczami oraz urządzeniami i innymi nośnikami kluczy	X	X	X	X	X	X
Ujawnienie klucza prywatnego	X	X	X	X	X	X
WPISY ZWIĄZANE Z WIARYGODNYMI KLUCZAMI PUBLICZNYMI, ICH USUNIĘCIE I SKŁADOWANIE						
Dowolne zmiany związane z wiarygodnymi kluczami publicznymi, w tym dopisanie i usunięcie	X	X	X	X	X	X
SKŁADOWANIE KLUCZY TAJNYCH						
Ręczne wpisy kluczy tajnych używanych w procedurach uwierzytelniania	X	X	X	X	X	X
EKSPORT KLUCZY PRYWATNYCH I TAJNYCH						
Eksport kluczy prywatnych i tajnych (nie dotyczy kluczy jednokrotnego użytku)	X	X	X	X	X	X
REJESTRACJA SUBSKRYBENTÓW						
Wstępne zarejestrowanie się w systemie urzędu certyfikacji.	X	X	X	X	X	X
Odrzucenie przez system próby wstępnej rejestracji subskrybenta o tym samym identyfikatorze.	X	X	X	X	X	X
Utworzenie i przysłanie potwierdzonego wniosku o rejestrację subskrybenta.	X	X	X	X	X	X
Zarejestrowanie subskrybenta w oparciu o potwierdzony wniosek o rejestrację.	X	X	X	X	X	X
Zapis unikalnych danych identyfikacyjnych subskrybenta	X	X	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Miejsce przechowywania kopii wniosku oraz dokumentów tożsamości subskrybenta	X	X	X	X	X	X
Dane identyfikacyjne operatora akceptującego wniosek (żądanie) subskrybenta.	X	X	X	X	X	X
Dane identyfikacyjne urzędu certyfikacji, do którego przesyłany jest potwierdzony wniosek	X	X	X	X	X	X
Dane identyfikacyjne urzędu rejestracji, w którym potwierdzony został wniosek	X	X	X	X	X	X
REJESTRACJA CERTYFIKATU						
Wszystkie żądania rejestracji certyfikatów, włączając w to żądania aktualizacji kluczy i recertyfikacji	X	X	X	X	X	X
W przypadku akceptacji żądania zapis wydanego certyfikatu, w przypadku odrzucenia – zapis przyczyny odmowy wydania certyfikatu (np. niepoprawne dane, brak akceptacji przez administratora bezpieczeństwa).	X	X	X	X	X	X
Wszystkie zdarzenia związane z zatwierdzaniem żądań certyfikacyjnych	X	X	X	X	X	X
Wszystkie zdarzenia związane z akceptacją certyfikatu przez podmiot tego certyfikatu	X	X	X	X	X	X
GENEROWANIE CERTYFIKATÓW						
Wszystkie zdarzenia związane z zarządzaniem cyklem życia certyfikatów podpisujących i certyfikatów infrastruktury	X	X	X	X	X	X
Wszystkie zdarzenia związane z zarządzaniem cyklem życia kluczy podpisujących	X	X	X	X	X	X
Wszystkie zdarzenia związane z zarządzaniem cyklem życia certyfikatów subskrybenta	X	X	X	X	X	X
Każde opublikowanie certyfikatu	X	X	X	X	X	X
Każde przesłanie do odbiorcy wystawionego certyfikatu	X	X	X	X	X	X
UNIEWAŻNIANIE CERTYFIKATÓW						
Wszystkie żądania unieważnienia certyfikatu	X	X	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Każde utworzenie nowej listy CRL	X	X	X	X	X	X
Każde przesłanie do odbiorcy informacji o unieważnieniu certyfikatu	X	X	X	X	X	X
ZARZĄDZANIE CYKLEM ŻYCIA MODUŁU KRYPTOGRAFICZNEGO						
Dostarczenie urządzenia przez producenta lub pośrednika	X	X	X	X	X	X
Przekazanie lub pobranie urządzenia z/do sejfu	X	X	X	X	X	X
Instalacja i każde uaktywnienie urządzenia i przygotowanie do użycia	X	X	X	X	X	X
Deinstalacja urządzenia	X	X	X	X	X	X
Przygotowanie urządzenia do serwisu i naprawy	X	X	X	X	X	X
Zniszczenie urządzenia	X	X	X	X	X	X
ZMIANY STATUSU CERTYFIKATU						
Zatwierdzenie lub odrzucenie żądania zmiany statusu certyfikatu (w tym także żądanie zawieszenia certyfikatu).	X	X	X	X	X	X
ZMIANY W KONFIGURACJI SYSTEMU INFORMATYCZNEGO						
Wszystkie zmiany w konfiguracji systemu informatycznego, mające wpływ na jego bezpieczeństwo	X	X	X	X	X	X
ADMINISTROWANIE KONTAMI UŻYTKOWNIKÓW						
Dodane lub usunięte role i konta użytkowników	X	X	X	X	X	X
Modyfikacje praw dostępu związanych z rola lub kontem użytkownika	X	X	X	X	X	X
ZARZĄDZANIE PROFILEM CERTYFIKATU						
Każda zmiana w profilu certyfikatu	X	X	X	X	X	X

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Wszystkie zdarzenia związane z żądaniami zmiany statusu certyfikatów, zarówno te które zostały zatwierdzone, jak i odrzucone	X	X	X	X	X	X
PROFIL ZARZĄDZANIA UNIEWAŻNIENIAMI						
Każda zmiana profilu zarządzania unieważnieniami	X	X	X	X	X	X
Wszystkie zdarzenia związane z żądaniami zmiany statusu certyfikatów, zarówno te które zostały zatwierdzone, jak i odrzucone	X	X	X	X	X	X
ZARZĄDZANIE PROFILEM LIST CERTYFIKATÓW UNIEWAŻNIONYCH						
Każda zmiana w profilu list CRL	X	X	X	X	X	X
ZARZĄDZANIE POLITYKĄ CERTYFIKACJI I KODEKSEM CERTYFIKACJI						
Zatwierdzenie lub odrzucenie zmian w Polityce Certyfikacji lub Kodeksie Postępowania Certyfikacyjnego.	X	X	X	X	X	X
AKREDYTACJA URZĘDÓW CERTYFIKACJI I URZĘDÓW REJESTRACJI						
Zatwierdzenie lub odrzucenie wniosków o zarejestrowanie nowego urzędu certyfikacji lub urzędu rejestracji (wpis do dziennika obejmuje także treść wniosku).	X	X	X	X	X	X
FIZYCZNE ZABEZPIECZENIA DOSTĘPU/POMIESZCZEŃ						
Dostęp personelu do pomieszczeń pracowniczych	X	X	X	X	X	X
Dostęp do serwerów urzędu certyfikacji	X	X	X	X	X	X
Znane lub podejrzewane naruszenia zabezpieczeń fizycznych	X	X	X	X	X	X
ANOMALIA						

Rejestrowane zdarzenie	Miejsce powstania zdarzenia		Nazwa polityki certyfikacji			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Przyczyny błędów w oprogramowaniu	X	X	X	X	X	X
Niepowodzenie weryfikacji integralności oprogramowania	X	X	X	X	X	X
Atak na sieć (podejrzewany lub potwierdzony)	X	X	X	X	X	X
Uszkodzenie sprzętu	X	X	X	X	X	X
Zanik napięcia	X	X	X	X	X	X
Awaria nieprzerwanego źródła zasilania (UPS)	X	X	X	X	X	X
Oczywisty i istotny błąd usługi sieciowej lub naruszenie dostępu do sieci	X	X	X	X	X	X
Naruszenie Polityki Certyfikacji	X	X	X	X	X	X
Naruszenie Kodeksu Postępowania Certyfikacyjnego	X	X	X	X	X	X

Rejestrowane wnioski o realizację usługi, pochodzące od subskrybentów oprócz wykorzystania ich do rozstrzygania sporów i wykrywania prób nadużyć, umożliwiają naliczanie zobowiązań finansowych subskrybenta wobec organu wydającego certyfikaty.

Dostęp do zapisów rejestrowanych zdarzeń (logów) posiadają jedynie administrator bezpieczeństwa, administrator urzędu certyfikacji oraz audytor (patrz rozdz.5.2).

4.10.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów)

Zapisy zarejestrowanych zdarzeń powinny być przeglądane szczegółowo przynajmniej raz w miesiącu. Wszystkie zauważone istotne zdarzenia muszą być wyjaśnione i opisane w dzienniku zdarzeń. Proces przeglądania dziennika zdarzeń obejmuje w pierwszym rzędzie sprawdzenie czy dziennik nie został sfałszowany, a następnie zweryfikowanie wszystkich występujących w dzienniku alarmów oraz anomalii. Wszystkie działania podjęte w wyniku zauważonych usterek muszą być odnotowane w dzienniku zdarzeń.

4.10.3. Okres przechowywania zapisów rejestrowanych zdarzeń (logów) dla potrzeb audytu

Zapisy rejestrowanych zdarzeń przechowywane są w plikach na dysku systemowym do momentu przekroczenia przydzielonych im maksymalnych pojemności. W tym okresie czasu dostępne są w trybie *on-line* na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu dzienniki zdarzeń umieszczane są w archiwum i udostępniane tylko w trybie *off-line*, na specjalnie do tego przygotowanym stanowisku.

Zarchiwizowane zdarzenia przechowywane są przez okres min. 2 miesięcy.

4.10.4. Ochrona zapisów rejestrowanych zdarzeń dla potrzeb audytu

Raz w tygodniu wszystkie zapisy z dzienników zdarzeń są kopiowne na taśmę magnetyczną. Po przekroczeniu założonej dla danego dziennika zdarzeń maksymalnej liczby wpisów, zawartość dziennika jest archiwizowana. Archiwa mogą być szyfrowane przy zastosowaniu algorytmu Triple DES lub AES. Klucz przy pomocy którego szyfrowane jest archiwum znajduje się wówczas pod kontrolą administratora bezpieczeństwa.

Dziennik zdarzeń może być przeglądany jedynie przez **administratora bezpieczeństwa**, **administratora urzędu certyfikacji** oraz **audytora**. Dostęp do dziennika jest tak skonfigurowany, że:

tylko podmioty występujące w jednej z trzech wymienionych powyżej ról mają prawo czytania rekordów z dzienników zdarzeń,

tylko administrator bezpieczeństwa może archiwizować i usuwać, po zarchiwizowaniu, z systemu pliki zawierające zarejestrowane zdarzenia,

możliwe jest wykrycie każdego naruszenia jego integralności; daje to możliwość upewnienia się, że rekordy nie zawierają luk lub sfałszowanych wpisów,

żaden podmiot nie posiada prawa modyfikowania jego zawartości.

Dodatkowo procedury ochrony dzienników zdarzeń są tak zaimplementowane, że nawet po ich zarchiwizowaniu niemożliwe jest ich usunięcie lub zniszczenie przed datą końca przewidywanego okresu przechowywania dzienników (patrz rozdz.4.10.3).

4.10.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury bezpieczeństwa Unizeto CERTUM - CCP wymagają, aby dzienniki zdarzeń oraz zapisy zdarzeń powstałe w czasie przeglądania w tych dzienników przez administratora bezpieczeństwa, administratora systemu lub audytora, takie jak czynności wykonywane na dziennikach, zestawienia zbiorcze, analizy, statystyki, wykryte zagrożenia, itp., były kopiowane przynajmniej raz w miesiącu. Kopie te przechowywane są w ośrodku zapasowym Unizeto CERTUM - CCP. Kopie mogą być oznaczone znacznikiem czasu.

4.10.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

Zaimplementowany w systemie moduł analizy dziennika bezpieczeństwa umożliwia bieżące przeglądanie wszystkich zdarzeń oraz automatycznie sygnalizuje zdarzenia podejrzane lub powodujące naruszenie istniejących zabezpieczeń. O zaistniałych zdarzeniach, mających wpływ na bezpieczeństwo systemu automatycznie informowany jest administrator bezpieczeństwa i administrator urzędu certyfikacji, w pozostałych przypadkach informacje przekazywane są administratorowi systemu.

Informowanie upoważnionych osób o sytuacjach krytycznych z punktu widzenia bezpieczeństwa systemu realizowane jest poprzez inne, odpowiednio zabezpieczone środki techniczne, np. pager, telefon komórkowy, poczta elektroniczna.

Powiadomione osoby podejmują odpowiednie działania mające na celu zapobieżenie pojawiającym się zagrożeniom.

4.10.7. Oszacowanie podatności na zagrożenia

Niniejszy Kodeks Postępowania Certyfikacyjnego wymaga przeprowadzenia przez urząd wydający certyfikaty, związane z nim urzędy rejestracji (w przypadku oddelegowania uprawnień w zakresie rejestracji subskrybentów) oraz repozytorium, analizy podatności na zagrożenia wszystkich wewnętrznie stosowanych procedur, oprogramowania oraz systemu komputerowego. Wymogi te mogą być także określone przez zewnętrzną instytucję, uprawnioną do przeprowadzania audytu w Unizeto CERTUM - CCP.

Za audyt wewnętrzny odpowiedzialny jest administrator bezpieczeństwa, którego zadanie polega na kontroli zgodności zapisów w dzienniku bezpieczeństwa, poprawności przechowywania jego kopii, działań podejmowanych w sytuacjach zagrożeń oraz przestrzegania postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego.

Zewnętrzna instytucja dokonująca audytu bezpieczeństwa realizuje kontrolę zgodnie z wytycznymi zawartymi w PN ISO/IEC 13355 oraz ISO/IEC 17799.

4.11. Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, danych o wnioskach napływających od subskrybentów, informacje o subskrybentach, generowane certyfikaty i listy CRL, historie kluczy, którymi posługują się urzędy certyfikacji oraz urzędy rejestracji, a także pełna korespondencja prowadzona wewnątrz Unizeto CERTUM - CCP oraz z subskrybentami.

Unizeto CERTUM - CCP utrzymuje dwa typy archiwów: archiwum dostępne w trybie *on-line* (archiwum *on-line*) oraz archiwum dostępne w trybie *off-line* (archiwum *off-line*).

Ważne certyfikaty (w tym także uśpione, wydane co najwyżej 15 lat wstecz od chwili obecnej) przechowywane są w archiwum *on-line* certyfikatów aktywnych i mogą być wykorzystywane do realizacji niektórych usług zewnętrznych urzędu certyfikacji, np. weryfikacji ważności certyfikatu, udostępniania certyfikatów właścicielom (odzyskiwanie certyfikatów) oraz uprawnionym do tego podmiotom.

Archiwum on-line może zawierać także certyfikaty wydane maksymalnie 25 lat wstecz.

Archiwum *off-line* zawiera m.in. certyfikaty (w tym także certyfikaty unieważnione) wydane w przedziale od 15 do 25 lat wstecz od chwili obecnej. Archiwum certyfikatów unieważnionych zawiera informację o identyfikatorze certyfikatu, datę unieważnienia, przyczynę unieważnienia, czy, kiedy i gdzie został umieszczony na liście CRL. Archiwum wykorzystywane jest do rozstrzygania sporów dotyczących starych dokumentów, opatrzonych (kiedyś) przez subskrybenta podpisem cyfrowym.

Na podstawie archiwów tworzone są ich kopie, przechowywane poza siedzibą Unizeto CERTUM - CCP.

Zaleca się szyfrowanie oraz oznaczanie znacznikiem czasu archiwizowanych danych. Klucz, przy pomocy, którego zaszyfrowano archiwum, znajduje się pod kontrolą administratora bezpieczeństwa lub administratora urzędu certyfikacji.

4.11.1. Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące dane:

dane z przeglądu i oceny (z audytu) zabezpieczeń logicznych i fizycznych systemu komputerowego urzędu certyfikacji, urzędu rejestracji oraz repozytorium,

otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub wiadomości elektronicznej,

baza danych subskrybentów,

baza danych certyfikatów,

wydane listy CRL,

historia kluczy urzędu certyfikacji, od ich wygenerowania do zniszczenia włącznie,

historia kluczy subskrybentów, od ich wygenerowania do zniszczenia włącznie, jeśli klucze te są archiwizowane przez subskrybenta w urzędzie certyfikacji,

wewnętrzna i zewnętrzna korespondencja (papierowa i elektroniczna) Unizeto CERTUM - CCP z subskrybentami oraz ufającymi stronami przy operacjach zawieszania i odwieszania certyfikatów.

4.11.2. Częstotliwość archiwizowania danych

Archiwizacja realizowana jest kilkupoziomowo w następujących odstępach czasowych:

baza danych certyfikatów oraz danych o subskrybentach przez okres trzech lat (od momentu wydania certyfikatu) znajduje się na nośnikach Unizeto CERTUM - CCP, duplikowanych przez macierze dyskowe. Przez okres następnych trzech lat dane te są przechowywane na taśmach magnetycznych lub płytach CD-ROM, ale nadal są dostępne na bieżąco (w trybie *on-line*). W siódmym roku (po upływie sześciu lat od wydania certyfikatu) wszystkie dane o subskrybencie oraz jego certyfikat składowane są na płycie CD-ROM i od tego momentu są dostępne tylko w trybie *off-line*,

listy CRL, korespondencja elektroniczna oraz wnioski przychodzące od subskrybentów oraz wydane decyzje archiwizowane są w taki sam sposób i z taką samą częstotliwością, jak w przypadku bazy danych certyfikatów oraz danych o subskrybentach,

klucze urzędu certyfikacji oraz urzędów rejestracji zapisywane są - po upływie ważności związanego z nimi certyfikatu – na nośniku jednokrotnego zapisu i szyfrowane przy pomocy klucza, do którego dostęp posiada jedynie administrator bezpieczeństwa; zarchiwizowane klucze dostępne są tylko w trybie *off-line*.

4.11.3. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej i papierowej), opisane w rozdz.4.11.1 przechowywane są przez minimalne okresy podane w Tab.4.4. Po upływie przyjętego okresu archiwizacji dane są niszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany jest ze szczególną starannością.

Tab.4.4 Minimalne okresy przechowywania archiwum

Nazwa polityki certyfikacji	Minimalny okres przechowywania
Certum Level I	25 lat
Certum Level II	25 lat
Certum Level III	25 lat
Certum Level IV	25 lat

4.11.4. Procedury tworzenia kopii zapasowych

Kopie zapasowe umożliwiają całkowite odtworzenie (jeśli jest to konieczne, np. po awarii systemu) danych niezbędnych do normalnego funkcjonowania Unizeto CERTUM - CCP. W tym celu kopiowaniu podlegają następujące aplikacje i pliki:

dyski instalacyjne z oprogramowaniem systemowym, m.in. systemami operacyjnymi,

dyski instalacyjne z aplikacjami urzędów certyfikacji i urzędów rejestracji

dyski instalacyjne serwera WWW i repozytorium,

historie kluczy urzędów, certyfikatów i list CRL,

dane z repozytorium,

dane o subskrybentach oraz personelu Unizeto CERTUM - Centrum Certyfikacji Powszechne,

dzienniki zdarzeń.

Metody tworzenia kopii zapasowych mają istotny wpływ na szybkość oraz koszt odtwarzania funkcji urzędu certyfikacji po wystąpieniu awarii systemu. W Unizeto CERTUM - CCP przyjęto dwie następujące metody:

gorąca rezerwa – codzinnie są tworzone kopie baz danych, które mogą być w razie konieczności wykorzystane przy odtworzeniu utraconych danych,

cotygodniowe kopie zapasowe – tworzone są w ośrodku podstawowym i mogą być w razie konieczności wykorzystane do odtworzenia utraconych danych oraz odtworzenia konfiguracji sprzętu i oprogramowania; kopie stanowią zabezpieczenie na wypadek utraty możliwości synchronizowania ośrodka zapasowego z ośrodkiem podstawowym; kopia powinna objąć pełny, aktualny stan systemu Unizeto CERTUM - Centrum Certyfikacji Powszechne; odtworzenie funkcji Unizeto CERTUM - Centrum Certyfikacji w pełnym zakresie ośrodek osiąga w ciągu maksymalnie 48 godzin.

Szczegółowe procedury tworzenia kopii zapasowych oraz odtwarzania po awariach opisane są w dokumencie „Księga Tworzenia Kopii Zapasowych i Awaryjnego Odtwarzania Serwerów". Dokumenty ma status „niejawny" i udostępniany jest tylko upoważnionemu do tego personelowi oraz audytorom.

4.11.5. Wymaganie znakowania danych znacznikiem czasu

Zaleca się, aby archiwizowane dane oznaczane były znacznikiem czasu, tworzonym przez wiarygodny organ znacznika czasu (TSA), posiadający certyfikat wydany przez operacyjny urząd

certyfikacji afiliowany przy **CA-Certum**. Usługa znacznika czasu udostępniona jest przez Unizeto CERTUM - CCP.

4.11.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

W celu sprawdzenia integralności zarchiwizowane dane są co pewien okres testowane oraz porównywane z danymi oryginalnymi (jeśli jeszcze funkcjonują w systemie). Czynność ta może być przeprowadzona tylko przez administratora bezpieczeństwa i jest odnotowywana w rejestrze zdarzeń.

W przypadku wykrycia uszkodzeń lub zniszczeń w danych oryginalnych lub w danych zarchiwizowanych, zauważone uszkodzenia są usuwane tak szybko jak to możliwe.

4.12. Zmiana klucza

Procedura zmiany klucza odnosi się do kluczy urzędów certyfikacji afiliowanych przy Unizeto CERTUM - CCP i dotyczy procesu zapowiedzi aktualizacji pary kluczy do podpisywania certyfikatów i list CRL, która zastąpi parę dotychczas używaną.

Procedura aktualizacji kluczy polega na wydaniu przez urząd certyfikacji specjalnych certyfikatów ułatwiających subskrybentom posiadającym stary certyfikat urzędu bezpieczne przejście do pracy z nowym certyfikatem, zaś nowym subskrybentom posiadającym nowy certyfikat na bezpieczne pozyskanie starego certyfikatu, umożliwiającego weryfikację istniejących danych (patrz RFC 2510, a także rozdz.6.1.1.2 i rozdz.6.1.1.3).

Każda zmiana kluczy urzędów certyfikacji anonsowana jest odpowiednio wcześniej za pośrednictwem strony WWW Unizeto CERTUM - CCP oraz rozgłaszana przy pomocy poczty elektronicznej wysyłanej do wszystkich klientów urzędu certyfikacji, których klucze zostały zaktualizowane. Dodatkowo, w przypadku zmiany kluczy przez urząd certyfikacji **CA-Certum** informacja o tym fakcie powinna być publikowana w środkach masowego przekazu w tygodniu poprzedzającym koniec okresu ważności klucza prywatnego.

Częstotliwości zmian kluczy urzędów certyfikacji afiliowanych przy Unizeto CERTUM - CCP wynikają z okresów ważności związanych z nimi certyfikatów, podanych w Tab.6.5.

Od momentu zmiany klucza urząd certyfikacji używa do podpisywania wystawianych certyfikatów oraz list CRL jedynie nowego klucza prywatnego.

4.13. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

Rozdział ten zawiera opis procedur postępowania, realizowanych przez Centrum Certyfikacji w wypadkach szczególnych (także klęsk żywiołowych) w celu przywrócenia gwarantowanego poziomu usług. Procedury te realizowane są według opracowanego planu podnoszenia systemu po katastrofie (*ang. disaster recovery plan*).

4.13.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Polityka bezpieczeństwa, realizowana przez Unizeto CERTUM - CCP bierze pod uwagę następujące zagrożenia, mające wpływ na dostępność i ciągłość świadczonych usług:

fizyczne uszkodzenie systemu komputerowego Unizeto CERTUM - CCP, w tym także sieci - obejmuje to przypadki uszkodzenia powstałe wskutek wypadków losowych,

awarie oprogramowania pociągające za sobą utratę dostępu do danych - awarie tego typu dotyczą systemu operacyjnego, oprogramowania użytkowego oraz działania oprogramowania złośliwego, np. wirusów, robaków, koni trojańskich,

utratę istotnych z punktu widzenia interesów Unizeto CERTUM - CCP usług sieciowych - związane jest to w pierwszym rzędzie z zasilaniem oraz połączeniami telekomunikacyjnymi,

awaria tej części sieci internetowej, za pośrednictwem której Unizeto CERTUM - CCP udostępnia swoje usługi - awaria taka oznacza zablokowanie i w istocie odmowę (niezamierzoną) świadczenia usług.

Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa Unizeto CERTUM - CCP musi obejmować następujące zagadnienia:

Plan podnoszenia systemu po katastrofie. Wszyscy subskrybenci oraz strony ufające są jak najszybciej i w sposób najbardziej odpowiedni do zaistniałej sytuacji powiadamiani o każdej poważnej awarii lub katastrofie, dotyczącej dowolnego komponentu systemu komputerowego i sieci. Plan podnoszenia systemu obejmuje szereg procedur, które są realizowane w momencie, gdy dowolna część systemu ulegnie skompromitowaniu (uszkodzeniu, ujawnieniu, itp.). Wykonywane są działania:

- tworzone i konserwowane są kopie obrazu dysków każdego z serwerów oraz stacji roboczej systemu Unizeto CERTUM - CCP; każda kopia przechowywana jest w bezpiecznym pomieszczeniu poza siedzibą Unizeto CERTUM - CCP,
- codziennie, zgodnie z procedurami opisanymi w rozdz.4.11.4 tworzone są kopie baz danych zawierające wszystkie zgłoszone żądania ze strony subskrybentów, wydane, aktualizowane i unieważnione certyfikaty; najbardziej aktualne kopie przechowywane są w bezpiecznym miejscu w siedzibie Unizeto CERTUM - CCP,
- raz w tygodniu zgodnie z procedurami opisanymi w rozdz.4.11.4 tworzone są kopie każdego z serwerów zawierające pełne kopie serwerów, wszystkie zgłoszone żądania ze strony subskrybentów, zapisy rejestrowanych zdarzeń (logi), wydane, aktualizowane i unieważnione certyfikaty; najbardziej aktualne kopie przechowywane są w bezpiecznym miejscu poza siedzibą Unizeto CERTUM - CCP,
- klucze Unizeto CERTUM - CCP, rozproszone zgodnie z zasadami sekretów współdzielonych przechowywane są przez zaufane osoby, w miejscach tylko im znanych;
- wymiana komputera jest wykonywana tak, aby możliwe było odtworzenie obrazu dysku, w oparciu o najbardziej aktualne dane oraz klucze (dotyczy to serwera podpisującego),
- proces podnoszenia systemu po katastrofie testowany jest na każdym elemencie systemu co najmniej raz w roku i jest częścią procedur audytu wewnętrznego.

Kontrolowanie zmian. W systemie docelowym instalacja uaktualnionych wersji oprogramowania możliwa jest tylko i wyłącznie po przeprowadzeniu na systemie modelowym intensywnych testów, wykonywanych według ściśle opracowanych procedur. Wszystkie zmiany dokonywane w systemie wymagają akceptacji

administratora bezpieczeństwa Unizeto CERTUM - CCP. Jeśli mimo stosowania się do tej procedury wdrożone nowe elementy spowodują awarię systemu docelowego, opracowane plany podnoszenia systemu po katastrofie pozwalają na powrót do stanu sprzed awarii.

System zapasowy. W przypadku awarii uniemożliwiającej funkcjonowanie Unizeto CERTUM - CCP w ciągu maksymalnie 24 godzin zostanie uruchomiony ośrodek zapasowy, który przejmie do czasu uruchomienia głównego ośrodka Unizeto CERTUM - CCP wszystkie funkcje urzędów certyfikacji Unizeto CERTUM - CCP. Z uwagi na regularne tworzenie kopii zapasowych, archiwizację, gromadzenie nieprzetworzonych przesyłek oraz redundancję sprzętowo-programową w przypadku awarii uniemożliwiającej funkcjonowanie Unizeto CERTUM - CCP możliwe jest:

- uruchomienie ośrodka zapasowego analogicznego do uruchomienia Unizeto CERTUM - CCP,
- przetworzenie wszystkich zgromadzonych i nieprzetworzonych żądań,
- do czasu regeneracji i ponownego uruchomienia ośrodka głównego - przetwarzanie na bieżąco przychodzących wiadomości od użytkowników.

System tworzenia kopii zapasowych. System Unizeto CERTUM - CCP korzysta z oprogramowania tworzącego kopie zapasowe z danych, które w każdej chwili umożliwiają ich odtworzenie oraz obsługę audytu. Kopie zapasowe oraz archiwa tworzone są ze wszystkich danych, mających istotny wpływ na bezpieczeństwo i normalne funkcjonowanie Unizeto CERTUM - CCP. Kopie tworzone są codziennie, co tydzień oraz co miesiąc i zapisywane na taśmach, archiwa zaś na płytach CD-ROM. Kopie zapasowe mogą być chronione przy pomocy hasła, płyty CD-ROM szyfrowane. Kopie danych i ich archiwa przechowywane są poza miejscem lokalizacji systemu przetwarzającego.

Usługi szczególne. W celu zapobieżenia czasowemu zanikowi zasilania i zapewnienia ciągłości usług stosuje się zasilanie awaryjne (UPS-y). Zapewniają one co najmniej sześciogodzinną nieprzerwaną pracę systemu od chwili zaniknięcia zasilania. Urządzenia UPS sprawdzane są co 6 miesięcy.

4.13.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

W przypadku ujawnienia lub podejrzenia ujawnienia kluczy prywatnych urzędów certyfikacji, funkcjonujących w ramach Unizeto CERTUM - CCP podjęte zostaną następujące kroki:

urząd certyfikacji generuje nową parę kluczy i tworzy nowy certyfikat,

w trybie natychmiastowym zostaną zawiadomieni o tym fakcie wszyscy użytkownicy certyfikatów za pośrednictwem komunikatu w środkach masowego przekazu oraz za pośrednictwem poczty elektronicznej,

skompromitowany certyfikat znajdzie się na liście certyfikatów unieważnionych z podaniem przyczyny unieważnienia,

unieważnione i umieszczone na liście certyfikatów unieważnionych wraz z podaniem odpowiedniej przyczyny unieważnienia zostaną także wszystkie certyfikaty znajdujące się w ścieżce certyfikacji skompromitowanego certyfikatu,

wygenerowane zostaną nowe certyfikaty użytkowników,

nowe certyfikaty użytkowników zostaną przesłane do użytkowników bez obciążania ich kosztami za powyższą operację.

4.13.3. Spójność zabezpieczeń po katastrofach

Po każdym przywróceniu systemu po katastrofie do normalnego stanu administrator bezpieczeństwa lub administrator urzędu certyfikacji powinien:

zmienić wszystkie poprzednio stosowane hasła,

usunąć i ponownie określić wszystkie upoważnienia dostępu do zasobów systemu,

zmienić wszystkie kody oraz numery PIN związane z fizycznym dostępem do pomieszczeń oraz elementów systemu,

jeśli usunięcie awarii wymagało ponownego zainstalowania systemu operacyjnego oraz użytkowego, należy zmienić wszystkie adresy IP elementów systemu oraz jego podsieci,

dokonać przeglądu polityki bezpieczeństwa sieci Unizeto CERTUM - CCP oraz fizycznego dostępu do pomieszczeń i elementów systemu,

zawiadomić wszystkich użytkowników o wznowieniu działalności systemu.

4.14. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Przedstawione poniżej obowiązki urzędu certyfikacji mają na uwadze redukcję wpływu skutków podjęcia przez ten urząd decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym wszystkich subskrybentów, urzędu który akredytował likwidowany urząd certyfikacji (jeśli taki istnieje) oraz przekazania odpowiedzialności - na drodze odpowiednich umów z innymi urzędami certyfikacji - za obsługę swoich subskrybentów, zarządzanie bazami danych oraz innymi zasobami.

4.14.1. Wymagania związane z przekazaniem obowiązków

Zanim urząd certyfikacji wstrzyma swoją działalność zobowiązany jest do:

poinformowania urzędu, który wydał mu certyfikat o swoim zamiarze zaprzestania działalności jako autoryzowanego urzędu certyfikacji; zawiadomienie takie musi być złożone co najmniej na 90 dni przed planowanym zakończeniem działalności;

zawiadomienia (co najmniej na 90 dni wcześniej) wszystkich subskrybentów, którzy posiadają jeszcze ważny, wydany przez siebie certyfikat, o zamiarze zakończenia działalności,

unieważnienia wszystkich certyfikatów, które pozostały aktywne w dniu upłynięcia deklarowanego terminu zakończenia działalności niezależnie od tego czy subskrybent złożył stosowny wniosek o unieważnienie, czy też nie,

poinformowania wszystkich subskrybentów związanych z urzędem certyfikacji o zaprzestaniu działalności,

uczynienia wszystkiego co możliwe, aby zaprzestanie działalności urzędu spowodowało jak najmniejsze szkody w działalności subskrybentów oraz osób prawnych,

zaangażowanych w proces ciągłego weryfikowania podpisów cyfrowych (będących jeszcze w obiegu) przy pomocy kluczy publicznych, poświadczonych certyfikatami wydanymi przez likwidowany urząd certyfikacji,

zawrzeć umowę (np. z innym urzędem certyfikacji, porównaj rozdz.4.11.2), gwarantującą ochronę zgromadzonych danych,

wypłacenie odszkodowań (nieprzekraczających opłaty za wydanie i przechowywanie certyfikatu) subskrybentom za unieważnienie ich certyfikatów przed upływem terminu ważności.

4.14.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji

W celu zapewnienia ciągłości usług certyfikacyjnych świadczonych subskrybentom, likwidowany urząd certyfikacji może zawrzeć z innym urzędem tego typu umowę, dotyczącą ponownego wydania pozostających jeszcze w obiegu certyfikatów subskrybentów likwidowanego urzędu certyfikacji.

Wydając ponownie certyfikat następca likwidowanego urzędu certyfikacji przejmuje na siebie prawa i obowiązki likwidowanego urzędu certyfikacji w zakresie zarządzania certyfikatami pozostającymi w obiegu.

Archiwum kończącego działalność urzędu certyfikacji musi być przekazane głównemu urzędowi certyfikacji **CA-Certum** (w przypadku zaprzestania działalności przez **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**) lub instytucji, z którą zawarta została odpowiednia umowa (w przypadku zaprzestania działalności przez **CA-Certum**).

5. Kontrola zabezpieczeń fizycznych, organizacyjnych oraz personelu

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w Unizeto CERTUM - CCP m.in. podczas generowania kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych.

5.1. Kontrola zabezpieczeń fizycznych

5.1.1. Nadzór nad bezpieczeństwem fizycznym Unizeto CERTUM - CCP

Sieciowy system komputerowy, terminale operatorskie oraz zasoby informacyjne Unizeto CERTUM - CCP znajdują się w wydzielonych pomieszczeniach, fizycznie chronionych przed nieupoważnionym dostępem, zniszczeniem oraz zakłóceniami ich pracy. Pomieszczenia te są nadzorowane. W zapisach zdarzeń (logach systemowych) rejestrowane jest każde wejście i wyjście, testowana jest stabilność zasilania, temperatura oraz wilgotność.

5.1.1.1. Miejsce lokalizacji oraz budynek

Unizeto CERTUM - CCP mieści się w budynku Unizeto Sp. z o.o., znajdującym się w Szczecinie przy ul. Królowej Korony Polskiej 21.

5.1.1.2. Dostęp fizyczny

Fizyczny dostęp do budynku oraz pomieszczeń Unizeto CERTUM - CCP jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. Ochrona portierska funkcjonuje 24 godziny na dobę. Funkcjonują także systemy ochrony przeciwpożarowej, przeciwzalaniowej, przeciwwłamaniowej oraz systemy zasilania awaryjnego, zapobiegające skutkom czasowego zaniku zasilania.

Ochrona portierska funkcjonuje 24 godziny na dobę. Siedziba UNIZETO oraz Centrum Certyfikacji jest publicznie dostępna w każdy dzień roboczy w godzinach od 8.00 do 16.00. W pozostałym czasie (w tym w dni nierobocze) w budynku mogą przebywać tylko osoby znane ochronie z imienia i nazwiska oraz posiadające pozwolenie Dyrekcji UNIZETO.

Goście odwiedzający pomieszczenia zajmowane przez Unizeto CERTUM - CCP mogą poruszać się po tych pomieszczeniach jedynie wraz z personelem Unizeto Certum.

Pomieszczenia Unizeto CERTUM - CCP dzielą się na:

pomieszczenie systemu komputerowego,

pomieszczenie operatorsko - administracyjne,

pomieszczenie projektantów i programistów.

Pomieszczenie systemu komputerowego wyposażone jest w nadzorowany system zabezpieczeń, zbudowany w oparciu o czujniki ruchu, przeciwpożarowe oraz przeciwpowodziowe. Dostęp do pomieszczenia posiadają tylko osoby upoważnione, tzn. administrator bezpieczeństwa, administrator urzędu certyfikacji oraz administrator systemu. Nadzorowanie praw dostępu realizowane jest w oparciu o posiadane przez nich karty identyfikacyjne oraz czytnik do ich odczytu, zamontowany przy wejściu do pomieszczenia. Każde wejście i wyjście odnotowywane jest w logach systemowych.

Dostęp do pomieszczenia operatorsko-administracyjnego chroniony jest w oparciu o karty identyfikacyjne oraz czytnik do ich odczytu. Ponieważ wszystkie informacje wrażliwe przechowywane są w sejfach trwale związanych z podłożem, do których dostęp jest możliwy jedynie przy użyciu dwóch kluczy (zasada dwóch par oczu), zaś dostęp do terminali operatorskich i administracyjnych wymaga uprzedniego uwierzytelnienia, zastosowane zabezpieczenie fizyczne jest wystarczające. Klucze do pomieszczenia są pobierane tylko przez upoważnione do tego osoby. W pomieszczeniu mogą przebywać jedynie pracownicy Unizeto CERTUM - CCP oraz inne uprawnione osoby, przy czym osoby te nie mogą w pomieszczeniu przebywać pojedynczo. Jedyne odstępstwo od tej zasady dotyczy pracowników, którzy pełnią w Unizeto CERTUM rolę sklasyfikowaną jako **zaufana**.

Pomieszczenie projektantów i programistów chronione są w sposób tradycyjny za pomocą zamka patentowego. Dozwolone jest przebywanie w tym pomieszczeniu pojedynczych osób. Programiści i projektanci nie posiadają dostępu do informacji wrażliwej. Jeśli taki dostęp jest konieczny odbywa się to w obecności oficera bezpieczeństwa w pomieszczeniu operatorsko - administracyjnym. Wdrażane projekty i ich oprogramowanie testowane jest na wersji rozwojowej Unizeto CERTUM - CCP oraz/lub na jego modelu.

5.1.1.3. Zasilanie oraz klimatyzacja

Pomieszczenia operatorsko-administracyjne, jak również pomieszczenie projektantów i programistów są klimatyzowane tylko w godzinach pracy. Od momentu zaniku zasilania zainstalowane zasilanie awaryjne (UPS) wystarcza na godzinę pracy.

Środowisko pracy w pomieszczeniu systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń. Zasilanie awaryjne (UPS) wystarcza na około 6 godzin pracy od momentu zaniku zasilania.

5.1.1.4. Zagrożenie zalaniem

W pomieszczeniu systemu komputerowego zainstalowane są czujniki wilgotności oraz wykrywające obecność wody. Czujniki te sprzęgnięte są systemem obrony całego budynku UNIZETO. O zagrożeniach informowana jest obsługa portierska, która w zależności od sytuacji zawiadamia odpowiednie służby miejskie, pełnomocnika ds. bezpieczeństwa UNIZETO oraz administratora Unizeto CERTUM - CCP.

5.1.1.5. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej zainstalowany w budynku UNIZETO, spełnia wymogi stosownych przepisów i norm przeciwpożarowych. Zainstalowano także urządzenia zraszające, które załączają się automatycznie w przypadku gwałtownie rozprzestrzeniającego się pożaru.

5.1.1.6. Nośniki informacji

W zależności od stopnia wrażliwości informacji nośniki na których przechowywane są archiwa oraz bieżące kopie danych składowane są w sejfach ognioodpornych zlokalizowanych w

pomieszczeniu operatorsko-administracyjnym oraz pomieszczeniu systemu komputerowego. Dostęp do sejfu możliwy jest jedynie przy użyciu dwóch kluczy będących w posiadaniu autoryzowanych osób.

5.1.1.7. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo Unizeto CERTUM - CCP po upływie okresu przechowywania (patrz rozdz.4.11) niszczone są w specjalnych urządzeniach niszczących. W przypadku kluczy kryptograficznych oraz numerów PIN nośniki na których informacje te były przechowywane są niszczone w urządzeniach klasy DIN-3 (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji, np. kryptograficzne karty procesorowe, i ich ponowne użycie do tych samych lub innych celów).

5.1.1.8. Przechowywanie kopii bezpieczeństwa poza siedzibą Unizeto CERTUM - CCP

Kopie haseł, numerów PIN oraz kluczy kryptograficznych przechowywane są skrytkach poza miejscem lokalizacji Unizeto CERTUM - CCP.

Poza siedzibą Unizeto CERTUM - CCP przechowywane są także archiwa, bieżące kopie informacji przetworzonej przez system komputerowy, a także pełna wersja instalacyjna oprogramowania Unizeto CERTUM - CCP. Umożliwia to awaryjne odtworzenie wszystkich funkcji Unizeto CERTUM - CCP w ciągu maksimum 48 godzin (w siedzibie Unizeto CERTUM - CCP lub w ośrodku zapasowym).

5.1.2. Nadzór nad bezpieczeństwem urzędów rejestracji

Komputery rejestrujące wnioski subskrybentów oraz wydające ich potwierdzenia powinny znajdować się w specjalnie przeznaczonym do tego celu pomieszczeniu oraz pracować w trybie *on-line* (muszą być włączone w sieć). Dostęp do nich jest fizycznie chroniony przed nieupoważnionymi osobami.

Każdy urząd rejestracji musi posiadać sprzętowy moduł kryptograficzny.

5.1.2.1. Miejsce lokalizacji oraz budynek

Urzędy rejestracji Centrum Certyfikacji zlokalizowane są w następujących miejscach:

Główny Urząd Rejestracji (GUR) - w pomieszczeniu operatorsko-administracyjnym Unizeto CERTUM - CCP (patrz rozdz.5.1.1.1),

lokalizacja innych urzędów rejestracji dostępna jest za pośrednictwem poczty elektronicznej: info@certum.pl.

5.1.2.2. Dostęp fizyczny

Dostęp do Głównego Urzędu Rejestracji musi być zgodny z wymogami rozdz.5.1.1.2. W przypadku pozostałych typów urzędów rejestracji nie narzuca się w tym zakresie żadnych dodatkowych wymagań. Zaleca się jedynie, aby pomieszczenie urzędu rejestracji było pomieszczeniem wydzielonym. Dostęp do niego powinien być kontrolowany i ograniczony tylko do grona osób związanych z funkcjonowaniem urzędu rejestracji (operatorów urzędu rejestracji, administratorów, agentów) oraz klientów urzędu rejestracji.

5.1.2.3. Zasilanie oraz klimatyzacja

Pomieszczenie urzędu rejestracji powinno być wyposażone w układ zasilania awaryjnego (UPS), wystarczający na kilka minut pracy systemu komputerowego od momentu zaniku zasilania. Po tym czasie uruchamiane są automatycznie agregaty prądotwórcze podtrzymujące napięcie w Unizeto CERTUM. Klimatyzacja nie jest wymagana.

5.1.2.4. Zagrożenie wodne

Niniejszy Kodeks Postępowania nie narzuca żadnych wymagań w tym zakresie.

5.1.2.5. Ochrona przeciwpożarowa

Niniejszy Kodeks Postępowania nie narzuca żadnych wymagań w tym zakresie.

5.1.2.6. Nośniki informacji

Nośniki informacji, na których przechowywane są archiwa oraz bieżące kopie danych, składowane są w sejfach zlokalizowanych w pomieszczeniu urzędu certyfikacyjnego.

5.1.2.7. Niszczenie informacji

Po upływie okresu przechowywania (patrz rozdz.4.6) papierowe oraz elektroniczne nośniki, zawierające informacje poufne lub sekretne są niszczone w specjalnych urządzeniach niszczących.

W przypadku kluczy kryptograficznych oraz numerów PIN nośniki, na których informacje te były przechowywane niszczone są w urządzeniach klasy DIN-3 (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji, np. kryptograficzne karty procesorowe, i ich ponowne użycie do tych samych lub innych celów). Sprzętowe urządzenia kryptograficzne (moduły) są zerowane zgodnie z dokumentacją producenta. Zerowanie urządzeń ma miejsce również w momencie oddawania modułu do serwisu.

5.1.2.8. Przechowywanie kopii bezpieczeństwa poza siedzibą urzędu rejestracji

Zaleca się przechowywanie poza urzędem rejestracji archiwów oraz bieżących kopii informacji przetworzonej przez system komputerowy.

5.1.2.9. Przechowywanie kopii bezpieczeństwa

Dane archiwalne, kopie zapasowe oraz inne, wrażliwe dane przechowywane są w skrytkach sejfu, do którego dostęp musi mieć przynajmniej dwoje ludzi.

5.1.3. Bezpieczeństwo subskrybenta

Subskrybent powinien chronić swoje hasło dostępu do systemu lub osobisty numer identyfikacyjny (PIN). Jeżeli używane hasło lub PIN są trudne do zapamiętania, mogą zostać zapisane jednak pod warunkiem przechowywania ich w sejfie, do którego dostęp mają tylko upoważnione osoby.

Użytkownik certyfikatu nie powinien pozostawiać bez opieki stacji roboczej oraz zainstalowanego na nim oprogramowania w momencie, gdy znajduje się ona w stanie kryptograficznie niezabezpieczonym, tzn. zostało wprowadzone hasło, PIN lub załadowany do obszaru kryptograficznego klucz prywatny.

W przypadku, gdy klucz prywatny subskrybenta (po zaszyfrowaniu przy pomocy hasła) jest umieszczony na niezabezpieczonym nośniku, np. na dyskietce, nośnik taki musi być chroniony przed niepowołanym dostępem podobnie jak portfel, karty kredytowe czy licencja na oprogramowanie. Jednym ze sposobów może być sejf.

Hasło używane do zabezpieczania nośnika wraz ze znajdującym się na nim kluczem prywatnym użytkownika nie mogą być przechowywane w tym samym miejscu co sam nośnik.

5.2. Kontrola zabezpieczeń organizacyjnych

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w Unizeto CERTUM - CCP, w urzędach rejestracji oraz w instytucjach, będących subskrybentami certyfikatów. Opisano także odpowiedzialność związaną z każdą pełnioną rolą.

5.2.1. Zaufane role

5.2.1.1. Zaufane role w Unizeto CERTUM - CCP

W Unizeto CERTUM - CCP określono następujące zaufane role, które mogą być pełnione przez jedną lub więcej osób:

Zespół ds. Rozwoju Usług PKI – określa kierunki rozwoju Unizeto CERTUM, wdraża oraz zarządza Polityką Certyfikacji, a także Kodeksem Postępowania Certyfikacyjnego;

Zespół Operacyjny Unizeto CERTUM - CCP – odpowiada za normalne funkcjonowanie Unizeto CERTUM - CCP;

administrator bezpieczeństwa – inicjuje instalację, konfiguruje oraz obsługuje oprogramowanie i sprzęt (w tym sieć) Unizeto CERTUM - CCP, inicjuje i wstrzymuje usługi świadczone przez Unizeto CERTUM - CCP, kieruje administratorami, inicjuje i nadzoruje proces generowania kluczy oraz sekretów współdzielonych, przydziela uprawnienia w zakresie zabezpieczeń oraz prawa dostępu użytkownikom, przydziela hasła nowym kontom, dokonuje przeglądów dzienników zdarzeń, nadzoruje prace serwisowe, nadzoruje audyty wewnętrzne i zewnętrzne, przyjmuje i odpowiada na raporty poaudycyjne, nadzoruje usuwanie usterek wskazanych w raportach,

administrator urzędu certyfikacji – kieruje operatorami urzędu certyfikacji, instaluje oprogramowanie użytkowe, konfiguruje system oraz sieć, uaktywnia i konfiguruje zabezpieczenia, zakłada konta innym użytkownikom systemu komputerowego Unizeto CERTUM - CCP, dokonuje przeglądu logów systemowych, weryfikuje zgodność Polityki Certyfikacji z Kodeksem Postępowania Certyfikacyjnego, generuje sekrety współdzielone oraz klucze, zarządza listami certyfikatów unieważnionych (CRL), tworzy kopie bezpieczeństwa, zmienia nazwy serwerów oraz adresy sieciowe,

operator urzędu certyfikacji – odzyskuje certyfikaty subskrybentów, unieważnia, zawiesza oraz odwiesza certyfikaty subskrybentów, żąda od subskrybentów uzyskania potwierdzeń wniosków w urzędzie rejestracji, zapewnia ciągłość kopiowania i archiwizowania baz danych oraz logów systemowych, zarządza bazami danych, ma dostęp do chronionych informacji o subskrybentach, ale nie posiada uprawnień do fizycznego dostępu do innych zasobów systemu komputerowego, lokuje kopie archiwów oraz bieżące kopie bezpieczeństwa poza siedzibą Unizeto CERTUM - CCP,

administrator systemowy – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, wstępnie konfiguruje system oraz sieć,

administrator repozytorium – zarządza publicznie dostępnymi katalogami używanymi przez Unizeto CERTUM - CCP, w szczególności tworzy oraz uaktualnia zawartość katalogów repozytorium, tworzy stronę WWW i zarządza dowiązaniami,

audytor – odpowiada za przegląd, archiwizowanie i zarządzanie dziennikami zdarzeń (w tym w szczególności sprawdzanie ich integralności) oraz prowadzenie audytów wewnętrznych pod kątem zgodności funkcjonowania urzędów certyfikacji zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego; odpowiedzialność ta rozciąga się także na wszystkie urzędy rejestracji, funkcjonujące w ramach Unizeto CERTUM - CCP,

wsparcie techniczne (serwis) – zapewnia ciągłość pracy systemu komputerowego oraz sieci, konserwuje oraz usuwa awarie systemu oraz sieci.

Przedstawiony podział ról zapobiega nadużyciom przy korzystaniu z systemu Unizeto CERTUM - CCP. Każdemu z użytkowników przydzielono tylko takie prawa, które wynikają z pełnionej przez niego roli i ponoszonej z tego tytułu odpowiedzialności.

Wymienione role mogą być łączone, kształtowane w inny sposób lub pozbawiane klauzuli zaufania, ale przy założeniu, że prowadzi to do wyróżnienia minimum czterech ról. Role te mogą obejmować: funkcje codziennie wykonywane przez system komputerowy Unizeto CERTUM - CCP, zarządzanie i audyt tych funkcji oraz zarządzanie zmianami mającymi istotny wpływ na system Unizeto CERTUM - CCP, m.in. jego politykę bezpieczeństwa, procedury oraz personel.

Podział odpowiedzialności pomiędzy wymienione role może być następujący:

administrator bezpieczeństwa – inicjuje instalację, konfigurację oraz obsługę oprogramowania i sprzętu (w tym sieci) Unizeto CERTUM - CCP, inicjuje i wstrzymuje usługi świadczone przez Unizeto CERTUM - CCP, kieruje administratorami, inicjuje i nadzoruje proces generowania kluczy oraz sekretów współdzielonych, bierze udział w uaktywnianiu modułu kryptograficznego i ładowaniu do niego kluczy operatorów (w ich obecności), przydziela uprawnienia w zakresie zabezpieczeń oraz prawa dostępu użytkownikom, przydziela hasła nowym kontom, raz w tygodniu dokonuje audytu logów systemowych, nadzoruje prace serwisowe, nadzoruje personel Unizeto CERTUM - CCP,

administrator urzędu certyfikacji – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, instaluje oprogramowanie aplikacyjne, konfiguruje system oraz sieć, uaktywnia i konfiguruje zabezpieczenia, zakłada konta innym użytkownikom systemu komputerowego Unizeto CERTUM - CCP, zmienia nazwy serwerów oraz adresy sieciowe, generuje sekrety współdzielone oraz klucze, zarządza listami certyfikatów unieważnionych (CRL), tworzy kopie ratunkowe,

operator urzędu certyfikacji – odzyskuje certyfikaty subskrybentów, unieważnia, zawiesza oraz odwiesza certyfikaty subskrybentów, zapewnia ciągłość kopiowania i archiwizowania baz danych oraz logów systemowych, zarządza bazami danych, ma dostęp do chronionych informacji o subskrybentach, ale nie posiada żadnych uprawnień do fizycznego dostępu do innych zasobów systemu komputerowego, lokuje kopie archiwów oraz bieżących kopii bezpieczeństwa poza siedzibą Unizeto CERTUM - CCP.

*Rola **audytora** nie może być łączona z żadną inną rolą w systemie Unizeto CERTUM - CCP. Żaden też podmiot występujący w innej roli niż audytor nie może przejmować jego odpowiedzialności.*

Dostęp do oprogramowania nadzorującego operacje realizowane przez Unizeto CERTUM - CCP posiadają tylko te osoby, których odpowiedzialność i obowiązki wynikają z pełnionych przez nie ról administratora systemowego oraz administratora urzędu certyfikacji.

5.2.1.2. Zaufane role w urzędzie rejestracji

Unizeto CERTUM - CCP musi być pewne, że obsługa urzędu rejestracji rozumie swoją odpowiedzialność wynikającą z identyfikacji oraz uwierzytelniania subskrybentów. Z tego powodu w urzędzie rejestracji wyróżnia się minimum trzy zaufane role:

administrator systemu – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, instaluje oprogramowanie aplikacyjne, konfiguruje system i oprogramowanie, uaktywnia i konfiguruje zabezpieczenia, zakłada konta i hasła operatorom, tworzy kopie bezpieczeństwa i archiwizuje informacje, przegląda zapisy zdarzeń (logi) oraz (razem z operatorem urzędu rejestracji) na polecenie administratora sekretów niszczy zbędną informację;

administrator sekretów – nadzoruje i przekazuje sekrety (klucze kryptograficzne i inne chronione dane) operatorom urzędu rejestracji, bierze udział w uaktywnianiu modułu kryptograficznego i ładowaniu do niego kluczy operatorów (w ich obecności), przekazuje i uaktywnia karty identyfikacyjne operatorów (jeśli znajdują się w stanie zablokowania), pośredniczy w kontaktach pomiędzy urzędem rejestracji a urzędem certyfikacji;

operator – weryfikuje tożsamość subskrybenta oraz poprawność złożonego przez niego wniosku, wydaje potwierdzenia wniosków i przekazuje je do urzędu certyfikacji, w przypadku operatora Głównego Urzędu Rejestracji (GUR) generuje klucze i pośredniczy w tworzeniu certyfikatu, wysyłając informację z wniosków do urzędu certyfikacji, zawiera umowy z subskrybentami na świadczenie usług przez urząd certyfikacji, archiwizuje w postaci papierowej wnioski i wydane potwierdzenia, które niszczy (na polecenie administratora sekretów) razem z administratorem.

Za sprawne działanie urzędu rejestracji odpowiada **agent Punktu Rejestracji**. Jego rola polega na zapewnieniu finansowania pracowników, zarządzaniu pracą operatora i administratora systemu, rozstrzyganiu sporów, podejmowaniu decyzji, wynikających z realizowanych przez urząd rejestracji czynności, nadzorowaniu audytu urzędu rejestracji. Agent może pośredniczyć także w kontaktach pomiędzy administratorem sekretów a operatorem urzędu rejestracji i administratorem systemu.

Administrator sekretów musi posiadać stały kontakt z osobami pełniącymi rolę administratora bezpieczeństwa i administratora urzędu certyfikacji w Unizeto CERTUM - CCP.

5.2.1.3. Zaufane role u subskrybenta

Subskrybent może wyznaczyć osobę (operatora), obsługującą oprogramowanie wspomagające elektroniczną wymianę dokumentów, np. z Unizeto CERTUM - CCP. Osoba taka jest osobiście odpowiedzialna za podpisanie, zaszyfrowanie i wysyłanie wiadomości. Osoba ta może również przygotowywać dane do elektronicznie wysyłanych wiadomości, chociaż ze względów praktycznych czynność tę może wykonywać osoba o mniejszych uprawnieniach.

5.2.2. Liczba osób wymaganych do realizacji zadania

Operacją, którą wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich generowaniu muszą być minimum dwie osoby, pełniące rolę administratora bezpieczeństwa oraz administratora systemu. Proces generowania kluczy urzędu certyfikacji mogą obserwować także osoby współdzielące klucz podzielony na części (sekret współdzielony) i przechowujące go w bezpiecznym miejscu.

W urzędzie certyfikacji wymagana jest obecność administratora bezpieczeństwa, administratora urzędu certyfikacji oraz odpowiedniej liczby osób współdzielących klucze (w tym klucz prywatny do podpisywania certyfikatów i list CRL) w trakcie ładowania ich do modułu kryptograficznego. Z kolei w urzędzie rejestracji ładowanie kluczy do modułu kryptograficznego odbywa się w obecności administratora sekretów oraz operatora urzędu rejestracji.

We wszystkich pozostałych przypadkach role wydzielone w Unizeto CERTUM - CCP oraz u subskrybenta mogą być wykonywane przez pojedyncze przypisane do tej roli osoby.

5.2.3. Identyfikacja oraz uwierzytelnianie ról

Personel Unizeto CERTUM - CCP jest poddawany procedurze identyfikacji oraz uwierzytelniania w następujących przypadkach:

umieszczania na liście osób posiadających dostęp do pomieszczeń Unizeto CERTUM - CCP,

umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci Unizeto CERTUM - CCP,

wydawania poświadczenia upoważniającego do wykonywania przypisanej roli,

przydzielania konta oraz hasła w systemie komputerowym Unizeto CERTUM - CCP.

Każde z powyższych poświadczeń oraz przypisanych kont:

musi być unikalne i bezpośrednio przypisane konkretnej osobie,

nie może być współdzielone z innymi osobami,

musi być ograniczone do funkcji (wynikających z roli pełnionej przez określoną osobę) realizowanych tylko za pośrednictwem dostępnego oprogramowania systemu Unizeto CERTUM - CCP, systemu operacyjnego oraz kontroli proceduralnych.

Operacje wykonywane w Unizeto CERTUM - CCP, które wymagają dostępu poprzez sieć dzieloną są zabezpieczone dzięki wprowadzonym mechanizmom silnego uwierzytelniania oraz szyfrowaniu przesyłanej informacji.

5.3. Kontrola personelu

Unizeto CERTUM - CCP musi mieć pewność, że osoby wykonujące swoje obowiązki wynikające z funkcji realizowanych przez urząd certyfikacji lub urząd rejestracji:

posiadają minimum wykształcenie średnie,

posiadają polskie obywatelstwo,

zawarły umowę, która dokładnie precyzuje rolę, którą mają pełnić oraz określa wynikające z niej prawa i obowiązki,

przeszły zaawansowane przeszkolenie z zakresu obowiązków, które będą wykonywały,

zostały przeszkolone w zakresie ochrony danych osobowych oraz informacji niejawnej,

w umowie lub regulaminie Unizeto CERTUM - CCP zawarto klauzule o nieujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa Unizeto CERTUM lub poufności danych subskrybenta,

nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem certyfikacji a działającymi w jego imieniu urzędami rejestracji.

5.3.1. Pochodzenie, kwalifikacje, doświadczenie oraz wymagane klauzule tajności

Zaleca się, aby osoby zatrudnione w Unizeto CERTUM - CCP lub w urzędzie rejestracji i pełniące zaufane role miały poświadczenie zaufania, wydane przez pełnomocnika ochrony. Poświadczenie takie nie jest wymagane w przypadku osób nie pełniących ról zaufanych.

Pełnienie zaufanej roli członka Zespołu ds. Rozwoju Usług PKI, administratora bezpieczeństwa, administratora urzędu certyfikacji oraz administratora sekretów w punkcie rejestracji, upoważnia do dostępu do informacji z klauzulą *niejawne*[38].

Procedury dostępu do informacji niejawnych oraz postępowania sprawdzającego zgodne są z ustawą *O ochronie informacji niejawnych z dnia 22 stycznia 1999 r.*, a zwłaszcza z art.36 i 37 dotyczącymi tzw. postępowania zwykłego.

Na wniosek administratora sekretów z postępowania sprawdzającego mogą być zwolnione osoby pełniące zaufane role w urzędach rejestracji poświadczających wnioski o wydanie certyfikatów. Zgodę na zwolnienie wyraża pełnomocnik ochrony Unizeto CERTUM - CCP.

5.3.2. Procedura postępowania sprawdzającego w przypadku ról nie wymagających zaufania

Niniejszy Kodeks Postępowania Certyfikacyjnego nie nakłada żadnych wymagań w tym zakresie.

5.3.3. Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w Unizeto CERTUM - CCP lub urzędzie rejestracji musi przejść cykl szkoleń dotyczących:

zasad Polityki Certyfikacji,

zasad Kodeksu Postępowania Certyfikacyjnego,

zasad zawartych w *„Księdze Urzędu Rejestracji”*,

zasad i mechanizmów zabezpieczeń stosowanych przez urząd certyfikacji oraz urzędy rejestracji,

oprogramowania systemu komputerowego urzędu certyfikacji oraz urzędu rejestracji,

obowiązków, które będą pełniły lub aktualnie pełnią,

[38] Klauzula *niejawne* oznacza, że nieuprawnione ujawnienia tego typu informacji mogłoby spowodować szkodę dla prawnie chronionych interesów obywateli albo jednostki organizacyjnej [11].

procedur realizowanych po awariach lub katastrofach systemu urzędu certyfikacji.

Po zakończeniu szkolenia jego uczestnicy podpisują dokument potwierdzający zapoznanie się z Polityką Certyfikacji, Kodeksem Postępowania Certyfikacyjnego oraz akceptację wynikających z nich ograniczeń.

5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione w rozdz.5.3.3 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu Unizeto CERTUM - CCP lub urzędów rejestracji.

5.3.5. Rotacja stanowisk

Niniejszy Kodeks Postępowania Certyfikacyjnego nie nakłada żadnych wymagań w tym zakresie.

5.3.6. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie administrator urzędu rejestracji w porozumieniu z administratorem bezpieczeństwa (w przypadku pracowników Unizeto CERTUM) lub administrator systemu (w przypadku pracowników urzędu rejestracji) może sprawcy takiego zdarzenia zawiesić dostęp do systemu Unizeto CERTUM lub urzędu rejestracji. Kary grożące pracownikowi za podejmowanie tego typu działań powinny być zgodne z obowiązującym prawem i zawarte w określonych procedurach.

5.3.7. Pracownicy kontraktowi

Pracownicy kontraktowi (serwis zewnętrzny, wykonawcy podsystemów i oprogramowania, producenci, itp.) poddawani są takiej samej procedurze, jak stali pracownicy Unizeto CERTUM - CCP i urzędu rejestracji (patrz rozdz.5.3.1, 5.3.2 i 5.3.3). Dodatkowo pracownicy kontraktowi podczas przebywania na terenie Unizeto CERTUM - CCP lub urzędu rejestracji muszą zawsze znajdować się w towarzystwie pracownika Unizeto CERTUM - CCP lub urzędu rejestracji.

5.3.8. Dokumentacja przekazana personelowi

Unizeto CERTUM - CCP, jak również urząd rejestracji muszą umożliwić swojemu personelowi dostęp do następujących dokumentów:

Polityki Certyfikacji,

Kodeksu Postępowania Certyfikacyjnego,

„Księgi Urzędu Rejestracji”,

zakresu obowiązków i uprawnień wynikających z pełnionej roli.

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych urzędów certyfikacji, urzędów rejestracji oraz użytkownika, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1. Generowanie i stosowanie par kluczy

Procedury zarządzania kluczami dotyczą bezpiecznego przechowywania i używania kluczy, będących pod kontrolą ich właścicieli. Szczególnej uwagi wymaga generowanie i ochrona par kluczy prywatnych Unizeto CERTUM, od których zależy bezpieczeństwo funkcjonowania całego systemu certyfikowania kluczy publicznych.

Urząd certyfikacji **CA-Certum** posiada przynajmniej jeden autocertyfikat. Klucz prywatny, komplementarny z zawartym w autocertyfikacie kluczem publicznym, stosowany jest jedynie do podpisywania certyfikatów kluczy publicznych urzędów certyfikacji **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** oraz wystawienia listy certyfikatów unieważnionych (CRL) i tzw. certyfikatów operacyjnych urzędu certyfikacji, koniecznych do funkcjonowania urzędu. Podobne zastosowania znajdują klucze prywatne, będące w posiadaniu każdego z urzędów **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** i komplementarne z odpowiednimi kluczami publicznymi zawartymi w certyfikatach wystawionych przez **CA-Certum** każdemu z tych urzędów.

Klucze będące w posiadaniu każdego z urzędów certyfikacji powinny umożliwić im:

podpisywanie certyfikatów i list CRL (klucz publiczny związany z kluczem prywatnym uwierzytelniony jest w postaci autocertyfikatu – przypadek **CA-Certum** lub certyfikatu – przypadek **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**);

podpisywanie wiadomości, wymienianych z subskrybentami oraz urzędami rejestracji (klucz operacyjny);

do uzgadniania kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem a otoczeniem (klucz operacyjny).

Do realizacji podpisu cyfrowego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1, zaś do uzgadniania kluczy – algorytm Diffie-Hellmana.

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędu certyfikacji **CA-Certum** , urzędów **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** oraz innych urzędów pośrednich generowane są w siedzibie Unizeto CERTUM - CCP w obecności wybranej, przeszkolonej grupy zaufanych osób (w grupie tej muszą znajdować się także administrator bezpieczeństwa, administrator urzędu certyfikacji). Taka grupa osób konieczna jest tylko w przypadku generowania kluczy do podpisywania certyfikatów i list CRL. Klucze operacyjne mogą być generowane w obecności administratora bezpieczeństwa oraz administratora urzędu certyfikacji.

Klucze urzędów certyfikacji funkcjonujących w ramach Unizeto CERTUM - CCP generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu generowania kluczy, spełniającego wymagania klasy FIPS 140-2 Level 3 lub wyżej.

Procedury generowania kluczy urzędów certyfikacji są zgodne z przyjętą w Unizeto CERTUM - CCP procedurą generowania kluczy. Czynności wykonywane w trakcie generowania każdej pary kluczy są rejestrowane, datowane i podpisywane przez każdą uczestniczącą w procedurze osobę. Zapisy te są przechowywane dla potrzeb audytu oraz bieżących przeglądów systemu.

Szczegółowy opis procedury generowania kluczy urzędów certyfikacji zamieszczony jest jest w dokumencie „Procedury generowania kluczy urzędu certyfikacji Unizeto CERTUM". Dokument ma status „niejawny" i udostępniany jest tylko administratorowi bezpieczeństwa i audytorowi.

Operatorzy urzędów rejestracji posiadają jedynie klucze do podpisywania (potwierdzania) wniosków subskrybentów oraz wiadomości wysyłanych do urzędu certyfikacji. Klucze te generowane są przez operatorów (w obecności administratora sekretów) przy użyciu wiarygodnego oprogramowania dostarczonego przez urząd certyfikacji oraz sprzężonego z nim certyfikowanego sprzętowego modułu kryptograficznego klasy przynajmniej FIPS 140-2 Level 2.

Każdy ze subskrybentów z zasady samodzielnie generuje dla swoich potrzeb każdą parę kluczy lub może to zadanie zlecić urzędowi certyfikacji.

Unizeto CERTUM - Centrum Certyfikacji Powszechne może na żądanie subskrybenta lub operatora urzędu rejestracji wygenerować klucze i bezpieczny sposób dostarczyć je wnioskodawcom. Do generowania kluczy używany jest w takich przypadkach sprzętowy moduł kryptograficzny, spełniający wymagania klasy FIPS 140-2 Level 3 lub wyżej (patrz rozdz.6.1.2).

Szczegółowy opis procedury generowania kluczy użytkowników końcowych opisana jest w dokumencie „Księga Urzędu Rejestracji". Dokument ma status „niejawne" i udostępniany jest tylko pracownikom Unizeto CERTUM.

6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji CA-Certum

Procedura generowania początkowych kluczy **CA-Certum** wykorzystywane jest zawsze podczas inicjowania pracy systemu Unizeto CERTUM - CCP lub w przypadku gdy istnieje podejrzenie, że któryś z kolejnych kluczy urzędu certyfikacji został ujawniony. Polega ona na:

bezpiecznym wygenerowaniu głównej pary kluczy do podpisu certyfikatów i list CRL - główna para kluczy ma postać $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(1)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(1)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),

utworzeniu autocertyfikatu klucza publicznego $\mathbf{K_{GPK(1)}}$.

Po wygenerowaniu pary kluczy do podpisu certyfikatów i list CRL, rozproszeniu klucza prywatnego i uaktywnieniu go w sprzętowym module kryptograficznym, klucze te mogą być

wykorzystywane w operacjach kryptograficznych do momentu utraty ważności lub ich ujawnienia.

6.1.1.2. Procedury aktualizacji kluczy CA-Certum

Klucze **CA-Certum** mają skończony okres życia, po którego upływie muszą zostać uaktualnione.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do podpisywania certyfikatów i list CRL (autocertyfikatu). Polega ona na wydaniu przez **CA-Certum** specjalnych certyfikatów ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym stary autocertyfikat **CA-Certum**, na bezpieczne przejście do pracy z nowym autocertyfikatem, zaś nowym użytkownikom końcowym posiadającym nowy autocertyfikat na bezpieczne pozyskanie starego autocertyfikatu, umożliwiającego weryfikację istniejących danych (patrz RFC 2510).

Aby uzyskać wspomniany wyżej efekt **CA-Certum** musi stosować procedurę, która po wygenerowaniu nowej pary kluczy zabezpieczy (uwiarygodni) nowy klucz publiczny przy pomocy starego (poprzednio stosowanego) klucza prywatnego, i odwrotnie, stary klucz publiczny zabezpieczony zostanie przy pomocy nowego klucza prywatnego. Oznacza to, że w momencie uaktualniania autocertyfikatu urzędu certyfikacji **CA-Certum**, oprócz nowego autocertyfikatu zostaną utworzone dwa dodatkowe certyfikaty. Łącznie istnieją cztery certyfikaty do podpisywania certyfikatów i list CRL: stary **autocertyfikat StaryStarym** (stary klucz publiczny podpisany starym kluczem prywatnym), nowy **autocertyfikat NowyNowym** (nowy klucz publiczny podpisany nowym kluczem prywatnym), **autocertyfikat StaryNowym** (stary klucz publiczny podpisany nowym kluczem prywatnym) oraz **autocertyfikat NowyStarym** (nowy klucz publiczny podpisany starym kluczem prywatnym).

Procedura aktualizacji nowej pary kluczy **CA-Certum**, przeznaczonej do podpisywania certyfikatów i list CRL przebiega następująco:

Generowanie nowej, kolejnej i-tej głównej pary kluczy $\mathbf{GPK_{(i)}=\{K^{-1}_{GPK(i)}, K_{GPK(i)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(i)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(i)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową).

Utworzenie autocertyfikatu zawierającego nowy klucz publiczny **CA-Certum**, podpisany przy pomocy starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ (**autocertyfikat NowyStarym**).

Deaktywacja starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ i aktywacja nowego klucza prywatnego $\mathbf{K^{1}_{GPK(1)}}$ – w sprzętowym module kryptograficznym znajduje się nowy klucz prywatny do podpisywania certyfikatów i list CRL.

Utworzenie autocertyfikatu zawierającego stary klucz publiczny CA-Certum, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(1)}}$ (**autocertyfikat StaryNowym**).

Utworzenie autocertyfikatu zawierającego nowy klucz publiczny **CA-Certum**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(1)}}$ (**autocertyfikat NowyNowym**).

Opublikowanie utworzonych certyfikatów w repozytorium, rozesłanie informacji o nowych certyfikatach oraz opcjonalnie umieszczenie skrótu z nowego klucza publicznego w wiarygodnej prasie.

Po wygenerowaniu i uaktywnieniu nowego klucza prywatnego (może to nastąpić w dowolnym momencie okresu ważności starego autocertyfikatu), urząd **CA-Certum** podpisuje certyfikaty użytkowników końcowych tylko przy pomocy nowego klucza prywatnego.

Stary klucz publiczny (stary autocertyfikat) jest w użyciu aż do momentu, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego autocertyfikatu (nowego klucza publicznego) **CA-Certum** (powinno to nastąpić najpóźniej w momencie minięcia okresu ważności starego autocertyfikatu).

Początek i koniec okresu ważności **autocertyfikatu StaryNowym** pokrywa się z początkiem i końcem okresu ważności starego autocertyfikatu.

Okres ważności **autocertyfikatu NowyStarym** rozpoczyna się w momencie wygenerowania nowej pary kluczy i kończy w chwili, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego autocertyfikatu (nowego klucza publicznego) **CA-Certum** (powinno to nastąpić najpóźniej w momencie minięcia okresu ważności starego autocertyfikatu).

Okres ważności **autocertyfikatu NowyNowym** rozpoczyna się w chwili wygenerowania nowej pary kluczy, zaś kończy się przynajmniej 180 dni po następnej przewidywanej chwili generowania kolejnej pary kluczy. Wymóg ten oznacza, że urząd certyfikacji **CA-Certum** zaprzestaje używać klucza prywatnego do podpisywania certyfikatów i list CRL przynajmniej na 180 dni przed datą upłynięcia aktualności autocertyfikatu, z którym klucz prywatny jest związany.

6.1.1.3. Procedury aktualizacji kluczy urzędów certyfikacji podległych CA-Certum

Procedury aktualizacji kluczy urzędów **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** realizowane są podobnie jak w przypadku aktualizacji kluczy urzędu **CA-Certum** (patrz rozdz.6.1.1.2), poza jednym wyjątkiem: **certyfikat NowyNowym** wystawiany jest przez urząd **CA-Certum**.

6.1.1.4. Procedury recertyfikacji kluczy CA-Certum i innych urzędów certyfikacji

Certyfikaty będące w posiadaniu urzędu certyfikacji CA-Certum oraz innych urzędów mogą być recertyfikowane. Realizowane jest to tylko w przypadkach opisanych w rozdz.3.2.2. Przed wydaniem nowego certyfikatu urząd certyfikacji ocenia, czy długość klucza gwarantuje mu dalsze bezpieczeństwo w okresie na który przedłużany jest certyfikat.

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

Jeśli klucze użytkowników końcowych generowane są centralnie przez urząd certyfikacji, to klucze te mogą przekazane przy pomocy dwóch metod:

realizowanej z wykorzystaniem schematu uzgadniania kluczy w oparciu o będącą w posiadaniu urzędu certyfikacji parę kluczy Diffie-Hellmana; urząd certyfikacji generuje klucz sesji (symetryczny), szyfruje wygenerowane klucze i w trybie *on-line* odsyła je subskrybentowi,

klucze zapisywane są w tokenie (np. identyfikacyjnej karcie elektronicznej) lub na dyskietce (tylko **Certum Level I**, w tym przypadku klucze są szyfrowane i zapisywane w formacie PKCS#12) i przekazywane subskrybentowi osobiście lub pocztą kurierską; dane do uaktywnienia karty (m.in. PIN) lub odszyfrowania kluczy (hasło) podane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji.

Unizeto CERTUM - Centrum Certyfikacji Powszechne gwarantuje, że w żadnym momencie po wygenerowaniu na żądanie subskrybenta klucza prywatnego nie użyje go do realizacji podpisu cyfrowego ani nie stworzy warunków, które umożliwią zrealizowanie takiego podpisu innemu podmiotowi, poza właścicielem tego klucza.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Subskrybenci oraz operatorzy urzędów rejestracji dostarczają wygenerowane przez siebie klucze publiczne w postaci żądań elektronicznych, których format musi być zgodny z realizowanymi przez urząd certyfikacji, urząd rejestracji oraz subskrybenta protokołami PKCS#10 *Certification Request Syntax*[39] (CRS).

W chwili obecnej Unizeto CERTUM - Centrum Certyfikacji Powszechne akceptuje jedynie żądania nadsyłane w formacie PKCS#10 Certification Request Syntax (CRS) oraz Netscape SPKAC (ang. Signed Public Key and Challenge).

Żądania wysyłane do urzędu certyfikacji mogą w niektórych przypadkach wymagać potwierdzenia w urzędzie rejestracji (patrz rozdz.3 i rozdz.4).

Dostarczenie kluczy publicznych staje się zbędne przypadku, gdy klucze na żądanie subskrybentów oraz operatorów urzędów rejestracji zostały wygenerowane przez ten urząd certyfikacji, który dla wygenerowanego klucza publicznego wystawia jednocześnie certyfikat.

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu wydającego certyfikaty rozpowszechniane są tylko w formie certyfikatów zgodnych z zaleceniem ITU-T X.509 v.3, przy czym w przypadku urzędu certyfikacji **CA-Certum** certyfikat ma postać autocertyfikatu.

Urzędy certyfikacji Unizeto CERTUM - CCP rozpowszechniają swoje certyfikaty dwoma sposobami:

umieszczają w ogólnie dostępnym repozytorium Unizeto CERTUM - CCP; pobranie certyfikatu wymaga udania się na serwisy webowe znajdujące się pod adresem: http://www.certum.pl/repozytorium.

dystrybuowane są razem z oprogramowaniem (przeglądarki internetowe, programy pocztowe, itp.), które umożliwia korzystanie z usług Unizeto CERTUM - CCP.

W przypadku aktualizacji kluczy urzędów certyfikacji Unizeto CERTUM - CCP w repozytorium umieszczane są wszystkie dodatkowe autocertyfikaty lub certyfikaty, powstałe w wyniku realizacji procedury opisanej w rozdz.6.1.1.2 lub 6.1.1.3.

6.1.5. Długości kluczy

Długości kluczy używanych przez Unizeto CERTUM - CCP przez operatorów urzędów rejestracji oraz użytkowników końcowych (subskrybentów) podano w Tab.6.1.

[39] RFC 2314 (CRS): B. Kaliski *PKCS #10: Certification Request Syntax, Version 1.5*, March 1998

Tab.6.1 Stosowane klucze i ich długości

Typ właściciela klucza	Główny rodzaj zastosowania klucza			
	RSA do podpisu certyfikatów i list CRL	RSA do podpisu wiadomości	RSA do wymiany kluczy	Diffie-Hellman
CA-Certum	2048 bitów	–	–	–
CA-Certum Level I	1024 bity	–	–	–
CA-Certum Level II	1024 bity	–	–	–
CA-Certum Level III	1024 bity	–	–	–
CA-Certum Level IV	1024 bity	–	–	–
Operator urzędu rejestracji	–	1024 bity	–	–
Osoby fizyczne oraz urządzenia osób fizycznych	–	1024 bity	1024 bity	1024 bity
Osoby prawne oraz urządzenia osób prawnych	–	1024 bity	1024 bity	1024 bity

6.1.6. Generowanie parametrów klucza publicznego

Niniejszy Kodeks Postępowania Certyfikacyjnego nie nakłada żadnych wymagań w tym zakresie. Zaleca się jednak, aby w przypadku generowania kluczy RSA i DSA spełnione były minimalne wymagania określone w *„Algorithms and Parameters for Secure Electronic Signatures”* [25].

6.1.7. Weryfikacja jakości klucza

Za jakość wygenerowanego klucza oraz jego weryfikację odpowiedzialność ponoszą ich twórcy. Wymaga się, aby weryfikacji poddano:

zdolność do realizacji operacji szyfrowania i deszyfrowania, w tym podpisu cyfrowego i jego weryfikacji,

proces generacji klucza, który musi bazować na silnych kryptograficznie generatorach liczb losowych, najlepiej opartych na fizycznych źródłach szumu,

odporność na znane ataki (dotyczy to algorytmów kryptograficznych RSA i DH).

Dodatkowo każdy urząd certyfikacji, po otrzymaniu lub wygenerowaniu (na żądanie subskrybenta) klucza publicznego poddaje go odpowiednim testom na zgodność z ograniczeniami nałożonymi przez Kodeks Postępowania Certyfikacyjnego (m.in. długość modułu oraz eksponenty).

Weryfikacja jakości parametrów klucza, obejmująca m.in. testy pierwszości w przypadku liczb pierwszych powinna być obligatoryjna w przypadku centralnego generowania kluczy i realizowana wg zaleceń określonych w *„Algorithms and Parameters for Secure Electronic Signatures”* [25].

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

Dopuszczalne sposoby generowania kluczy uzależnione są od typu polityki certyfikacji i przedstawione są Tab.6.2.

W przypadku urzędów certyfikacji klucze generowane są przy pomocy sprzętowych modułów kryptograficznych, zgodnych z wymaganiami opisanymi w rozdz.6.2.1.

Klucze operatorów urzędów rejestracji generowane są także przy pomocy sprzętowych modułów kryptograficznych, jednak o mniejszych wymaganiach nakładanych na ich własności (rozdz.6.2.1).

W przypadku subskrybentów dopuszcza się zarówno sprzętowe, jak i programowe generowanie kluczy (rozdz.6.2.1).

Tab.6.2 Sposób generowania kluczy subskrybenta

Nazwa polityki certyfikacji	Sposób generowania kluczy
Certum Level I	Sprzętowy lub programowy
Certum Level II	Sprzętowy lub programowy
Certum Level III	Sprzętowy lub programowy
Certum Level IV	Sprzętowy lub programowy

6.1.9. Zastosowania kluczy

Sposób użycia klucza określony jest w polu **KeyUsage** (patrz rozdz.7.1.1.2) rozszerzeń standardowych certyfikatu zgodnego z X.509 v3. Pole to jednak nie musi być obligatoryjnie weryfikowane przez aplikacje, które korzystają z tego certyfikatu.

Użycie poszczególnych bitów w polu **KeyUsage** musi być zgodne z następującymi zasadami (ustawiony bit oznacza odpowiednio):

a) **digitalSignature**: przeznaczenie certyfikatu do weryfikacji podpisu cyfrowego, złożonego w innych celach niż określonych w pkt. b), f) i g);

b) **nonRepudiation**: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt. f) i g). Ustawiony bit **nonRepudiation** może być tylko w certyfikatach kluczy publicznych użytkowników służących do weryfikacji podpisów cyfrowych i nie może być łączony z innymi przeznaczeniami, w szczególności z tymi o których mowa w pkt. c) - e) związanymi z zapewnieniem poufności;

c) **keyEncipherment**: do szyfrowania kluczy algorytmów symetrycznych zapewniających poufność danych;

d) **dataEncipherment**: do szyfrowania danych użytkownika, innych niż określonych w pkt. c) i e);

e) **keyAgreement**: do protokołów uzgadniania klucza;

f) **keyCertSign**: klucz publiczny jest używany do weryfikacji podpisów cyfrowych w certyfikatach i zaświadczeniach certyfikacyjnych wydanych przez podmiot świadczący usługi certyfikacyjne;

g) **cRLSign**: klucz publiczny jest używany do weryfikacji podpisów cyfrowych w listach unieważnionych i zawieszonych certyfikatów wydanych przez podmiot świadczący usługi certyfikacyjne;

h) **encipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do szyfrowania danych w protokołach uzgadniania klucza;

i) **decipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do odszyfrowania danych w protokołach uzgadniania klucza.

W przypadku certyfikatów wydanych według polityk **Certum Level I**, **Certum Level II**, **Certum Level III** i **Certum Level IV** dopuszcza się stosowanie jednego klucza zarówno w operacjach realizacji podpisu cyfrowego (bit **digitalSignature**), jak i też szyfrowania danych (bit **dataEncipherment**). Dzięki temu możliwe jest użycie tego typu certyfikatu np. w aplikacjach bazujących na protokole *Secure Multipurpose Internet Mail Extensions (S/MIME).*

Certyfikaty używane jednocześnie do podpisywania i szyfrowania mogą być wydawane jedynie subskrybentom. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie do weryfikacji podpisów cyfrowych, poza przypadkami wyraźnie określonymi w niniejszym Kodeksie Postępowania Certyfikacyjnego.

6.2. Ochrona klucza prywatnego

Każdy subskrybent, a także operatorzy urzędów certyfikacji i urzędy certyfikacji generują oraz przechowują swój klucz prywatny, wykorzystując w tym celu godny zaufania system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu. Jeśli urząd certyfikacji (patrz rodz.6.1.1) generuje parę kluczy w imieniu upoważniającego go subskrybenta, musi przekazać go w sposób bezpieczny oraz narzucić subskrybentowi ochronę klucza prywatnego (patrz rozdz.6.1.2).

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji i urzędy rejestracji są zgodne z wymaganiami normy FIPS 140-2. W przypadku używania przez subskrybenta sprzętowej ochrony klucza prywatnego zaleca się, aby spełniał on także wymagania FIPS 140-2 lub ITSEC.

Tab. 6.3 Minimalne wymagania nakładane na moduł kryptograficzny

Nazwa polityki certyfikacji	Urzędy certyfikacji	Subskrybent	Urząd rejestracji
Certum CA	Sprzętowy FIPS 140-2 Level 3 i wyżej	–	–
Certum Level I	Sprzętowy FIPS 140-2 Level 2 i wyżej	–	Sprzętowy FIPS 140-2 Level 1 i wyżej lub ITSEC E2 lub wyżej
Certum Level II	Sprzętowy FIPS 140-2 Level 2 i wyżej	Sprzętowy FIPS 140-2 Level 1 i wyżej lub ITSEC E2 lub wyżej	Sprzętowy FIPS 140-2 Level 1 i wyżej lub ITSEC E2 lub wyżej
Certum Level III	Sprzętowy FIPS 140-2 Level 2 i wyżej	Sprzętowy FIPS 140-2 Level 1 i wyżej lub ITSEC E2 lub wyżej	Sprzętowy FIPS 140-2 Level 2 i wyżej lub ITSEC E3 lub wyżej
Certum Level IV	Sprzętowy FIPS 140-2 Level 2 i wyżej	Sprzętowy FIPS 140-2 Level 1 i wyżej lub ITSEC E2 lub wyżej	Sprzętowy FIPS 140-2 Level 2 i wyżej lub ITSEC E3 lub wyżej

Realizacja podpisu cyfrowego oraz szyfrowanie informacji są zgodne z zaleceniem PKCS#7.

Klucze prywatne (a także publiczne) mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku (aktualna data jest mniejsza od daty początku okresu ważności klucza),

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów cyfrowych), zaś aktualna data zawiera się w okresie ważności klucza i klucz nie jest unieważniony,

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu cyfrowego - klucz jest przeterminowany lub też klucza publicznego do szyfrowania - klucz publiczny jest przeterminowany); aktualna data jest większa od daty końca okresu ważności klucza i klucz nie jest unieważniony.

6.2.2. Podział klucza prywatnego na części

Ochronie za pomocą podziału klucza na części podlegają klucze prywatne urzędów certyfikacji **CA-Certum** i **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** stosowane do realizacji podpisów certyfikatów i list CRL oraz innych operacji kryptograficznych, np. szyfrowanie wiadomości.

W Unizeto CERTUM - CCP dopuszcza się bezpośrednią i pośrednią metodę podziału klucza prywatnego. W przypadku zastosowania metody bezpośredniej podziałowi na części poddawany jest klucz prywatny, z kolei w przypadku metody pośredniej podziałowi na części podlega kluczy symetryczny, którego wcześniej użyto do zaszyfrowania klucza prywatnego.

W obu przypadkach klucze (odpowiednio asymetryczny lub symetryczny) dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Tab.6.4.

Sekrety współdzielone zapisywane są na kartach elektronicznych, chronione numerem PIN i w uwierzytelniony sposób przekazywane posiadaczom sekretu współdzielonego.

Tab.6.4 Podział i dystrybucja sekretów współdzielonych

Organ wydający certyfikaty	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego, wykorzystywanego przy podpisywaniu certyfikatów subskrybentów i list CRL	Całkowita liczba dystrybuowanych sekretów
CA-Certum	3	5
CA Certum Level I	2	3
CA Certum Level II	2	3
CA Certum Level III	2	3
CA Certum Level IV	2	3

Procedura przekazania sekretów musi przewidywać udział posiadacza sekretu w procesie generowania kluczy i ich podziału, obejmować akceptację przekazanego sekretu, akceptację

odpowiedzialności za przechowywany sekret oraz określać warunki i zasady udostępniania sekretu współdzielonego upoważnionym do tego osobom.

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

Każdy posiadacz sekretu współdzielonego, zanim wejdzie w jego posiadanie, powinien osobiście obserwować tworzenie, weryfikację poprawności utworzenia sekretu oraz jego dystrybucję. Każda część sekretu musi być przekazana posiadaczowi sekretu współdzielonego na karcie elektronicznej, chronionej tylko jemu znanym numerem PIN. Fakt otrzymania sekretu oraz zgodność sposobu jego utworzenia z zasadami niniejszego Kodeksu posiadacz sekretu potwierdza własnoręcznym podpisem, złożonym na odpowiednim formularzu, którego kopia przekazywana jest urzędowi certyfikacji, właścicielowi sekretu (części klucza).

6.2.2.2. Zabezpieczenie sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien chronić go przed ujawnieniem. Z wyjątkami, opisanymi dalej, posiadacz sekretu współdzielonego deklaruje, że:

nie ujawni, nie skopiuje, nie udostępni stronom trzecim, ani też nie użyje sekretu w sposób nieautoryzowany,

nie wyjawi (bezpośrednio lub pośrednio), że jest posiadaczem sekretu współdzielonego,

nie będzie przechowywał sekretu współdzielonego w miejscu, które uniemożliwi odzyskanie sekretu w przypadku, gdy posiadacz sekretu będzie poza miejscem normalnego pobytu lub będzie nieosiągalny.

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien udostępniać współdzielony sekret autoryzowanym osobom prawnym (wyszczególnionym w formularzu, podpisanym przez posiadacza w momencie powierzania sekretu) tylko po uprzedniej autoryzacji czynności przekazania sekretu. Fakt ten powinien zostać odnotowany w systemie zabezpieczeń postaci odpowiedniego logu transakcji.

W sytuacjach klęsk żywiołowych (deklarowanych wcześniej przez wydawcę sekretu współdzielonego), posiadacz sekretu współdzielonego powinien zgłosić się do ośrodka zapasowego Unizeto CERTUM - CCP, zgodnie z instrukcją otrzymaną od wydawcy sekretu. Zanim posiadacz sekretu współdzielonego stawi się w żądane miejsce powinien uzyskać od wydawcy sekretu uwierzytelnione potwierdzenie zaistniałego faktu oraz polecenie udania się w zalecane miejsce. Do ośrodka zapasowego Unizeto CERTUM - CCP sekret współdzielony powinien zostać dostarczony osobiście w sposób, który umożliwi użycie go w przypadku klęski żywiołowej w procedurze powrotu urzędu certyfikacji do stanu normalnego.

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien wykonywać swoje obowiązki zgodnie z postanowieniami niniejszego Kodeksu oraz w sposób odpowiedzialny i rozważny we wszystkich możliwych sytuacjach. Posiadacz sekretu powinien poinformować wydawcę sekretu współdzielonego o zgubieniu, kradzieży, niewłaściwym ujawnieniu lub naruszeniu ochrony sekretu, natychmiast po zorientowaniu się, że fakt taki miał miejsce. Posiadacz sekretu współdzielonego nie odpowiada za zaniedbanie swoich obowiązków wskutek przyczyn, które

były poza kontrolą posiadacza sekretu, ale ponosi odpowiedzialność za niewłaściwe ujawnienie sekretu lub zaniedbanie obowiązku poinformowania wydawcy sekretów współdzielonych o niewłaściwym ujawnieniu lub naruszenia ochrony sekretu, wynikającymi z własnego błędu, w tym z zaniedbania lub lekkomyślności.

6.2.3. Deponowanie klucza prywatnego

Klucze prywatne urzędów certyfikacji, ani też innych subskrybentów, dla potrzeb których Unizeto CERTUM - CCP generuje klucze lub które są dostępne, nie podlegają operacji deponowania (*ang. escrow*).

Kopie prywatnych kluczy subskrybentów mogą być jednak archiwizowane w urzędzie certyfikacji lub u subskrybenta i następnie odzyskiwane. Może to być robione na dwa sposoby:

subskrybent może wygenerować klucz symetryczny, zaszyfrować nim klucz prywatny i przekazać urzędowi certyfikacji albo zaszyfrowany klucz prywatny (klucz symetryczny przechowuje subskrybent) albo w bezpieczny sposób klucz symetryczny (zaszyfrowany klucz prywatny przechowywany jest u subskrybenta),

subskrybent w bezpieczny sposób przesyła klucz prywatny do urzędu certyfikacji, gdzie jest on deponowany w skarbcu elektronicznym (*ang. Electronic Vault*).

Jeśli subskrybent chce odzyskać złożoną w urzędzie certyfikacji kopię klucza prywatnego, to musi zażądać:

w pierwszym przypadku przysłania albo zaszyfrowanego klucza prywatnego (klucz deszyfrujący posiada subskrybent) albo klucza deszyfrującego (zaszyfrowana kopia klucza prywatnego jest w posiadaniu subskrybenta), zaś

w drugim bezpiecznego przekazania subskrybentowi zarchiwizowanego w urzędzie certyfikacji klucza prywatnego.

6.2.4. Kopie zapasowe klucza prywatnego

Urzędy certyfikacji funkcjonujące w ramach Unizeto CERTUM - CCP tworzą kopie swoich kluczy prywatnych. Kopie te wykorzystywane są w przypadku potrzeby realizacji normalnej lub awaryjnej (np. po wystąpieniu klęski żywiołowej) procedury odzyskiwania kluczy.

W zależności od zastosowanej metody podziału klucza na części (odpowiednio bezpośredniej lub pośredniej, patrz rozdz.6.2.2) kopie klucza prywatnego przechowywane są w częściach lub w całości (po zaszyfrowaniu kluczem symetrycznym).

Sekrety współdzielone, kopie klucza szyfrującego sekrety, jak też chroniące je numery PIN przechowywane są w różnych, fizycznie chronionych, miejscach. W żadnym z tych miejsc nie jest przechowywany taki zestaw kart oraz numerów PIN, który umożliwia odtworzenie klucza urzędu certyfikacji.

Urzędy Unizeto CERTUM - CCP nie przechowują kopii kluczy prywatnych operatorów urzędów rejestracji. Kopie kluczy subskrybentów tworzone są jedynie na ich żądanie i zgodnie z metodami opisanymi w rozdz.6.2.3.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędów certyfikacji stosowane do realizacji podpisów cyfrowych nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywania przy ich użyciu operacji

podpisywania lub upływie okresu ważności komplementarnego z nimi certyfikatu lub jego unieważnieniu.

Klucze prywatne urzędów certyfikacji stosowane w operacjach uzgadniania lub szyfrowania kluczy muszą być archiwizowane po utracie okresu ważności odpowiadającego im certyfikatu lub po jego unieważnieniu. Archiwizowane klucze muszą być dostępne przez 25 lat, z tego przez okres 15 lat musi być dostępny w trybie *on-line*.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Operacja wprowadzania kluczy prywatnych do modułu kryptograficznego jest realizowana w trzech sytuacjach:

klucze są generowane poza modułem kryptograficznym; sytuacja taka ma miejsce np. w przypadku generowania (na żądanie subskrybenta) kluczy przez urząd certyfikacji, załadowania ich na kartę elektroniczną lub inny token sprzętowy przed planowanym przekazaniem ich subskrybentowi; podobną operację ładowania kluczy może wykonać subskrybent w przypadku, gdy klucze te są przekazywane mu w postaci zaszyfrowanej i wymagają lokalnego zapisania na kartę lub token,

w przypadku tworzenia kopii zapasowych kluczy prywatnych, przechowywanych w module kryptograficznym może być czasami konieczne (np. w przypadku jego awarii) załadowanie kluczy do innego modułu kryptograficznego,

może być konieczne przeniesienie klucza prywatnego z modułu operacyjnego, wykorzystywanego codziennie przez podmiot do innego modułu; sytuacja taka może wystąpić np. w przypadku defektu modułu lub konieczności jego zniszczenia.

Wprowadzanie klucza prywatnego do modułu kryptograficznego jest operacją krytyczną. Z tego względu w trakcie jej realizacji stosowane są takie środki i procedury, które zapobiegają ujawnieniu klucza, jego modyfikacji lub podstawienia.

W Unizeto CERTUM - Centrum Certyfikacji Powszechne stosuje się dwie metody zapewnienia integralności ładowanemu kluczowi:

po pierwsze, jeśli klucz występuje w całości, to nie jest on nigdy dostępny poza modułem w postaci jawnej; oznacza to, że w momencie wygenerowania klucza i konieczności załadowania go do innego modułu, klucz ten jest szyfrowany przy pomocy klucza tajnego; klucz tajny jest tak przechowywany, że nigdy osoba do tego nieupoważniona nie jest w posiadaniu obu tych informacji jednocześnie,

po drugie, jeśli klucz lub chroniące go hasło przechowywane są w częściach, to dzięki ładowaniu kolejnych fragmentów sam moduł jest w stanie zweryfikować potencjalne próby ataków lub oszustw.

Wprowadzenie klucza prywatnego do obszaru sprzętowego modułu kryptograficznego urzędu certyfikacji **CA-Certum** lub **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** wymaga odtworzenia klucza z kart w obecności wymaganej w tym celu liczby posiadaczy sekretów współdzielonych lub kart administratorskich chroniących moduł z kluczami (patrz rozdz.6.2.2). Ponieważ każdy urząd certyfikacji może posiadać także zaszyfrowane kopie kluczy prywatnych (rozdz.6.2.4), stąd klucze te można w takiej postaci przenosić także pomiędzy modułami.

Klucz prywatny operatora urzędu rejestracji występuje zawsze tylko w jednym egzemplarzu (brak kopii) i z tego powodu nie jest wymagana operacja wprowadzania klucza do modułu kryptograficznego.

Z kolei zainstalowanie klucza prywatnego w module kryptograficznym subskrybenta końcowego może wymagać załadowania go z posiadanego nośnika, np. plik chroniony hasłem na dyskietce (operację tę może wykonać sam subskrybent) lub bezpośrednio z modułowego generatora kluczy (operacja realizowana jest przez operatora urzędu certyfikacji lub urzędu rejestracji).

6.2.7. Metody aktywacji klucza prywatnego

Metody aktywacji kluczy prywatnych, będących w posiadaniu różnych uczestników i użytkowników systemu Unizeto CERTUM - CCP odnoszą się do sposobów uaktywniania kluczy przed każdym ich użyciem lub przed rozpoczęciem każdej sesji (np. połączenia internetowego), w trakcie której klucze te są stosowane. Raz uaktywniony klucz prywatny jest gotowy do użycia aż do momentu jego dezaktywacji.

Przebieg procedur aktywacji (i dezaktywacji) klucza prywatnego jest uzależniony od typu podmiotu, w którego posiadaniu jest klucz (użytkownik końcowy, urząd rejestracji, urząd certyfikacji, urządzenia, itp.), ważności danych, które są chronione przy pomocy tego klucza oraz tego czy klucz po uaktywnieniu pozostaje aktywny tylko na czas wykonania jednej operacji z użyciem klucza, jednej sesji lub na czas nieokreślony.

Wszystkie klucze prywatne **CA-Certum** lub **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**, załadowane do modułu kryptograficznego po ich wygenerowaniu, przeniesieniu w postaci zaszyfrowanej z innego modułu lub odtworzeniu z części współdzielonych przez zaufane osoby pozostają w stanie aktywności aż do momentu ich fizycznego usunięcia z modułu lub wyłączenia z użytku w systemie Unizeto CERTUM - CCP. Uaktywnienie kluczy prywatnych poprzedzone jest zawsze uwierzytelnieniem administratora bezpieczeństwa. Uwierzytelnienie to realizowane jest w oparciu o identyfikacyjną kartę elektroniczną, będącą w posiadaniu administratora bezpieczeństwa. Po włożeniu karty do modułu kryptograficznego i podaniu numeru PIN klucz prywatny pozostaje w stanie aktywności aż do momentu wyjęcia karty z modułu.

Klucze prywatne podpisujące operatorów urzędów rejestracji stosowane do podpisywania informacji są uaktywniane dopiero po uwierzytelnieniu operatora (podaniu numeru PIN) i tylko na czas wykonania pojedynczej operacji kryptograficznej z użyciem tego klucza. Po zakończeniu wykonywania operacji klucz prywatny jest automatycznie dezaktywowany i musi być ponownie uaktywniany przed wykonaniem kolejnej operacji. Inne klucze prywatne, np. używane do uwierzytelnienia aplikacji urzędu rejestracji lub utworzenia szyfrowanego połączenia sieciowego uaktywniane są automatycznie na okres trwania sesji, natychmiast po uwierzytelnieniu operatora. Zakończenie sesji dezaktywuje wszystkie uaktywnione wcześniej klucze prywatne.

Aktywacja kluczy prywatnych subskrybentów realizowana jest podobnie jak w przypadku kluczy operatorów urzędów rejestracji, niezależnie od tego czy klucze przechowywane są na karcie elektronicznej, czy też w postaci zaszyfrowanej na dyskietce lub innym nośniku. W przypadku subskrybentów którzy są osobami prawnymi (organizacjami, instytucjami, itp.) aktywacji powinna dokonać osoba fizyczna, która posiada odpowiednie pełnomocnictwa wystawione przez subskrybenta.

Każde uaktywnienie klucza prywatnego jest odnotowywane w dzienniku zdarzeń.

6.2.8. Metody dezaktywacji klucza prywatnego

Metody dezaktywacji kluczy prywatnych odnoszą się do sposobów dezaktywowania kluczy po każdym ich użyciu lub po zakończeniu każdej sesji (np. połączenia internetowego) w trakcie której klucze te są stosowane.

W przypadku kluczy subskrybenta końcowego lub operatora urzędu rejestracji dezaktywowanie kluczy podpisujących następuje natychmiast po zrealizowaniu podpisu cyfrowego lub po zakończeniu sesji (np. wyrejestrowania się z aplikacji). Jeśli w trakcie wykonywania operacji kryptograficznych klucz prywatny znajdował się w pamięci operacyjnej aplikacji, to aplikacja musi zadbać o to aby niemożliwe było nieautoryzowane odtworzenie klucza prywatnego.

Jeśli klucz prywatny należy do subskrybenta który jest osobą prawną, to klucz może być dezaktywowany tylko przez uprawomocnionego do tej czynności przedstawiciela tej osoby.

W przypadku Unizeto CERTUM - CCP dezaktywowanie kluczy jest wykonane przez oficera bezpieczeństwa i tylko w przypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego. Dezaktywacja klucza polega na wyjęciu karty z modułu kryptograficznego.

Każda dezaktywacja klucza prywatnego jest odnotowywana w dzienniku zdarzeń.

6.2.9. Metody niszczenia klucza prywatnego

Niszczenie kluczy subskrybentów końcowych lub operatorów urzędu rejestracji polega odpowiednio na ich bezpiecznym wymazaniu z nośnika (z dyskietki, karty elektronicznej, pamięci operacyjnej, sprzętowego modułu kryptograficznego, itp.), zniszczeniu nośnika kluczy (np. karty elektronicznej) lub przynajmniej przejęcie nad nim kontroli w przypadku, gdy mechanizmy karty nie zezwalają na definitywne usunięcie z niej informacji o kluczu prywatnym.

Jeśli klucz prywatny należy do subskrybenta który jest osobą prawną, to klucz może być zniszczony tylko przez uprawomocnionego do tej czynności przedstawiciela tej osoby.

Niszczenie klucza prywatnego urzędów certyfikacji oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników, na których są przechowywane kopie lub archiwizowane sekrety współdzielone.

Każde zniszczenie klucza prywatnego jest odnotowywane w dzienniku zdarzeń.

Szczegółowy opis procedur niszczenia kluczy prywatnych opisany jest w dokumentach: „Księga nośników", „Procedura generowania kluczy urzędu certyfikacji Unizeto CERTUM" oraz „Procedura archiwizacji i niszczenia kluczy urzędu certyfikacji Unizeto CERTUM". Oba dokumenty są niejawne, dostępne tylko wybranym pracownikom urzędu certyfikacyjnego i przedstawicielom audytora.

6.3. Inne aspekty zarządzania kluczami

Z punktu widzenia technologii możliwe jest używanie tej samej pary kluczy zarówno do realizacji podpisu cyfrowego, jak też do szyfrowania informacji. Niniejszy Kodeks Postępowania Certyfikacyjnego nie zaleca jednak takiego postępowania, poza przypadkami opisanymi w rozdz.6.1.9. W przypadku certyfikatów wydawanych zgodnie z polityką Certum Level IV postępowanie takie jest zabronione.

Pozostałe wymagania tego rozdziału dotyczą procedury archiwizowania kluczy publicznych oraz okresów ważności kluczy publicznych i prywatnych wszystkich subskrybentów, w tym także urzędów certyfikacji.

6.3.1. Archiwizacja kluczy publicznych

Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów cyfrowych już po usunięciu certyfikatu z repozytorium (patrz rozdz.2.6). Jest to szczególnie ważne w przypadku świadczenia usług niezaprzeczalności, takich jak np. usługa znacznika czasu lub usługa weryfikacji statusu certyfikatu.

Archiwizowanie kluczy publicznych polega na archiwizowaniu certyfikatów, w których te klucze występują.

Każdy z urzędów wydających certyfikaty przechowuje klucze publiczne tych subskrybentów, którym wydał je w postaci certyfikatów. Własne klucze publiczne urzędu certyfikacji archiwizowane są razem z kluczami prywatnymi, w sposób przedstawiony w rozdz.6.2.5.

Certyfikaty mogą być także archiwizowane lokalnie przez subskrybentów, zwłaszcza w przypadkach, gdy wymagają tego używane przez nich aplikacje, np. poczta elektroniczna.

Archiwa kluczy publicznych powinny być chronione w taki sposób, aby możliwe było zapobieganie nieautoryzowanemu dodawaniu kluczy do archiwum, kasowaniu lub modyfikacji. Tego typu ochronę osiąga się dzięki uwierzytelnianiu podmiotów archiwizujących oraz autoryzowaniu ich żądań.

W systemie Unizeto CERTUM - CCP archiwizowane są tylko klucze używane do weryfikacji podpisów cyfrowych. Każdy inny typ klucza publicznego (np. klucz używany do szyfrowania wiadomości) jest natychmiast niszczony po usunięciu go z repozytorium.

Administrator bezpieczeństwa dokonuje raz w miesiącu audytu archiwum kluczy, sprawdzając jego integralność. Sprawdzenie to ma na celu upewnienie się, że archiwum nie zawiera luk i że certyfikaty w nim przechowywane nie zostały zmodyfikowane. Mechanizmy zapewniające integralność archiwum biorą pod uwagę fakt, iż okres przechowywania archiwum może być większy, aniżeli odporność na złamanie kluczy użytych do ich budowy.

Klucze publiczne przechowywane są w archiwum kluczy publicznych przez okres 25 lat (patrz także rozdz.4.11).

Każde zarchiwizowanie lub zniszczenie klucza publicznego jest odnotowywane w dzienniku zdarzeń.

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole validity każdego certyfikatu klucza publicznego (patrz rozdz.7.1). Jest to także okres ważności klucza prywatnego.

Standardowe maksymalne okresy ważności certyfikatów urzędów certyfikacji podane są w Tab.6.5, zaś certyfikatów subskrybentów w Tab.6.6.

Okresy ważności certyfikatu i tym samym klucza prywatnego mogą ulec skróceniu w wyniku zawieszenia lub unieważnienia kluczy.

Standardowo początkowa data ważności certyfikatu pokrywa się z datą jego wydania. Nie dopuszcza się, aby data ta ulokowana była w przeszłości ani w przyszłości.

Tab.6.5 Maksymalne okresy ważności certyfikatów urzędów

Typ właściciela klucza	Główny rodzaj zastosowania klucza			
	RSA do podpisu certyfikatów i list CRL	RSA do podpisu wiadomości	RSA do wymiany kluczy	Diffie-Hellman
CA-Certum	25 lat	–	–	–
CA-Certum Level I	10 lat	–	–	–
CA-Certum Level II	10 lat	–	–	–
CA-Certum Level III	10 lat	–	–	–
CA-Certum Level IV	10 lat	–	–	–

Każdy z użytkowników, w tym przede wszystkim urzędy certyfikacji, może w dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji podpisów, mimo że certyfikat jest nadal aktualnie ważny. Urząd certyfikacji jest jednak zobowiązany do poinformowania o tym fakcie (związanym ze zmianą kluczy) swoich subskrybentów.

Tab.6.6 Maksymalne okresy ważności certyfikatów subskrybentów

Typ właściciela klucza	Nazwa polityki certyfikacji	Główny rodzaj zastosowania klucza		
		RSA do podpisu wiadomości	RSA do wymiany kluczy	Diffie-Hellman
Operator urzędu rejestracji	Certum Level II	1 rok	1 rok	1 rok
	Certum Level III	1 rok	1 rok	1 rok
	Certum Level IV	2 lata	2 lata	2 lata
Osoby fizyczne oraz urządzenia osób fizycznych	Certum Level I	min. 3 miesiące	min. 3 miesiące	min. 3 miesiące
	Certum Level II	1 rok	1 rok	1 rok
	Certum Level III	1 rok	1 rok	1 rok
	Certum Level IV	2 lata	2 lata	2 lata
Osoby prawne oraz urządzenia osób fizycznych	Certum Level I	min. 3 miesiące	min. 3 miesiące	min. 3 miesiące
	Certum Level II	1 rok	1 rok	1 rok
	Certum Level III	1 rok	1 rok	1 rok
	Certum Level IV	2 lata	2 lata	2 lata

6.4. Dane aktywujące

Dane aktywujące stosowane są do uaktywniania kluczy prywatnych stosowanych przez urzędy rejestracji, urzędy certyfikacji oraz subskrybentów. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Dane aktywujące używane są w dwóch podstawowych przypadkach:

jako element jedno- lub dwuczynnikowej procedury uwierzytelniania (tzw. frazy uwierzytelniania, np. hasła, numery PIN, itp.),

jako część sekretu współdzielonego, który po zainstalowaniu w systemie umożliwią odtworzenie klucza lub kluczy kryptograficznych.

Operatorzy urzędów rejestracji, urzędów certyfikacji oraz inne osoby pełniące role określone w rozdz.5.2 posługują się hasłami odpornymi na ataki brutalne (zwane także wyczerpującymi). Zaleca się, aby w podobny sposób tworzone były hasła subskrybentów.

W przypadku aktywacji kluczy prywatnych zaleca się stosowanie dwuczynnikowych procedur uwierzytelniania, np. token kryptograficzny (w tym także identyfikacyjna karta elektroniczna) i fraza uwierzytelniania lub token kryptograficzny i biometria (np. odcisk palca).

Frazy uwierzytelnienia, o których była mowa powyżej, powinny być generowane zgodnie z wymaganiami określonymi w FIPS-112 (patrz [26]).

Sekrety współdzielone używane do ochrony kluczy prywatnych urzędów certyfikacji generowane są zgodnie z wymaganiami określonymi w rozdz.6.2 i zapisywane w tokenach kryptograficznych. Tokeny chronione są numerem PIN, którego procedura tworzenia jest zgodna z FIPS-112. Sekrety współdzielone stają się danymi aktywacyjnymi dopiero po ich uaktywnieniu, tj. prawidłowym podaniu numeru PIN chroniącego token.

6.4.2. Ochrona danych aktywujących

Ochrona danych aktywujących obejmuje takie metody kontroli danych aktywujących, które zapobiegają ich ujawnieniu. Metody kontroli ochrony danych aktywujących zależą z jednej strony od tego czy są to frazy uwierzytelniania, z drugiej zaś strony od tego czy kontrola ta sprawowana jest na podstawie podziału na części (sekrety współdzielone) klucza prywatnego lub też aktywujących go danych.

W przypadku ochrony fraz uwierzytelniania należy stosować się do zaleceń określonych w FIPS 112, z kolei przy ochronie sekretów współdzielonych do zaleceń FIPS 140.

Zaleca się, aby dane aktywujące stosowane do uaktywniania kluczy prywatnych były chronione przy zastosowaniu mechanizmów kryptograficznych oraz fizycznej kontroli dostępu. Dane aktywujące powinny być danymi biometrycznymi lub pamiętanymi (nie zapisywanymi) przez podmiot uwierzytelniany. Jeśli dane aktywujące są zapisywane, to ich poziom zabezpieczenia powinien być taki sam jak danych, do których ochrony użyto tokena kryptograficznego. Kilkakrotne nieudane próby dostępu do takiego modułu powinny prowadzić do zablokowania tokena. Zapisywane dane aktywujące nie są nigdy przechowywane razem z tokenem kryptograficznym.

6.4.3. Inne problemy związane z danymi aktywującymi

Dane aktywujące przechowywane są zawsze tylko w jednej kopii. Jedynym odstępstwem od tej zasady są numery PIN, chroniące dostęp do sekretów współdzielonych – każdy posiadacz sekretu może stworzyć kopie numeru PIN i przechowywać w innym miejscu niż sekret współdzielony.

Dane aktywujące chroniące dostęp do kluczy prywatnych zapisanych w tokenach kryptograficznych mogą być okresowo zmieniane.

Dane aktywujące nie są archiwizowane.

6.5. Sterowanie zabezpieczeniami systemu komputerowego

Zadania urzędów rejestracji i urzędów certyfikacji funkcjonujących w ramach systemu Unizeto CERTUM - CCP realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzących system który spełnia wymagania określone w dokumencie *„Procedury postępowania i utrzymania bezpieczeństwa systemu Unizeto CERTUM - Centrum Certyfikacji Powszechne”*.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania, używanego w systemie Unizeto CERTUM - CCP. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery zlokalizowane w urzędach certyfikacji oraz w powiązanych z nimi komponentach (np. urzędach rejestracji) wyposażone są w następujące funkcje zabezpieczające:

obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),

uznaniową kontrolę dostępu,

możliwość prowadzenia audytu zabezpieczeń,

komputer udostępniany jest tylko pracownikom serwisu oraz personelowi, który pełni zaufane role w Unizeto CERTUM - CCP,

wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,

identyfikację i uwierzytelnienie ról oraz pełniących je osób,

zapobieganie ponownemu użyciu obiektu przez inne procesy po zwolnieniu obiektu przez proces uprawniony,

kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,

archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,

bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,

mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,

mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

Ocena zabezpieczeń systemów komputerów prowadzona jest zgodnie wytycznymi zawartymi w *Information Technology Security Evaluation Cryteria*[40] (ITSEC) i dotyczącymi zabezpieczeń poziomu E4.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe Unizeto CERTUM - CCP spełniają wymagania określone w *Information Technology Security Evaluation Cryteria* (ITSEC). Zostało to potwierdzone przez niezależnego audytora, oceniającego funkcjonowanie systemu Unizeto CERTUM - CCP na podstawie kryteriów określonych w *WebTrust Principles and Criteria for Certification Authorities*. Ocena ta jest dostępna w repozytorium Unizeto CERTUM - CCP.

6.6. Cykl życia kontroli technicznej

6.6.1. Kontrola zmian systemu

Aplikacje stosowane w systemie Unizeto CERTUM - CCP są projektowane i implementowane przez Unizeto Sp. z o.o. Wszystkie aplikacje są rozwijane i uaktualniane za pośrednictwem systemu CVS. W systemie CVS tworzona jest również dokumentacja systemu.

Każda aplikacja przed załadowaniem do systemu komputerowego Unizeto CERTUM - CCP jest podpisywana cyfrowo. Ułatwia to bieżące kontrolowanie wersji oprogramowania oraz zapobiega nieuprawnionej wymianie oprogramowania lub jego modyfikacji.

Podobnym zasadom podlega każda wymiana sprzętu w systemie. W szczególności:

sprzęt jest dostarczany w sposób, który umożliwia prześledzenie całej drogi przebytej przez sprzęt od dostawcy do miejsca zainstalowania,

dostawa sprzętu na wymianę jest realizowana w taki sam sposób jak dostawa sprzętu oryginalnego; sama wymiana jest dokonywana przez zaufany i przeszkolony personel w sposób określony w dokumencie *„Procedury postępowania i utrzymania bezpieczeństwa systemu Unizeto CERTUM - Centrum Certyfikacji Powszechne”*.

6.6.2. Kontrola zarządzania bezpieczeństwem

Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania systemu Unizeto CERTUM - CCP, które daje pewność że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.

Aktualna konfiguracja systemu Unizeto CERTUM - CCP, jak również dowolne modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Konfigurowanie systemu realizowane jest zgodnie z wytycznymi zawartymi w dokumencie *„Procedury postępowania i utrzymania bezpieczeństwa systemu Unizeto CERTUM - Centrum Certyfikacji Powszechne”*.

Zastosowane w systemie Unizeto CERTUM - CCP mechanizmy pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia sprzętu.

6.6.3. Ocena cyklu życia zabezpieczeń

Niniejszy Kodeks Postępowania Certyfikacyjnego nie narzuca żadnych wymagań w tym zakresie.

[40] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

6.7. Kontrola zabezpieczeń sieci

Serwery oraz zaufane stacje robocze systemu komputerowego Unizeto CERTUM - CCP połączone są przy pomocy wydzielonej dwusegmentowej sieci wewnętrznej LAN. Dostęp od strony internetu do każdego z segmentów chroniony jest przy pomocy inteligentnych zapór sieciowych (firewall) o klasie E3 wg ITSEC oraz systemów wykrywania intruzów IDS.

Pierwsza podsieć zawiera serwer WWW oraz serwer SMTP (łącznie – repozytorium systemu) oraz wydzieloną, oddzieloną logicznie część wewnętrzną obsługującą właściwy proces certyfikacji (zawiera ona m.in. serwer certyfikujący oraz serwer bazy danych). Druga podsieć spełnia rolę systemu modelowego, wykorzystywanego w pracach projektowych oraz do testów.

System komputerowy Unizeto CERTUM - CCP zabezpieczony jest przed atakiem typu odmowa usługi oraz chroniony jest przez system wykrywania intruzów. Mechanizmy ochrony zbudowane są w oparciu o śluzę bezpieczeństwa (*ang. firewalls*) oraz filtrowanie ruchu w routerach i serwisach PROXY.

Zabezpieczenia zapór sieciowych akceptują jedynie wiadomości przysyłane i wysyłane w oparciu o protokoły: http, https, NTP, POP3 oraz SMTP. Zapisy zdarzeń (logi) rejestrowane przez dzienniki systemowe umożliwiają nadzorowanie przypadków niewłaściwego korzystania z usług świadczonych przez Unizeto CERTUM - CCP.

Szczegółowy opis konfiguracji sieci Unizeto CERTUM - CCP oraz jej zabezpieczeń zawarty jest w „Księga Serwerów".

6.8. Kontrola wytwarzania modułu kryptograficznego

Kontrola wytwarzania modułu kryptograficznego obejmuje wymagania nakładane na proces projektowania, produkcji i dostarczania modułów kryptograficznych. Unizeto CERTUM - CCP nie definiuje własnych wymagań w tym zakresie. Akceptuje jednak tylko takie moduły kryptograficzne, które spełniają wymagania określone w rozdz.6.2.

6.9. Znaczniki czasu

Wnioski tworzone w ramach protokołu CMP lub CRS (rozdz.6.1.3) nie wymagają znakowania wiarygodnym czasem. W przypadku innych wiadomości przesyłanych pomiędzy urzędem certyfikacji, urzędem rejestracji i subskrybentem zaleca się stosować znaczniki czasu.

Znaczniki czasu tworzone w ramach Unizeto CERTUM - CCP są zgodne z zaleceniem RFC 3161.

7. Profile certyfikatów, listy CRL i OCSP

Profile certyfikatów oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3, zaś profil OCSP z RFC 2560. Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu, list CRL i OCSP, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek Unizeto CERTUM - CCP.

7.1. Struktura certyfikatów

Certyfikat według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu (**tbsCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu (**signatureAlgorithm**), zaś trzecie – podpis cyfrowy, składany na certyfikacie przez urząd certyfikacji (**signatureValue**).

7.1.1. Zawartość certyfikatu

Na treść certyfikatu składają się wartości **pól podstawowych** oraz **rozszerzeń** (standardowych, określonych przez normę oraz prywatnych, definiowanych przez organ wydający certyfikaty).

Rozszerzenia zdefiniowane w certyfikatach wg normy umożliwiają przypisanie dodatkowych atrybutów subskrybentowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną strukturą certyfikatów. Certyfikaty wg normy X.509 v.3 umożliwiają także definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

7.1.1.1. Pola podstawowe

Unizeto CERTUM - CCP obsługuje następujące pola podstawowe certyfikatu:

Version: wersję trzecią (X.509 v.3) formatu certyfikatu,

SerialNumber: numer seryjny certyfikatu, unikalny w ramach domeny urzędu certyfikacji,

Signature Algorithm: identyfikator algorytmu stosowanego przez urząd certyfikacji wydający certyfikaty do podpisania certyfikatu,

Issuer: nazwa wyróżniająca (DN) urzędu certyfikacji,

Validity: data ważności certyfikatu określona przez początek (**notBefore**) oraz koniec (**notAfter**) ważności certyfikatu,

Subject: nazwę wyróżniająca (DN) subskrybenta, otrzymującego certyfikat,

SubjectPublicKeyInfo: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

W certyfikatach wydawanych przez Unizeto CERTUM wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab.7.1.

Tab.7.1 Profil podstawowych pól certyfikatu

Nazwa pola	Wartość lub ograniczenie wartości	
Version	Version 3	
Serial Number	Unikalne wartości we wszystkich certyfikatach wydawanych przez urzędy certyfikacji Unizeto CERTUM - CCP	
Signature Algorithm	md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) lub sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (nazwa DN)	Common Name (CN) =	Certum {CA,Level{I,II,III,IV},…}
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar Unizeto CERTUM jest znany jako ogólnoświatowe wiarygodne źródło usług czasu klasy Stratum I.	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). Unizeto CERTUM - CCP posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar Unizeto CERTUM jest znany jako ogólnoświatowe wiarygodne źródło usług czasu klasy Stratum I.	
Subject (nazwa DN)	Nazwa DN jest zgodna z wymaganiami X.501. Wszystkie atrybuty tego pola są opcjonalne, z wyjątkiem pól: emailAddress (występuje w większości certyfikatów subskrybenta), organizationName (występuje w certyfikatach urzędów certyfikacji i podmiotów świadczących usługi niezaprzeczalności), commonName (tylko w certyfikatach serwerów), unstructured{Address or Name} (w certyfikatach VPN), które są obligatoryjne.	
Subject Public Key Info	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 2459 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego); długości kluczy RSA określone są w rozdz.6.1.5	
Signature	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 2459.	

7.1.1.2. Pola rozszerzeń standardowych

Funkcja każdego z rozszerzeń określona jest przez standardową wartość związanego z nim identyfikatora obiektu (**OBJECT IDENTIFIER**). Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być **krytyczne** lub **niekrytyczne**. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać. Z kolei każde niekrytyczne rozszerzenie może być ignorowane.

Unizeto CERTUM - CCP obsługuje następujące pola rozszerzeń podstawowych certyfikatu:

AuthorityKeyIdentifier: identyfikator certyfikatu klucza publicznego urzędu certyfikacji powiązanego z tym kluczem prywatnym, przy pomocy którego urząd certyfikacji podpisał wydany certyfikat – **rozszerzenie nie jest krytyczne**,

SubjectKeyIdentifier: identyfikator klucza podmiotu – **rozszerzenie nie jest krytyczne**,

KeyUsage: dozwolone użycie klucza – **rozszerzenie może być krytyczne**. Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do szyfrowania danych, klucz do wymiany kluczy, klucz do podpisu cyfrowego, itp. (patrz niżej);

```
digitalSignature          (0), -- klucz do realizacji podpisu cyfrowego
nonRepudiation            (1), -- klucz związany z realizacją usług
                               -- niezaprzeczalności
keyEncipherment           (2), -- klucz do wymiany kluczy
dataEncipherment          (3), -- klucz do szyfrowania danych
keyAgreement              (4), -- klucz do uzgadniania kluczy
keyCertSign               (5), -- klucz do podpisywania certyfikatów
cRLSign                   (6), -- klucz do podpisywania list CRL
encipherOnly              (7), -- klucz tylko do szyfrowania
decipherOnly              (8)  -- klucz tylko do deszyfrowania
```

ExtKeyUsage: sprecyzowanie (ograniczenie) użycia klucza – **rozszerzenie nie jest krytyczne**. Pole to określa jeden lub więcej obszarów, w uzupełnieniu podstawowego zastosowania określonego przez pole **keyUsage**, w obrębie których może być stosowany certyfikat. Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**. Unizeto CERTUM - CCP wydaje certyfikaty, które mogą zawierać jedną z poniższych wartości lub ich kombinację:

```
serverAuth  - uwierzytelnianie TLS Web serwera; bity pola keyUsage,
              które są zgodne z tym polem: digitalSignature,
              keyEncipherment lub keyAgreement
clientAuth  - uwierzytelnianie TLS Web klient; bity pola keyUsage,
              które są zgodne z tym polem: digitalSignature
              i/lub keyAgreement
codeSigning - podpisywanie ładowalnego kodu wykonywalnego;
              bity pola keyUsage, które są zgodne z tym polem:
              digitalSignature
emailProtection - ochrona E-mail; bity pola keyUsage, które są zgodne
                  z tym polem: digitalSignature, nonRepudiation i/lub
                  (keyEncipherment lub keyAgreement)
ipsecEndSystem - ochrona protokołu IPSEC
ipsecTunnel    - tryb tunelowania protokołu IPSEC
ipsecUser      - ochrona protokołu IP w aplikacjach użytkownika
timeStamping - wiązanie wartości skrótu z czasem z wcześniej
               uzgodnionego wirygodnego źródła czasu; bity pola
               keyUsage, które są zgodne z tym polem:
               digitalSignature, nonRepudiation
OCSPSigning - oznacza prawo do wystawiania w imieniu CA poświadczeń
              statusu certyfikatu; bity pola keyUsage, które są zgodne
              z tym polem: digitalSignature, nonRepudiation
dvcs - wystawianie poświadczeń przez urząd notarialny w oparciu
       o protokół DVCS; bity pola keyUsage, które są zgodne z tym
       polem: digitalSignature, nonRepudiation, keyCertSign, cRLSign
```

PolicyInformation: informacja (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez dany organ wydający certyfikaty – **rozszerzenie nie jest krytyczne**,

Tab.7.2 Identyfikatory polityk i ich nazwy

Identyfikator polityki	Nazwa polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-	Certum Level I Identyfikuje politykę certyfikacji o nazwie

Identyfikator polityki	Nazwa polityki certyfikacji
ccert(2) id-certum(2) id-certum-level-I(1))[41]	Certum Level I
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-II(2))	Certum Level II Identyfikuje politykę certyfikacji o nazwie Certum Level II
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-III(3))	Certum Level III Identyfikuje politykę certyfikacji o nazwie Certum Level III
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-IV(4))	Certum Level IV Identyfikuje politykę certyfikacji o nazwie Certum Level IV

W certyfikatach wydawanych przez urzędy certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 2459.

PolicyMapping: odwzorowanie polityki – **rozszerzenie nie jest krytyczne**; pole to zawiera jedną lub więcej par OID, które określają równoważność polityki wydawcy z polityką podmiotu,

IssuerAlternativeName: alternatywna nazwa wydawcy certyfikatu – **rozszerzenie nie jest krytyczne**,

SubjectAlternativeName: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**,

BasicContraints: więzy podstawowe - **rozszerzenie jest krytyczne w certyfikatach urzędów certyfikacji i niekrytyczne w certyfikatach subskrybentów**. Rozszerzenie umożliwia określenie czy subskrybent certyfikatu jest urzędem certyfikacji (pole **cA**) oraz ile maksymalnie (przy założeniu hierarchicznego uporządkowania urzędów certyfikacji) może być urzędów certyfikacji na ścieżce prowadzącej od rozpatrywanego urzędu certyfikacji do subskrybenta końcowego (pole **pathLength**),

CRLDistributionPoints: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**. Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL, wydaną przez **cRLIssuer**,

SubjectDirectoryAttributes: atrybuty katalogu podmiotu - **rozszerzenie nie jest krytyczne**; pole zawiera dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**; w rozszerzeniu tym występują atrybuty, które nie należą do elementów wchodzących w skład nazwy DN podmiotu,

AuthorityInfoAccessSyntax: dostęp do informacji urzędu certyfikacji - **rozszerzenie nie jest krytyczne**; pole wskazuje, w jaki sposób udostępniane są informacje i usługi przez wystawcę certyfikatu, w którego certyfikacie to rozszerzenie występuje,

BiometricSyntax: informacje o cechach biometrycznych podmiotu certyfikatu - **rozszerzenie nie jest krytyczne**; dostępne są dwa typy informacji biometrycznej:

[41] Unizeto CERTUM - Centrum Certyfikacji Powszechne zostal przydzielony identyfikator obiektu o postaci: {iso(1) member-body(2) pl(616) organization(1) unizeto(113527) ccert(2) certum(2)}.

podpis odręczny oraz zdjęcie; w certyfikacie umieszczany jest jedynie skrót z cechy biometrycznej; wartość skrótu umieszczana jest w polu **biometricDataHash**, zaś identyfikator funkcji skrótu przy pomocy której policzono tę wartość w polu **hashAlgorithm**; pełna informacja biometryczna o podmiocie (jego wzorzec biometryczny) przechowywana jest w bazie danych, której adres URI podany jest w polu **sourceDataUri**. Efektywne wykorzystanie informacji biometrycznej umieszczonej w certyfikacie (skrót) możliwe jest jedynie w przypadku, gdy nastąpi porównanie wzorca zawartego w bazie (informacja pełna) ze skrótem odczytanym z certyfikatu.

7.1.2. Rozszerzenia certyfikatów

Certyfikaty wydawane przez urzędy Unizeto CERTUM - CCP mogą zawierać różne kombinacje rozszerzeń wymienionych w rozdz.7.1.1.2. Ich dobór jest uzależniony głównie od zastosowania certyfikatu oraz tego komu jest on wydawany.

7.1.2.1. Certyfikaty urzędów certyfikacji

Autocertyfikat urzędu certyfikacji **CA-Certum** oraz certyfikaty podległych mu urzędów certyfikacji **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** i **CA-Certum Level IV** mogą zawierać rozszerzenia określone w Tab.7.3.

Tab.7.3 Rozszerzenia w certyfikatach urzędów certyfikacji

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji={brak,1,2,...}	Krytyczne

7.1.2.2. Certyfikaty do uwierzytelniania serwerów

Certyfikaty wydawane przez urzędy certyfikacji na potrzeby uwierzytelniania serwerów (w tym także certyfikaty stosowane w serwisach bezprzewodowych i OFX) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.4.

Tab.7.4 Rozszerzenia w certyfikatach do uwierzytelniania serwerów

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage	Klucz do szyfrowania (key encipherment), bit 2	Niekrytyczne
Extended Key Usage	Server Authentication (serverAuth) Netscape SGC Microsoft SGC	Niekrytyczne
Netscape Cert Type	SSL Server (bit 1)	Niekrytyczne
Subject Alternative Name	DNS.1: Pełna nazwa DNS serwisu (FQDN) DNS.2: Alternatywna nazwa serwisu (opcja)	Niekrytyczne
CRL Distribution Points	URI: http://crl.certum.pl/class{1,2,3,4}.crl	Niekrytyczne

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Info Access	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.2.{1,2,3,4} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): 1 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.2.3. Certyfikaty do uwierzytelniania kodu oprogramowania

Certyfikaty wydawane przez urzędy certyfikacji do uwierzytelniania kodu oprogramowania (w tym także formularzy oraz kanałów kryptograficznych) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.5.

Tab.7.5 Rozszerzenia w certyfikatach do uwierzytelniania kodu oprogramowania

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Niekrytyczne
Extended Key Usage	Code Signing	Niekrytyczne
Netscape Cert Type	Object Signing (bit 3)	Niekrytyczne
Subject Alternative Name	URI: http://www.customer-site.somwhere.pl	Niekrytyczne
CRL Distribution Points	URI: http://crl.certum.pl/class{1,3}.crl	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.2.{1,3} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): 2 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.2.4. Certyfikaty osób fizycznych

Certyfikaty wydawane osobom fizycznym (w tym także certyfikaty na potrzeby systemów szyfrowania plików EFS i elektronicznej wymiany dokumentów EDI, certyfikaty kwalifikowane w sensie normy RFC 3039 zawierające informacje biometryczne oraz certyfikaty jako silne identyfikatory w sieci Internet, tzw. Strong Internet ID's) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.6.

Tab.7.6 Rozszerzenia w certyfikatach osób fizycznych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1 Klucz do szyfrowania (key encipherment), bit 2	Niekrytyczne
Extended Key Usage	Encrypted File System TLS Client Authentication	Niekrytyczne
Netscape Cert Type	SSL Client (bit 0)	Niekrytyczne
Subject Alternative Name	Email: customer@somewhere-in-world.com	Niekrytyczne
CRL Distribution Points	URI: http://crl.certum.pl/class{1,2,3,4}.crl	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certum.pl	Niekrytyczne
Biometric Info	Dane biometryczne: Zdjęcie podmiotu, DNA, wzór siatkówki oka, odcisk palca (bit 0) Wzór podpisu odręcznego podmiotu (bit 1) URI: lokalizacja danych biometrycznych	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.2.{1,3} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): 3 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.2.5. Certyfikaty dla potrzeb budowania prywatnych sieci wirtualnych (VPN)

Certyfikaty umożliwiające budowanie sieci VPN mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.7.

Tab.7.7 Rozszerzenia w certyfikatach VPN

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=użytkownik końcowy Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Extended Key Usage	IPsec Client IPsec Tunnel IPsec End System	Niekrytyczne
Subject Alternative Name	DNS: pełna nazwa domeny (FQDN) routera VPN IP: Adres IP Routera VPN	Niekrytyczne
CRL Distribution Points	URI: http://crl.certum.pl/class{1,3}.crl	Niekrytyczne

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Info Access	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.2.{1,3} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): 4 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.2.6. Certyfikaty wzajemne i certyfikaty dla potrzeb usług niezaprzeczalności

Certyfikaty wzajemne i certyfikaty dla potrzeb usług niezaprzeczalności mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.8.

Tab.7.8 Rozszerzenia w certyfikatach wzajemnych i dla potrzeb usług niezaprzeczalności

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji={brak,1,2,...}	Niekrytyczne
Key Usage	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Niekrytyczne
Extended Key Usage	Validation Authority (OCSP) Time-Stamp Authority (TSA) Notary Authority (DVCS)	Niekrytyczne
Subject Alternative Name	URI: http://www.customer-service.somwhere Lokalizacja serwisu klienta	Niekrytyczne
Authority Info Access	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies	Polityki: 1.2.616.1.113527.2.2.{1,3} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): 5 Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny)	Niekrytyczne

7.1.3. Typ stosowanego algorytmu podpisu cyfrowego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji podpisu cyfrowego, składanego przez urząd certyfikacji na certyfikacie. W przypadku Unizeto CERTUM - CCP stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

7.1.4. Pole podpisu cyfrowego

Wartość pola podpisu cyfrowego (**signatureValue**) jest wynikiem zastosowania algorytmu funkcji skrótu do wszystkich pól certyfikatu, określonych przez pola jego treści (**tbsCertificate**) i następnie zaszyfrowania wyniku przy pomocy klucza prywatnego urzędu certyfikacji (wydawcy).

7.2. Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z ciągu trzech pól. Pierwsze pole (**tbsCertList**) zawiera informacje o unieważnionych certyfikatach, drugie i trzecie pole (**signatureAlgorithm** oraz **signatureValue**) – odpowiednio informację o typie algorytmu użytego do podpisania listy oraz podpis cyfrowy, składany na certyfikacie przez urząd certyfikacji. Znaczenie dwóch ostatnich pól jest dokładnie takie samo jak w przypadku certyfikatu.

Pole informacyjne **tbsCertList** jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty oraz rozszerzenia listy CRL.

Na treść pól obowiązkowych oraz opcjonalnych listy CRL składają się następujące pola:

Version: wersja formatu listy CRL,

Signature: Pole to zawiera identyfikator algorytmu stosowanego przez urząd certyfikacji do podpisania listy **CRL**; urzędy Unizeto CERTUM - CCP podpisują listy CRL przy użyciu algorytmu **sha1WithRSAEncryption**,

Issuer: nazwa urzędu certyfikacji wydającego listę CRL; każdy urząd Unizeto CERTUM - CCP wystawia własną listę certyfikatów unieważnionych; wymóg ten dotyczy następujących urzędów: **CA-Certum**, **CA-Certum Level I**, **CA-Certum Level II, CA-Certum Level III** i **CA-Certum Level IV**,

ThisUpdate: data publikacji listy CRL,

NextUpdate: zapowiedź daty następnej publikacji listy CRL; jeśli pole wystąpi, wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy (publikacja może nastąpić więc wcześniej),

RevokedCertificates: lista unieważnionych certyfikatów (pole puste w przypadku braku certyfikatów unieważnionych); Informacja ta składa się z trzech podpól:

```
userCertificate     - numer seryjny unieważnianego certyfikatu
revocationDate      - data unieważnienia certyfikatu
crlEntryExtensions  - rozszerzony dostęp do listy CRL (zawiera
                      dodatkowe informacje o unieważnionych
                      certyfikatach - opcjonalnie)
```

crlExtensions: poszerzone informacje o liście CRL (pole opcjonalne). Spośród wielu rozszerzeń najbardziej istotne są dwa, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL (pole **AuthorityKeyIdentifier**, patrz także rozdz.7.1.1.2), zaś drugie (pole **cRLNumber**) - zawiera monotonicznie zwiększany numer listy CRL, wydawanej przez urząd certyfikacji (dzięki temu rozszerzeniu użytkownik listy jest w stanie określić, kiedy jakiś CRL zastąpił inny CRL).

7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL

Funkcje oraz sens rozszerzeń są takie same jak w przypadku rozszerzeń certyfikatu (patrz rozdz.7.1.1.2). Obsługiwane przez Unizeto CERTUM - CCP rozszerzenia dostępu do listy CRL (**crlEntryExtensions**) zawierają następujące pola:

ReasonCode: kod przyczyny unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie przyczyny unieważnienia certyfikatu. Dopuszcza się następujące przyczyny unieważnienia certyfikatu:

```
unspecified – nieokreślona (nieznana);
keyCompromise – ujawnienie klucza;
cACompromise – ujawnienie klucza urzędu certyfikacji;
affiliationChanged – zamiana danych (afiliacji) subskrybenta;
superseded – zastąpienie certyfikatu (recertyfikacja);
cessationOfOperation – zaprzestanie operacji z wykorzystaniem klucza;
certificateHold – certyfikat zawieszony (wstrzymany);
removeFromCRL – certyfikat wycofany z listy CRL;
```

HoldInstructionCode: kod czynności po zawieszeniu certyfikatu. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które definiuje zarejestrowany identyfikator instrukcji, określającej działanie jakie powinno zostać podjęte po napotkaniu certyfikatu na liście CRL z adnotacją (przyczyną unieważnienia): certyfikat zawieszony (**certificateHold**). Jeśli aplikacja napotka kod **id-holdinstruction-callissuer** musi poinformować użytkownika o konieczności skontaktowania się z Unizeto CERTUM - CCP w celu wyjaśnienia przyczyn zawieszenia certyfikatu lub musi odrzucić certyfikat (uznać go za nieważny). W przypadku napotkania z kolei kodu **id-holdinstruction-reject** należy obligatoryjnie odrzucić rozpatrywany certyfikat. Kod **id-holdinstruction-none** jest semantycznie równoważny pominięciu rozszerzenia **holdInstructionCode**; stosowanie tego rodzaju kodu w listach CRL wydawanych przez Unizeto CERTUM - CCP jest zabronione.

InvalidityDate: data unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie daty faktycznego lub przypuszczalnego skompromitowania klucza lub wystąpienia innej przyczyny.

7.2.2. Certyfikaty unieważnione a listy CRL

Certyfikaty unieważnione pozostają na listach certyfikatów unieważnionych (wydawanych przez urzędy certyfikacji Unizeto CERTUM - Centrum Certyfikacji Powszechne) przez okres 25 lat, licząc od daty pierwszego umieszczenia certyfikatu na liście. Zasada ta dotyczy także unieważnionych certyfikatów urzędów certyfikacji: certyfikaty muszą być umieszczane na kolejnych listach CRL publikowanych przez wydawcę unieważnionego certyfikatu (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium innego, np. nadrzędnego organu wydającego certyfikaty (patrz także rozdz.4.14).

Przedstawiona powyżej zasada nie stosuje się do unieważnionych certyfikatów klasy Certum Level I. Zalecane jest, aby certyfikaty te z chwilą ich przeterminowania usuwane były z listy certyfikatów unieważnionych.

7.3. Profil zaświadczeń OCSP

Protokół weryfikacji statusu certyfikatu w trybie *on-line* (OCSP) jest stosowany przez urzędy certyfikacji i umożliwia określenie stanu certyfikatu.

Usługa OCSP jest świadczona przez Unizeto CERTUM - CCP w imieniu wszystkich działających w jego ramach urzędów certyfikacji. Serwer OCSP, który z upoważnienia urzędów

wystawia poświadczenia o statusie certyfikatu, posługuje się specjalną parą kluczy, przeznaczoną jedynie do tego celu.

Certyfikat serwera OCSP musi zawierać w swojej treści rozszerzenie o nazwie **extKeyUsage**, określone w RFC 2459. Rozszerzenie to powinno być zaznaczone jako **niekrytyczne** i oznacza, że urząd certyfikacji wystawiając certyfikat serwerowi OCSP poświadcza swoim podpisem fakt oddelegowania mu prawa wystawiania w jego imieniu poświadczeń o statusie certyfikatów klientów danego urzędu.

Certyfikat OCSP może zawierać także informację o sposobie kontaktowania się z serwerem OCSP. Informacja ta zawarta jest w polu rozszerzenia **AuthorityInfoAccessSyntax** (patrz rozdz.7.1.1.2).

7.3.1. Numer wersji

Serwer OCSP funkcjonujący w ramach systemu Unizeto CERTUM - CCP wystawia zaświadczenia o statusie certyfikatu zgodnie z RFC 2560. Z tego powodu jedynym dozwolonym numerem wersji jest 0 (odpowiada to wersji v1).

7.3.2. Informacja o statusie certyfikatu

Informacja o statusie certyfikatu umieszczana jest w polu **certStatus** struktury **SingleResponse**. Może ona przyjmować jedną z trzech dozwolonych wartości, zdefiniowanych w rozdz.4.9.11. W przypadku, gdy serwer zwróci status poprawny, to podmiot żądający informacji o statusie certyfikatu powinien sprawdzić dodatkowo rozszerzenie **CertHash** zawarte w odpowiedzi (patrz rozdz.7.3.4) w celu przekonania się, że weryfikowany certyfikat został opublikowany przez wystawcę oraz rozszerzenie **ArchveCutoff**, którego wartość jest lewostronnym przedziałem czasu począwszy od którego serwer OCSP weryfikował status certyfikatu (wartość prawostronnego przedziału czasu określona jest przez moment wystawienia poświadczenia OCSP, określony w polu **producedAt**). Pozytywny wynik tych weryfikacji pozwala na uzyskanie tzw. **pozytywnego potwierdzenia** statusu certyfikatu.

7.3.3. Obsługiwane rozszerzenia standardowe

Zgodnie z RFC 2560 serwer OCSP Unizeto CERTUM - CCP obsługuje następujące rozszerzenia:

Frazę (*ang. nonce*), która wiąże żądanie z odpowiedzią i zapobiega atakowi powtórzeniowemu. Wartość frazy umieszcza się w polu **requestExtensions** żądania **OCSPRequest** oraz powtarza w polu **responseExtensions** odpowiedzi **OCSPResponse**.

W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, w odpowiedzi umieszczane są dane identyfikacyjne tej listy. Informacja o liście CRL zawiera adres URL listy CRL, jej numer oraz czas jej utworzenia. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.

W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, dodatkowo w odpowiedzi należy umieścić wszystkie trzy rozszerzenia listy CRL, opisane w rozdz.7.2.1. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.

Typy odpowiedzi akceptowane przez podmiot (dokładniej, działające w jego aplikacji) wysyłający żądanie weryfikacji statusu do serwera OCSP. Rozszerzenie to określa deklarowane typy odpowiedzi, które rozumie aplikacja. Informacja o akceptowanych

typach odpowiedzi (m.in. **id-pkix-ocsp-basic**) umieszczana jest w żądaniu w rozszerzeniu **AcceptableResponses**.

Graniczna data archiwizacji dotyczy daty do której włącznie przechowywane są w archiwum Unizeto CERTUM - CCP informacje o statusie certyfikatów (rozszerzenie **ArchiveCutoff**). Umieszczenie tej informacji w odpowiedzi przez serwer OCSP oznacza, że serwer OCSP posiada informacje o unieważnieniach certyfikatów także wtedy, gdy same certyfikaty są już przeterminowane. Tego typu informacja dostarcza dowodu na to czy podpis cyfrowy związany z weryfikowanym certyfikatem był lub nie był ważny w momencie wystawienia odpowiedzi przez serwer OCSP, nawet jeśli w tym momencie certyfikat był już przeterminowany. Ponieważ informacje o statusie certyfikatów są dostępne w trybie *on-line* przez okres 15 lat (patrz rozdz.6.3.1), to wartość granicznej daty archiwizacji jest różnicą pomiędzy datą wystawienia poświadczenia o statusie certyfikatu a okresem przechowania informacji o unieważnieniach certyfikatów przez serwer OCSP.

Każdy odbiorca poświadczenia wystawionego przez serwer OCSP musi być w stanie obsłużyć standardowy typ odpowiedzi o identyfikatorze **id-pkix-ocsp-basic**.

7.3.4. Obsługiwane rozszerzenia prywatne

Jeśli w odpowiedzi na żądanie wysłane do serwera OCSP podmiot otrzyma poświadczenie zawierające status **poprawny**, to bez posiadania dodatkowych informacji nie musi to oznaczać że certyfikat był kiedykolwiek wystawiony lub też że moment utworzenia odpowiedzi zawiera się w okresie ważności tego certyfikatu. Drugi z problemów można rozwiązać dzięki umieszczeniu w odpowiedzi rozszerzenia **graniczna data archiwizacji** (**ArchieveCutoff**), opisanego w rozdz.7.3.3.

Rozwiązanie pierwszego z problemów jest możliwe dzięki wprowadzeniu do zaświadczeń wystawianych przez serwer OCSP Unizeto CERTUM - CCP rozszerzenia prywatnego **CertHash**.

Rozszerzenie **CertHash** jest oznaczone jako niekrytyczne. Opisująca je struktura danych oraz jej identyfikator mają postać:

```
id-ccert-CertHash           OBJECT IDENTIFIER ::= { id-ccert-ext 4}
CertHash ::= SEQUENCE {
    hashAlgorithm   DigestAlgorithmIdentifier,
    hashedCert      OCTET STRING
}

id-unizeto                  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
                              organization(1) unizeto(113527)}
id-ccert-ext                OBJECT IDENTIFIER ::= { id-unizeto ccert(2) 0}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier
AlgorithmIdentifier ::= SEQUENCE {
    algorithm               OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL
}
```

Pole **hashAlgorithm** określa identyfikator silnej funkcji skrótu. Oznacza to, że funkcja skrótu powinna być funkcją jednokierunkową, odporną na kolizje (np. SHA-1).

Wartość pola **hashedCert** zawiera skrót z certyfikatu, którego aktualny status jest umieszczony w odpowiedzi serwera OCSP. Wielkość tego pola zależy od typu zastosowanej funkcji skrótu.

7.3.5. Oświadczenie wystawcy zaświadczeń OCSP

Aktualna wersja serwera OCSP Unizeto CERTUM - Centrum Certyfikacji Powszechne nie umieszcza w odpowiedzi rozszerzeń ***CertHash*** *oraz* ***ArchiveCutoff****. Unizeto oświadcza jednak, że otrzymany w odpowiedzi status certyfikatu poprawny oznacza, że certyfikat ten był wydany przez (dowolny) urząd certyfikacji oraz, że nie był on nigdy unieważniony w okresie ostatnich 15 lat. Jeśli certyfikat był unieważniony w okresie ostatnich 15 lat, to serwer OCSP zwraca status* ***unieważniony*** *oraz podaje datę unieważnienia, jego przyczynę oraz informacje o liście certyfikatów na której wystąpił certyfikat.*

8. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego obowiązuje (posiada status aktualny) do czasu opublikowania i zatwierdzenia nowej wersji (patrz rozdz.8.3). Nowa wersja opracowywana jest przez Zespół ds. Rozwoju Usług PKI i ze statusem **w ankiecie** przekazana do ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety Kodeks Postępowania Certyfikacyjnego przekazywany jest do zatwierdzenia. O Kodeksie Postępowania Certyfikacyjnego poddanego procedurze zatwierdzania mówimy, że posiada status w **zatwierdzeniu**. Po zakończeniu procedury zatwierdzania nowa wersja Kodeksu Postępowania Certyfikacyjnego osiąga status **aktualny**.

Przedstawione poniżej zasady administrowania Kodeksem Postępowania Certyfikacyjnego są przestrzegane także podczas administrowania Polityką Certyfikacji.

Subskrybenci muszą się zawsze stosować tylko do aktualnie obowiązującej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.

8.1. Procedura wprowadzania zmian

Zmiany w Kodeksie Postępowania Certyfikacyjnego mogą być wynikiem zauważonych błędów, uaktualnień Kodeksu oraz sugestii ze strony zainteresowanych stron. Propozycje zmian nadsyłane mogą być zwykłą pocztą lub pocztą elektroniczną na adresy kontaktowe Unizeto CERTUM - CCP. Propozycja powinna opisywać zmiany, ich uzasadnienie oraz adres kontaktowy osoby żądającej wprowadzenia zmian.

Propozycje wprowadzania zmian do istniejącego Kodeksu Postępowania Certyfikacyjnego mają prawo zgłaszać następujące podmioty:

sponsor,

instytucje audytujące,

instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Kodeks Postępowania Certyfikacyjnego jest sprzeczny z zasadami prawnymi obowiązującymi w Rzeczypospolitej Polskiej oraz może działać na niekorzyść subskrybenta,

administrator bezpieczeństwa, administrator oraz inni pracownicy Unizeto CERTUM – CCP,

Zespół ds. Rozwoju Usług PKI,

subskrybenci Unizeto CERTUM - CCP,

eksperci z zakresu zabezpieczeń systemów informatycznych.

Po wprowadzeniu każdej zmiany uaktualniana jest data opublikowania Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego oraz modyfikowany jest identyfikator dokumentu, numer jego wersji.

Wprowadzane zmiany można ogólnie podzielić na dwie kategorie: takie o których nie trzeba informować subskrybentów oraz takie które wymagają (zwykle odpowiednio wczesnego) poinformowania.

8.1.1. Zmiany nie wymagające informowania

Jedynymi zmianami, które według Kodeksu Postępowania Certyfikacyjnego nie wymagają wcześniejszego informowania subskrybentów są zmiany wynikające z wprowadzenia korekt edycyjnych lub zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie Kodeksem. Wprowadzone zmiany nie podlegają procedurze zatwierdzania.

8.1.2. Zmiany wymagające informowania

8.1.2.1. Lista elementów

Po uprzednim poinformowaniu zmianom mogą podlegać dowolne elementy Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich, rozważanych przez Zespół ds. Rozwoju Usług PKI zmianach w Kodeksie jest przesyłana wszystkim zainteresowanym stronom w postaci nowej wersji Kodeksu Postępowania Certyfikacyjnego o statusie **w ankiecie**. Proponowane zmiany publikowane są na stronie WWW Unizeto CERTUM - CCP oraz rozsyłane pocztą elektroniczną. Do nowego Kodeksu dołączona jest także informacja o wprowadzonych zmianach, istotnie odróżniających nowy Kodeks od wersji poprzedniej.

8.1.2.2. Okres oczekiwania na komentarze

Komentarze do zmian proponowanych przez Zespół ds. Rozwoju Usług PKI zainteresowane strony mogą nadsyłać w ciągu 30 dni od daty ich ogłoszenia. Jeśli w wyniku nadesłanych komentarzy Zespół ds. Rozwoju Usług PKI dokonał **istotnych modyfikacji** w proponowanych zmianach, modyfikacje te muszą być ponownie opublikowane i poddane ocenie. Jeśli nie, nowa wersja Kodeksu Postępowania Certyfikacyjnego przyjmuje status w zatwierdzeniu i poddana jest procedurze zatwierdzenia (rozdz.8.3)

Zespół ds. Rozwoju Usług PKI może w pełni akceptować zgłaszane uwagi, akceptować ze zmianami lub odrzucać je po upływie terminu nadsyłania odpowiedzi na rozesłaną i opublikowaną ankietę.

8.1.2.3. Zmiany wymagające nowego identyfikatora Kodeksu

W przypadku zmian które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników Polityki, Zespół ds. Rozwoju Usług PKI może przydzielić zmodyfikowanemu dokumentowi Kodeksu nowy identyfikator (OBJECT IDENTIFIER). Zmianie mogą ulec także identyfikatory polityk certyfikacji według których urzędy mogą wystawiać certyfikaty.

Zmiana identyfikatora Kodeksu Postępowania Certyfikacyjnego następuje po zmianie następujących jego elementów:

poszerzeniu grona użytkowników certyfikatów na obszary związane np. z elektronicznymi płatnościami, wymianę informacji wewnątrz banków oraz pomiędzy bankami, itp.,

wprowadzeniu nowych typów certyfikatów,

dopuszczeniu w systemie certyfikacji wzajemnej pomiędzy organami wydającymi certyfikaty,

istotnej zmiany zawartości i interpretacji pól certyfikatu oraz list CRL, np. zmiana znaczenia pól z niekrytycznych na krytyczne lub odwrotnie,

wprowadzeniu w przypadku subskrybenta końcowego dwóch oddzielnych typów certyfikatów: do podpisywania oraz do wymiany kluczy sesji,

wdrożeniu w ramach Unizeto CERTUM - CCP usługi zawieszania i odwieszania certyfikatu.

8.2. Publikowanie Kodeksu i informowanie o nim

8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego

Publicznie nie są dostępne zastosowane zabezpieczenia systemu komputerowego, procedury oraz mechanizmy uwierzytelniania, a także te elementy, których ujawnienie może osłabić zabezpieczenia oraz zasugerować ataki na nie. W szczególności nie ujawnia się:

zastosowanych platform sprzętowo-programowych,

szczegółów użytej konfiguracji sprzętowej,

planu podnoszenia systemu po awariach i katastrofach,

miejsc przechowywania kluczy Unizeto CERTUM - CCP i chroniących je numerów PIN,

listy osób posiadających sekrety współdzielone,

przedsięwziętych sposobów ochrony personelu Unizeto CERTUM - CCP,

zabezpieczeń sieci,

procedury logowania się do systemu,

zabezpieczeń terminali operatorów.

Nie publikowane elementy udostępniane są administratorowi bezpieczeństwa, administratorowi urzędu certyfikacji oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie Unizeto CERTUM - CCP w specjalnie przeznaczonym do tego celu pomieszczeniu. Każde udostępnienie dokumentacji jest odnotowywane przez administratora bezpieczeństwa w dzienniku zdarzeń.

8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego

Kopia Kodeksu Postępowania Certyfikacyjnego dostępna jest w formie elektronicznej:

na stronie WWW pod adresem: http://www.certum.pl/CPS

via e-mail o adresie: info@certum.pl

W repozytorium oraz za pośrednictwem strony WWW dostępne są zawsze trzy wersje (jeśli jest to możliwe) Kodeksu Postępowania Certyfikacyjnego: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz.8.3).

Za pośrednictwem tych samych adresów zaleca się dostępnienie także dokumentu, opisującego istotne różnice pomiędzy aktualnym (jeszcze obowiązującym Kodeksem) a Kodeksem poddanym procedurze zatwierdzania.

8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego

Jeśli w ciągu 30 dni od daty opublikowania zmian w Kodeksie Postępowania Certyfikacyjnego, wniesionych na podstawie uwag uzyskanych na etapie jego ankietowania (w sposób przedstawiony w rozdz.8.2), Zespół ds. Rozwoju Usług PKI nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości, nowa wersja Kodeksu o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią Kodeksu Postępowania Certyfikacyjnego, respektowaną przez wszystkich subskrybentów Unizeto CERTUM - CCP i przyjmuje status **aktualny**.

Użytkownicy którzy nie akceptują nowych, zmodyfikowanych treści Kodeksu Postępowania Certyfikacyjnego, zobowiązani są do złożenia stosownego oświadczenia w ciągu 15 dni od daty zatwierdzenia nowej wersji Kodeksu Postępowania Certyfikacyjnego.

Dodatek: Słownik pojęć

Audyt – dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się czy system działa zgodnie z ustaloną Polityką Certyfikacji i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Bezpieczna ścieżka (*ang. trusted path*) – łącze zapewniające wymianę informacji związanych z uwierzytelnieniem użytkownika komputera, aplikacji lub innego urządzenia (np. identyfikacyjnej karty elektronicznej), zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

Certyfikat (certyfikat klucza publicznego) – wiadomość (patrz wiadomość), która zawiera co najmniej nazwę lub identyfikator urzędu certyfikacji, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisany przez urząd certyfikacji.

UWAGA: Certyfikat może znajdować się w jednym z trzech podstawowych stanów (patrz Stany klucza kryptograficznego): w oczekiwaniu na aktywność, aktywny i uśpiony.

Certyfikat ważny – certyfikat klucza publicznego jest ważny wtedy i tylko wtedy, gdy: (a) został wydany przez urząd certyfikacji, (b) został zaakceptowany przez podmiot wymieniony w tym certyfikacie oraz (c) nie jest unieważniony.

Certyfikat unieważniony – certyfikat, który został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia (np. po odwieszeniu certyfikatu).

Certyfikat wzajemny (*ang. cross-certificate*) – jest to taki certyfikat klucza publicznego wydany urzędowi certyfikacji, w którym nazwy wystawcy i podmiotu tego certyfikatu są różne, klucz publiczny zawarty w certyfikacie może być używany jedynie do weryfikacji podpisów oraz wyraźnie jest zaznaczone, że certyfikat należy do urzędu certyfikacji.

Certyfikacja wzajemna (*ang. cross–certification*) – procedura wydawania certyfikatu przez urząd certyfikacji innemu urzędowi certyfikacji, który nie pozostaje z urzędem wydającym certyfikat w relacji bezpośredniego podporządkowania lub jest mu bezpośrednio podporządkowany. Zwykle certyfikat wzajemny wydawany jest w celu uproszczenia budowy i weryfikacji ścieżek certyfikatów, złożonych z certyfikatów wydawanych przez różne urzędu certyfikacji. Wydanie certyfikatów wzajemnych może być, ale nie jest to konieczne, realizowane na zasadzie wzajemności: tj. dwa urzędy certyfikacji wydają sobie nawzajem certyfikaty wzajemne.

Dane do audytu – chronologiczne zapisy aktywności w systemie pozwalające na zrekonstruowanie i analizowanie sekwencji zdarzeń oraz zmian, z którymi związane jest zarejestrowane zdarzenie.

Dostęp – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

Dowód posiadania klucza prywatnego (POP, *ang. proof of possesion*) – informacja przekazana przez nadawcę do odbiorcy w takiej postaci, która umożliwia odbiorcy zweryfikowanie ważności powiązania istniejącego pomiędzy nadawcą a kluczem prywatnym, którym jest w stanie posłużyć się lub posługuje się; sposób przeprowadzenia dowodu jest uzależniony zwykle od rodzaju zastosowania pary kluczy; np. w przypadku kluczy podpisujących wystarczy, aby subskrybent przedłożył podpisany tekst (pozytywnie zakończona weryfikacja podpisu stanowi dowód posiadania klucza prywatnego), z kolei w

przypadku kluczy szyfrujących subskrybent musi być w stanie odszyfrować informację zaszyfrowaną przy użyciu należącego do niego klucza publicznego. W Unizeto CERTUM - CCP weryfikacja powiązań pomiędzy parami kluczy stosowanych do podpisu i szyfrowania realizowana jest tylko przez urzędy rejestracji i urzędy certyfikacji.

Identyfikator obiektu (OID, *ang. Object Identifier*) – identyfikator alfanumeryczny/ numeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.

Główny Urząd Rejestracji (GUR) – urząd rejestracji, który akredytuje inne urzędy rejestracji i oprócz standardowych czynności może generować – w imieniu urzędu rejestracji – pary kluczy, które poddaje następnie procesowi certyfikacji.

Infrastruktura klucza publicznego (PKI) – architektura, organizacja, techniki, zasady oraz procedury, które wspólnie wspomagają implementację i działanie kryptograficznych systemów klucza publicznego, opartych na certyfikatach. PKI składa się z powiązanych ze sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych, które dzięki współpracy realizują oraz udostępniają usługi certyfikacyjne, jak również inne związane z tymi elementami usługi (np. usługi znacznika czasu).

Klucz prywatny – klucz pary kluczy asymetrycznych podmiotu, który jest stosowany jedynie przez ten podmiot. W przypadku systemu podpisu asymetrycznego klucz prywatny określa przekształcenie podpisu. W przypadku systemu szyfrowania asymetrycznego klucz prywatny określa przekształcenie deszyfrujące.

UWAGI: (1) W kryptografii z kluczem publicznym klucz który jest przeznaczony do deszyfrowania lub podpisywania, do wyłącznego stosowania przez swego właściciela. (2) W systemie kryptograficznym z kluczem publicznym ten klucz z pary kluczy użytkownika, który jest znany jedynie przez tego użytkownika.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

Klucz tajny – klucz wykorzystywany w symetrycznych technikach kryptograficznych i stosowany jedynie przez zbiór określonych subskrybentów.

UWAGA: Klucz tajny jest przeznaczony do stosowania przez bardzo mały zbiór korespondentów do szyfrowania i deszyfrowania danych.

Kontrola dostępu – proces przekazywania dostępu do zasobów systemów informacyjnych tylko autoryzowanym użytkownikom, programom, procesom oraz innym systemom.

Lista certyfikatów unieważnionych (CRL, *ang. Certificate Revocation List*) – periodycznie (lub w trybie pilnym) wydawana lista podpisana cyfrowo przez urząd certyfikacji, umożliwiająca identyfikację certyfikatów które zostały zawieszone lub unieważnione przez upływem terminu ich ważności. Lista CRL zawiera nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy, numery seryjne zawieszonych lub unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia.

Moduł kryptograficzny – zestaw składający się ze sprzętu, oprogramowania, mikrokodu lub ich określona kombinacja, realizujący operacje lub procesy kryptograficzne obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu.

Naruszenie (np. danych) – ujawnienie informacji nieuprawnionym osobom lub taka ingerencja naruszająca politykę bezpieczeństwa systemu, w wyniku której wystąpi nieuprawnione

(zamierzone lub niezamierzone) ujawnienie, modyfikacja, zniszczenie lub udostępnienie dowolnego obiektu.

Nazwa wyróżniona (DN, *ang. distinguished name*) – zbiór atrybutów, tworzących nazwę wyróżnioną osoby prawnej, odróżniającą go od innych podmiotów tego samego typu; np. C=PL/S=zachodniopomorskie/OU=UNIZETO Sp z o.o., itp.

Obiekt – jednostka do której dostęp jest kontrolowany, np. plik, program, obszar w pamięci głównej; gromadzone i utrzymywane dane osobowe (PN-2000:2002).

Okres aktywności certyfikatu – okres czasu pomiędzy początkową a końcową datą ważności certyfikatu lub pomiędzy datą początku ważności certyfikatu a datą jego unieważnienia lub zawieszenia.

Podpis cyfrowy – przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem przez odbiorcę; asymetryczne podpisy cyfrowe mogą być generowane przez jeden podmiot przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

Polityka certyfikacji – dokument w postaci zestawu reguł, które są ściśle przestrzegane przez organ wydający certyfikaty w trakcie świadczenia przez niego usług certyfikacyjnych.

Polityka podpisu – szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki potwierdzania oraz weryfikacji podpisu elektronicznego, których przestrzeganie umożliwia stwierdzenie ważności podpisu.

Posiadacz sekretu współdzielonego – autoryzowany posiadacz karty elektronicznej, na której przechowywany jest sekret współdzielony.

Procedura postępowania w sytuacji awaryjnej – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu jeśli wystąpi sytuacja nadzwyczajna, lecz przewidywana.

Przejścia między stanami klucza – stan klucza kryptograficznego może ulec zmianie tylko w przypadku, gdy nastąpi jedno z przejść (zgodnie z normą ISO/IEC 11770-1):

generowanie – proces tworzenia klucza; generowanie klucza powinno być wykonywane zgodnie z ustalonymi zasadami generowania kluczy; proces może obejmować procedurę testową, służącą weryfikacji stosowania tych zasad,

aktywacja – powoduje, że klucz staje się uzyskuje ważność i może być stosowany w operacjach kryptograficznych,

deaktywacja – ogranicza użycie klucza; sytuacja taka może zdarzyć się na skutek upływu terminu ważności klucza lub unieważnienia klucza,

reaktywacja – umożliwia ponowne użycie klucza znajdującego się w stanie ustania aktywności do operacji kryptograficznych,

zniszczenie – powoduje zakończenie cyklu życia klucza; pod tym pojęciem rozumie się logiczne zniszczenie klucza, ale może także oznaczać zniszczenie fizyczne.

Publikowanie certyfikatów i list certyfikatów unieważnionych (CRL) (*ang. certificate and certificate revocation lists publication*) – Procedury dystrybucji utworzonych i unieważnionych certyfikatów. Dystrybucja certyfikatu obejmuje przesłanie go do subskrybenta oraz może obejmować jego publikację w repozytorium. Z kolei dystrybucja list certyfikatów unieważnionych oznacza umieszczenie ich w repozytorium, przesłanie do użytkowników końcowych lub przekazanie podmiotom które świadczą usługę weryfikacji statusu certyfikatu w trybie on-line. W obu przypadkach dystrybucja powinna być realizowana przy pomocy odpowiednich środków (np. LDAP, FTP, etc.).

Punkt zaufania – najbardziej zaufany urząd certyfikacji, któremu ufa subskrybent lub strona ufająca. Certyfikat tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez subskrybenta lub stronę ufająca. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot świadczący usługi certyfikacyjne.

Recertyfikacja (*ang. certificate update*) – Przed upływem okresu ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności.

Stany klucza kryptograficznego (prywatnego, publicznego) - klucze kryptograficzne mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku,

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów cyfrowych),

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu cyfrowego lub deszyfrowania.

Urząd rejestracji – zaufana osoba prawna, działająca na podstawie upoważnienia urzędu certyfikacji, rejestrująca inne osoby prawne i przydzielająca im nazwy wyróżnione. Procedura rejestracji w każdej domenie rejestracji wymaga, aby każda rejestrowana wartość była jednoznacznie określona w ramach takiej domeny. Urząd rejestracji nie generuje – w imieniu osób prawnych – pary kluczy które można by poddać później procesowi certyfikacji (patrz: nazwa wyróżniona, certyfikat).

Uwierzytelniać – potwierdzać deklarowaną tożsamość podmiotu.

Uwierzytelnienie – mechanizm zabezpieczeń, którego zadaniem jest zapewnienie wiarygodności przesyłanych danych, wiadomości lub nadawcy, albo mechanizmy weryfikowania autoryzacji osoby przed otrzymaniem przez nią określonych kategorii informacji.

Sekret współdzielony – część sekretu kryptograficznego, np. klucza, podzielonego pomiędzy n zaufanych użytkowników (dokładniej tokenów kryptograficznych typu, np. karty elektroniczne) w taki sposób, aby do jego zrekonstruowania potrzeba było m (m<n) części.

Strona ufająca (*ang. relaying party*) – odbiorca, który otrzymał informację zawierającą certyfikat lub z nią powiązany oraz podpis cyfrowy weryfikowalny przy pomocy klucza publicznego umieszczonego w tym certyfikacie i znajdujący się w sytuacji, gdy na podstawie zaufania do certyfikatu musi podjąć decyzję o uznaniu lub odrzuceniu podpisu.

Sponsor subskrybenta – instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu.

Subskrybent – jednostka (osoba fizyczna, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej, urządzenie, które jest pod opieką tych osób lub jednostki organizacyjnej), która; (1) jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej jednostce, (2) posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie, oraz (3) sama nie wydaje certyfikatów innym stronom.

System informacyjny – całość infrastruktury, organizacja, personel oraz komponenty służące do gromadzenia, przetwarzania, przechowywania, przesyłania, prezentowania, rozgłaszania i zarządzanie informacją.

Ścieżka certyfikacji – uporządkowany ciąg certyfikatów, prowadzący od certyfikatu **punktu zaufania**, wybranego przez weryfikującego, aż do weryfikowanego certyfikatu, utworzony w celu weryfikacji certyfikatu. Ścieżka certyfikacji spełnia następujące warunki:

dla każdego certyfikatu Cert(x) należącego do ścieżki certyfikacji {Cert(1), Cert(2), ..., Cert(n-1)} podmiot certyfikatu Cert(x) jest wydawcą certyfikatu Cert(x+1),

certyfikat Cert(1) jest wydany przez urząd certyfikacji (**punkt zaufania**), któremu ufa weryfikator,

Cert(n) jest weryfikowanym certyfikatem.

Z każdą ścieżką certyfikacji można związać jedną lub więcej polityk certyfikacji lub też taka polityka może nie istnieć. Polityki przypisane określonej ścieżce certyfikacji są częścią wspólną (iloczynem) zbiorów polityk, których identyfikatory są zawarte w każdym certyfikacie, należącym do ścieżki certyfikacji i zdefiniowane w ich rozszerzeniu **certificatePolicies**.

Token – element danych stosowany w wymianach pomiędzy stronami zawierający informację, która została przekształcona z wykorzystaniem technik kryptograficznych. Token jest podpisany przez operatora urzędu rejestracji i może być wykorzystany do uwierzytelnienia jego nadawcy w trakcie kontaktów z urzędem certyfikacji.

Unizeto CERTUM - Centrum Certyfikacji Powszechne (Unizeto CERTUM - CCP) – obdarzona zaufaniem instytucja (lub urządzenie pod kontrolą instytucji), będąca elementem składowym zaufanej trzeciej strony, zdolna do tworzenia, podpisywania i wydawania certyfikatu (porównaj: Punkt Rejestracji, zaufana trzecia strona).

Unieważnienie certyfikatów (*ang. certificates revocation*) – określa procedury protokołu CMP odwołania ważności pary kluczy (wycofania certyfikatu) w przypadku, gdy zachodzi konieczność uniemożliwienia subskrybentowi dostępu do tej pary i użycia jej w operacjach szyfrowania lub podpisu elektronicznego. Unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Użytkownik (certyfikatu, *ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – weryfikacja statusu certyfikatów umożliwia określenie czy certyfikat jest unieważniony, czy też nie. Tego typu problem może być rozwiązany przez sam zainteresowany podmiot w oparciu o listy CRL albo też przez wystawcę certyfikatu lub upoważnionego przez niego przedstawiciela na wyraźne zapytanie podmiotu skierowane do serwera OCSP.

Wnioskodawca – określenie używane w stosunku do subskrybenta w okresie pomiędzy chwilą, gdy wystąpił z jakimkolwiek żądaniem (wnioskiem) do urzędu certyfikacji a momentem ukończenia procedury wydawania certyfikatu.

Zaufana Trzecia Strona (TTP) – instytucja lub jej przedstawiciel mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

Zespół Operacyjny Unizeto CERTUM - Centrum Certyfikacji Powszechne – personel odpowiedzialny za funkcjonowanie Unizeto CERTUM - CCP. Odpowiedzialność ta dotyczy finansowania pracowników, rozstrzygania sporów, podejmowania decyzji oraz kształtowania polityki rozwoju Centrum. Osoby zatrudnione w Zespole Operacyjnym nie posiadają dostępu do stacji roboczych i systemu komputerowego Unizeto CERTUM - CCP.

Literatura

[1] ITU-T Recommendation X.509 – *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, June 1997 (odpowiednik ISO/IEC 9594-8)

[2] ITU-T Recommendation X.520 – *Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types*, 1993

[3] *CARAT Guidelines – Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*, National Automated Clearing House Association (NACHA), The Internet Council CARAT Task Force, v.1.0, Draft September 21, 1998

[4] *VeriSign CPS – VeriSign Certification Practice Statement*, ver.2.0, August 31, 2001, http://www.verisign.com

[5] *ARINC Digital Signature Service (ADSS) – Certification Practice Statement (CPS),* ver.2.0, August 6, 1998

[6] ISO/IEC JTC 1/SC27 N691 *Guidelines on the Use and Management of Trusted Third Party Services*, August 1993

[7] RFC 822 D.Crocker – *Standard for the format of ARPA Internet text messages*, August 1982

[8] RFC 1738 T.Berners-Lee, L.Masinter, M.McCahill – *Uniform Resource Locators (URL),* December 1994

[9] RFC 1778 T.Howes, S.Kille, W.Yeong, C.Robbins *The String Representation of Standard Attribute Syntaxes*, March 1995

[10] RFC 2247 S.Kille, M.Wahl, A.Grimstad, R.Huber, S.Sataluri – *Using Domains in LDAP/X.500 Distinguished Names*, January 1998

[11] RFC 2459 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile*, 1999

[12] Steven Castell *Trusted Third Party Services – User Requirements for Trusted Third Party Services*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, July 29, 1993

[13] Steven Castell *Trusted Third Party Services - Functional model*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, December 13, 1993

[14] *Ustawa z dnia 22 stycznia 1999 O ochronie informacji niejawnych*, Dziennik Ustaw Rzeczpospolitej Polskiej, Nr.11, Warszawa, 8 lutego 1999 r.

[15] Simson Garfinkel, Gene Spafford *Bezpieczeństwo w Unixie i internecie*, Wyd. RM, Warszawa 1997

[16] S.Chkhani, W.*Ford Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, RFC 2527, March, 1999

[17] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. *Wu Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, July 12, 2001, < draft-ietf-pkix-ipki-new-rfc2527-00.txt >

[18] European Telecommunications Standards Institute *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456 V1.1.1 (2000-12)

[19] *Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure* (Working Draft), v.2.0 August 1998

[20] RFC 3161 *Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP), PKIX Working Group*, January 2001

[21] *PKI Assessment Guidelines - Guidelines to Help Assess and Facilitate Interoperable Trustworthy Public Key Infrastructures, PAG v0.30*, Public Draft for Comment, June 18, 2001, Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law, American Bar Association,

[22] *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

[23] CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*, CEN (European Committee for Standardization) November 2001,

[24] *Digital Signature Standard*, FIPS 186-2 NIST (Jan. 2000)

[25] *EESSI-SG Algorithms and Parameters for Secure Electronic Signatures*, 19 October 2001

[26] FIPS 112 *Password Usage*, 30 May 1985, http://csrs.nist.gov/fips/

Historia dokumentu

Historia zmian dokumentu		
V 1.0	15 kwietnia 2000 r.	Szkic dokumentu do dyskusji
V 1.33	12 marca 2002 r.	Pełna wersja dokumentu. Dokument zatwierdzony
V 2.0	15 lipca 2002 r.	Zdefiniowanie dodatkowych typów certyfikatów. Modyfikacje procedur certyfikacji, doprecyzowanie profilu certyfikatów i list CRL. Przeredagowano rozdz.3, 4, 6.1, 2.6, 6.2-6.9 i 7. Zatwierdzenie dokumentu.