Polityka Certyfikacji Kwalifikowanych Usług CERTUM

Wersja 2.3

Data: 01 stycznia 2006

Status: poprzedni

Unizeto Technologies S.A.
(dawniej Unizeto Sp. z o.o.)
„CERTUM - Powszechne Centrum Certyfikacji”
ul. Królowej Korony Polskiej 21
70-486 Szczecin
http://www.certum.pl

Klauzula: Prawa Autorskie

Wszelkie pytania związane z prawami autorskimi należy adresować do Unizeto Technologies S.A., ul. Królowej Korony Polskiej 21, 70-486 Szczecin, Polska, tel. +48 91 4801 201, fax +48 91 4801 222, email: info@certum.pl.

Spis treści

1.Wstęp

Polityka Certyfikacji Kwalifikowanych Usług CERTUM określa szczegółowe rozwiązania (w tym techniczne i organizacyjne) stosowane przez jednostkę organizacyjną **CERTUM (pełna nazwa: CERTUM - Powszechne Centrum Certyfikacji)** świadczącą kwalifikowane usługi certyfikacyjne wskazujące sposób, zakres, oraz warunki tworzenia i stosowania certyfikatów (*Ustawa z dnia 18 września 2001r. o podpisie elektronicznym* - Dz.U. Nr 130, poz. 1450 z późn. zm.*, dalej w tekście zwanej Ustawą*).

Z polityką certyfikacji ściśle związany jest kodeks postępowania certyfikacyjnego. Kodeks postępowania certyfikacyjnego definiowany jest jako *deklaracja procedur stosowanych przez urząd certyfikacji w procesie wydawania certyfikatu*[1] oraz znakowania czasem.

Firma Unizeto Technologies S.A. (dawniej Unizeto Sp. z o.o.) jest następcą prawnym Unizeto Sp. z o.o. Zgodnie z Kodeksu Spółek Handlowych (Dz.U. Nr 94, poz. 1037 z późn. zm.) nastąpiła sukcesja uniwersalna na podstawie której Unizeto Technologies S.A. wstąpiła we wszelkie prawa i obowiązki Unizeto Sp. z o.o.

1.1. Wprowadzenie

Przedstawiona w niniejszym dokumencie Polityka Certyfikacji opisuje zakres działania **CERTUM** świadczącego kwalifikowane usługi certyfikacyjne (działającej w ramach Unizeto Technologies S.A.) oraz związanych z nim **punktów sieci systemu rejestracji**, **subskrybentów**, jak również **stron ufających**. Określa także zasady **wydawania kwalifikowanych certyfikatów** obejmującą rejestrację subskrybentów, certyfikację kluczy publicznych i aktualizację kluczy oraz certyfikatów, **unieważniania i zawieszania certyfikatów**, **weryfikowania statusu certyfikatów w trybie *on-line*** oraz zasady wystawiania **tokenów znaczników czasu**. Certyfikaty kwalifikowane wydawane przez CERTUM wystawiane są zgodnie z zasadami **polityki certyfikacji**, określonymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. *w sprawie określenia warunków technicznych o organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.*.

CERTUM działa zgodnie z prawem obowiązującym na terytorium Rzeczpospolitej Polskiej, zasadami obowiązującymi kwalifikowane podmioty świadczące usługi certyfikacyjne, określonymi w *Ustawie* oraz niniejszą Polityką Certyfikacji. Unizeto Technologies S.A., z siedzibą w Szczecinie, przy ulicy Królowej Korony Polskiej 21, którego jednostką organizacyjną jest CERTUM, świadczące kwalifikowane usługi certyfikacyjne, jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne, w myśl ww. *Ustawy*, wpisanym do rejestru kwalifikowanych podmiotów świadczących usług certyfikacyjne pod numerem 1.

Strukturę i merytoryczna zawartość Polityki Certyfikacji oparto na powszechnie akceptowanych zaleceniach i normach, m.in. RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. Daje to subskrybentom **CERTUM** możliwość szybkiego porównania Polityki Certyfikacji z podobnymi dokumentami, wydanymi przez inne urzędy certyfikacji.

1.2. Nazwa dokumentu i jego identyfikacja

Identyfikator niniejszej Polityki Certyfikacji, zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów ma postać:

[1] ABA Digital Signature Guidelines, Rozdzial 1.8 "Certification Practice Statement"

```
id-cck-pc-v1  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
          organization(1) id-unizeto(113527) id-ccert(2) id-cck(4)
          id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-pc(1)
          version(2) 0}
```

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

Dokument ten jest dostępny:

w postaci elektronicznej w repozytorium o adresie http://www.certum.pl/repozytorium lub na żądanie wysłane na adres e-mail info@certum.pl .

w postaci kopii papierowej na żądanie wysłane na adres CERTUM (patrz rozdz.1.6).

W certyfikatach wydawanych przez CERTUM umieszcza się identyfikatory polityk certyfikacji, które należą do zbioru polityk certyfikacji wspieranych przez niniejszą dokument Polityki Certyfikacji, którego identyfikator określono powyżej. Identyfikatory polityki certyfikacji, publikowane w certyfikacie, opisano w rozdz. 7.1.1.2.

1.3. Uczestnicy Polityki Certyfikacji oraz zakres jej stosowania

Elementami infrastruktury CERTUM, świadczącego kwalifikowane usługi certyfikacyjne są:

urzędu certyfikacji CERTUM QCA,

urzędu znacznika czasu CERTUM QTSA,

Głównego Punktów Rejestracji (GPR),

punktów rejestracji (PR),

notariuszy lub osób potwierdzających tożamość,

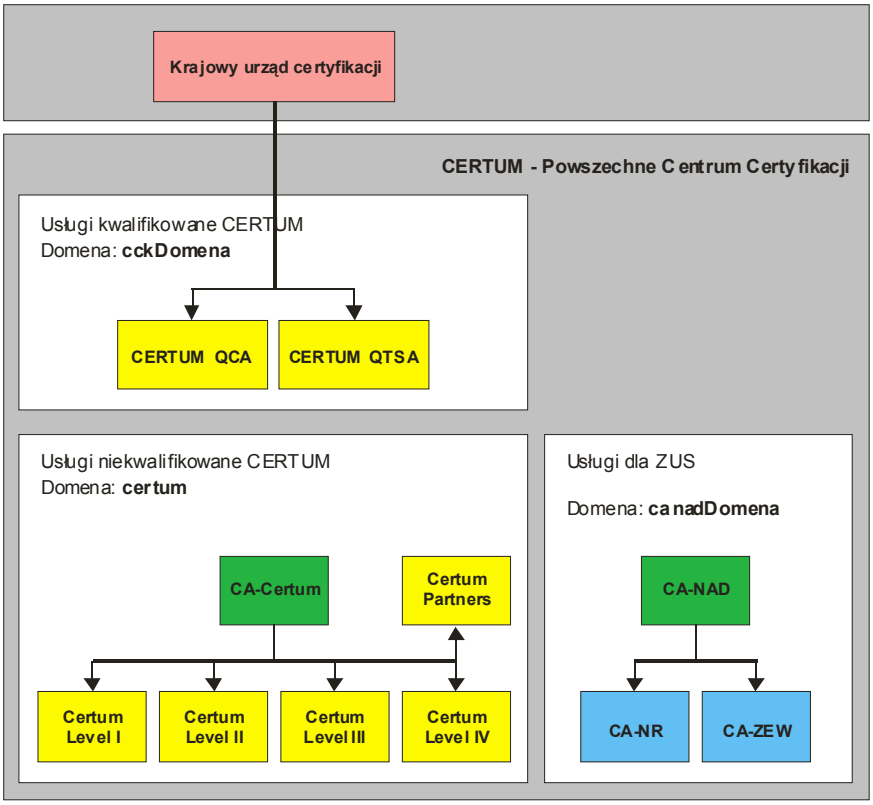
subskrybentów,

stron ufających.

1.3.1. Urząd certyfikacji

W skład CERTUM świadczącego usługi kwalifikowane wchodzi jeden urząd certyfikacji **CERTUM QCA** (rys.1), działające na podstawie wpisu Unizeto Technologies S.A. (dawniej Unizeto Sp. z o.o.) na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem certyfikacji **CERTUM QCA** sprawuje minister właściwy ds. gospodarki lub wskazany przez niego podmiot (**krajowy urząd certyfikacji**).

Urząd CERTUM QCA jest nowym urzędem, który powstał po aktualizacji zaświadczenia certyfikacyjnych, zgodnie z *Rozporządzeniem Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1101)*. Stare zaświadczenie certyfikacyjne będzie służyło jedynie do tworzenia i publikowania list certyfikatów unieważnionych przez okres do 30 grudnia 2007 16:16:49 GMT.



Rys.1 Urzędy działające w **ramach kwalifikowanych usług CERTUM** na tle innych urzędów.

Urząd certyfikacji **CERTUM QCA** wydaje kwalifikowane certyfikaty, certyfikaty kluczy infrastruktury i zaświadczenia certyfikacyjne zgodnie z *Ustawą o podpisie elektronicznym z dnia 18 września 2002 r.*, *Rozporządzeniem Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1094)* oraz *Rozporządzeniem Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1101).*

Tab.1 Identyfikatory polityk certyfikacji umieszczane w certyfikatach i zaświadczeniach certyfikacyjnych wydawanych przez **CERTUM QCA**

Nazwa certyfikatu /zaświadczenia certyfikacyjnego	Identyfikator polityki certyfikacji
Certyfikaty kwalifikowane	1.2.616.1.113527.2.4.1.1
Zaświadczenia certyfikacyjne	2.5.29.32.0
Certyfikaty kluczy infrastruktury	1.2.616.1.113527.2.4.1.10

1.3.2. Urząd znacznika czasu

Kolejnym elementem CERTUM, świadczącego kwalifikowane usługi certyfikacyjne (również działającym w domenie certyfikacji **cckDomena)**, jest urząd znacznika czasu **CERTUM QTSA** (rys.1). Urząd znacznika czasu działaja na podstawie wpisu Unizeto Technologies S.A. (dawniej Unizeto Sp. z o.o.) na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem znacznika czasu CERTUM QTSA sprawuje minister właściwy ds. gospodarki lub wskazany przez niego podmiot (**krajowy urząd certyfikacji**).

Urząd CERTUM QTSA jest nowym urzędem, który powstał po aktualizacji zaświadczenia certyfikacyjnych, zgodnie z Rozporządzeniem Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Dz.U. 2002 nr 128 poz. 1101).

Tab.2 Identyfikator polityki certyfikacji umieszczany przez **CERTUM QTSA** w tokenach znacznika czasu

Nazwa tokena	Identyfikator polityki certyfikacji
Token znacznika czasu	1.2.616.1.113527.2.4.1.2

Znaczniki czasu, wydawane zgodnie z polityką określoną w Tab.2, znajdują zastosowanie przede wszystkim do zabezpieczania długookresowych podpisów elektronicznych[2] oraz transakcji zawieranych w sieci globalnej.

Urząd znacznika czasu **CERTUM QTSA** przy świadczeniu usług znacznika czasu stosuje rozwiązania zapewniające synchronizację z międzynarodowym wzorcem czasu (Coordinated Universal Time - UTC), z dokładnością do 1 sekundy.

1.3.3. Punkty rejestracji i potwierdzania tożsamości

Z urzędem certyfikacji **CERTUM QCA** ściśle współpracują Główny Punkt Rejestracji, punkty rejestracji oraz punkty potwierdzania tożsamości. Punkty rejestracji i punkty potwierdzania tożsamości reprezentują urząd certyfikacji w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez urząd certyfikacji uprawnień w zakresie potwierdzania tożsamości i rejestracji aktualnego lub przyszłego subskrybenta. CERTUM może również stwierdzić tożsamość osoby ubiegającej się o certyfikat bez jej osobistego stawiennictwa w punkcie rejestracji, na podstawie notarialnego potwierdzenia tożsamości. CERTUM może również wyznaczyć inne osoby potwierdzające w jego imieniu tożsamość wnioskodawcy oraz uprawnione do przyjmowania wniosków i zawierania umów na świadczenie usług certyfikacyjnych.

Punkty potwierdzania tożsamości, w odróżnieniu od punktów rejestracji, nie zajmują się tworzeniem zgłoszeń certyfikacyjnych. Służą jedynie weryfikacji tożsamości subskrybenta i poprawności wypełnienia wniosku o usługę certyfikacyjną oraz udzielają informacji o podpisie elektronicznym, w tym o skutkach jakie wywołuje, zawieraniu umowy na świadczenie usług certyfikacyjnych.

Lista aktualnie akredytowanych punktów rejestracji i punktów potwierdzania tożsamości dostępna jest w repozytorium CERTUM pod adresem: http://www.certum.pl/repozytorium.

1.3.4. Użytkownicy końcowi

1.3.4.1. Subskrybenci

Subskrybentami CERTUM mogą być osoby fizyczne, prawne lub podmioty nieposiadające osobowości prawnej oraz urządzenia infrastruktury klucza publicznego będące pod ich kontrolą.

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

[2] IETF RFC 3126 *Electronic Signature Formats for long term electronic signatures*, September 2001

1.3.4.2. Strony ufające

Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji podpisu elektronicznego uzależnioną w jakikolwiek sposób od ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez urząd certyfikacji **CERTUM QCA**, lub powiązania podpisu elektronicznego z tokenem znacznika czasu, wydanym przez urząd znacznika czasu CERTUM QTSA.

1.4. Zakres stosowania certyfikatów i zaświadczeń certyfikacyjnych

Certyfikaty kwalifikowane wystawione przez CERTUM mogą być stosowane tylko do składania bezpiecznych podpisów, które są niezaprzeczalnym dowodem złożenia aktu woli i powiązania z podpisywaną informacją o różnym poziomie wrażliwości.

Zaświadczenia certyfikacyjne wydawane są krajowemu urzędowi certyfikacji, działającego w imieniu i z upoważnienia ministra właściwego ds. gospodarki urzędom certyfikacji lub na potrzeby procesu wymiany kluczy urzędu certyfikacji.

Certyfikaty kluczy infrastruktury wydawane są personelowi CERTUM oraz urządzeniom będącym pod opieką tego urzędu. Subskrybenci i strony ufające mogą wchodzą w kontakt z tymi certyfikatami jedynie w momencie korzystania z serwisów usługowych CERTUM. Certyfikaty kluczy infrastruktury nie mogą być używane do składania bezpiecznych podpisów elektronicznych (nawet, jeśli certyfikat posiada ustawiony bit **digitalSignature** lub **nonRepudiation** w rozszerzeniu **keyUsage**).

1.5. Zakres stosowania znaczników czasu

Urząd znacznika czasu **CERTUM QTSA** wystawia tokeny znacznika czasu, które zgodnie z *Ustawą* wywołują w szczególności skutki prawne daty pewnej w rozumieniu przepisów *Kodeksu cywilnego (Art.7, §2)*. Głównym zastosowaniem znaczników czasu jest znakowanie czasem bezpiecznych podpisów elektronicznych w przypadku ich długookresowej ważności. Znaczniki czasu wystawiane przez urząd znacznika czasu mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości usługi znakowania czasem.

1.6. Kontakt

W celu uzyskania dalszych informacji dotyczących usług i działalności CERTUM, świadczącego kwalifikowane usługi certyfikacyjne należy kontaktować się z:

Unizeto Technologies S.A. (dawniej Unizeto Sp. z o.o.)

„CERTUM - Powszechne Centrum Certyfikacji”

70-486 Szczecin, ul. Królowej Korony Polskiej 21

E-mail: info@certum.pl

Numer telefonu: (+48 91) 4801 201

Numer faksu: (+48 91) 4801 222

2. Postanowienia ogólne

W rozdziale tym przedstawione są zobowiązania (gwarancje) i odpowiedzialność CERTUM, punktów rejestracji, subskrybentów oraz użytkowników certyfikatów (stron ufających).

2.1. Zobowiązania

2.1.1. Zobowiązania CERTUM i punktów rejestracji

CERTUM, świadczące kwalifikowane usługi certyfikacyjne, zobowiązuje się do:

przedsięwzięcia stosownych kroków, mających na celu weryfikację informacji identyfikującej tożsamość subskrybenta wniosków składanych przez strony;

wydania, zawieszenia lub unieważnienia kwalifikowanego certyfikaty na podstawie prawidłowego wniosku oraz powiadomienia wnioskodawcy o realizacji lub odrzucenia wniosku;

unieważnienie lub zawieszenia certyfikatu w przypadku gdy zawartość certyfikatu zdezaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.);

udostępnieniu informacji o wydaniu (gdy subskrybent wyrazi na to zgodę), unieważnieniu lub zawieszeniu kwalifikowanego certyfikatu;

zapewnienia właściwej długości i struktury certyfikowanych kluczy publicznych oraz unikalności (w ramach swojej domeny) nazw wyróżnionych (DN) stosowanych w certyfikatach;

respektowanie praw subskrybentów i stron ufających wynikających z przepisów prawa, uregulowań CERTUM i zawartych umów ;

zapewnienia należytej ochrony danych osobowych subskrybenta;

stosowania co najmniej takich samych parametrów algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w „Wymaganiach dla algorytmów szyfrowych" stanowiących załącznik nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*).

Punkty rejestracji oraz osoby i punkty potwierdzające tożsamość zobowiązują się ponadto do:

przestrzegania procedur potwierdzania tożsamości wnioskodawców wydania, zawieszanie bądź unieważnienia certyfikatu oraz wydawania koniecznych tokenów zgłoszenia certyfikacyjnego, upoważniających do skorzystania z określonej usługi CERTUM,

podporządkowania się zaleceniom CERTUM,

ochrony kluczy prywatnych operatorów punktu rejestracji i punktów potwierdzania tożsamości;

nie używania kluczy prywatnych operatorów do innych celów niż tych, które określono w niniejszej Polityce Certyfikacji.

2.1.1.1. Zobowiązania urzędu znacznika czasu

Urząd znacznika czasu **CERTUM QTSA** gwarantuje, że świadczy usługi znacznika czasu zgodnie z wymaganiami określonymi w Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*) oraz w niniejszej Polityce Certyfikacji.

W szczególności CERTUM QTSA:

stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania czasem,

stosuje co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w „Wymaganiach dla algorytmów szyfrowych" stanowiących załącznik nr 3 do Rozporządzenia Rady Ministrów z dnia 7 sierpnia 2002 r. (*Dz.U. 2002 nr 128 poz. 1094*),

określa przynajmniej jeden algorytm funkcji skrótu, który może być stosowany do obliczenia wartości skrótu z danych, które podlegają oznakowaniu czasem,

gwarantuje, że czas UTC, który zostaje umieszczony w tokenie znacznika czasu, podawany jest z dokładnością do 1 sekundy.

2.1.2. Zobowiązania użytkowników końcowych

2.1.2.1. Zobowiązania subskrybenta

Subskrybent certyfikatów kwalifikowanych wydawanych przez CERTUM zobowiązuje się do:

używania certyfikatów i zaświadczeń tylko zgodnie z ich przeznaczeniem,

używania certyfikatów i zaświadczeń tylko w ich okresie ważności,

podjęcia wszelkie środki ostrożności w celu bezpiecznego przechowywania klucza prywatnego z certyfikowanej pary kluczy,

w przypadku konieczności zawieszenia lub unieważnienia certyfikatu – do niezwłocznego zgłoszenia tego faktu w CERTUM.

2.1.2.2. Zobowiązania stron ufających

Strona ufająca zobowiązana jest do:

rzetelnej weryfikacji każdego podpisu lub poświadczenia elektronicznego umieszczonego na dokumencie lub certyfikacie lub tokenie znacznika który do niej dotrze,

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

2.2. Odpowiedzialność CERTUM

CERTUM, świadczące kwalifikowane usługi certyfikacyjne, ponosi odpowiedzialność za skutki działań urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, Głównego Punktu Rejestracji, punktów systemu rejestracji i innych osób potwierdzających tożsamość w zakresie określonym w zawartych umowach.

CERTUM ponosi odpowiedzialność za szkody poniesione przez subskrybenta lub stronę ufającą w wyniku błędów popełnionych przez CERTUM, zwłaszcza w zakresie niezgodności procesu weryfikacji tożsamości z deklarowanymi procedurami, niewłaściwej ochrony klucza prywatnego urzędu certyfikacji lub braku dostępu do świadczonych usług, np. do list certyfikatów unieważnionych,

CERTUM nie ponosi odpowiedzialności za szkody poniesione przez subskrybenta lub stronę ufającą w wyniku instalacji, użytkowania oraz zarządzania aplikacjami innymi niż dostarczone przez CERTUM lub za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów.

CERTUM nie ponosi również odpowiedzialności za szkody poniesione przez subskrybenta lub stronę ufającą w przypadku podania przez subskrybenta fałszywych danych które - mimo zachowania przez CERTUM należytej staranności - umieszczone zostaną zarówno w bazach CERTUM, jak też w wydanym certyfikacie klucza publicznego.

2.3. Odpowiedzialność finansowa

Odpowiedzialność finansowa Unizeto Technologies S.A., w imieniu której CERTUM świadczy kwalifikowane usługi, w stosunku do jednego zdarzenia wynosi równowartość w złotych 250.000 Euro, ale nie więcej niż 1.000.000 Euro w odniesieniu do wszystkich takich zdarzeń. Odpowiedzialność finansowa dotyczy okresów 12-miesięcznych począwszy od dnia wpisania Unizeto Technologies S.A. do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacji.

2.4. Akty prawne i rozstrzyganie sporów

2.4.1. Obowiązujące akty prawne

Funkcjonowanie CERTUM oparte jest na zasadach zawartych w niniejszej Polityce Certyfikacji, Kodeksie Postępowania Certyfikacyjnego oraz obowiązujących przepisach prawa.

2.4.2. Rozstrzyganie sporów

Spory bądź zażalenia powstałe na tle użytkowania certyfikatów CERTUM będzie rozstrzygał na podstawie pisemnych informacji w drodze mediacji.

W przypadku nie rozstrzygnięcia kwestii spornych w drodze mediacji stronom przysługuje zapis na sąd polubowny bądź droga sądowa.

2.5. Opłaty

Za świadczone usługi CERTUM pobiera opłaty. Wysokości opłat, oraz rodzaje usług objętych opłatami, są publikowane przez repozytorium CERTUM pod adresem:

http://www.certum.pl/repozytorium

2.6. Repozytorium i publikacje

2.6.1. Informacje publikowane przez CERTUM

Wszystkie informacje publikowane przez **CERTUM** dostępne są w repozytorium pod następującym ogólnym adresem:

http://www.certum.pl/repozytorium

Są to następujące informacje:

Regulamin Kwalifikowanych Usług Certyfikacyjnych,

Polityka Certyfikacji Kwalifikowanych Usług Certyfikacyjnych,

Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług Certyfikacyjnych,

nieprzeterminowane i nieunieważnione zaświadczenia certyfikacyjne: urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, oraz certyfikaty subskrybentów

list bezpiecznych urządzeń, rekomendowanych przez **CERTUM**,

list akredytowanych punktów systemu rejestracji, notariuszy i innych osób potwierdzających tożsamość,

listy certyfikatów unieważnionych (CRL),

informacje pomocnicze, np. ogłoszenia.

2.6.2. Częstotliwość publikacji

Wymienione poniżej publikacje CERTUM są ogłaszane z następującą częstotliwością:

Regulamin Kwalifikowanych Usług Certyfikacyjnych, Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego (patrz rozdz.8),

zaświadczenia certyfikacyjne urzędów certyfikacji i urzędu znakowania czasem CERTUM – każdorazowo, gdy nastąpi emisja nowych zaświadczeń,

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

listy certyfikatów unieważnionych i zawieszonych,

informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.6.3. Dostęp do publikacji

Wszystkie informacje publikowane przez CERTUM w jego repozytorium pod adresem: http://www.certum.pl/repozytorium są dostępne publicznie.

2.7. Audyt

Audyt CERTUM może być prowadzony przez komórki wewnętrzne Unizeto Technologies S.A. (**audyt wewnętrzny**) oraz przez jednostki organizacyjne niezależne od Unizeto Technologies S.A. (**audyt zewnętrzny**). Audyt zewnętrzny może być przeprowadzony na wniosek ministra właściwego ds. gospodarki w trybie Art.36 *Ustawy*.

2.8. Ochrona informacji

Unizeto Technologies S.A. gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującymi w tym zakresie przepisami prawa, a w szczególności *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych*.

Unizeto Technologies S.A. gwarantuje, że stronom trzecim udostępniane są tylko te informacje, które są publicznie dostępne w certyfikacie i na których publikację zgodę wyraził subskrybent certyfikatu.

2.9. Prawo do własności intelektualnej

Wszystkie używane przez Unizeto Technologies S.A. znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli.

Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez CERTUM jest – w przypadku subskrybenta indywidualnego - własnością podmiotu tego certyfikatu lub - w przypadku subskrybenta sponsorowanego - sponsora certyfikatu.

2.10. Synchronizacja czasu

Wszystkie zegary funkcjonujące w ramach systemu CERTUM świadczące kwalifikowane usługi i wykorzystywane w trakcie świadczenia usług są synchronizowane z międzynarodowym wzorcem czasu (Coordinated Universal Time), z dokładnością do 1 sekundy.

3.Identyfikacja i uwierzytelnianie

Poniżej przedstawiono ogólne zasady identyfikacji i uwierzytelnienia (weryfikacji) tożsamości subskrybentów, którymi kieruje się CERTUM podczas wydawania, unieważniania i zawieszania certyfikatów i zaświadczeń certyfikacyjnych.

3.1. Rejestracja subskrybenta urzędu certyfikacji

Akt rejestracji subskrybenta ma miejsce zawsze wtedy, gdy nie był on wcześniej znany urzędowi certyfikacji CERTUM oraz nie posiada żadnego **ważnego certyfikatu** wydanego przez ten urząd.

Każdy subskrybent ubiegający się o wydanie certyfikatu musi wykonać następujące podstawowe czynności, poprzedzające wydanie certyfikatu:

stawić się wraz z wymaganymi dokumentami w punkcie rejestracji lub u notariusza,

podpisać umowę na świadczenie usług przez CERTUM,

wypełnić wniosek o wydanie kwalifikowanego certyfikatu, stosowny do żądanego rodzaju certyfikatu; wzór wniosku jest dostępny w repozytorium,

określić, zgodnie z postanowieniami *art.20 ust.2 Ustawy*, w jakim charakterze będzie działać posługując się kwalifikowanym certyfikatem (w imieniu własnym, jako przedstawiciel innej osoby fizycznej, prawnej lub organu władzy publicznej).

Wnioskodawca podczas wizyty w punkcie rejestracji lub potwierdzania tożsamości jest informowany na piśmie lub za pomocą informacji trwale zapisanej na nośniku elektronicznym, w sposób jasny i powszechnie zrozumiały o dokładnych warunkach użycia kwalifikowanego certyfikatu, w tym o sposobie rozpatrywania skarg i sporów, a w szczególności o istotnych warunkach obejmujących:

zakres i ograniczenia stosowania certyfikatu,

skutki prawne składania podpisów elektronicznych weryfikowanych przy pomocy tego certyfikatu,

informacje o systemie dobrowolnej rejestracji kwalifikowanych podmiotów świadczących usługi certyfikacyjne i ich znaczeniu.

Rejestracja subskrybentów występujący jako przedstawiciel innej osoby fizycznej, prawnej lub organu władzy publicznej przebiega podobnie jak w przypadku rejestracji subskrybentów indywidualnych. Poprzedzona jest zawarciem umowy sponsorowanej miedzy Unizeto Technologies S.A. a sponsorem (reprezentowaną osobą fizyczną, prawną lub organem władzy publicznej) subskrybenta.

3.1.1. Nazwy wyróżnione i kategorie certyfikatów

Nazwa wyróżniona (DN) zawiera niektóre lub wszystkie atrybuty zawarte w następującym zbiorze atrybutów:

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

pole ST: województwo, na którego terenie działa lub mieszka subskrybent;

pole L: miasto, w którym ma siedzibę lub mieszka subskrybent;

pole S: nazwisko subskrybenta (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),

pole G: imię (imiona) subskrybenta,

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

pole CN: nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje subskrybent,

pole O: nazwa instytucji, w której pracuje subskrybent,

pole OU: nazwa jednostki organizacyjnej, zatrudniającej subskrybenta,

pole SN: numer seryjny, zawierający NIP lub PESEL subskrybenta,

pole A: adres do korespondencji z subskrybentem**.**

Certyfikaty mogą być wydawane różnym kategoriom podmiotów:

kategoria I zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona), numer seryjny.

kategoria II zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwa powszechna, numer seryjny.

kategoria III zawiera przynajmniej następujące atrybuty: nazwa kraju i pseudonim.

CERTUM gwarantuje (w ramach swojej domeny) unikalność nazw DN.

3.1.2. Uwierzytelnienie tożsamości subskrybentów

Weryfikacja osób fizycznych, może być realizowana w punkcie systemu rejestracji, przez notariusza lub osobę potwierdzającą tożsamość.

Potwierdzenie tożsamości subskrybenta - osoby fizycznej w punkcie systemu rejestracji, przy udziale notariusza lub innej osoby potwierdzającej tożsamość realizowane jest na podstawie:

dwóch dokumentów tożsamości, z których co najmniej jeden to ważny dowód osobisty lub paszport,

dokumentu potwierdzającego przydzielone numery PESEL lub NIP,

oraz dodatkowo w przypadku, gdy subskrybent jest osobą fizyczną dla której wydawany jest certyfikat kategorii II lub III (pracownikiem organizacji lub jej reprezentantem):

stosownego upoważnienia wystawionego przez daną organizację do reprezentowania jej interesów i umieszczenie danych organizacji w certyfikacie,

aktualnego wypisu z Krajowego Rejestru Sądowego lub potwierdzonego za zgodność z oryginałem wypisu z ewidencji działalności gospodarczej.

Dokumenty potwierdzające tożsamość subskrybenta oraz pozostałe dokumenty wymagane do realizacji procesu certyfikacji, podlegają kopiowaniu i są archiwizowane w CERTUM przez stosowany okres czasu. Część danych, zgodnie z wymaganiami GIODO, jest trwale usuwana z kopiowanych dokumentów.

Uwierzytelnianie subskrybenta składającego wnioski drogą elektroniczną realizowane jest w oparciu o informacje zawarte w bazach danych CERTUM i polega na zweryfikowaniu podpisu elektronicznego złożonego pod przesłanym wnioskiem oraz potwierdzeniu autentyczności związanego z podpisem certyfikatu (w oparciu o tzw. ścieżkę certyfikacji).

Uwierzytelnienie subskrybenta potwierdzane jest przez inspektora ds. rejestracji lub osobę potwierdzającą tożsamość poprzez podpisanie stosowanego oświadczenia wraz z podaniem swojego numeru PESEL.

3.2. Uwierzytelnienie w przypadku certyfikacji, aktualizacji kluczy lub modyfikacji certyfikatu

W przypadku certyfikacji, aktualizacji kluczy lub modyfikacji certyfikatu, subskrybent zobowiązany jest złożyć odpowiedni wniosek do CERTUM. Wniosek musi być uwierzytelnione, tzn.:

podpisany przez subskrybenta przy użyciu ważnego klucza prywatnego, związanego z nieprzetereminowanym certyfikatem, lub

potwierdzony przez inspektora ds. rejestracji w Głównym Punkcie Rejestracji lub przez operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość.

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie certyfikatu lub zaświadczenia certyfikacyjnego mogą być składane przy udziale punktu systemu rejestracji, telefonicznie, faksem lub pocztą poleconą.

W przypadku realizacji unieważnienia za pośrednictwem poczty, telefonu lub faksu, subskrybent (podmiot przez niego reprezentowany lub inny uprawniony podmiot) przekazuje wniosek o unieważnienie do Głównego Punktu Rejestracji. Inspektor ds. rejestracji dzwoniąc pod wskazany we wniosku telefon weryfikuje dane zawarte we wniosku oraz znajomość sekretu, powiązanego z danym certyfikatem. W przypadku niezgodności danych lub nieznajomości sekretu, certyfikat zostaje zawieszony do momentu wyjaśnienia powstałych niezgodności.

Identyfikacja i uwierzytelnienie subskrybenta (podmiot przez niego reprezentowany lub inny uprawniony podmiot) w punkcie systemu rejestracji przebiega podobnie jak w przypadku rejestracji.

3.4. Rejestracja subskrybenta urzędu znacznika czasu

Rejestracja subskrybenta urzędu znacznika czasu nie jest obowiązkowa. Rejestracja subskrybenta usług urzędu znacznika czasu CERTUM QTSA może być połączona z rejestracją subskrybenta urzędu certyfikacji CERTUM QCA. W momencie zawierania umowy z Unizeto

Technologies S.A. subskrybent (lub podmiot przez niego reprezentowany) może zawrzeć także umowę na świadczenie usług znacznika czasu.

4. Wymagania funkcjonalne

Poniżej przedstawiono sposób realizacji usług certyfikacji. Każdy etap rozpoczyna się od złożenia przez subskrybenta stosownego wniosku w punkcie systemu rejestracji lub urzędzie znacznika czasu. CERTUM podejmuje decyzję, co do dalszej realizacji wniosku, realizując żądaną usługę lub odmawiając jej realizacji.

4.1. Składanie wniosków

Wnioski subskrybenta są składane przy udziale punktu systemu rejestracji. Bezpośrednio do Głównego Punktu Rejestracji mogą być składane jedynie wnioski o unieważnienie lub zawieszenie certyfikatu.

4.1.1. Wniosek o rejestrację i certyfikację

Wniosek o rejestrację i certyfikację składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście, za pośrednictwem notariusza lub innej osoby potwierdzającej tożsamość.

Po zweryfikowaniu tożsamości wnioskodawcy przez, operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość (patrz rozdz. 3.1.2), wniosek przekazywany jest do Głównego Punktu Rejestracji, gdzie inspektor ds. rejestracji przygotowuje **token zgłoszenia certyfikacyjnego** i przesyła go do urzędu certyfikacji.

Formularz wniosku opublikowany jest w repozytorium.

4.1.2. Wniosek o certyfikację, aktualizację kluczy lub modyfikację certyfikatu

Wniosek składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście, za pośrednictwem notariusza lub innej osoby potwierdzającej tożsamość.

Formularz wniosku opublikowany jest w repozytorium.

4.1.3. Wniosek o unieważnienie lub zawieszenie

Wniosek o unieważnienie lub zawieszenie certyfikatu składany jest przez upoważnione do tego osoby (patrz rozdz. 4.7.2) w punkcie systemu rejestracji lub przekazywany do Głównego Punktu Rejestracji faksem, telefonicznie lub pocztą poleconą. Wniosek musi być potwierdzony przez inspektora ds. rejestracji.

Formularz wniosku opublikowany jest w repozytorium.

O unieważnieniu lub zawieszeniu certyfikatu są informowani subskrybenci i sponsorzy, jeśli certyfikat był sponsorowany.

4.1.4. Przetwarzanie wniosków w punkcie systemu rejestracji

Zweryfikowany wniosek wraz z wymaganym kompletem dokumentów przekazywany jest do Głównego Punktu Rejestracji.

Inspektor ds. rejestracji, w przypadku przetwarzania elektronicznego wniosku o aktualizację kluczy nie musi poświadczać potwierdzenia tożsamości wnioskodawcy własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu. Musi jednak przechowywać wynik weryfikacji podpisów w postaci zarchiwizowanej, zalecanej przez ETSI w dokumencie ETSI TS 101 733 - Electronic Signature Format.

4.2. Wydanie certyfikatu lub zaświadczenia certyfikacyjnego

Urząd certyfikacji, po otrzymaniu tokena zgłoszenia certyfikacyjnego oraz jego pomyślnym przetworzeniu wydaje certyfikat lub zaświadczenie certyfikacyjne. Data wydania certyfikatu lub zaświadczenia certyfikacyjnego jest odnotowywana w bazie danych urzędu certyfikacji.

O wydaniu certyfikatu informowany jest subskrybent oraz sponsor subskrybenta.

Każdy wydany certyfikat po uprzednim uzyskaniu zgody subskrybenta, publikowany jest w repozytorium CERTUM. Opublikowanie certyfikatu jest równoważne zawiadomieniu innych stron ufających, że urząd certyfikacji wydał certyfikat subskrybentowi.

4.2.1. Okres oczekiwania na wydanie certyfikatu

CERTUM dokłada wszelkich starań, aby w jak najkrótszym czasie od momentu otrzymania wniosku o rejestrację i certyfikację, aktualizację kluczy lub modyfikację certyfikatu przeprowadzić jego weryfikację oraz wydać certyfikat. Jeśli nie wystąpią przyczyny niezależne od CERTUM, to czas ten nie może przekroczyć 7 dni od momentu podpisania umowy pomiędzy Unizeto Technologies S.A. a subskrybentem.

4.2.2. Odmowa wydania certyfikatu

CERTUM może odmówić wydania certyfikatu w następujących przypadkach

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

uzasadnionego podejrzenia, że subskrybent sfałszował lub podał nieprawdziwe dane,

z innych ważnych nie wymienionych powyżej przyczyn, po uprzednim uzgodnieniu odmowy z **inspektorem bezpieczeństwa**.

Informacja o odmowie wydania certyfikatu przesyłana jest wnioskodawcy w postaci odpowiedniej decyzji z uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do CERTUM.

4.3. Akceptacja certyfikatu

Po otrzymaniu certyfikatu oraz identyfikacyjnej karty elektronicznej subskrybent zobowiązany jest do sprawdzenia jego zawartości, w tym w szczególności poprawności zawartych w nim danych oraz komplementarności klucza publicznego z kluczem prywatnym. Jeśli certyfikat zawiera jakiekolwiek wady, to certyfikat powinien być natychmiast unieważniony.

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

odręcznego podpisania oświadczenia o akceptacji przez subskrybenta certyfikatu i przesłanie go do CERTUM,

braku w tym okresie pisemnej odmowy akceptacji certyfikatu.

Wydany certyfikat jest publikowany w repozytorium CERTUM i publicznie dostępny po jego zaakceptowaniu przez subskrybenta.

4.4. Recertyfikacja

Recertyfikacja oznacza zastąpienie używanego (**aktualnie ważnego**) certyfikatu lub zaświadczenia certyfikacyjnego nowym certyfikatem lub zaświadczeniem bez zmiany klucza publicznego lub jakiejkolwiek innej informacji (poza nowym okresem ważności, numerem seryjnym i podpisem urzędu certyfikacji) zawartej w zastępowanym certyfikacie lub zaświadczeniu certyfikacyjnym.

Recertyfikacja nie jest usługą udostępnianą subskrybentom. Procedurze recertyfikacji mogą podlegać jedynie zaświadczenia urzędu certyfikacji **CERTUM QCA i QTSA**. O zajściu tego zdarzenia informowani są wszyscy subskrybenci i klienci urzędu certyfikacji.

CERTUM świadczy usługę recertyfikacji tej samej pary kluczy kryptograficznych tylko na własne potrzeby. Zaświadczenie certyfikacyjne, które było przedmiotem recertyfikacji nie jest unieważniane i umieszczane na liście CRL.

4.5. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy ma miejsce zawsze wtedy, gdy zarejestrowany subskrybent zażąda wystawienia nowego certyfikatu. Certyfikację i aktualizację kluczy należy interpretować następująco

certyfikacja kluczy nie jest związana z żadnym innym ważnym certyfikatem (służy uzyskaniu nowego certyfikatu) - subskrybent jednakże powinien być zarejestrowany w CERTUM, tzn. posiadać co najmniej jeden certyfikat – nawet jeśli ma on status unieważniony lub przeterminowany,

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

Certyfikacja lub aktualizacja kluczy odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem odpowiedniego wniosku, weryfikowanego przez inspektora ds. rejestracji lub potwierdzony przez inną uprawnioną osobę potwierdzającą tożsamość.

4.6. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza zastąpienie używanego (**aktualnie ważnego**) certyfikatu nowym certyfikatem, w którym - w stosunku do zastępowanego certyfikatu - zmianie mogą ulec zawarte w nim 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,

nazwa stanowiska pracy lub jednostki organizacyjnej,

adres poczty elektronicznej, jeśli jest umieszczony w certyfikacie,

uprawnienia lub pełnione role,

rodzaj zobowiązań lub limit transakcji,

inne zmiany zawartości rozszerzeń certyfikatu.

Wniosek o modyfikację certyfikatu musi być potwierdzony przez punkt systemu rejestracji. Wymaga to kontaktu subskrybenta z operatorem punkt systemu rejestracji, notariuszem lub inną osobą potwierdzającą tożsamość i poddanie się procedurze identyfikacji i uwierzytelnienia

4.7. Unieważnienie i zawieszenie certyfikatu

Kwalifikowany podmiot świadczący usługi certyfikacyjne wydający kwalifikowane certyfikaty CERTUM zapewnia możliwość zgłoszenia wniosku o unieważnienie lub zawieszenie certyfikatu przez całą dobę.

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

Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia). **Odwieszenie to musi jednak nastąpić nie później niż 7 dni od daty zawieszenia.**

4.7.1. Okoliczności unieważnienia certyfikatu

Unieważnienie certyfikatu jest wykonywane w przypadku utraty (lub zaistnienia podejrzenia takiej utraty) kontroli nad kluczem prywatnym, będącym w posiadaniu subskrybenta certyfikatu, rażącego naruszania przez subskrybenta zasad Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego lub na każde żądanie subskrybenta, sponsora lub innej upoważnionej osoby

Wniosek o unieważnienie może być składany przy udziale punktu systemu rejestracji, telefonicznie, faksem lub pocztą poleconą.

4.7.2. Kto może żądać unieważnienia certyfikatu

CERTUM przestrzega ogólnej zasady, iż unieważnienia certyfikatu może żądać jedynie osoba występująca w certyfikacie, jego właściciel lub podmiot przez niego reprezentowany. Możliwe są jednak sytuacje, kiedy z wnioskiem o unieważnienie mogą wystąpić inne zainteresowane strony. Lista takich stron oraz sytuacje, w których może to nastąpić przedstawione są Kodeksie Postępowania Certyfikacyjnego.

4.7.3. Procedura unieważniania certyfikatu

Po pozytywnej weryfikacji przez urząd certyfikacji żądania unieważnienia, certyfikat jest **unieważniany**. W przypadku, gdy istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, jednakże podmiot świadczący usługi certyfikacyjne nie jest w stanie w ciągu 1 godziny od momentu otrzymania żądania wyjaśnić wszystkich wątpliwości dotyczących unieważnienia, certyfikat jest **zawieszany**.

Informacja o unieważnionym lub zawieszonym certyfikacie umieszczana jest na liście **CRL**, wydawanej przez urząd certyfikacji

Urząd certyfikacji przekazuje wnioskodawcy, subskrybentowi i jego sponsorowi potwierdzenie unieważnienia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy.

4.7.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

CERTUM gwarantuje, że maksymalne okresy zwłoki w przetwarzaniu wniosków o unieważnienie certyfikatów wynoszą 1 godzinę.

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

4.7.5. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu wykonywane jest w przypadku, gdy dane w certyfikacie budzą uzasadnione podejrzenia, wniosek o unieważnienie nie został potwierdzony w wymaganym czasie, podejrzenie, że osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych lub innych okolicznościach wymagających wyjaśnień ze strony subskrybenta, jego sponsora lub wnioskodawcy.

Zaleca się, aby wszystkie wnioski o zawieszenie (w formie elektronicznej oraz papierowej) zgłaszane były za pośrednictwem punktów rejestracji.

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

4.7.6. Kto może żądać zawieszenia certyfikatu

O zawieszenie certyfikatu mogą wnioskować te same strony, co w przypadku wniosku o unieważnienie certyfikatu. Z wnioskiem o unieważnienie nie może jednakże występować subskrybent zawieszanego certyfikatu.

4.7.7. Procedura zawieszenia i odwieszania certyfikatu

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

Odwieszenie certyfikatu odbywa się tylko i wyłącznie z inicjatywy subskrybenta, po uprzednim uwierzytelnionym potwierdzeniu wniosku o odwieszenie certyfikatu. Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, urząd certyfikacji usuwa certyfikat z listy CRL.

Jeśli przyczyny zawieszenia potwierdzą się lub certyfikat pozostaje w stanie zawieszenia dłużej niż 7 dni, wówczas certyfikat jest unieważniany, bez możliwości anulowania tej operacji.

Jeśli w trakcie trwania zawieszenia certyfikatu następuje jego unieważnienie, to data unieważnienia certyfikatu jest datą początku zawieszenia (tj. nie może być datą końca zawieszenia).

Urząd certyfikacji przekazuje wnioskodawcy, subskrybentowi i jego sponsorowi potwierdzenie zawieszenia i odwieszenia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy.

4.7.8. Gwarantowany czas zawieszenia certyfikatu

Gwarantowane przez urząd certyfikacji czas na rozpatrzenie wniosków o zawieszenie certyfikatu, jak również dostępność statusu certyfikatu po jego zawieszeniu jest taki sam jak w przypadku unieważnienia certyfikatu (patrz rozdz. 4.7.4).

4.7.9. Częstotliwość publikowania list CRL

Urząd certyfikacji **CERTUM QCA** tworzy i publikuje listę certyfikatów unieważnionych (CRL).

Wszystkie listy CRL uaktualniane są nie rzadziej, niż co 24 godziny i publikowane automatycznie w repozytorium. W przypadku unieważnienia certyfikatu nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie (patrz rozdz. 4.7.4).

4.7.10. Sprawdzanie list 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.

4.8. Usługa znakowania czasem

Podstawowym celem usługi znakowania czasem, świadczonej przez urząd znacznika czasu **CERTUM QTSA** jest kryptograficzne związanie z dowolnymi danymi, mającymi postać dokumentów, wiadomości, podpisu elektronicznego, itd. wiarygodnych znaczników czasu. Wiązanie znacznika czasu z danymi (token znacznika czasu) umożliwia udowodnienie, że dane zostały utworzone przed określonym momentem czasu.

Uzyskanie znacznika czasu przebiega następująco:

wnioskodawca wysyła żądanie, zawierające wartość skrótu (powiązana z dokumentem, wiadomością, itd.), identyfikator funkcji skrótu oraz identyfikator sesji (*ang. nonce*),

urząd znacznika czasu weryfikuje poprawność formatu wniosku oraz jego kompletność,

urząd znacznika czasu tworzy znacznik,

urząd znacznika czasu odsyła token znacznika czasu podmiotowi żądającemu,

podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena znacznika czasu, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

4.9. Rejestrowanie zdarzeń

W celu nadzoru nad sprawnym działaniem systemu CERTUM, rozliczania użytkowników oraz personelu z ich działań. Rejestrowane są wszystkie te zdarzenia występujące w systemie, które mają istotny wpływ na bezpieczeństwo funkcjonowania CERTUM.

4.9.1. Typy rejestrowanych zdarzeń

Rejestry zdarzeń CERTUM przechowują zapisy o wszystkich zdarzeniach generowanych przez komponenty programowe, fizyczne i logiczne, wchodzące w skład systemu. Rejestrowane

są działania związane z pełnieniem roli kwalifikowanego podmiotu świadczącego usługi certyfikacyjne. Opis rejestrowanych zdarzeń znajduje się w Kodeksie Postępowania Certyfikacyjnego i wewnętrznych dokumentach CERTUM.

4.9.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń

W celu rozpoznania ewentualnych nieuprawnionych działań administrator systemu i inspektorzy ds. audytu powinni analizować rejestry zdarzeń przynajmniej raz w każdym dniu roboczym. Dodatkowo inspektor bezpieczeństwa dokonuje raz w miesiącu przeglądu i oceny poprawności, kompletności zapisów zdarzeń w rejestrze bezpieczeństwa oraz stopnia przestrzegania procedur bezpieczeństwa.

4.9.3. Okres przechowywania zapisów rejestrowanych zdarzeń

Zapisy rejestrowanych zdarzeń przechowywane są w plikach na dysku systemowym przez okres przynajmniej 6 miesięcy. W tym okresie czasu dostępne są w trybie *on-line* na każde żądanie upoważnionej do tego osoby lub upoważnionego procesu. Po upływie tego okresu rejestry zdarzeń są archiwizowane i udostępniane tylko w trybie *off-line*.

Zarchiwizowane zdarzenia przechowywane są przez okres min. 20 lat.

4.9.4. Ochrona zapisów rejestrowanych zdarzeń

Rejestr zdarzeń może być przeglądany jedynie przez upoważniony personel lub audytorów. Zapisy rejestru zdarzeń nie mogą być modyfikowane.

Archiwa rejestru zdarzeń są szyfrowane, podpisywane i znakowane czasem. Klucz przy pomocy, którego szyfrowane jest archiwum znajduje się pod kontrolą inspektora bezpieczeństwa.

4.9.5. Tworzenie kopii zapisów rejestrowanych zdarzeń

CERTUM wymaga, aby zapisy zdarzeń były kopiowane zgodnie z harmonogramem tworzenia kopii bezpieczeństwa systemu. Kopie te przechowywane są w ośrodku głównym i zapasowym CERTUM. Kopie oznaczone są znacznikiem czasu.

4.10. 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 punkty systemu rejestracji, a także pełna korespondencja prowadzona pomiędzy CERTUM oraz z subskrybentami.

Archiwum zawiera certyfikaty wydane maksymalnie do 25 lat wstecz. Archiwizowane są także wszystkie listy CRL wydane przez CERTUM.

Archiwum zawiera również wszelkie dokumenty papierowe, związane ze świadczeniem usług certyfikacyjnych. Okres przechowywania dokumentów papierowych wynosi minimum 20 lat.

Archiwalne kopie danych elektronicznych przechowywane są w siedzibie ośrodku głównym oraz w ośrodku zapasowym CERTUM

Zaleca się, aby archiwizowane dane elektroniczne oznaczane były znacznikiem czasu, tworzonym przez urząd znacznika czasu **CERTUM QTSA.**

4.11. Zmiana klucza

Procedura zmiany klucza odnosi się do kluczy urzędu certyfikacji **CERTUM QCA** oraz urzędu znacznika czasu **CERTUM QTSA** i dotyczy procesu aktualizacji kluczy, które zastąpią klucze używane dotychczas odpowiednio do podpisywania certyfikatów i list CRL oraz do podpisywania znaczników czasu.

Procedura aktualizacji kluczy urzędu certyfikacji **CERTUM QCA** lub urzędu znacznika czasu **CERTUM QTSA** polega na wystąpieniu do krajowego urzędu certyfikacji z wnioskiem o wydanie nowego zaświadczenia certyfikacyjnego. Jeśli wniosek dotyczył kluczy urzędu CERTUM QCA, to po otrzymaniu zaświadczenia urząd ten wydaje krajowemu urzędowi certyfikacji wzajemne zaświadczenia certyfikacyjne.

Każda zmiana kluczy urzędu CERTUM anonsowana jest odpowiednio wcześniej za pośrednictwem repozytorium CERTUM.

4.12. Naruszenie ochrony klucza i uruchamianie po awariach oraz klęskach żywiołowych

CERTUM posiada wdrożoną polityka bezpieczeństwa, zapewniającą bezpieczeństwo i ciągłość świadczenia krytycznych usług urzędu certyfikacji w przypadku fizycznego uszkodzenia systemu komputerowego, awarii oprogramowania oraz sieci telekomunikacyjnej i zasilania.

CERTUM zapewnia możliwość unieważnienia certyfikatów oraz tworzenia i publikowania list CRL również w przypadku awarii, w szczególności poprzez użycie zapasowego ośrodka przetwarzania danych, z zachowaniem obowiązku określonego w rozdz. 4.7.4 i 4.7.9.

W przypadku kompromitacji lub podejrzenia kompromitacji któregokolwiek z kluczy prywatnych urzędu certyfikacji CERTUM informowany jest krajowy urząd certyfikacji, zaś do wszystkich klientów CERTUM wysyłana jest w postaci elektronicznej informacja o zaistniałym fakcie. Unieważniany jest certyfikat związany z ujawnionym kluczem prywatnym oraz wszystkie aktualnie ważne certyfikaty, podpisane przy pomocy ujawnionego klucza prywatnego. Po uzyskaniu nowego zaświadczenia certyfikacyjnego, CERTUM tworzy nowe certyfikaty subskrybentów, które przesyła bez obciążania subskrybentów kosztami za powyższą operację.

4.13. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

CERTUM zobowiązany jest **na co najmniej 90 dni przed planowanym zakończeniem swojej działalności** do pisemnego poinformowania o tym fakcie wszystkich subskrybentów, posiadających ważny certyfikat, oraz krajowego urzędu certyfikacji.

Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważniony muszą być także certyfikaty urzędu certyfikacji i urzędu znacznika czasu. Klucze prywatne urzędu certyfikacji **CERTUM QCA** i urzędu znacznika czasu **CERTUM QTSA** muszą być zniszczone.

CERTUM zwraca subskrybentowi (lub jego sponsorowi) koszty wydanego certyfikatu, proporcjonalnie do pozostałego okresu ważności wydanego certyfikatu

Archiwum kończącego działalność urzędu certyfikacji zawierające dokumenty i dane przekazywane jest ministrowi właściwemu ds. gospodarki albo wskazanemu przez niego podmiotowi.

Likwidowany urząd certyfikacji może zawrzeć umowę z innym kwalifikowanym podmiotem świadczącym usługi certyfikacyjne, dotyczącą ponownego wydania pozostających jeszcze w obiegu aktualnie ważnych certyfikatów subskrybentów likwidowanego urzędu certyfikacji (certyfikaty mogą być potwierdzeniem aktualnie używanych przez subskrybentów kluczy publicznych). Umowa ta powinna dotyczyć także przekazania obowiązków dalszego zarządzania dziennikami zdarzeń i archiwami.

5. Zabezpieczenia fizyczne, organizacyjne oraz personelu

W rozdziale opisano wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w CERTUM m.in. podczas generowania kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów, audytu oraz wykonywania kopii zapasowych. Opis rozszerzony tych wymagań zawiera Kodeks Postępowania Certyfikacyjnego.

5.1. Zabezpieczenia fizyczne

5.1.1. Bezpieczeństwo fizyczne CERTUM

Sieciowy system komputerowy, terminale operatorskie oraz zasoby informacyjne CERTUM znajdują się w wydzielonych pomieszczeniach, fizycznie chronionych przed nieupoważnionym dostępem, zniszczeniem oraz zakłóceniami ich pracy. Pomieszczenia te są nadzorowane.

CERTUM mieści się w budynku Unizeto Technologies S.A., znajdującym się w Szczecinie przy ul. Królowej Korony Polskiej 21.

Fizyczny dostęp do budynku oraz pomieszczeń CERTUM jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. Ochrona portierska i ochrona na zewnątrz budynku funkcjonuje 24 godziny na dobę. Funkcjonują także systemy ochrony przeciwpożarowej, przeciwzalaniowej, przeciwwłamaniowej oraz systemy zasilania awaryjnego, zapobiegające skutkom czasowego i długotrwałego zaniku zasilania.

Kopie haseł, numerów PIN oraz kluczy kryptograficznych przechowywane są skrytkach poza miejscem lokalizacji CERTUM. Poza siedzibą CERTUM przechowywane są także archiwa, bieżące kopie informacji przetworzonej przez system komputerowy, a także pełna wersja instalacyjna oprogramowania CERTUM.

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo CERTUM po upływie okresu przechowywania niszczone są w specjalnych urządzeniach niszczących.

5.1.2. Bezpieczeństwo punktów systemu rejestracji

Komputery rejestrujące wnioski subskrybentów oraz wydające im potwierdzenia, jak również komputery punktów potwierdzania tożsamości administrowane przez Unizeto Technologies S.A. znajdują się w specjalnie przeznaczonym do tego celu pomieszczeniu. Dostęp do nich jest fizycznie chroniony przed nieupoważnionymi osobami. Do ich obsługi dopuszczone są jedynie upoważnione osoby. Komputery zlokalizowane w notarialnych punktach potwierdzania tożsamości chronione są zgodnie z wymaganiami stosowanymi dla kancelarii notarialnych. Komputery zlokalizowane w pozostałych punktach potwierdzania tożsamości podlegają ochronie, której zakres opisany jest w stosownych umowach pomiędzy CERTUM a administratorem danego punktu.

5.2. Zabezpieczenia organizacyjne

CERTUM zapewnia realizację zabezpieczeń organizacyjnych poprzez określenie, między innymi:

zaufanych ról, które mogą być pełnione przez jedną lub więcej osób – zarówno w urzędzie certyfikacji jak i w punktach systemu rejestracji,

łączenia określonych ról,

zakresu obowiązków i odpowiedzialności osób pełniących określone role,

liczby osób koniecznych do realizacji poszczególnych zadań,

identyfikacji oraz uwierzytelnianiu personelu.

Rozszerzony opis zabezpieczeń organizacyjnych zawiera Kodeks Postępowania Certyfikacyjnego oraz wewnętrzne dokumenty CERTUM.

5.3. Kontrola personelu

CERTUM gwarantuje, że osoby wykonujące swoje obowiązki wynikające z funkcji realizowanych przez urząd certyfikacji:

posiadają minimum wykształcenie średnie,

posiadają polskie obywatelstwo,

zawarły umowę o pracę lub inną umowę cywilno-prawną precyzującą rolę, którą mają pełnić i określającą wynikające z niej prawa i obowiązki,

przeszły niezbędne przeszkolenie z zakresu obowiązków, które będą wykonywały,

zostały przeszkolone w zakresie ochrony danych osobowych,

podpisały klauzule o nieujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa urzędu certyfikacji lub poufności danych subskrybenta,

nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem certyfikacji a działającymi w jego imieniu punktami rejestracji.

5.3.1. Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w CERTUM lub działających w jego imieniu punktach systemu rejestracji musi przejść cykl szkoleń dotyczących problemów ochrony informacji, infrastruktury klucza publicznego, zasad Polityki Certyfikacji i Kodeksu Postępowania Certyfikacyjnego, znajomości swoich obowiązków, procedur awaryjnych oraz niezbędnego oprogramowania.

5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione powyżej muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu CERTUM lub punktów systemu rejestracji, bądź zostały opublikowane nowe wersje Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego.

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych CERTUM oraz użytkowników, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

6.1. Generowanie 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 CERTUM**,** od których zależy bezpieczeństwo funkcjonowania całego systemu certyfikowania kluczy publicznych.

Klucze, będące własnością urzędu certyfikacji, mogą być używane do:

elektronicznego poświadczania certyfikatów i list CRL,

elektronicznego poświadczania wiadomości, wymienianych z klientami,

elektronicznego poświadczania zaświadczeń certyfikacyjnych,

uzgadniania kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem a otoczeniem.

Do realizacji podpisu elektronicznego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1, zaś do uzgadniania kluczy – algorytm Diffiego-Hellmana lub RSA.

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędu certyfikacji, używane do podpisywania certyfikatów i list CRL oraz wystawiania tokenów znacznika czasu generowane są w siedzibie CERTUM w obecności wybranej, przeszkolonej grupy zaufanych osób. Klucze urzędu certyfikacji i urzędu znacznika czasu generowane są zgodnie z wewnętrznymi procedurami CERTUM, przy użyciu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu generowania kluczy, spełniającego wymagania klasy FIPS 140-1 level 3 lub wyżej.

Operatorzy punktów systemu rejestracji posiadają jedynie klucze do podpisywania (potwierdzania) wniosków subskrybentów oraz wiadomości wysyłanych do urzędu certyfikacji. Klucze te generowane są przy użyciu oprogramowania dostarczonego przez urząd certyfikacji oraz sprzężonego z nim sprzętowego modułu kryptograficznego, spełniającego wymagania klasy FIPS 140 Level 2.

Klucze subskrybentów generowane są wyłącznie w urzędzie certyfikacji.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

Klucze subskrybentów generowane są przez urząd certyfikacji na kryptograficznej karcie elektronicznej i mogą być przekazywane subskrybentowi osobiście lub pocztą kurierską; dane do uaktywnienia karty (m.in. PUK/PIN) podane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji.

6.1.3. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu wydającego certyfikaty rozpowszechniane są tylko w formie zaświadczeń certyfikacyjnych zgodnych z zaleceniem ITU-T X.509 v.3, wydanych przez **krajowy urząd certyfikacji**.

Urząd certyfikacji CERTUM rozpowszechnia swoje zaświadczenia certyfikacyjne dwoma sposobami:

umieszczają w ogólnie dostępnym repozytorium CERTUM w Internecie pod adresem: http://www.certum.pl/repozytorium.

za pomocą dedykowanego oprogramowania, które umożliwia korzystanie z usług CERTUM.

6.1.4. Długości kluczy

Długości kluczy używanych przez CERTUM, operatorów punktów systemu rejestracji oraz użytkowników końcowych (subskrybentów) podano w Kodeksie Postępowania Certyfikacyjnego.

6.2. Ochrona klucza prywatnego

Każdy subskrybent, a także operatorzy urzędów certyfikacji i punktów rejestracji przechowują, użytkują i niszczą swój klucz prywatny, wykorzystując w tym celu zaufany system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu.

Klucze infrastruktury wykorzystywane do zapewnienia poufności przekazu podpisywanych danych przez osobę składającą bezpieczny podpis elektroniczny lub do zapewnienia poufności przekazu danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego przez kwalifikowany podmiot świadczący usługi certyfikacyjne, przechowuje się w indywidualnych modułach kluczowych lub komponentach technicznych.

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urząd certyfikacji, urząd znacznika czas, punkty rejestracji i subskrybentów są zgodne z wymaganiami normy FIPS 140 (level 2 i wyżej) lub ITSEC (E3 i wyżej).

6.2.2. Podział klucza prywatnego na części

Ochronie za pomocą podziału klucza na części podlegają klucze urzędu certyfikacji **CERTUM QCA** i urzędu znacznika czasu **CERTUM QTSA.** Klucze 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 Kodeksie Postępowania Certyfikacyjnego.

Sekrety współdzielone zapisywane są na kartach elektronicznych, chronione numerem PIN i w uwierzytelniony sposób przekazywane posiadaczom sekretu współdzielonego.

6.2.3. Deponowanie klucza prywatnego

Klucze prywatne urzędów certyfikacji, ani też innych subskrybentów, dla potrzeb których CERTUM generuje klucze lub które są dostępne, nie podlegają operacji deponowania.

6.2.4. Kopie zapasowe klucza prywatnego

Urząd certyfikacji **CERTUM QCA** i urząd znacznika czasu **CERTUM QTSA** tworzą kopie swoich kluczy prywatnych. Kopie te wykorzystywane są w przypadku potrzeby realizacji normalnej lub awaryjnej (np. po wystąpieniu klęski żywiołowej) procedury odzyskiwania kluczy.

Sekrety współdzielone oraz 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 CERTUM nie przechowują kopii kluczy prywatnych operatorów punktów rejestracji i subskrybentów.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędu certyfikacji stosowane do realizacji elektronicznych poświadczeń nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywania przy ich użyciu operacji podpisywania lub upływie okresu ważności komplementarnego z nimi zaświadczenia certyfikacyjnego lub unieważnieniu.

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

Operacja wprowadzania kluczy prywatnych do modułu kryptograficznego jest realizowana w dwóch sytuacjach:

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,

konieczności przeniesienia 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.

6.2.7. Metody aktywacji klucza prywatnego

Wszystkie klucze prywatne urzędu certyfikacji **CERTUM QCA** lub urzędu znacznika czasu **CERTUM QTSA** 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 CERTUM.

Klucze prywatne operatorów punktów systemu rejestracji oraz subskrybentów 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 uaktywniony przed wykonaniem kolejnej operacji.

Inne klucze prywatne, np. używane do uwierzytelnienia aplikacji punktu rejestracji lub utworzenia szyfrowanego połączenia sieciowego uaktywniane są automatycznie na okres trwania sesji, natychmiast po uwierzytelnieniu operatora systemu. Zakończenie sesji dezaktywuje wszystkie uaktywnione wcześniej klucze prywatne.

6.2.8. Metody dezaktywacji klucza prywatnego

W przypadku CERTUM dezaktywowanie kluczy jest wykonywane przez inspektora bezpieczeństwa i tylko w przypadku, gdy minął okres ważności klucza, klucz został unieważniony lub zachodzi potrzeba czasowego wstrzymania działania serwera podpisującego. Dezaktywowanie klucza polega na wyczyszczeniu pamięci modułu kryptograficznego z załadowanych kluczy. Każda dezaktywacja klucza prywatnego jest odnotowywana w rejestrze zdarzeń.

W przypadku kluczy subskrybenta lub operatora punktu systemu rejestracji dezaktywowanie kluczy podpisujących następuje natychmiast po zrealizowaniu podpisu elektronicznego..

6.2.9. Metody niszczenia klucza prywatnego

Niszczenie klucza prywatnego urzędu certyfikacji lub urzędu znacznika czasu oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników, na których są przechowywane kopie lub archiwizowane sekrety współdzielone lub ich bezpieczne wymazanie z nośnika (z karty elektronicznej, sprzętowego modułu kryptograficznego, itp.).

Niszczenie kluczy subskrybentów lub operatorów punktu systemu rejestracji polega na ich bezpiecznym wymazaniu z karty elektronicznej, zniszczeniu karty elektronicznej lub przynajmniej przejęcie nad nim kontroli w przypadku, gdy mechanizmy karty nie zezwalają na definitywne usunięcie z niej informacji o kluczu prywatnym.

6.3. Inne aspekty zarządzania kluczami

6.3.1. Archiwizacja kluczy publicznych

Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów i poświadczeń elektronicznych już po usunięciu certyfikatu z repozytorium. Jest to szczególnie ważne w przypadku świadczenia usług niezaprzeczalności.

Archiwizowanie kluczy publicznych polega na archiwizowaniu certyfikatów, w których te klucze występują.

W systemie CERTUM archiwizowane są tylko klucze używane do weryfikacji podpisów lub poświadczeń elektronicznych.

Klucze publiczne oraz listy CRL przechowywane są w archiwum kluczy publicznych przez okres 25 lat.

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole **validity** każdego certyfikatu lub zaświadczenia certyfikacyjnego. Przyjmuje się, że jest to także okres ważności klucza prywatnego, chociaż może on być krótszy niż okres ważności certyfikatu lub zaświadczenia certyfikacyjnego

(wynika to z możliwości zaprzestania używania klucza w dowolnym momencie lub wymagań stawianych urzędom certyfikacji lub znacznika czasu).

Standardowe maksymalne okresy ważności kluczy prywatnych oraz związanych z nimi zaświadczeń certyfikacyjnych urzędu certyfikacji i urzędu znacznika czasu podane są w Tab.3, zaś certyfikatów subskrybentów w Tab.4.

Nie dopuszcza się, aby data początkowa ważności certyfikatu lub zaświadczenia certyfikacyjnego ulokowana była w przeszłości lub przyszłości.

Tab.3 Maksymalne okresy ważności zaświadczeń certyfikacyjnych i certyfikatów klucza infrastruktury urzędów

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza		
		RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokenów	Klucz RSA infrastruktury
CERTUM QCA	zaświadczenie lub certyfikat klucza infrastruktury	5 lat	–	3 lata
	klucz prywatny	3 lata	–	3 lata
CERTUM QTSA	zaświadczenie lub certyfikat klucza infrastruktury	–	5 lat	–
	klucz prywatny	–	5 lat	–

Tab.4 Maksymalne okresy ważności kwalifikowanych certyfikatów

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza
		RSA do składania bezpiecznych podpisów
Osoby fizyczne	Kwalifikowany certyfikat	2 lata
	Klucz prywatny	2 lata

6.4. Zabezpieczenia systemu komputerowego

Zadania punktów rejestracji, urzędów certyfikacji i urzędów znakowania czasem funkcjonujących w ramach kwalifikowanego systemu CERTUM realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzącego system, który spełnia wymagania określone w *Information Technology Security Evaluation Criteria* (ITSEC) przynajmniej na poziomie E3.

6.5. Zabezpieczenia sieci komputerowej

Serwery oraz zaufane stacje robocze systemu komputerowego CERTUM 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.

6.6. Znaczniki czasu jako element bezpieczeństwa

W przypadku wiadomości przesyłanych pomiędzy urzędem certyfikacji, punktem rejestracji i subskrybentem, innych niż tworzone w ramach protokołu CMP lub CRS zaleca się stosować znaczniki czasu.

Znaczniki czasu tworzone w ramach CERTUM są zgodne z zaleceniem RFC 3161.

7. Profile certyfikatów i zaświadczeń certyfikacyjnych, listy CRL, tokenów znacznika czasu

Profile kwalifikowanych certyfikatów, certyfikatów kluczy infrastruktury, zaświadczeń certyfikacyjnych oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3 oraz profilami zawartymi w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*. Z kolei profile tokena znacznika z RFC 3161 (patrz także *ETSI Time stamping profile, TS 101 861 v1.2.1*).

7.1. Struktura certyfikatów

Certyfikat lub zaświadczenie certyfikacyjne według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu lub zaświadczenia certyfikacyjnego (**tbsCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu lub zaświadczenia certyfikacyjnego (**signatureAlgorithm**), zaś trzecie – poświadczenie elektroniczne, składane na certyfikacie lub zaświadczeniu certyfikacyjnym przez urząd certyfikacji (**signatureValue**).

7.1.1. Treść certyfikatu

Na treść certyfikatu składają się wartości **pól podstawowych** oraz **rozszerzeń** (standardowych, określonych przez normę oraz prywatnych, definiowanych przez organ wydający certyfikaty).

7.1.1.1. Pola podstawowe

CERTUM obsługuje pola podstawowe certyfikatu opisane w Tab. 5:

Tab.5 Profil podstawowych pól kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego

Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	Version 3	
Serial Number (numer seryjny)	Unikalne wartości we wszystkich certyfikatach wydawanych przez kwalifikowany urząd certyfikacji CERTUM.	
Signature Algorithm (algorytm podpisu)	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (wystawca, nazwa DN)	Common Name (CN) =	CERTUM QCA

Nazwa pola	Wartość lub ograniczenie wartości	
	Organization (O) =	Unizeto Technologies S.A.
	Country (C) =	PL
	Serial Number (SN) =	Nr wpisu: 1
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Subject (podmiot, nazwa DN)	Nazwa DN jest zgodna z wymaganiami określonymi w *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.* Struktura nazwy DN zależy od typu podmiotu, któremu wystawiany jest certyfikat.	
Subject Public Key Info (klucz publiczny podmiotu)	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 3280 i może zawierać informacje o kluczach publicznych RSA, DSA lub ECDSA (tzn. o identyfikatorze klucza, długości klucza w bitach oraz wartości klucza publicznego).	
Signature (podpis)	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 3280 i Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002.	

7.1.1.2. Pola rozszerzeń

CERTUM obsługuje pola rozszerzeń opisane w Tab. 6:

Tab.6 Profil rozszerzeń standardowych certyfikatu lub zaświadczenia certyfikacyjnego

Nazwa rozszerzenia	Uwagi	Status rozszerzenia
AuthorityKeyIdentifier (identyfikator klucza wydawcy)	Skrót SHA-1 z wartości klucza publicznego zaświadczenia certyfikacyjnego urzędu	Niekrytyczne
SubjectKeyIdentifier (identyfikator klucza podmiotu)	Identyfikator klucza podmiotu	Niekrytyczne
KeyUsage (użycie klucza)	Dozwolone użycie klucza. W przypadku certyfikatów kwalifikowanych możliwa jedynie wartość **nonRepudiation**	Krytyczne
ExtKeyUsage (rozszerzone użycie klucza)	Sprecyzowanie (ograniczenie) użycia klucza. Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**	Niekrytyczne

Nazwa rozszerzenia	Uwagi	Status rozszerzenia
CertificatePolicies (polityka certyfikacji)	Informacja o polityce certyfikacji, realizowanej przez urząd certyfikacji: iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 1 – dla certyfikatów kwalifikowanych joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32) – dla zaświadczeń certyfikacyjnych iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 10 – dla kluczy infrastruktury	Krytyczne
PolicyMapping (równoważne polityki)	Pole to zawiera jedną lub więcej par OID, które określają równoważność polityki wydawcy z polityką podmiotu	Niekrytyczne
IssuerAlternativeName (alternatywna nazwa urzędu certyfikacji)	Alternatywna nazwa urzędu certyfikacji	Niekrytyczne
SubjectAlternativeName (alternatywna nazwa podmiotu)	Alternatywna nazwa podmiotu, np. adres email	Niekrytyczne
BasicContraints (podstawowe ograniczenia)	Umożliwia określenie czy podmiot jest urzędem certyfikacji (pole **cA**) oraz maksymalną długość ścieżki (pole **pathLength**)	Zaświadczenia: Krytyczne; Certyfikaty: Niekrytyczne;
CRLDistributionPoints (punkty dystrybucji listy CRL)	Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL urzędu (np. http://crl.certum.pl/qca.crl)	Niekrytyczne
SubjectDirectoryAttributes (atrybuty katalogu podmiotu)	Atrybuty podmiotu dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**	Niekrytyczne
AuthorityInfoAccessSyntax	Dostęp do informacji urzędu certyfikacji, wskazuje, w jaki sposób wystawca certyfikatu udostępnia informacje i usługi (np. http://qocsp.certum.pl)	Niekrytyczne
QCStatements (deklaracje wydawcy certyfikatu kwalifikowanego)	Deklaracje wystawcy certyfikatu kwalifikowanego (świadczenie, że certyfikat jest kwalifikowanym certyfikatem, limit transakcji, wskazanie, w czyim imieniu działa podmiot składając podpis)	Niekrytyczne
BiometricSyntax (informacje biometryczne)	Informacje o cechach biometrycznych podmiotu certyfikatu: podpisie odręcznym lub zdjęciu	Niekrytyczne

7.1.2. Typ stosowanego algorytmu poświadczenia elektronicznego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji poświadczenia elektronicznego, składanego przez urząd

certyfikacji na certyfikacie lub zaświadczeniu certyfikacyjnym. W przypadku CERTUM stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

7.1.3. Pole poświadczenia elektronicznego

Wartość pola poświadczenia elektronicznego (**signatureValue**) jest wynikiem zastosowania algorytmu funkcji skrótu do wszystkich pól zaświadczenia certyfikacyjnego, określonych przez pola jego treści (**tbsCertificate**) i następnie zaszyfrowania wyniku przy pomocy klucza prywatnego urzędu certyfikacji (wydawcy).

7.2. Struktura listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z ciągu trzech pól. Pierwsze pole (**tbsCertList**) zawiera informacje o unieważnionych certyfikatach i zaświadczeniach certyfikacyjnych, drugie i trzecie pole (**signatureAlgorithm** oraz **signatureValue**) – odpowiednio informację o typie algorytmu użytego do podpisania listy oraz poświadczenie elektroniczne, składane na liście CRL przez urząd certyfikacji. Znaczenie dwóch ostatnich pól jest dokładnie takie samo jak w przypadku certyfikatu lub zaświadczenia certyfikacyjnego.

Pole informacyjne **tbsCertList** jest sekwencją pól opisanych w Tab. 7:

Tab.7 Profil listy CRL

	Nazwa pola	Krytyczne	Uwagi
Pola podstawowe	Version	n/d	wersja formatu listy CRL (3)
	Signature		Identyfikator algorytmu stosowanego przez urząd certyfikacji do poświadczenia elektronicznego listy **CRL** (**sha1WithRSAEncryption**)
	Issuer		nazwa urzędu wydającego listę CRL (**CERTUM QCA**)
	ThisUpdate		data publikacji listy CRL
	NextUpdate		zapowiedź daty następnej publikacji listy CRL (pole może nie wystąpić)
	RevokedCertificates		lista unieważnionych certyfikatów; składa się z podpól: **userCertificate** - numer seryjny unieważnianego certyfikatu **revocationDate** - data unieważnienia certyfikatu **crlEntryExtensions** - opcjonalnie informacje o unieważnionych certyfikatach
	crlExtensions		opcjonalne, poszerzone informacje o liście CRL (m.in. pola **AuthorityKeyIdentifier** i **cRLNumber**)

	Nazwa pola	Krytyczne	Uwagi
Pola rozszerzeń	ReasonCode	Nie	kod przyczyny unieważnienia; dopuszczalne wartości: **unspecified** – nieokreślona (nieznana); **keyCompromise** – ujawnienie klucza; **cACompromise** – ujawnienie klucza urzędu certyfikacji; **affiliationChanged** – zamiana danych subskrybenta; **superseded** – zastąpienie klucza publicznego certyfikatu lub zaświadczenia certyfikacyjnego; **cessationOfOperation** – zaprzestanie operacji z wykorzystaniem klucza; **certificateHold** – zawieszenie certyfikatu lub zaświadczenia certyfikacyjnego; **removeFromCRL** – wycofanie certyfikatu lub zaświadczenie certyfikacyjnego z listy CRL; **privilegeWithdrawn** – zmiana danych określających rolę właściciela certyfikatu; **aaCompromise –** identycznie jak powyżej, dotyczy jednak certyfikatu atrybutów;
	HoldInstructionCode	Nie	instrukcja postępowania z zawieszonym certyfikatem
	InvalidityDate	Nie	data unieważnienia

Unieważnione certyfikaty i zaświadczenia certyfikacyjne pozostają na listach certyfikatów unieważnionych (wydawanych przez urząd certyfikacji **CERTUM**) przez okres 25 lat, licząc od daty pierwszego umieszczenia certyfikatu lub zaświadczenia certyfikacyjnego na liście.

7.3. Profil tokena znacznika czasu

Token znacznika czasu wystawiony przez urząd znacznika czasu **CERTUM QTSA** zawiera w sobie informację o znaczniku czasu (struktura **TSTInfo**), umieszczoną w strukturze **SignedData**, podpisanej przez urząd znacznika i zagnieżdżonej w strukturze **ContentInfo**.

Rozszerzony opis profilu tokena znaczniku czasu publikowany jest w Kodeksie Postępowania Certyfikacyjnego.

8. Administrowanie Polityką Certyfikacji

Każda z wersji Polityki Certyfikacji obowiązuje (posiada status **aktualny**) do czasu zatwierdzenia i opublikowania nowej wersji (patrz rozdz. 8.3). Nowa wersja opracowywana jest przez Zespół ds. Usług PKI i ze statusem **w ankiecie** przekazana do rozpatrzenia. Po otrzymaniu i uwzględnieniu uwag z ankiety Polityka Certyfikacja przekazywana jest do akceptacji ministra właściwego ds. gospodarki, a następnie przekazana jest do zatwierdzenia przez Zespół ds. Usług PKI i opublikowania. W czasie trwania procedury zatwierdzania nowa wersja dokumentu posiada status – **w zatwierdzeniu,** a po zakończeniu procedury osiąga status – **aktualny**.

Subskrybenci zobowiązani są stosować się jedynie do aktualnie obowiązującej Polityki.

8.1. Procedura wprowadzania zmian

Zmiany w Polityce Certyfikacji mogą być wynikiem zauważonych błędów, uaktualnień Polityki oraz sugestii zainteresowanych stron.

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 nie wymagają wcześniejszego informowania subskrybentów i innych użytkowników systemu, dotyczą zmian wynikających z wprowadzenia korekt edycyjnych lub zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie Polityką. 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 Polityki Certyfikacji. Informacja o wszystkich, rozważanych przez Zespół ds. Rozwoju Usług PKI zmianach w Polityce jest przesyłana wszystkim zainteresowanym stronom w postaci nowej wersji Polityki Certyfikacji o statusie **w ankiecie**. Proponowane zmiany publikowane są na stronie WWW **CERTUM** oraz rozsyłane pocztą elektroniczną.

8.1.2.2. Okres oczekiwania na komentarze

Zainteresowane strony, w ciągu 10 dni roboczych od daty ich ogłoszenia mogą nadsyłać komentarze do zmian proponowanych przez Zespół ds. Usług PKI. Jeśli w wyniku nadesłanych komentarzy Zespół ds. Usług PKI dokonał **istotnych modyfikacji** w proponowanych zmianach, modyfikacje te muszą być ponownie opublikowane i poddane ocenie. W pozostałych przypadkach, nowa wersja Polityki Certyfikacji przyjmuje status **w zatwierdzeniu** i poddana jest procedurze zatwierdzenia

8.1.2.3. Zmiany wymagające nowego identyfikatora

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników Polityki, Zespół ds. Rozwoju Usług PKI może przydzielić zmodyfikowanemu dokumentowi Polityki nowy identyfikator (OBJECT IDENTIFIER). Zmianie może ulec także identyfikator polityki certyfikacji, według której są świadczone usługi certyfikacyjne.

8.2. Publikacja

Kopia Polityki Certyfikacji dostępna jest w formie elektronicznej:

na stronie WWW pod adresem: http://www.certum.pl/repozytorium

via e-mail o adresie: info@certum.pl

W repozytorium oraz za pośrednictwem strony WWW dostępne są zawsze trzy wersje (jeśli jest to możliwe) Polityki Certyfikacji: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia.

8.3. Procedura zatwierdzania Polityki Certyfikacji

Jeśli w ciągu 10 dni roboczych od daty opublikowania zmian w Polityce Certyfikacji, wniesionych na podstawie uwag uzyskanych na etapie jej ankietowania (w sposób przedstawiony w rozdz. 8.2), Zespół ds. Rozwoju Usług PKI nie otrzyma istotnych zastrzeżeń odnośnie ich merytorycznej zawartości, nowa wersja dokumentu o statusie **w zatwierdzeniu** staje się obowiązującą wykładnią polityki certyfikacji, respektowaną przez wszystkich subskrybentów **CERTUM** i przyjmuje status **aktualny**.

Historia dokumentu

Historia zmian dokumentu		
1.0	20 sierpnia 2002 r.	Pełna wersja dokumentu. Dokument zatwierdzony.
1.1	23 października 2002 r.	Poprawki edytorskie, uwzględnienie uwag Ministerstwa Gospodarki, dodanie urzędu weryfikacji statusu certyfikatu. Dokument zatwierdzony.
2.0	01 lutego 2005 r.	Skrócenie Polityki i aktualizacja informacji, zgodnie z zaleceniami uwag audytorskich.
2.1	02 maja 2005 r.	Zmiana formy prawnej spółki, przekształcenie Unizeto Sp. z o.o. w Unizeto Technologies S.A.
2.2	20 lipiec 2005 r.	Zmiana nazwy urzędu certyfikacji z "Centrum Certyfikacji Unizeto CERTUM" na "CERTUM - Powszechne Centrum Certfikacji".
2.3	01 stycznia 2006 r.	Dodanie informacji po generacji nowych zaświadczeń certyfikacyjnych. Podkreślenie faktu kopiowania dokumentów subskrybentów, wymaganych w realizacji procesu certyfikacji. Zmiana numeru faksu

Dodatek 1: Skróty i oznaczenia

CA urząd certyfikacji (*ang. certification authority*)

CMP protokół zarządzania certyfikatami (*ang. Certificate Management Protocol*)

CRL lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów

DN nazwa wyróżniona (*ang. Distinguished Name*)

GPR Główny Punkt Rejestracji

PKI Infrastruktura Klucza Publicznego (*ang. Public Key Infrastructure*)

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

TSA urząd znacznika czasu (*ang. Time Stamping Authority*)

Dodatek 2: Słownik pojęć

Aktualizacja certyfikatu (*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.

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, Kodeksem Postępowania Certyfikacyjnego i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Certyfikat (certyfikat klucza publicznego) – elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji podpisu elektronicznego są przyporządkowane do osoby składającej podpis elektroniczny i które umożliwiają identyfikację tej osoby.

Certyfikat kluczy infrastruktury – klucz publiczny użytkownika z należącej do niego pary asymetrycznych kluczy infrastruktury, który wraz z innymi danymi opatrzony jest przez urząd certyfikacji poświadczeniem certyfikacyjnym w taki sposób, że poświadczenie to w sposób wiarygodny i obliczeniowo niemożliwy do sfałszowania związuje ten klucz z tożsamością użytkownika.

Certyfikat unieważniony – certyfikat, który został kiedyś umieszczony na liście certyfikatów unieważnionych, bez anulowania przyczyny unieważnienia (np. po odwieszeniu certyfikatu).

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.

Dane służące do składania podpisu elektronicznego – niepowtarzalne i przyporządkowane osobie fizycznej dane, które są wykorzystywane przez tą osobę do składania podpisu elektronicznego.

Dostęp – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

Główny Punkt Rejestracji (GPR) – punkt rejestracji, który oprócz standardowych czynności akredytuje inne punkty rejestracji i może generować, w imieniu urzędu certyfikacji, pary kluczy, które poddawane są następnie procesowi 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.

Infrastruktura klucza publicznego (PKI) – składa się z powiązanych z 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 temu 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.

Klucze infrastruktury – klucze kryptograficzne algorytmów szyfrowych stosowane do innych celów niż składanie lub weryfikacja podpisu elektronicznego lub poświadczenia elektronicznego, a w szczególności klucze stosowane: (a) w protokołach uzgadniania lub dystrybucji kluczy zapewniających poufność danych, (b) dla zapewnienia, podczas transmisji lub przechowywania, poufności i integralności zgłoszeń certyfikacyjnych, kluczy użytkowników, rejestrów zdarzeń, (c) do weryfikacji dostępu do urządzeń lub aplikacji.

UWAGA: Pod pojęciem kluczy infrastruktury rozumieć będziemy także klucze stosowane przez podmioty (fizyczne i prawne) w takich przypadkach jak uzgadnianie kluczy, uwierzytelnianie podmiotów i podsystemów, podpisywanie rejestrów zdarzeń, szyfrowanie przesyłanych lub przechowywanych danych.

Kodeks Postępowania Certyfikacyjnego (KPC) – dokument opisujący szczegółowo proces certyfikacji klucza publicznego, uczestników tego procesu, oraz określający obszary zastosowań uzyskanych w jego wyniku certyfikatów.

Komponent techniczny - sprzęt stosowany w celu wygenerowania lub użycia danych służących do składania bezpiecznego podpisu elektronicznego lub poświadczenia elektronicznego.

Kontrola dostępu – proces przekazywania dostępu do zasobów systemów informacyjnych tylko autoryzowanym użytkownikom, programom, procesom oraz innym systemom.

Krajowy urząd certyfikacji – minister właściwy ds. gospodarki lub podmiot upoważniony przez niego w trybie art. 23 ust. 4 lub 5 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym* do wydawania zaświadczeń certyfikacyjnych, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do ministra właściwego do spraw gospodarki lub tego podmiotu.

Kwalifikowany certyfikat – certyfikat spełniający warunki określone w *Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym*, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne.

Kwalifikowany podmiot świadczący usługi certyfikacyjne – podmiot świadczący usługi certyfikacyjne, wpisany do rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

Lista certyfikatów unieważnionych (CRL, ang. Certificate Revocation List) – elektroniczne zaświadczenia zawierające numery seryjne zawieszonych lub unieważnionych certyfikatów oraz daty i przyczyny ich zawieszenia lub unieważnienia, nazwę wydawcy CRL, datę publikacji listy, datę następnej planowanej publikacji listy. Powyższe dane są poświadczane elektronicznie przez urząd certyfikacji.

Moduł kryptograficzny – (a) zestaw składający się ze sprzętu, oprogramowania, mikrokodu lub ich określona kombinacja, realizujące operacje lub procesy kryptograficzne, obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu, (b) wiarygodna implementacja kryptosystemu, który w bezpieczny sposób wykonuje operacje szyfrowania i deszyfrowania.

Nazwa wyróżniona (DN, *ang. distinguished name*) – zbiór atrybutów, tworzących nazwę wyróżnioną osoby prawnej, odróżniającą go od innych podmiotów tego samego typu; np. C=PL/OU=Unizeto Technologies S.A., itp.

Okres aktywności certyfikatu – okres czasu pomiędzy początkową a końcową datą ważności certyfikatu lub pomiędzy datą początku ważności certyfikatu a datą jego unieważnienia lub zawieszenia.

Osoba składająca podpis elektroniczny – osoba fizyczna posiadająca urządzenie służące do składania podpisu elektronicznego, która działa w imieniu własnym albo w imieniu innej osoby fizycznej, prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej**.**

PIN (*ang. Personal Identification Number*) – osobisty numer identyfikacyjny, kod zabezpieczający kartę kryptograficzną przed możliwością złożenia podpisu elektronicznego przez osoby niepowołane.

Podpis elektroniczny – dane w postaci elektronicznej, które wraz z innymi danymi do których zostały dołączone lub z którymi są logicznie powiązane, służą do identyfikacji osoby składającej podpis elektroniczny.

Polityka certyfikacji – dokument określający ogólne zasady stosowane przez urząd certyfikacji podczas procesu certyfikacji kluczy publicznych, definiujący uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań.

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.

Poświadczenie elektroniczne – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne oraz spełniają dodatkowe wymagania określone w Art.3, ust.19 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym.*

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 Potwierdzania Tożsamości (PPT) – jego funkcją jest potwierdzanie tożsamości subskrybenta i zawarcie umowy o świadczenie kwalifikowanych usług certyfikacyjnych w procesie wydawania kwalifikowanych certyfikatów.

Punkt Rejestracji (PR) – miejsce, gdzie świadczone są usługi w zakresie weryfikacji i potwierdzania tożsamości osób ubiegających się o certyfikat oraz zawarcie umowy o świadczenie kwalifikowanych usług certyfikacyjnych, ich funkcją jest kompleksowa obsługa subskrybentów w zakresie świadczenia usług certyfikacyjnych.

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.

Regulamin Kwalifikowanych Usług Certyfikacyjnych – dokument regulujący podstawowe prawa i obowiązki stron umowy o świadczenie usług certyfikacyjnych.

Repozytorium – zbiór publicznie dostępnych katalogów elektronicznych zawierających wydane certyfikaty oraz dokumenty związane z funkcjonowaniem urzędu certyfikacji.

Sekret unieważnienia certyfikatów – tajna informacja znana tylko subskrybentowi i urzędowi certyfikacji, wykorzystywana przez niego do uwierzytelniania żądań unieważniania certyfikatów w przypadku, gdy subskrybent nie posiada dostępu do prywatnego klucza podpisującego lub nie chce go użyć. Sekret unieważniania może być okresowo zmieniany.

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.

Sponsor Subskrybenta (płatnik) – osoba lub instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty lub podmiot reprezentowany przez Subskrybenta. Sponsor jest właścicielem certyfikatu i przysługuje mu prawo do zgłoszenia jego unieważnienia w przypadkach przewidzianych w *Ustawie z dnia 18 września 2001 r. o podpisie elektronicznym*, uregulowaniach Kodeksu Postępowania Certyfikacyjnego oraz zawartej umowie.

Sprzętowy moduł kryptograficzny – patrz **moduł kryptograficzny**.

Strona ufająca (*ang. relaying party*) – odbiorca, który otrzymał informację zawierającą certyfikat oraz podpis elektroniczny weryfikowalny przy pomocy klucza publicznego umieszczonego w tym certyfikacie i decydujący na podstawie zaufania do certyfikatu o uznaniu lub odrzuceniu podpisu.

Subskrybent – osoba fizyczna, która jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej osobie, posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie oraz sama nie wydaje certyfikatów innym stronom.

Subskrybent indywidualny – osoba fizyczna, która jest podmiotem wydanego mu certyfikatu; subskrybent indywidualny zamawia certyfikat we własnym imieniu, do realizacji własnych potrzeb i jest właścicielem.

Subskrybent sponsorowany – osoba fizyczna, która jest podmiotem wydanego mu certyfikatu; certyfikat jest zamawiany przez subskrybenta sponsorowanego, bądź otrzymuje go na wniosek sponsora i stosowany jest przez niego do działania w imieniu sponsora; właścicielem certyfikatu jest sponsor.

Ścieżka certyfikacji (def.1) – uporządkowana sekwencja zaświadczeń certyfikacyjnych i/lub certyfikatu subskrybenta, które należy rozpatrzyć aby nabrać przekonania, że analizowany certyfikat lub zaświadczenie certyfikacyjne jest poświadczone elektronicznie przez urząd certyfikacji, któremu ufa dany subskrybent.

Ścieżka certyfikacji (def.2) – uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i certyfikatu utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce możliwe jest wykazanie, że dla każdych dwóch

bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i certyfikatu poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego „punktem zaufania".

Token zgłoszenia certyfikacyjnego – dane w postaci elektronicznej, zawierające zgłoszenie certyfikacyjne: (1) utworzone przez podmiot świadczący usługi certyfikacyjne, (2) potwierdzające tożsamość osoby i prawdziwość danych identyfikacyjnych zawartych w zgłoszeniu certyfikacyjnym oraz w przypadkach gdy jest to konieczne potwierdzające, że klucz prywatny komplementarny z kluczem publicznym służącym do weryfikacji podpisu elektronicznego znajdującymi się w zgłoszeniu certyfikacyjnym, znajdują się w posiadaniu osoby starającej się o certyfikat, (3) opatrzone przez podmiot świadczący usługi certyfikacyjne czasem jego przygotowania z minimalną dokładnością do jednej minuty, bez konieczności synchronizacji czasu oraz (4) opatrzone podpisem elektronicznym inspektora ds. rejestracji.

Token znacznika czasu – dane w postaci elektronicznej, które związują dowolny fakt lub działanie z określonym momentem w czasie, ustanawiając w ten sposób poświadczenie, że fakt lub działanie miało miejsce przed tym momentem w czasie.

Umowa subskrybenta indywidualnego – umowa zawierana jest pomiędzy Unizeto Technologies S.A. a subskrybentem zamawiającym certyfikat do działania we własnym imieniu, realizacji potrzeb własnych lub zawodowych; subskrybent jest zarazem użytkownikiem jak i właścicielem certyfikatu.

Umowa subskrybenta sponsorowanego – umowa zawierana jest pomiędzy Unizeto Technologies S.A. a subskrybentem, dla którego certyfikat jest zamawiany przez sponsora i wykorzystywany jest przez subskrybenta do wykonywania zadań zleconych przez sponsora; właścicielem certyfikatu jest sponsor i przysługuje mu prawo jego unieważnienia, subskrybent jest zaś jedynie jego użytkownikiem.

Umowa sponsorska – umowa zawierana jest pomiędzy Unizeto Technologies S.A. a sponsorem; umowa ma charakter umowy zbiorowej, upoważniającej Unizeto Technologies S.A. do zawierania indywidualnych umów z każdym ze **subskrybentów sponsorowanych**, będących podmiotem umowy sponsorskiej.

Unieważnienie certyfikatów (*ang. certificates revocation*) – procedury odwołania ważności pary kluczy (wycofania certyfikatu) w przypadku, gdy zachodzi konieczność uniemożliwienia subskrybentowi dostępu do tej pary i użycia jej w operacjach podpisu elektronicznego. Unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

CERTUM - Powszechne Centrum Certyfikacji (w skrócie: CERTUM) – jednostka usługowa Unizeto Technologies S.A., świadcząca niekwalifikowane i kwalifikowane usługi certyfikacyjne. Kwalifikowane usługi certyfikacyjne świadczy w zakresie wydawania kwalifikowanych certyfikatów klucza publicznego oraz znakowania czasem zgodnie z *Ustawą z dnia 18 września 2001 r. o podpisie elektronicznym* (Dz. U. Nr 130, poz. 1450).

Urząd certyfikacji – podmiot świadczący usługi certyfikacyjne, będący elementem składowym zaufanej trzeciej strony, zdolny do tworzenia, poświadczania i wydawania certyfikatów, zaświadczeń certyfikacyjnych oraz tokenów znacznika czasu i statusu certyfikatu.

Urząd znacznika czasu (TSA) – podmiot świadczący usługi certyfikacyjne, który wydaje tokeny znacznika czasu.

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.

Użytkownik (certyfikatu, *ang. end entity*) – uprawniony podmiot, posługujący się certyfikatem jako subskrybent lub strona ufająca, z wyłączeniem urzędu certyfikacji.

Ważny certyfikat – patrz certyfikat ważny.

Ważne zaświadczenie certyfikacyjne – zaświadczenie certyfikacyjne, które nie jest unieważnione.

Weryfikacja podpisu elektronicznego – ma na celu określenie, czy 1) podpis elektroniczny został zrealizowany przy pomocy klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez urząd certyfikacji certyfikacie subskrybenta, oraz 2) podpisana wiadomość (dokument) nie został zmodyfikowany już po złożeniu na nim podpisu.

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – umożliwia określenie czy certyfikat jest unieważniony. Problem ten może być rozwiązany przez zainteresowany podmiot w oparciu o listy CRL albo też przez wystawcę certyfikatu lub upoważnionego przez niego przedstawiciela na 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.

Wydawanie kwalifikowanych certyfikatów – te spośród usług kwalifikowanego urzędu certyfikacji, które obejmują usługę rejestracji subskrybentów lub usługę certyfikacji klucza publicznego albo usługę aktualizacji klucza oraz certyfikatu, i kończą się utworzeniem certyfikatu kwalifikowanego, a następnie powiadomieniem o tym fakcie podmiotu wymienionego w treści tego certyfikatu lub fizycznym dostarczeniem mu utworzonego certyfikatu.

Zaświadczenie certyfikacyjne – elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu, o którym mowa w art. 30 ust. 1 *Ustawy z dnia 18 września 2001 r. o podpisie elektronicznym*, i które umożliwiają identyfikację tego podmiotu lub organu.

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.

Zawieszenie certyfikatu (ang. suspension) – szczególna forma unieważnienia certyfikatu (i związanej z nim pary kluczy), której wynikiem jest czasowy brak akceptacji certyfikatu w operacjach kryptograficznych (niezależnie od statusu tej operacji); zawieszony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

Zgłoszenie certyfikacyjne – zbiór dokumentów i danych identyfikujących podmiot podlegający certyfikacji.

Znakowanie czasem – usługa polegającą na dołączaniu do danych w postaci elektronicznej logicznie powiązanych z danymi opatrzonymi podpisem lub poświadczeniem elektronicznym, oznaczenia czasu w chwili wykonania tej usługi oraz poświadczenia elektronicznego tak powstałych danych przez podmiot świadczący tę usługę.