Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM

Wersja 2.5

Data: 12 maja 2008

Status: poprzedni

Unizeto Technologies S.A.
„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

Kodeks Postępowania Certyfikacyjnego[1] **Niekwalifikowanych Usług CERTUM** (nazywany dalej **Kodeksem Postępowania Certyfikacyjnego** lub w skrócie **KPC**) jest uszczegółowieniem ogólnych zasad postępowania certyfikacyjnego, opisanych w **Polityce Certyfikacji Niekwalifikowanych Usług CERTUM** (nazwanej dalej **Polityką Certyfikacji** lub w skrócie **PC**) opisuje proces certyfikacji klucza publicznego oraz określa obszary zastosowań uzyskanych w jego wyniku certyfikatów. Znajomość natury, celu oraz roli Kodeksu Postępowania Certyfikacyjnego jest szczególnie istotna z punktu widzenia **subskrybenta**[2] oraz **strony ufającej**[3].

Polityka Certyfikacji określa ogólne zasady stosowane w CERTUM – Powszechnym Centrum Certyfikacji (zwanym dalej CERTUM) podczas procesu certyfikacji kluczy publicznych, definiuje uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Polityka Certyfikacji określa, jaki stopień zaufania można związać z określonym typem certyfikatu wydanego przez **CERTUM** świadczące niekwalifikowane usługi certyfikacyjne. Z kolei Kodeks Postępowania Certyfikacyjnego pokazuje, w jaki sposób CERTUM zapewnia osiągnięcie gwarantowanego przez politykę poziomu zaufania.

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

Kodeks Postępowania Certyfikacyjnego opisuje zbiór czterech podstawowych oraz dodatkowe polityki certyfikacji (*ang. Certificate Policies*[4]), według których CERTUM wydaje certyfikaty urzędom i użytkownikom końcowym. Polityki te reprezentują różne poziomy wiarygodności[5] przypisane certyfikatom klucza publicznego. Obszary zastosowań certyfikatów wystawianych zgodnie z tymi politykami mogą się pokrywać, inna jest jednak odpowiedzialność (w tym prawna) urzędu certyfikacji oraz użytkowników certyfikatu.

Struktura i merytoryczna zawartość Kodeksu Postępowania Certyfikacyjnego są zgodne z zaleceniem RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. Kodeks Postępowania Certyfikacyjnego został utworzony przy założeniu, że czytelnik jest ogólnie

---

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

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

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

[4] Informacja (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez CERTUM. Należy odróżnić Politykę Certyfikacji jako dokument, od polityki certyfikacji jako zestawu parametrów charakterystycznych dla certyfikatu o danym poziomie.

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

zaznajomiony z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz Infrastruktury Klucza Publicznego (PKI).

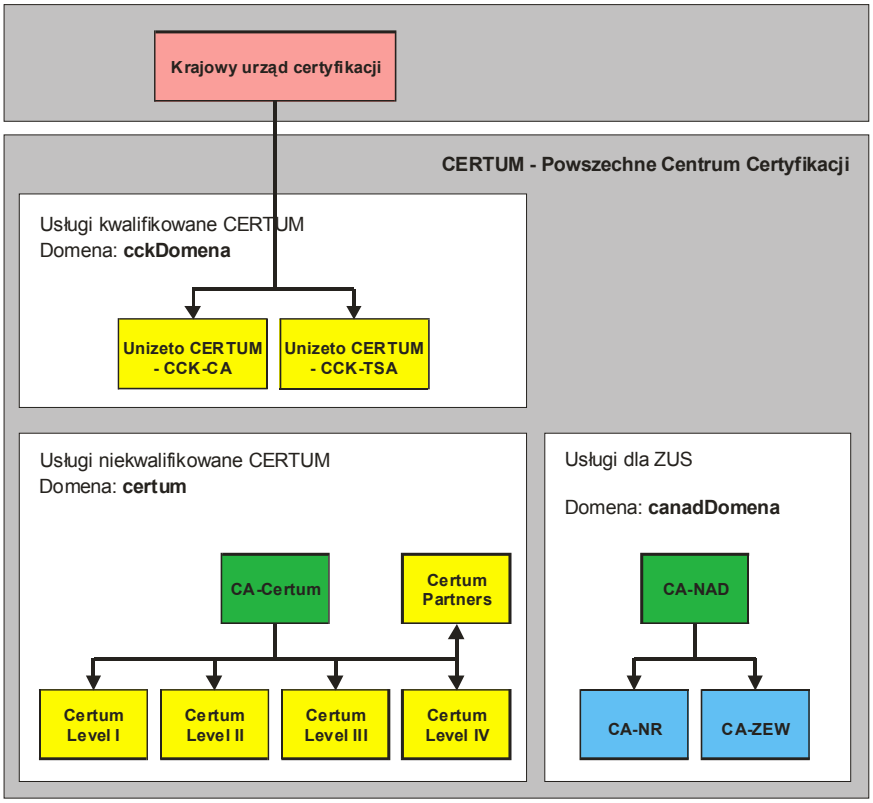
*Szereg pojęć i ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym na końcu dokumentu.*

Firma Unizeto Technologies S.A. 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

Kodeks Postępowania Certyfikacyjnego opisuje i stanowi podstawę zasad działania CERTUM oraz wszystkich związanych z nim **urzędów certyfikacji**, **punktów rejestracji**, **subskrybentów**, jak również **stron ufających**. Określa także zasady świadczenia usług certyfikacyjnych, począwszy od rejestracji subskrybentów, certyfikacji kluczy publicznych, aktualizacji kluczy i certyfikatów, a na unieważnianiu certyfikatów kończąc.

Niekwalifikowane usługi CERTUM tworzą w jej obrębie oddzielną domenę certyfikacji **certum** (patrz rys.1), z wydzielonym głównym urzędem certyfikacji Certum CA. Główny urząd certyfikacji **Certum CA** jest niezależny od domeny **canadDomena** oraz **cckDomena** i sam sobie wystawia tzw. autocertyfikat[6].



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

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

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

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

Certyfikaty wydawane przez CERTUM zawierają identyfikatory polityk certyfikacji[7], które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Deklarowane przeznaczenie certyfikatu można określić na podstawie wpisów umieszczanych w strukturze **PolicyInformation** rozszerzenia **certificatesPolicies** (patrz rozdz.7.1.1.2) każdego certyfikatu wydawanego przez CERTUM.

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

Z Kodeksem Postępowania Certyfikacyjnego związane są inne dodatkowe dokumenty, które wykorzystywane są w systemie CERTUM i regulują jego funkcjonowanie (patrz Tab.1). Dokumenty te mają różny status. Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane.

[7] Identyfikatory polityk certyfikacji CERTUM budowane są w oparciu o identyfikator obiektu Unizeto Sp. z o.o. zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów (KRIO, http://www.krio.pl). Identyfikator ten ma wartość:

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

Tab.1 Ważniejsze dokumenty towarzyszące Kodeksowi Postępowania Certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Polityka Certyfikacji Niekwalifikowanych Usług CERTUM	Jawny	http://www.certum.pl
2.	Polityka Niekwalifikowanego Urzędu Znacznika Czasu	Jawny	http://www.certum.pl
3.	Regulamin Niekwalifikowanych Usług Certyfikacyjnych CERTUM	Jawny	http://www.certum.pl
4.	Dokumentacja personelu, zakres obowiązków i odpowiedzialności	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytorzy
5.	Dokumentacja punktu rejestracji	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytorzy
6.	Dokumentacja infrastruktury technicznej	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytorzy
7.	Dokumentacja zarządzania ciągłością działalności systemu	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytorzy
8.	Program Partnerski (Cross Root CA)	Niejawny	Dostępny na żądanie
9.	Instrukcja weryfikacji tożsamości	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor

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

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Kodeksu Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci **Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM** i jest on dostępny:

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

Z dokumentem Kodeksu Postępowania Certyfikacyjnego związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113527.2.2.0.1.2.5):

```
id-ccert-kpc-v3  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
          organization(1) id-unizeto(113527) id-ccert(2) id-certum(2)
          id-certPolicy-doc(0) id-ccert-kpc(1) version(2) 5}
```

w którym dwie ostatnie wartości liczbowe odnoszą się do aktualnej wersji i podwersji tego dokumentu.

Identyfikator Kodeksu Postępowania Certyfikacyjnego nie jest umieszczany w treści wystawianych certyfikatów. W wydawanych przez siebie certyfikatach CERTUM umieszcza jedynie identyfikatory tych polityk certyfikacji, które należą do zbioru polityk certyfikacji określonych w Polityce Certyfikacji i rozdz. 7.1.1.2 niniejszego dokumentu.

1.3. Strony Kodeksu Postępowania Certyfikacyjnego

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

- urzędów certyfikacji **Certum CA**, **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV**, **Certum Partners** oraz każdego innego urzędu, który zostanie utworzony zgodnie z zasadami określonymi w niniejszym Kodeksie Postępowania Certyfikacyjnego,
- Głównego Punktu Rejestracji (GPR),
- punktów rejestracji (PR),
- subskrybentów,
- stron ufających.

CERTUM świadczy usługi certyfikacyjne wszystkim osobom fizycznym i prawnym lub podmiotom nie posiadającym osobowości prawnej, akceptującym postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego. Postanowienia te (m.in. zasady generowania kluczy i wystawiania certyfikatów, zastosowane mechanizmy zabezpieczeń systemu informatycznego) mają na celu przekonanie użytkowników usług CERTUM, że deklarowana wiarygodność wydawanych certyfikatów jest praktycznym odzwierciedleniem postępowania urzędów certyfikacji.

1.3.1. Urzędy certyfikacji

W skład CERTUM wchodzą urzędy certyfikacji, tworzące wspólną domenę urzędów certyfikacji o nazwie **certum** (rys.1). Urząd certyfikacji **Certum CA** jest głównym urzędem certyfikacji domeny certum, któremu podlegają wszystkie urzędy certyfikacji z tej domeny.

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

1.3.1.1. Główny urząd certyfikacji Certum CA

Główny urząd certyfikacji Certum CA może rejestrować i wydawać certyfikaty tylko urzędom certyfikacji oraz urzędom wystawiającym elektroniczne poświadczenia niezaprzeczalności, należącym do domeny **certum**. Urząd **Certum CA** działa w oparciu o wystawiony przez siebie autocertyfikat. W autocertyfikacie nie umieszcza się rozszerzenia **certificatePolicies**, co należy interpretować jako brak ograniczeń na zbiór **ścieżek certyfikacji**[8], do których można dołączać certyfikat **Certum CA**.

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

Urząd certyfikacji **Certum CA** świadczy usługi certyfikacyjne dla:

[8] Patrz **Słownik pojęć**

- samego siebie (wystawia i aktualizuje autocertyfikaty),
- urzędów **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV** i **Certum Partners** oraz innym urzędom certyfikacji zarejestrowanym w domenie certyfikacji **certum**,
- podmiotów świadczących usługi weryfikacji statusu certyfikatu w trybie on-line (OCSP) oraz innym podmiotom świadczącym usługi niezaprzeczalności (m.in. usługi znacznika czasu).

1.3.1.2. Pośrednie urzędy certyfikacji

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

Tab.1.2 Nazwy pośrednich urzędów certyfikacji i identyfikatory polityk certyfikacji umieszczane w wystawianych przez te urzędy certyfikatach

Nazwa polityki certyfikacji	Identyfikator polityki certyfikacji
Certum Level I	1.2.616.1.113527.2.2.1
Certum Level II	1.2.616.1.113527.2.2.2
Certum Level III	1.2.616.1.113527.2.2.3
Certum Level IV	1.2.616.1.113527.2.2.4
Certum Partners	1.2.616.1.113527.2.2.9

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

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

*Innym urzędom certyfikacji certyfikaty mogą wystawiać tylko dwa urzędy: **Certum Level I** (testowe urzędy certyfikacji) oraz **Certum Partners** (komercyjne urzędy certyfikacji).*

Z CERTUM ściśle współpracuje Główny Punkt Rejestracji oraz punkty rejestracji. Punkty rejestracji reprezentują CERTUM w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez urzędy certyfikacji uprawnień w zakresie identyfikacji i rejestracji subskrybentów. Sposób funkcjonowania oraz zakres obowiązków punktów rejestracji zależy od rodzaju certyfikatu wydawanego subskrybentom i związaną z nim polityką certyfikacji.

Pośrednie urzędy certyfikacji przystosowane są do wydawania certyfikatów dla:

- pracowników CERTUM i operatorów punktów rejestracji,
- użytkowników certyfikatów, którzy dzięki certyfikatom chcą zapewnić bezpieczeństwo swojej poczcie elektronicznej i przechowywanym danym, zapewnić bezpieczeństwo i wiarygodność serwerom usługowym (np. sklepom internetowym, bibliotekom informacji i oprogramowania, itp.),
- urządzeń (fizycznych i logicznych) będących pod opieką osób fizycznych lub prawnych;

- podmiotów świadczących usługi niezaprzeczalności, np. urzędom znaczników czasu (TSA) lub urzędom notarialnym (dotyczy to tylko pośrednich urzędów **Certum Level I** i **Certum Partners**),
- innym urzędom certyfikacji (dotyczy to tylko pośrednich urzędów **Certum Level I** i **Certum Partners**).

1.3.2. Urząd znacznika czasu

Elementem infrastruktury CERTUM jest urząd znacznika czasu **Certum Time-Stamping Authority**, który także działa w domenie certyfikacji **certum** (rys.1).

Urząd znacznika czasu wydaje znaczniki czasu zgodnie z zaleceniami ETSI[9]. Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość określona jest w Tab.3 oraz w rozdz. 7.3) oraz poświadczany jest wyłącznie przy pomocy klucza prywatnego wytworzonego specjalnie dla usługi znakowania czasem.

Tab.3 Identyfikator polityki certyfikacji umieszczany przez **Certum Time-Stamping Authority** w tokenach znacznika czasu

Nazwa tokena	Identyfikator polityki certyfikacji
Token znacznika czasu	1.2.616.1.113527.2.2.5

Znaczniki czasu, wydawane zgodnie z polityką określoną w Tab.3, znajdują zastosowanie przede wszystkim do zabezpieczania długookresowych podpisów cyfrowych[10] oraz transakcji zawieranych w sieci globalnej.

Urząd znacznika czasu **Certum Time-Stamping Authority** przy świadczeniu usług znacznika czasu stosuje rozwiązania zapewniające synchronizację z międzynarodowym wzorcem czasu (Coordinated Universal Time - UTC), z dokładnością większą niż 1 sekunda.

1.3.3. Urząd weryfikacji statusu certyfikatu

CERTUM oprócz standardowego sposobu weryfikacji statusu certyfikatów w oparciu o pobieranie listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu certyfikatu w trybie *on-line* (OCSP). Usługa ta świadczona jest przez urząd weryfikacji statusu certyfikatu **Certum Validation Service**.

1.3.4. Punkty rejestracji

Punkty rejestracji przyjmują, weryfikują i następnie aprobują lub odrzucają - otrzymywane od wnioskodawców - wnioski o zarejestrowanie i wydanie certyfikatu oraz aktualizację, odnowienie lub unieważnienie certyfikatu. Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dostarczonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Punkty rejestracji mogą występować także z wnioskami do właściwego urzędu certyfikacji o wyrejestrowanie subskrybenta i tym samym o unieważnienie jego certyfikatu. Stopień dokładności weryfikacji tożsamości subskrybenta wynika z potrzeb samego subskrybenta, a także narzucany jest przez klasę certyfikatu, o wydanie którego stara się subskrybent (patrz rozdz. 3). W przypadku najprostszej weryfikacji subskrybenta punkt rejestracji sprawdza tylko

[9] ETSI TS 101 861 *Time stamping profile*, August 2001

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

prawidłowość podanego adresu email. Najdokładniejsza weryfikacja może z kolei wymagać osobistego stawienia się subskrybenta w punkcie rejestracji i przedłożenia stosownych dokumentów. Wymogi te oznaczają, że tego typu weryfikacja może być realizowana albo całkowicie automatycznie, albo ręcznie przez operatora punktu rejestracji.

Punkty rejestracji działają z upoważnienia odpowiedniego urzędu certyfikacji należącego do domeny **certum** w zakresie weryfikacji tożsamości aktualnego lub przyszłego subskrybenta oraz weryfikacji dowodu posiadania klucza prywatnego. W przypadku punktów rejestracji zarządzanych przez podmioty inne niż Unizeto Technologies S.A. (zewnętrzne punkty rejestracji), szczegółowy zakres obowiązków punktów rejestracji i jego operatorów może być określony poprzez osobną umowę zawartą pomiędzy Unizeto Technologies S.A. a danym punktem rejestracji, niniejszy Kodeks oraz procedury funkcjonowania punktu rejestracji, które są integralną częścią tej umowy.

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

Lista aktualnie akredytowanych przez GPR punktów rejestracji dostępna jest w repozytorium dostępnym pod adresem:

http://www.certum.pl

Wyróżnia się dwa typy punktów rejestracji, którym urzędy certyfikacji działające w ramach CERTUM mogą przekazać część swoich uprawnień:

- punkty rejestracji,
- Główny Punkt Rejestracji (GPR).

Podstawowa różnica pomiędzy wymienionymi dwoma typami punktów rejestracji polega na tym, że punkty rejestracji nie mogą – w przeciwieństwie do Głównego Punktu Rejestracji – akredytować innych punktów rejestracji oraz rejestrować nowych urzędów certyfikacji. Dodatkowo punkty rejestracji nie posiadają uprawnień do poświadczania wszystkich żądań subskrybentów. Uprawnienia te mogą być ograniczone tylko do niektórych spośród wszystkich dostępnych typów[11] certyfikatów. Stąd:

- **PR** rejestrują subskrybentów końcowych (osoby fizyczne i prawne), którzy ubiegają się o certyfikaty o wiarygodności do poziomu Certum Level IV włącznie,
- **GPR** rejestruje punkty rejestracji, nowe urzędy certyfikacji oraz subskrybentów końcowych (osoby fizyczne i prawne, urządzenia); nie nakłada się żadnych ograniczeń (poza tymi, które wynikają z roli pełnionych w infrastrukturze klucza publicznego CERTUM) na typy certyfikatów wydawanych subskrybentom zarejestrowanym w GPR; dodatkowo GPR zatwierdza także nazwy wyróżnione aktualnych i tworzonych w przyszłości punktów rejestracji.

Główny Punkt Rejestracji zlokalizowany jest w siedzibie CERTUM. Adresy kontaktowe Głównego Punktu Rejestracji podane są w rozdz. 1.5.

[11] Typy certyfikatów omówione są w rozdz.1.4

1.3.5. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych katalogów zawierających:

- Certyfikaty wszystkich urzędów certyfikacji, należących do domeny certum lub z nią związanych (np. certyfikaty nowych urzędów certyfikacji zarejestrowane w Głównym Punkcie Rejestracji),
- subskrybentów końcowych (osób prawnych i fizycznych, w tym także pracowników CERTUM oraz urządzeń pod ich opieką, niezbędnych do funkcjonowania usług PKI).

Dodatkowo w repozytorium znajdują się informacje ściśle związane z funkcjonowaniem certyfikatów, m.in. listy certyfikatów unieważnionych (CRL), aktualna i poprzednia wersja Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego, jak również inne na bieżąco modyfikowane informacje (np. lista rekomendowanych aplikacji lub lista punktów rejestracji).

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

Zawartość repozytorium dostępna jest za pośrednictwem protokołu HTTP pod adresem:

http://www.certum.pl

1.3.6. Użytkownicy końcowi

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

1.3.6.1. Subskrybenci

Subskrybentami CERTUM mogą być dowolne osoby fizyczne, prawne lub podmioty nieposiadające osobowości prawnej oraz urządzenia będące pod ich kontrolą, o ile tylko spełniają warunki definicji subskrybenta podanej w rozdz.1.3.6.

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.

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

1.3.6.2. Strony ufające

Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji tego certyfikatu uzależnioną w jakikolwiek sposób od ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym przez jeden z urzędów certyfikacji podległych **Certum CA**.

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu do zweryfikowania podpisu cyfrowego, zidentyfikowania źródła lub twórcy wiadomości lub

utworzenia sekretnego kanału komunikacyjnego z właścicielem certyfikatu. Informacje zawarte w certyfikacie (m.in. identyfikatory i kwalifikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.4. Zakres stosowania certyfikatów

Zakres stosowania certyfikatów określa obszary tzw. dozwolonego użycia certyfikatu. Obszar ten określa naturę (charakter) zastosowania certyfikatu (np. podpis cyfrowy lub poufność, uwierzytelnienie).

Certyfikaty wystawiane przez CERTUM mogą być stosowane do przetwarzania i ochrony informacji (także uwierzytelniania) o różnym poziomie wrażliwości. Poziom wrażliwości informacji oraz jej podatność na **naruszenie**[12] powinny zostać oszacowane przez subskrybenta. W Polityce Certyfikacji oraz niniejszym Kodeksie Postępowania Certyfikacyjnego wprowadza się cztery poziomy wrażliwości: poziom I, określany także jako testowy, poziom II lub podstawowy, poziom III lub średni oraz poziom IV lub wysoki. Wymienione poziomy powiązane są relacją jeden do jeden z poziomami wiarygodności certyfikatów, które wymienione są w Tab.1.3[13].

Tab.1.3 Poziomy wrażliwości informacji a nazwy polityk certyfikacji

Poziom wrażliwości informacji	Nazwa polityki certyfikacji	Zakres stosowalności
Poziom I/testowy	Certum Level I	Najniższy poziom wiarygodności tożsamości podmiotu certyfikatu. Certyfikaty tego poziomu powinny być stosowane jedynie do testowania kompatybilności usług CERTUM z usługami świadczonymi przez innych dostawców usług PKI oraz funkcjonalności certyfikatów we współpracy z testowanymi aplikacjami. Można używać ich także do innych celów, o ile nie jest istotne zapewnienie wiarygodności wysyłanej/otrzymywanej informacji.
Poziom II/podstawowy	Certum Level II	Ten poziom zapewnia podstawową ochronę informacji w środowisku, w którym występuje małe ryzyko naruszenia[14] danych, niepociągające za sobą dalszych istotnych następstw. Dotyczyć to może dostępu do prywatnych informacji w przypadkach, gdy prawdopodobieństwo nieuprawnionego dostępu nie jest zbyt wysokie. Certyfikatów tego poziomu można używać do uwierzytelniania, kontroli integralności informacji, która została podpisana oraz zapewnienia poufności informacji, w tym w szczególności poczty elektronicznej.
Poziom III/średni	Certum Level III	Poziom dotyczy ochrony informacji w środowisku, w którym występuje ryzyko naruszenia danych informacji oraz skutki tego naruszenia są średnie. Certyfikatów tego poziomu można używać w transakcjach finansowych lub transakcjach o znacznym poziomie ryzyka wystąpienia oszustw, a także w tych przypadkach dostępu do prywatnych informacji, w których prawdopodobieństwo nieuprawnionego dostępu jest istotne.

[12] Patrz **Słownik pojęć**

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

[14] Patrz **Słownik pojęć**

Poziom IV/wysoki	Certum Level IV	Ten poziom jest odpowiedni w przypadkach, gdy zagrożenie naruszenia danych jest wysokie lub bardzo istotne mogą być następstwa awarii usług zabezpieczających. Certyfikatów tego poziomu można używać w transakcjach o nieograniczonej wartości finansowej, (chyba że inaczej zaznaczono w certyfikacie) lub o wysokim poziomie ryzyka wystąpienia oszustw.

Za określenie poziomu wiarygodności certyfikatu, przydatnego do określonego zastosowania, odpowiada strona ufająca lub sam subskrybent. Strony ta na podstawie różnych istotnych czynników ryzyka powinna określić, które z wystawianych przez CERTUM certyfikatów spełniają sformułowane wymagania. Wymagania strony ufającej powinny być znane (np. opublikowane w postaci **polityki podpisu** lub szerzej polityki zabezpieczeń systemu informatycznego) subskrybentom, którzy na ich podstawie mogą wystąpić do CERTUM o wydanie odpowiedniego certyfikatu, spełniającego te wymagania.

CERTUM wydaje także certyfikaty zgodnie z polityką Certum Partners, która nie ma określonego poziomu wrażliwości ze względu na wydawanie certyfikatów urzędów certyfikacji i certyfikatów służących do cross certyfikacji.

1.4.1. Typy certyfikatów i zalecane obszary ich zastosowań

CERTUM wydaje dziewięć podstawowych typów certyfikatów, określających jednocześnie obszary ich zastosowania. Są to:

1) **certyfikaty osobiste** – umożliwiają szyfrowanie i podpisywanie poczty elektronicznej oraz znajdują zastosowanie w zabezpieczaniu dokumentów elektronicznych (poczta elektroniczna wg standardu S/MIME lub PGP),
2) **certyfikaty do poświadczania autentyczności serwera** – stosowane przez globalne oraz ekstranetowe serwisy usługowe pracujące w osłonie protokołu SSL/TLS/WTLS,
3) **certyfikaty do uwierzytelniania subskrybentów** (osób prawnych i fizycznych, urządzeń) - stosowane m.in. w protokołach SSL/TLS/WTLS,
4) **certyfikaty do poświadczania statusu certyfikatów** – wydawane są na serwery działające zgodnie z protokołem OCSP i wystawiające tokeny aktualnego statusu weryfikowanego certyfikatu,
5) **certyfikaty do szyfrowania** – umożliwiają zabezpieczanie plików, katalogów oraz systemów plików,
6) **certyfikaty do zabezpieczania kodu** – certyfikaty przeznaczone dla programistów służące do zabezpieczania oprogramowania przed sfałszowaniem,
7) **certyfikaty urzędów certyfikacji** – ich użycia nie ogranicza się z góry do określonych obszarów, ale obszar taki może wynikać z przyjętych w certyfikacie zastosowań klucza prywatnego (patrz pole **keyUsage**, rozdz. 7) lub pełnionych ról (subskrybenta, urzędu certyfikacji lub innego urzędu świadczącego usługi w ramach PKI); do tego typu certyfikatów należą także certyfikaty operacyjne[15] urzędów certyfikacji,

[15] **Certyfikaty operacyjne** są to certyfikaty uniwersalne wydane urzędom certyfikacji. Certyfikaty te umożliwiają funkcjonowanie urzędów certyfikacji i obejmują certyfikaty służące do: weryfikacji podpisu pod wiadomościami, szyfrowania danych, weryfikacji

8) **certyfikaty urzędów znacznika czasu** – wydawane są na serwery, które w odpowiedzi na żądanie wystawiają tokeny znacznika czasu wiążące dowolne dane (dokumenty, wiadomości, podpisy cyfrowe, itd.) ze znacznikami czasu umożliwiającymi (w szczególnych przypadkach jednoznaczne) uporządkowanie danych,

9) **certyfikaty urzędów notarialnych** – wykorzystywane są przez serwer DVCS (*ang. Data Validation and Certification Server*), potwierdzający i certyfikujący dane.

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

Tab.1.4 Typy certyfikatów oraz ich zastosowania

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
Certum Level I	Private Email	Testowe zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Private WEB Server	Testowe zabezpieczanie transmisji danych dla serwerów WWW
	Private Microsoft Authenticode	Testowe zabezpieczanie oprogramowania przed sfałszowaniem, dystrybucja oprogramowania w sieci globalnej zgodnie z Microsoft Authenticode™
	Private Java Code Signing	Testowe zabezpieczanie oprogramowania zgodnie z technologią Sun Microsystems® Java
	Private Software Publisher	Testowe zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633, UNIX® Code Signing (uniwersalny certyfikat programisty)
	Private VPN	Testowe zabezpieczanie transmisji danych – protokół IPsec. Dla urządzeń sieciowych, serwerów i kanałów VPN
	Private Strong Internet	Testowe uwierzytelnianie klienta do zasobów sieci, serwera usługowego, stacji roboczej, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	Private SSL Server	Testowe zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.
	Private IPsec Client	Testowy klient szyfrowanej transmisji danych wg protokołu IPsec
	Private Data Encryption	Testowe szyfrowanie danych dla osób indywidualnych, kryptograficzne systemy plików
	Private Microsoft VBS	Certyfikaty niedostępne w ofercie publicznej
	Private Netscape Object Signing	Certyfikaty niedostępne w ofercie publicznej
	Private WAP Server	Certyfikaty niedostępne w ofercie publicznej
	Private Time-Stamping	Certyfikaty niedostępne w ofercie publicznej

podpisów na wystawianych certyfikatach i listach CRL, wymiany kluczy, uzgadniania kluczy, świadczenia usług niezaprzeczalności (patrz rozszerzenie certyfikatu **keyUsage**)

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
	Private Netscape Form Signing	Certyfikaty niedostępne w ofercie publicznej
	Private CA	Certyfikaty niedostępne w ofercie publicznej
	Private EDI	Certyfikaty niedostępne w ofercie publicznej
	Private Apple Code Signing	Certyfikaty niedostępne w ofercie publicznej
	Private Biometric Data	Certyfikaty niedostępne w ofercie publicznej
	Private Castanet Signing	Certyfikaty niedostępne w ofercie publicznej
	Private OCSP	Certyfikaty niedostępne w ofercie publicznej
	Private Notary Service	Certyfikaty niedostępne w ofercie publicznej
Certum Level II	Certum Silver	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Commercial Data Encryption	Szyfrowanie danych, zabezpieczenia kryptograficznych systemów plików
	Commercial Strong Internet	Uwierzytelnianie klienta do zasobów sieci, serwera usługowego, stacji roboczej, uwierzytelnianie do systemu Kerberos V (żetony na bazie certyfikatów X.509)
	Commercial IPsec Client	Klient szyfrowanej transmisji danych wg protokołu IPsec
	Commercial SSL Server	Certyfikaty niedostępne w ofercie publicznej
	Commercial VPN	Certyfikaty niedostępne w ofercie publicznej
Certum Level III	Certum Gold	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, PGP
	Enterprise Web Server	Zabezpieczanie transmisji danych dla serwerów WWW
	Enterprise SSL Server	Zabezpieczanie transmisji danych między serwisem a klientem LDAP, NTP, POP3, SMTP itp.
	Wildcard Domain	Zabezpieczanie połączeń SSL/TLS dla domen internetowych (*ang. Wildcard certificate*)
	Microsoft Authenticode	Zabezpieczanie oprogramowania przed sfałszowaniem, dystrybucja oprogramowania w sieci globalnej zgodnie z Microsoft Authenticode™
	Java Code Signing	Zabezpieczanie oprogramowania zgodnie z technologią Sun Microsystems® Java
	Software Publisher	Zabezpieczanie oprogramowania zgodnie z rekomendacją IETF RFC 2315 i IETF RFC 2633, UNIX® Code Signing (uniwersalny certyfikat programisty)
	Enterprise WAP Server	Certyfikaty niedostępne w ofercie publicznej
	Microsoft VBS	Certyfikaty niedostępne w ofercie publicznej

Nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
	Netscape Object Signing	Certyfikaty niedostępne w ofercie publicznej
	Enterprise VPN	Certyfikaty niedostępne w ofercie publicznej
	Netscape Form Signing	Certyfikaty niedostępne w ofercie publicznej
	Enterprise EDI	Certyfikaty niedostępne w ofercie publicznej
	Apple Code Signing	Certyfikaty niedostępne w ofercie publicznej
	Castanet Signing	Certyfikaty niedostępne w ofercie publicznej
Certum Level IV	Certum Platinum	Zabezpieczanie poczty elektronicznej, podpisy cyfrowe dokumentów elektronicznych, wymagane jest stosowanie mikroprocesorowej karty kryptograficznej
	Trusted WEB Server	Zabezpieczanie transmisji danych dla serwerów WWW, w szczególności serwisów bankowości elektronicznej i płatności on-line
	Trusted VPN	Zabezpieczanie transmisji danych – protokół IPsec Dla urządzeń sieciowych, serwerów i kanałów VPN, w szczególności routerów bankowości elektronicznej
	Trusted Strong Internet	Certyfikaty niedostępne w ofercie publicznej
	Trusted EDI	Certyfikaty niedostępne w ofercie publicznej
	Trusted Biometric Data	Certyfikaty niedostępne w ofercie publicznej
	Trusted IPsec Client	Certyfikaty niedostępne w ofercie publicznej
	Trusted Data Encryption	Certyfikaty niedostępne w ofercie publicznej
Certum Partners	Trusted Time-Stamping	Oznaczanie czasem obiektów oraz transakcji elektronicznych o dużej wartości
	Trusted CA	Świadczenie usług certyfikacyjnych
	Trusted OCSP	Serwis OCSP poświadczający statusy certyfikatów
	Trusted Notary Service	Urząd notariatu elektronicznego

1.4.2. Rekomendowane aplikacje

Certyfikaty wystawione zgodnie z jedną z czterech polityk certyfikacji mogą być stosowane z aplikacjami, które:

- prawidłowo zarządzają kluczami publicznymi i prywatnymi, ich przynajmniej następujące wymagania: przesyłaniem oraz używaniem,
- certyfikaty oraz związane z nimi klucze prywatne używają zgodnie z ich deklarowanym przeznaczeniem, potwierdzonym przez CERTUM,
- posiadają wbudowane mechanizmy weryfikacji statusu certyfikatu, budowania ścieżek certyfikacji oraz sprawdzania jego ważności (ważności podpisu, okresu ważności, itp.),
- przekazują użytkownikowi prawidłowe informacje o stanie aplikacji, certyfikatów, itp.

Lista aplikacji zalecanych i aprobowanych przez CERTUM opublikowana jest w repozytorium pod adresem:

http://www.certum.pl

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

1.4.3. Nierekomendowane aplikacje

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

Lista aplikacji, których nie rekomenduje się lub zabronione jest w nich używanie certyfikatów (może to być uzależnione od poziomu wiarygodności certyfikatu) wydanych przez CERTUM opublikowana jest w repozytorium pod adresem:

http://www.certum.pl

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

1.5. Kontakt

Niniejszym Kodeksem Postępowania Certyfikacyjnego, Polityką Certyfikacji oraz innymi dokumentami dotyczącymi usług PKI, świadczonymi przez CERTUM bezpośrednio administruje Zespół ds. Rozwoju Usług PKI. Oceny zgodności Kodeksu Postępowania Certyfikacyjnego z Polityką Certyfikacji dokonuje Zespół ds. Rozwoju Usług PKI. Wszelkie zapytania i uwagi związane z zawartością wymienionych dokumentów powinny być kierowane pod następujący adres:

Unizeto Technologies S.A.

CERTUM – Powszechne Centrum Certyfikacji

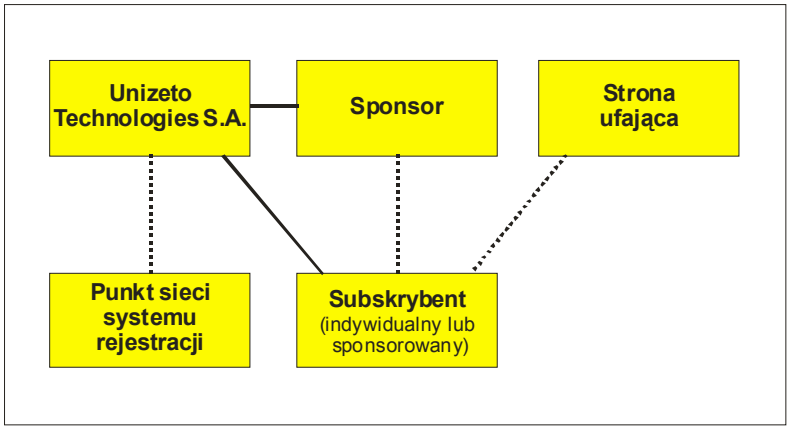
70-486 Szczecin, ul. Królowej Korony Polskiej 21

E-mail: info@certum.pl

Numer telefonu: +48 91 4801 340

2.Postanowienia ogólne

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



Rys.2.1 Umowy zawierane pomiędzy stronami

Umowy CERTUM ze stronami ufającymi oraz subskrybentami opisują typy usług, które udostępniane są przez CERTUM, wzajemne zobowiązania oraz odpowiedzialności, w tym finansowe Unizeto Technologies S.A.

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

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

2.1. Zobowiązania

2.1.1. Zobowiązania CERTUM i punktów rejestracji

CERTUM świadcząc niekwalifikowane usługi certyfikacyjne gwarantuje, że:

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie tworzące system, który spełnia wymagania określone w CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements* i normie FIPS PUB 140 *Security Requirements for Cryptographic Modules*,
- jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami:

  - usługi certyfikacyjne z zaleceniami normy X.509, PKCS#10, PKCS#7 i PKCS#12,
  - usługi znacznika czasu z zaleceniem RFC 3161,
  - weryfikacja statusu certyfikatu (OCSP) z zaleceniem RFC 2560,
  - usługi notarialne (DVCS) z zaleceniem RFC 3029,
- przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym Kodeksie Postępowania Certyfikacyjnego, w szczególności w zakresie:
  - weryfikacji tożsamości subskrybenta, któremu wydawany jest certyfikat w ramach domeny **certum**; przyjęte procedury weryfikujące tożsamość subskrybenta zależą od informacji zawartej w certyfikacie i zmieniają się w zależności od wysokości opłaty za certyfikat, natury certyfikatu oraz obszaru zastosowań, w obrębie którego wydany certyfikat jest wiarygodny (szczegóły patrz rozdz. 3 i 4),
  - certyfikatów, które są zawsze unieważniane, jeśli tylko istnieje przekonanie lub pewność, iż zawartość certyfikatu zdezaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.),
  - powiadamiania subskrybenta oraz innych podmiotów zainteresowanych faktem wydawania, unieważnienia lub zawieszenia certyfikatu,
  - publikowania list certyfikatów unieważnionych i zawieszonych,
  - generowania i stosowania kluczy prywatnych wyłącznie do celów, które określono w niniejszym Kodeksem Postępowania Certyfikacyjnego oraz takiej ich ochrony, która nie pozwala na ich użycie niezgodne z tymi celami,
  - personalizacji i wydawania elektronicznych kart kryptograficznych, na których zapisywane są certyfikaty oraz pary kluczy (w przypadku wygenerowania jej przez urząd certyfikacji),
  - okresowego i terminowego publikowania informacji, które niezbędne są do prawidłowego pozyskiwania, posługiwania się oraz unieważniania certyfikatów.
- wystawiane certyfikaty nie zawierają żadnych sfałszowanych danych, które byłyby znane lub które pochodziłyby od osób zatwierdzających wnioski o wystawienie certyfikatów lub wystawiających te certyfikaty,
- wystawiane certyfikaty nie zawierają żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty,
- nazwy wyróżnione (DN) subskrybentów umieszczane w certyfikatach są unikalne w domenie **certum**,
- zapewnia ochronę danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* z późn. zm. oraz dokumentami wykonawczymi do tej ustawy,
- w przypadku generowania pary kluczy z upoważnienia subskrybenta klucze te zostaną w sposób poufny przekazane subskrybentowi.

Ponadto CERTUM zobowiązuje się do:

- rejestrowania i wydawania certyfikatów tylko tym urzędom certyfikacji, w przypadku których stosowane zasady świadczenia usług certyfikacyjnych zapewniają nie mniejszy poziom bezpieczeństwa niż zapewniany przez CERTUM oraz Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego uzyskają aprobatę CERTUM,
- zawierania umów z subskrybentami, urzędami certyfikacji oraz punktami rejestracji; usługi certyfikacyjne świadczone są tylko na podstawie zawartych umów i zawsze na wniosek subskrybenta, urzędu certyfikacji lub punktu rejestracji,
- prowadzenia listy zarejestrowanych punktów rejestracji, z którymi posiada umowy o współpracy oraz rekomendowania wykorzystywanego przez te urzędy sprzętu i oprogramowania,
- prowadzenia listy rekomendowanego oprogramowania i sprzętu do generowania par kluczy asymetrycznych,
- przeprowadzania zgodnych z harmonogramem audytów w urzędach certyfikacji i punktach rejestracji należących do, lub powiązanych z domeną **certum**,
- zlecania planowanych audytów domeny **certum** niezależnym audytorom, udostępniania im wszystkich niezbędnych informacji i dokumentów oraz stosowania się do ich zaleceń pokontrolnych.

2.1.2. Zobowiązania punktów rejestracji

Każdy punkt rejestracji, który funkcjonuje w domenie **certum,** lub z którym CERTUM jest związane umowami gwarantuje, że:

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie, który posiada rekomendację CERTUM,
- jego działalność oraz świadczone usługi są zgodne z prawem i w szczególności nie naruszają praw autorskich i licencyjnych stron trzecich,
- dołożył wszelkich starań, aby dane identyfikacyjne każdego z subskrybentów, umieszczane w bazach danych CERTUM, były zgodne z prawdą oraz, że informacja ta była aktualna w momencie ich potwierdzania,
- potwierdzane informacje subskrybenta, przesyłane następnie do urzędu certyfikacji w celu ich umieszczenia w certyfikacie są dokładne,
- nie przyczynił się w sposób zamierzony do powstania błędów lub niedokładności w informacji umieszczanej w certyfikacie,
- świadczone usługi są zgodne z powszechnie akceptowanymi normami (de jure i de facto): X.509, PKCS#10, PKCS#7 i PKCS#12,
- świadczone usługi realizowane są na podstawie procedur, które są dostosowane do zaleceń niniejszego Kodeksu Postępowania Certyfikacyjnego; w szczególności dotyczy to:
    - procedur weryfikacji tożsamości subskrybentów,
    - przeprowadzania **dowodu posiadania klucza prywatnego**[16], powiązanego z przedstawionym do certyfikacji kluczem publicznym,

[16] Patrz **Słownik pojęć**

- procedur przyjmowania od klientów, rozpatrywania i potwierdzania lub odrzucania wniosków o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie,
- procedur występowania do urzędu certyfikacji, na podstawie wcześniej zaakceptowanego wniosku subskrybenta, o wydanie certyfikatu, jego aktualizację, unieważnienie, zawieszenie lub odwieszenie; procedury te określają także okoliczności, w których urząd certyfikacji może samodzielnie występować z takimi wnioskami,
- procedur rejestrowania innych punktów rejestracji, z którymi CERTUM zawarło umowy (procedury te nie dotyczą Głównego Punktu Rejestracji),
- archiwizowania wniosków i informacji otrzymywanych od subskrybentów, wydanych decyzji oraz informacji przekazanych do urzędów certyfikacji,
- procedur generowania kluczy subskrybentom, o ile dopuszcza to umowa zawarta pomiędzy urzędem certyfikacji a subskrybentem,
- procedur personalizacji i wydawania elektronicznych kart kryptograficznych, na których zapisywane są certyfikaty oraz para kluczy (w przypadku wygenerowania jej przez punkt rejestracji),

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

Punkt rejestracji zobowiązuje się ponadto do:

- podporządkowania się zaleceniom CERTUM, zwłaszcza tym, które są wynikiem przeprowadzonego audytu,
- zapewnienia ochrony danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* z późn. zm. oraz dokumentami wykonawczymi do tej ustawy,
- ochrony kluczy prywatnych operatorów zgodnie z wymogami bezpieczeństwa określonymi szczegółowo w Kodeksie Postępowania Certyfikacyjnego;
- nieużywania kluczy prywatnych operatorów do innych celów niż te, które określono w niniejszym Kodeksie Postępowania Certyfikacyjnego, chyba że uzyska na to specjalną zgodę CERTUM,
- pozyskania **aktywnych**[17] certyfikatów kluczy publicznych i list CRL urzędów certyfikacji CERTUM z wiarygodnych źródeł oraz ich rzetelnej weryfikacji.

2.1.3. Zobowiązania subskrybenta końcowego

Poprzez złożenie w punkcie rejestracji wniosku o rejestrację oraz ręczne podpisanie potwierdzenia rejestracji lub zaakceptowanie certyfikatu (patrz rozdz. 4.3) subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w niniejszym dokumencie.

W zależności od wzajemnych relacji pomiędzy CERTUM a subskrybentem, a także od poziomu wiarygodności certyfikatu, o który występuje subskrybent, zobowiązania mogą być

[17] Patrz **Słownik pojęć**

wyrażone w postaci formalnej umowy lub mogą mieć charakter nieformalnego porozumienia pomiędzy subskrybentem a CERTUM.

Niezależnie od charakteru umowy subskrybent końcowy zobowiązany jest do:

- wyrażenia zgody na warunki określone w formalnej lub nieformalnej umowie pomiędzy subskrybentem a CERTUM; zgoda ta powinna mieć charakter podpisu odręcznego w przypadku umowy formalnej lub elektronicznego oświadczenia woli (umowa nieformalna) w chwili akceptacji danych do wydawanego certyfikatu; treść oświadczenia woli subskrybenta opublikowana jest w repozytorium,
- zaakceptowania (patrz 4.4) wydanego mu certyfikatu; gwarancje oraz odpowiedzialność CERTUM związane z danym certyfikatem rozpoczynają się z chwilą jego akceptacji,
- podjęcia takich środków ostrożności, które pozwolą na prawidłowe wygenerowanie (samodzielnie, punktowi rejestracji lub urzędowi certyfikacji) i bezpieczne przechowywanie klucza prywatnego z certyfikowanej pary kluczy, tzn. jego ochronę przed zgubieniem, ujawnieniem, modyfikacją oraz nieautoryzowanym użyciem,
- podawania prawdziwych danych we wnioskach przekazywanych do punktu rejestracji lub urzędu certyfikacji i umieszczanych następnie w bazach danych jednostki usługowej CERTUM oraz w wydawanych przez tę jednostkę certyfikatach klucza publicznego; jednocześnie subskrybent musi być świadom odpowiedzialności za szkody (bezpośrednie lub pośrednie) będące konsekwencją sfałszowania danych,
- sprawdzenia lub zapewnienia, że każdy podpis cyfrowy złożony przy pomocy należącego do niego klucza prywatnego, związanego z zaakceptowanym certyfikatem klucza publicznego jest jego podpisem i że certyfikat ten nie był przeterminowany (nie minął jego okres ważności) ani też unieważniony lub zawieszony w momencie składania podpisu,
- ogólnego zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz infrastruktury klucza publicznego (PKI).

Subskrybent końcowy zobowiązuje się ponadto:

- stosować się do zasad niniejszego Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji,
- okazać lub dostarczyć kopie wymaganych dokumentów, potwierdzających informacje zawarte w składanym wniosku oraz tożsamość wnioskodawcy lub podmiotu działającego z jego upoważnienia,
- w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie zawiadamiać o tym fakcie wystawcę certyfikatu lub dowolny punkt rejestracji, zarejestrowany przy CERTUM,
- wykorzystywać certyfikaty klucza publicznego oraz odpowiadające im klucze prywatne tylko zgodnie z deklarowanym w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w Kodeksie Postępowania Certyfikacyjnego (patrz rozdz. 1.4)
- do generowania kluczy kryptograficznych, zarządzania hasłami, kluczami publicznymi i prywatnymi oraz wymiany informacji z urzędami certyfikacji oraz punktami rejestracji używać tylko i wyłącznie oprogramowania rekomendowanego przez CERTUM; dostęp do tego oprogramowania oraz do nośników lub urządzeń na których przechowywane są klucze lub hasła powinien być należycie kontrolowany,

- traktować utratę lub ujawnienie (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,
- nie udostępniać innym osobom swoich kluczy prywatnych,
- nigdy jako subskrybent nie używać klucza prywatnego, powiązanego z certyfikatem wystawionym przez CERTUM do podpisywania jakichkolwiek certyfikatów lub list CRL,
- dostarczać do punktu rejestracji lub urzędu certyfikacji dowód posiadania klucza prywatnego lub w inny sposób dowieść fakt jego posiadania,
- pozyskiwać certyfikaty kluczy publicznych urzędów certyfikacji i punktów rejestracji oraz innych jednostek usługowych CERTUM.

2.1.4. Zobowiązania stron ufających

Przedmiotem umowy pomiędzy stroną ufającą a:

- Unizeto Technologies S.A. może być świadczenie przez tę jednostkę usług repozytoryjnych, usług znacznika czasu oraz usług weryfikacji statusu certyfikatów (OCSP),
- subskrybentem jest określenie warunków które musi spełnić podpis cyfrowy, aby być uznanym przez stronę ufającą za ważny lub określenie zasad świadczenia usług certyfikacyjnych.

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

Niezależnie od charakteru umowy strona ufająca zobowiązana jest do:

- akceptacji warunków określonych w Kodeksie Postępowania Certyfikacyjnego, Polityce Certyfikacji, Polityce Urzędu Znacznika czasu, itp. Strona ufająca akceptuje ww. warunki w chwili pierwszego odwołania się do dowolnej usługi świadczonej przez CERTUM lub pierwszego zaakceptowania podpisu subskrybenta. Gwarancje oraz odpowiedzialność CERTUM lub subskrybenta obowiązują od momentu akceptacji wydanego certyfikatu przez subskrybenta,
- **rzetelnej weryfikacji**[18] każdego podpisu cyfrowego umieszczonego na dokumencie który do niej dotrze; w celu zweryfikowania podpisu strona ufająca powinna:
    - określić **ścieżkę certyfikacji**[19], zawierającą wszystkie certyfikaty innych urzędów certyfikacji, które umożliwią wiarygodne przeprowadzenie weryfikacji podpisu na certyfikacie wystawcy podpisu,
    - sprawdzić, czy certyfikaty tworzące ścieżkę certyfikacji nie występują w repozytorium CERTUM na liście certyfikatów unieważnionych lub

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

[19] Patrz **Słownik pojęć**

zawieszonych; unieważnienie lub zawieszenie któregokolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony,

- sprawdzić, czy wszystkie certyfikaty należące do ścieżki certyfikacji należą do urzędów certyfikacji oraz czy nadano im prawo podpisywania innych certyfikatów,
- opcjonalnie określić datę oraz czas złożenia podpisu na wiadomości lub dokumencie. Jest to możliwe tylko w przypadku, gdy wiadomość lub dokument zostały przed podpisaniem opatrzone znacznikiem czasu, uzyskanym z urzędu znacznika czasu (TSA) lub też znacznik czasu został związany z podpisem cyfrowym już po jego umieszczeniu na dokumencie; tego typu weryfikacja umożliwi świadczenie usług niezaprzeczalności i rozstrzyganie ewentualnych sporów,
- korzystając ze zdefiniowanej ścieżki certyfikacji zweryfikować prawdziwość certyfikatu wystawcy podpisu na wiadomości lub dokumencie, a następnie prawidłowość samego podpisu na wiadomości lub dokumencie.

- właściwego i poprawnego realizowania operacji kryptograficzne przy użyciu oprogramowania i sprzętu, których poziom bezpieczeństwa jest zgodny z poziomem wrażliwości przetwarzanej informacji i poziomu wiarygodności stosowanych certyfikatów,
- uznania podpisu cyfrowego za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis cyfrowy jest ważny lub uzyskany wynik weryfikacji jest negatywny,
- zaufania tylko tym certyfikatom klucza publicznego:
  - które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca, np. w formie polityki podpisu (patrz rozdz. 1.4),
  - których status został zweryfikowany w oparciu o aktualne listy certyfikatów unieważnionych lub przy zastosowaniu usługi OCSP, udostępnianej przez CERTUM,
- określenia warunków, jakie musi spełniać certyfikat klucza publicznego oraz podpis cyfrowy, aby został uznany przez tą stronę za ważny; warunki te mogą zostać sformułowane np. w postaci odpowiedniej polityki podpisu i opublikowane.

Każdy dokument z wykrytą wadą w podpisie cyfrowym lub wynikłymi z niego wątpliwościami powinien zostać odrzucony, ewentualnie poddany innym procedurom wyjaśniającym jego ważność. Każdy, kto taki dokument zaakceptuje ponosi wszelkie związane z tym konsekwencje, niezależnie od szeroko akceptowanych cech podpisu cyfrowego, określających go jako skuteczny mechanizm weryfikacji tożsamości subskrybenta składającego podpis.

2.1.5. Zobowiązania repozytorium

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

- zagwarantowania, że wszystkie certyfikaty opublikowane w repozytorium należą do subskrybentów wskazanych w certyfikacie oraz że subskrybenci ci zaakceptowali certyfikat zgodnie z wymaganiami przedstawionymi w rozdz. 2.1.3 i rozdz. 4.4,
- terminowego publikowania i archiwizowania certyfikatów urzędów certyfikacji, punktów rejestracji, należących do domeny **certum** oraz certyfikatów subskrybentów, po uprzednim uzyskaniu na to ich zgody,
- publikowania i archiwizowania Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego oraz wzorów umów zawieranych z subskrybentami,
- udostępniania informacji o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL), serwer OCSP lub zapytania kierowane za pośrednictwem protokołu HTTP,
- zagwarantowania urzędom certyfikacji, punktom rejestracji, subskrybentom oraz stronom ufającym gwarancji, ciągłego dostępu do informacji zgromadzonej w repozytorium,
- szybkiego i zgodnego z okresami określonymi w niniejszym dokumencie publikowania list CRL oraz innej informacji,
- gwarancji bezpiecznego i kontrolowanego dostępu do informacji zawartych w repozytorium.

Wszyscy subskrybenci, poza stronami ufającymi, mają nieograniczony dostęp do wszystkich informacji zgromadzonych w repozytorium. Ograniczenia w dostępie stron ufających do repozytorium dotyczą zwykle certyfikatów subskrybentów.

2.2. Odpowiedzialność

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

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

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

2.2.1. Odpowiedzialność pośrednich urzędów certyfikacji

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

- są wynikiem udowodnionych błędów popełnionych przez CERTUM, zawłaszcza w zakresie niezgodności procesu weryfikacji tożsamości z deklarowanymi procedurami, niewłaściwej ochrony klucza prywatnego urzędów certyfikacji lub braku dostępu do świadczonych usług, np. do list certyfikatów unieważnionych,
- powstały wskutek naruszenia innych gwarancji CERTUM, określonych w rozdz. 2.1.1, 2.1.5 i 2.1.2.

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

- dane i dokumenty, które podał w urzędzie są prawdziwe i dokładne,
- zgadza się, że akceptacja certyfikatu jest równoznaczna z faktem, iż certyfikat nie zawiera żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty.

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

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

- za szkody powstałe wskutek działania siły wyższej: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,
- za szkody powstałe na skutek instalacji i użytkowania aplikacji oraz sprzętu stosowanego do generowania kluczy kryptograficznych, zarządzania nimi, szyfrowania oraz realizacji podpisu cyfrowego, które znajduje się na liście aplikacji nieakredytowanych (zastrzeżenie to dotyczy stron ufających) lub nie znajduje się na liście aplikacji akredytowanych (zastrzeżenie to dotyczy subskrybentów),
- za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonego oraz używanie niezgodnie z deklarowanym przeznaczeniem wynikającym z typu certyfikatu, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego,
- w przypadku braku potwierdzonej przez subskrybenta akceptacji certyfikatu i użycie takiego certyfikatu; całą odpowiedzialność ponosi subskrybent i powinna ona być ona określona w umowie pomiędzy subskrybentem a stroną ufającą,
- w przypadku podania przez subskrybenta fałszywych danych i umieszczenie ich na jego wniosek zarówno w bazach CERTUM, jak też w wydanym mu certyfikacie klucza publicznego.

W przypadku realizacji zamówień zbiorowych, odpowiedzialność za przedłożone dane, które zostaną umieszczone w certyfikatach, dystrybucję kluczy wewnątrz organizacji oraz zarządzanie certyfikatami klucza publicznego spoczywa na podmiocie występującym z wnioskiem o wydanie/odnowienie certyfikatów. Urząd certyfikacji zastrzega sobie również prawo do weryfikacji sposobów zarządzania certyfikatami klucza publicznego wewnątrz takiej organizacji.

2.2.2. Odpowiedzialność punktów rejestracji

Odpowiedzialność Głównego Punktu Rejestracji przenosi się automatycznie na CERTUM i wynika łącznie z gwarancji określonych w rozdz. 2.1.1, 2.1.2 i 2.1.5. Warunki tej odpowiedzialności regulują umowy zawarte przez CERTUM z subskrybentami.

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

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

2.2.3. Odpowiedzialność subskrybentów

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

2.2.4. Odpowiedzialność stron ufających

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz. 2.1.4. Warunki tej odpowiedzialności może regulować umowa zawarta z subskrybentem oraz z CERTUM.

Umowy z subskrybentami lub CERTUM wymagają aby strony ufające dysponowały wystarczającą ilością informacji umożliwiającą im podjęcie świadomej decyzji o akceptacji lub odrzuceniu podpisu cyfrowego w momencie jego przedłożenia.

Strony ufające powinny określić wysokość kwot transakcji, które będą przez nie akceptowane jedynie na podstawie informacji zawartych w certyfikacie oraz zapoznać się z informacjami, zawartymi w rozdz. 2.1.4 niniejszego dokumentu.

2.2.5. Odpowiedzialność repozytorium

Pełną odpowiedzialność za funkcjonowanie repozytorium i wynikłe z tego skutki ponosi CERTUM.

2.3. Odpowiedzialność finansowa

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

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

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

Tab.2.1 Maksymalne gwarancje finansowe

Nazwa polityki certyfikacji	Wysokość gwarancji
Certum Level I	0 zł
Certum Level II	400 zł
Certum Level III	20 000 zł
Certum Level IV	100 000 zł
Certum Partners	Określona w umowach

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

2.4. Akty prawne i rozstrzyganie sporów

2.4.1. Obowiązujące akty prawne

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

2.4.2. Postanowienia dodatkowe

2.4.2.1. Rozłączność postanowień

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

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

2.4.2.2. Ciągłość postanowień

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

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

Postanowienia umów lub Kodeksu Postępowania Certyfikacyjnego nie mogą być przenoszone na osoby trzecie.

2.4.2.3. Łączenie postanowień

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

- zostało to wyrażone w formie klauzuli w niniejszym dokumencie lub umowie,
- postanowienia, do których odwołuje się niniejszym dokumencie lub umowa mają formę pisemną.

2.4.2.4. Powiadamianie

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

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

Niektóre komunikaty i informacje muszą być przekazywane stronom zgodnie z wcześniej uzgodnionym harmonogramem lub odstępstwami od tego harmonogramu. Dotyczy to w szczególności publikowania list certyfikatów unieważnionych, publikowania nowych certyfikatów punktów rejestracji i urzędów certyfikacji, w taki sposób aby były one osiągalne cały czas dla wszystkich zainteresowanych stron, w tym strony ufającej. Wszelkie naruszenia bezpieczeństwa klucza prywatnego jednego z urzędów certyfikacyjnych powinny być publikowane, aby o tym fakcie mogły dowiedzieć się wszystkie zainteresowane strony.

2.4.3. Rozstrzyganie sporów

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

Spory bądź zażalenia powstałe na tle użytkowania certyfikatów, tokenów znacznika czasu lub poświadczeń weryfikacji statusu, wystawianych przez CERTUM będą rozstrzygane na

podstawie pisemnych informacji w drodze mediacji. Postępowanie ze skargami jest zastrzeżone do wyłącznego działania Prezesa Zarządu Unizeto Technologies S.A.. Podlegają one pisemnemu rozpatrzeniu w terminie do 10 dni.

W przypadku braku rozstrzygnięcia sporu w terminie 30 dni od rozpoczęcia postępowania pojednawczego, stronom przysługuje prawo do wystąpienia na drogę sądową. Sądem właściwym do rozpoznania sprawy będzie Sąd Powszechny właściwy dla pozwanego.

W przypadku wystąpienia innych sporów będących konsekwencją użycia certyfikatu wydanego lub innych kwalifikowanych usług świadczonych przez CERTUM, Subskrybent zobowiązuje się pisemnie poinformować CERTUM o przedmiocie powstałego sporu.

CERTUM rozstrzyga tylko spory z klientami (subskrybentami, punktami rejestracji, urzędami certyfikacji, stronami ufającymi, itp.) wynikłe z zawartych umów.

2.5. Opłaty

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

http://www.certum.pl

CERTUM stosuje cztery modele pobierania opłat za świadczone usługi:

- **sprzedaż detaliczną** – opłaty pobierane są oddzielnie za każdą jednostkę usługową, np. za każdy pojedynczy certyfikat lub mały pakiet certyfikatów,
- **sprzedaż hurtową** – opłaty pobierane są za pakiet usług, np. dużą liczbę certyfikatów sprzedanych jednorazowo.
- **sprzedaż abonamentową** – opłaty są pobierane raz w miesiącu; wysokość opłaty abonamentowej uzależniona jest od rodzaju i liczby jednostek usługowych i jest stosowana zwłaszcza w przypadku usługi znacznika czasu oraz weryfikacji statusu certyfikatu przy wykorzystaniu protokołu OCSP,
- **sprzedaż pośrednią** – opłata jest pobierana za każdą jednostkę usługową od klienta, który świadczy usługi zbudowane na bazie infrastruktury CERTUM; np. jeśli nowy komercyjny urząd certyfikacji otrzyma certyfikat od CERTUM, to CERTUM pobiera opłatę za każdy certyfikat wydany przez ten urząd.

Opłaty mogą być wnoszone przy pomocy przelewów bankowych lub bezpośrednich wpłat w kasach oddziałów Unizeto Technologies S.A., na podstawie faktury lub zamówienia.

2.5.1. Opłaty za wydanie lub recertyfikację

CERTUM pobiera opłaty za wydanie i recertyfikację[20].

Ze względu na odmienność procedur wydawania certyfikatu i recertyfikacji opłaty realizowane według jednego z czterech modeli wymienionych w rozdz. 2.5 można podzielić na trzy składowe: koszty identyfikacji i uwierzytelnienia lub szerzej koszty obsługi w punkcie rejestracji, koszty wytworzenia certyfikatu oraz koszty personalizacji i wydania kryptograficznej karty elektronicznej. Składniki te mogą tworzyć oddzielne pozycje w cenniku i być przydatne

[20] Patrz **Słownik pojęć**

zwłaszcza w przypadku recertyfikacji (można pominąć koszty identyfikacji i uwierzytelnienia subskrybenta oraz wydania karty).

2.5.2. Opłaty za dostęp do certyfikatów

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

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

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

2.5.3. Opłaty za unieważnienie i informacje o statusie certyfikatu

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

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

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

2.5.4. Inne opłaty

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

- generowania kluczy urzędom certyfikacji lub subskrybentom,
- testowania aplikacji i umieszczania jej na liście aplikacji rekomendowanych,
- sprzedaży licencji,
- realizacji prac projektowych, wdrożeniowych i instalacyjnych,
- sprzedaży Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji, podręczników, przewodników itp., wydanych w formie drukowanej,
- przeprowadzania audytów w punktach rejestracji i podległych urzędach,
- szkoleń.

2.5.5. Zwrot opłat

CERTUM dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. Jeśli jednak subskrybent lub strona ufająca nie są zadowoleni ze świadczonych usług, to mogą w ciągu 30 dni od wydania certyfikatu zażądać unieważnienia certyfikatu i zwrotu wniesionej opłaty. Po upływie 30 dni subskrybent może zażądać unieważnienia certyfikatu i zwrotu wniesionej opłaty jedynie w przypadku, gdy CERTUM nie wywiązuje się ze swoich zobowiązań oraz obowiązków określonych w niniejszym Kodeksie Postępowania Certyfikacyjnego.

Żądania o zwrot opłat należy kierować pod adres podany w rozdz. 1.5.

2.6. 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

Informacje te to:

- Polityka Certyfikacji,
- Kodeks Postępowania Certyfikacyjnego,
- wzory umów z subskrybentami,
- certyfikaty: urzędów certyfikacji **Certum CA**, **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV**, **Certum Partners**, innych urzędów certyfikacji, punktów rejestracji, certyfikaty subskrybentów,
- listy certyfikatów unieważnionych (CRL); listy certyfikatów unieważnionych dostępne są w tzw. punktach dystrybucji CRL, których adresy umieszczane są w każdym certyfikacie wydanym przez CERTUM; podstawowym punktem dystrybucji list CRL jest repozytorium http://crl.certum.pl,
- raporty z audytu dokonywanego przez upoważnioną instytucję (w możliwie szczegółowej postaci);
- informacje pomocnicze, np. ogłoszenia.

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

http://www.certum.pl

Certyfikaty poczty elektronicznej publikowane są dodatkowo za pośrednictwem serwisów usług katalogowych:

ldap://directory.certum.pl

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

2.6.2. Częstotliwość publikacji

Wymienione poniżej publikacje CERTUM są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego – patrz rozdz. 8;
- certyfikaty urzędów certyfikacji funkcjonujących w ramach CERTUM – każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- certyfikaty punktów rejestracji – każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- certyfikaty subskrybentów – za ich zgodą każdorazowo, gdy nastąpi emisja nowych certyfikatów;
- listy certyfikatów unieważnionych – patrz rozdz. 4.9.4 i 4.9.9;
- raporty z audytu dokonywanego przez upoważnioną instytucję – każdorazowo, po otrzymaniu go przez CERTUM;
- 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 są dostępne publicznie.

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

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

2.7. Audyt

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

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

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). W obu przypadkach audyt jest prowadzony na wniosek i pod nadzorem **inspektora bezpieczeństwa** (patrz rozdz. 5.2.1).

2.7.1. Częstotliwość audytu

Audyt (wewnętrzny i zewnętrzny) sprawdzający prawidłowość i zgodność z uregulowaniami proceduralnymi i prawnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) jest wykonywany przynajmniej raz do roku.

2.7.2. Tożsamość/kwalifikacje audytora

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

- zatrudniać pracowników, którzy posiadają odpowiednie udokumentowane przygotowanie techniczne w zakresie infrastruktury klucza publicznego (PKI), technik i narzędzi zabezpieczania informacji oraz prowadzenia audytów bezpieczeństwa,
- być zarejestrowaną organizacją lub stowarzyszeniem, dobrze znaną i posiadającą wysoką renomę pośród tego typu instytucji.

Audyt wewnętrzny realizowany jest przez odpowiednią jednostkę organizacyjną, funkcjonującą w strukturze Unizeto Technologies S.A.

2.7.3. Związek audytora z audytowaną jednostką

Patrz punkt 2.7.2

2.7.4. Zagadnienia obejmowane przez audyt

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

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

- zabezpieczenia fizyczne CERTUM,
- procedury weryfikacji tożsamości subskrybentów,
- usługi certyfikacyjne i procedury ich świadczenia,
- zabezpieczenia oprogramowania i dostępu do sieci,
- ochrona personelu CERTUM,
- rejestry systemowe i procedury monitorowania systemu,
- procedury sporządzania kopii zapasowych oraz ich odtwarzania.
- realizacja procedur archiwizacji,
- dokumentowanie zmian parametrów konfiguracyjnych CERTUM,
- dokumentowanie przeglądów i serwisu sprzętu oraz oprogramowania.

2.7.5. Podejmowane działania w celu usunięcia usterek wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są **inspektorowi bezpieczeństwa** CERTUM. Inspektor bezpieczeństwa zobowiązany jest w ciągu 14 dni od daty otrzymania raportów do przygotowania stanowiska wobec wszelkich uchybień wskazanych w raportach. Informacja o usunięciu usterek przekazywana jest instytucji audytującej.

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

2.7.6. Informowanie o wynikach audytu

Raport z audytu w możliwie szczegółowej postaci wraz z ogólną opinią instytucji audytującej o zgodności funkcjonowania CERTUM z wymaganiami określonymi w *WebTrust* po każdym audycie jest publikowany w repozytorium.

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 z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych* wraz z późniejszymi zmianami i aktami wykonawczymi.

Unizeto Technologies S.A. gwarantuje, że stronom trzecim udostępniane są tylko te informacje, które publicznie dostępne są w certyfikacie. Pozostałe dane spośród tych, które dostarczane są we wnioskach kierowanych do CERTUM nie zostaną nigdy, w żadnych okolicznościach, dobrowolnie lub świadomie ujawnione innym podmiotom, z wyjątkiem żądania ze strony władz państwowych i sądowych, mającego umocowanie w obowiązującym prawie.

CERTUM nie kopiuje ani nie przechowuje kluczy prywatnych subskrybentów, które służą do składania podpisów lub innych danych, które mogłyby służyć do ich odtworzenia.

2.8.1. Informacje, które muszą być traktowane jako tajemnica

Unizeto Technologies S.A. i osoby w niej zatrudnione, jak również podmioty za których pośrednictwem wykonywane są czynności certyfikacyjne, są obowiązane zachować w tajemnicy rozumianej jako tajemnica przedsiębiorstwa[21], w trakcie zatrudnienia oraz po jego zakończeniu. Informacje stanowiące tajemnicę przedsiębiorstwa regulowane są przez wewnętrzne zarządzenia firmy i dotyczą one w szczególności:

- informacji otrzymywanej od subskrybentów, z wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych; we wszystkich pozostałych przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub prawomocnego nakazu sądowego;
- informacji wpływającej od/do subskrybentów (m.in. treści umów z subskrybentami i stronami ufającymi, rozliczenia, wnioski o zarejestrowanie, wydanie, odnowienie lub unieważnienie certyfikatów; z wyjątkiem informacji umieszczonych w certyfikatach lub repozytorium, zgodnie z postanowieniami niniejszego Kodeksu Postępowania

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

Certyfikacyjnego); część z powyższych informacji może być udostępniana wyłącznie za zgodą i w zakresie pisemnie określonym przez jej właściciela (subskrybenta),

- zapisów transakcji systemowych (zarówno w całości, jak też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. logi transakcji systemowych);
- zapisów informacji o zdarzeniach (logi) związanych z usługami certyfikacyjnym i zachowywanymi przez CERTUM oraz punkty rejestracji;
- raportów kontroli wewnętrznej oraz zewnętrznej, o ile stanowić to może zagrożenie bezpieczeństwa CERTUM (zgodnie z rozdz. 2.8.2 większa część tych informacji powinna być publicznie dostępna);
- plany działań awaryjnych,
- informacje o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie, informacje o administrowaniu usługami certyfikacyjnymi oraz projektowanymi zasadami rejestrowania.

Unizeto Technologies S.A. obowiązuje zachowanie tajemnicy wobec strony umowy o świadczenie usług certyfikacyjnych. Osoby odpowiedzialne za zachowanie tajemnicy i zasad postępowania z informacjami ponoszą odpowiedzialność karną zgodnie z przepisami prawa.

2.8.2. Informacje, które mogą być traktowane jako jawne

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

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

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

- Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego,
- wzorce umów CERTUM z subskrybentami,
- cennik usług,
- poradniki dla użytkowników,
- certyfikaty urzędów certyfikacji, punktów rejestracji,
- certyfikaty subskrybentów, którzy wyrazili na to zgodę
- listy certyfikatów unieważnionych (CRL),
- wyciągi z raportów pokontrolnych, dokonywanych przez upoważnioną instytucję (w możliwie szczegółowej postaci).

Publikowane przez CERTUM wyciągi z raportów pokontrolnych dotyczą:

- zagadnień, jakie obejmował audyt,
- ogólnej oceny wystawionej przez instytucję wykonującą audyt,
- stopień realizacji zaleceń.

2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu

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

2.8.4. Udostępnianie informacji stanowiącej tajemnicę w przypadku nakazów sądowych

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

2.8.5. Udostępnianie informacji stanowiącej tajemnicę w celach naukowych

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

2.8.6. Udostępnianie informacji stanowiącej tajemnicę na żądanie właściciela

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

2.8.7. Inne okoliczności udostępniania informacji stanowiącej tajemnicę

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

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. CERTUM zobowiązuje się do umieszczania odpowiednich (wymaganych przez właścicieli) uwag w tej dziedzinie.

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

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

2.9.1. Znak towarowy

Unizeto Technologies S.A. posiada zastrzeżony znak towarowy składający się ze znaku graficznego oraz napisu stanowiących łącznie logo o następującej postaci:

Rys.3.1. Logo CERTUM

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

Znak CERTUM jest dodatkowym elementem logo każdego punktu rejestracji działającego z upoważnienia CERTUM. Zgoda na używanie logo CERTUM wydawana jest automatycznie w momencie rejestracji przez urząd nowego punktu rejestracji.

3.Identyfikacja i uwierzytelnianie

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

Procedura weryfikacji przeprowadzana jest **obligatoryjnie** zawsze w fazie rejestracji subskrybenta oraz **na żądanie** CERTUM w przypadku każdej innej usługi certyfikacyjnej.

3.1. Rejestracja początkowa

Rejestracja subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składający wniosek o rejestrację nie posiada żadnego **ważnego certyfikatu**[22] wydanego przez dowolny z urzędów wydających certyfikaty, afiliowanych przy CERTUM.

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

Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po pomyślnym zweryfikowaniu dostarczonych danych subskrybent zostaje wpisany na listę uprawnionych użytkowników usług CERTUM i zaopatrzony w żądany certyfikat klucza publicznego.

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

- zdalnie, na stronie WWW CERTUM wypełnić formularz rejestracyjny lub dostarczyć dane niezbędne do wydania certyfikatu (np. w postaci Zamówienia),
- wygenerować parę kluczy asymetrycznych RSA lub DSA i dostarczyć urzędowi rejestracji dowód posiadania klucza prywatnego (patrz rozdz. 3.1.6); opcjonalnie subskrybent może zlecić wygenerowanie pary kluczy urzędowi certyfikacji lub punktowi rejestracji,
- zaproponować nazwę wyróżniającą (**DN**, patrz rozdz. 3.1.1);
- opcjonalnie stawić się (jeśli jest to wymagane przez daną politykę certyfikacji, według której wydawany jest certyfikat będący przedmiotem wniosku) wraz z wymaganymi dokumentami we wskazanym punkcie rejestracji,
- opcjonalnie (w zależności od typu certyfikatu) zawrzeć umowę z Unizeto Technologies S.A. na świadczenie usług przez CERTUM.

[22] Patrz **Słownik pojęć**

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

3.1.1. Typy nazw

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

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

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

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

Tab.3.1 Wymagania nakładane na nazwę podmiotu certyfikatu

Nazwa polityki certyfikacji	Wymagania
Certum Level I	Niepusta wartość pola subject lub pusta w przypadku, gdy występuje pole alternatywnej nazwy podmiotu (SubjectAltName) i jest zaznaczone jako niekrytyczne[23].
Certum Level II	Niepusta wartość pola subject i opcjonalnie pole alternatywnej nazwy podmiotu (SubjectAltName) w przypadku, gdy jest zaznaczone jako niekrytyczne.
Certum Level III	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.
Certum Level IV	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.
Certum Partners	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.

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

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

3.1.2. Konieczność używania nazw znaczących

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

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

Nazwa DN może składać się z następujących pól (opis pola poprzedzano jego skróconą nazwą przyjętą za zaleceniem RFC 3280 i X.520):

- **pola C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),
- **pola ST** – region/województwo, na którego terenie działa lub mieszka subskrybent,
- **pola L** – miasto, w którym ma siedzibę lub mieszka subskrybent,
- **pola CN** – nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje subskrybent, jeśli w nazwie DN wystąpiły pola O lub OU (patrz niżej); w polu tym może być podana także nazwa produktu lub urządzenia,
- **pola O** – nazwa podmiotu w imieniu którego występuje subskrybent lub dodatkowa nazwa wyróżniająca,
- **pola OU** – nazwa jednostki organizacyjnej podmiotu w imieniu którego występuje subskrybent lub dodatkowa nazwa wyróżniająca,
- **pola E** – adres email subskrybenta,
- **pola UN** – nazwa routera lub urządzenia sieciowego,
- **pola D** – dodatkowa nazwa wyróżniająca subskrybenta.

Nazwa subskrybenta DN musi być zatwierdzona przez operatora punktu rejestracji oraz zaakceptowana przez urząd certyfikacji.

3.1.3. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez CERTUM w wydawanych przez siebie certyfikatach jest zgodna z profilem certyfikatów opisanym w rozdziale 7 niniejszego Kodeksu. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz. 3.1.2 niniejszego dokumentu.

3.1.4. Unikalność nazw

Nazwa DN subskrybenta jest proponowana przez samego subskrybenta. Jeśli nazwa ta jest zgodna z ogólnymi wymaganiami określonymi w rozdz. 3.1.1 i 3.1.2 to zgłoszona propozycja jest wstępnie akceptowana.

W celu zapewnienia unikalności certyfikatów, CERTUM dla każdego wydanego certyfikatu przyznaje unikalny (w domenie CERTUM) numer seryjny. Stanowi on wyróżnik certyfikatu, który wraz z nazwą wyróżnioną DN precyzyjnie i unikalnie określa właściwego subskrybenta.

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

3.1.5. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

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

W przypadku powstania sporu na tle reklamacji nazw CERTUM rezerwuje sobie prawo do odrzucenia wniosku subskrybenta lub jego zawieszenia, bez ponoszenia jakiejkolwiek odpowiedzialności z tego tytułu. CERTUM rezerwuje sobie także prawo do podejmowania wszelkich decyzji dotyczących składni nazwy subskrybenta i przydzielania mu wynikłych z tego nazw.

3.1.6. Dowód posiadania klucza prywatnego

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

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

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

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

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

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

Klucze prywatne powinny być generowane wewnątrz tokena (np. kryptograficznej karcie elektronicznej). Dowolny podmiot może być w posiadaniu tokena już w momencie generowania, jak również zapisywania na nim kluczy lub też token ten jest mu dostarczony dopiero po

wygenerowaniu kluczy[24]. W ostatnim przypadku CERTUM musi zagwarantować bezpieczne dostarczenie tokena wraz z kluczem do podmiotu, dla którego jest przeznaczony (patrz rozdz. 6.1.2).

3.1.7. Uwierzytelnienie tożsamości osób prawnych

Punkt rejestracji zobowiązany jest do zażądania od wnioskodawcy przedstawienia odpowiednich dokumentów, które w sposób niebudzący wątpliwości potwierdzą tożsamość instytucji w imieniu której składany jest wniosek oraz osoby, która ją reprezentuje (lub składa wniosek). Punkt rejestracji może również dane służące potwierdzeniu tożsamości zdobyć samodzielnie, np. poprzez użycie publicznie dostępnych źródeł informacji. Uwierzytelnienie tożsamości osoby prawnej musi spełniać dwa cele. Po pierwsze należy wykazać, że w momencie rozpatrywania wniosku podana we wniosku osoba prawna istniała, po drugie, należy dowieść, że osoba fizyczna, która wystąpiła z wnioskiem o wydanie certyfikatu lub go odbiera jest upoważniona przez tę osobę prawną do reprezentowania jej interesów. Dostarczone dokumenty (lub zebrane informacje) powinny potwierdzić:

- tożsamość subskrybenta certyfikatu lub administratora certyfikatu (w przypadku certyfikatów wydawanych dla osób prawnych lub urządzeń)
- istnienie jednostki lub osoby prawnej,
- prawo subskrybenta lub administratora do występowania w imieniu jednostki lub osoby prawnej.

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

Szczegółowe wymagania dotyczące dokumentów oraz potwierdzania danych opisano w osobnym dokumencie – Instrukcji weryfikacji tożsamości.

Punkt rejestracji zobligowany jest do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku.

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

- przydziela osobie prawnej nazwę wyróżnioną DN lub akceptuje jej postać zaproponowaną w złożonym wniosku,
- wystawia **token**, który poświadcza prawdziwość danych zawartych w rozpatrywanym wniosku i wysyła go do urzędu certyfikacji,
- rejestruje wszystkie dokumentów i zaświadczenia (lub informację o użytym źródle publicznym), na podstawie których operator weryfikował tożsamość osoby prawnej oraz działającego w jego imieniu uprawnionego przedstawiciela,

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

- (opcjonalnie) w imieniu urzędu certyfikacji zawiera z osobą prawną umowę na świadczenie usług certyfikacyjnych; umowa taka może być zawierana zarówno w przypadku występowania osoby prawnej w charakterze subskrybenta, punktu rejestracji, urzędu certyfikacji, jak też w charakterze podmiotu świadczącego dodatkowe usługi certyfikacyjne.

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

- tożsamości operatora punktu rejestracji, weryfikującego tożsamość subskrybenta,
- złożenia przez operatora oświadczenia, że tożsamość wnioskodawcy zweryfikował zgodnie z wymaganiami niniejszego Kodeksu Postępowania Certyfikacyjnego,
- daty weryfikacji,
- identyfikatora operatora oraz wnioskodawcy w przypadku jego osobistego pobytu w punkcie rejestracji i wcześniejszego przypisania mu takiego identyfikatora.

Jeśli osoba prawna nie jest w stanie w dostateczny sposób uwierzytelnić swojego wniosku lub zażąda tego urząd certyfikacji, to wtedy upoważniony przedstawiciel tej osoby musi osobiście stawić się w punkcie rejestracji i potwierdzić wniosek.

W przypadku, gdy podmiot posiada już zarejestrowane w CERTUM certyfikaty, które podlegały już procedurze weryfikacji wymaganej dla wydania certyfikatu danej klasy, weryfikacja może być oparta na tychże danych i dokumentach.

3.1.8. Uwierzytelnienie tożsamości osób fizycznych

Uwierzytelnienie tożsamości osoby fizycznej musi spełniać dwa cele. Po pierwsze musi wykazać, że podane we wniosku dane odnoszą się do istniejącej osoby fizycznej i po drugie, że wnioskodawca jest rzeczywiście tą osobą fizyczną, która została wymieniona we wniosku. Procedury i wymagania dla uwierzytelniania tożsamości osób fizycznych są analogiczne jak w przypadku uwierzytelnienia tożsamości osób prawnych. Nie potwierdza się jednak istnienia jednostki prawnej i prawa do występowania w jej imieniu a jedynie prawo do posługiwania się danymi wyróżniającymi innymi niż imię i nazwisko.

3.1.9. Uwierzytelnienie pochodzenia urządzeń

Uwierzytelnienie w przypadku certyfikatów dla urządzeń przebiega analogicznie jak w przypadku uwierzytelnienia tożsamości osób prawnych. Dodatkowo, w przypadku certyfikatów dla urządzeń sieciowych, operator PR może sprawdzić – w przypadkach budzących wątpliwość – rejestrację domeny w publicznie dostępnych serwisach WHOIS.

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

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

- wniosek został uwierzytelniony jedynie przy pomocy hasła,

- modyfikacji uległy dane zawarte w wystawionym certyfikacie,
- na każde żądanie operatora urzędu certyfikacji,
- gdy dotyczy certyfikacji kluczy, której wynikiem ma być certyfikat wydany po raz pierwszy danemu subskrybentowi według nowej polityki certyfikacji.

Subskrybenci przesyłający wnioski bezpośrednio do urzędu certyfikacji są uwierzytelniani przez ten urząd na podstawie autentyczności podpisu cyfrowego i związanego z nim certyfikatu klucza publicznego lub przy pomocy innych metod, które zostały z nimi wcześniej uzgodnione i są zgodne z niniejszym dokumentem.

3.2.1. Aktualizacja kluczy

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

Weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest na podstawie dokumentów dostarczonych do aktualizowanego (odnawianego) certyfikatu. Szczegółowe wymagania określono w osobnym dokumencie – Instrukcji weryfikacji tożsamości.

3.2.2. Recertyfikacja

Subskrybenci lub urzędy certyfikacji korzystają z recertyfikacji w przypadku, gdy posiadają już certyfikat i komplementarny z nim klucz prywatny, i chcą nadal korzystać z tej samej pary kluczy. Nowy certyfikat utworzony w wyniku recertyfikacji posiada ten sam klucz publiczny, tą samą nazwę podmiotu certyfikatu oraz inne informacje z poprzedniego certyfikatu, ale nowy okres ważności, numer seryjny i nowy podpis wystawcy certyfikatu (szczegóły patrz rozdz. 4.6).

Recertyfikacji podlegają tylko te certyfikaty które nie zostały unieważnione oraz zmianie nie uległa nazwa i inne atrybuty podmiotu certyfikatu.

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

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

3.2.3. Modyfikacja certyfikatu

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

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

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

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku aktualizacji kluczy po unieważnieniu

Jeśli subskrybent w wyniku unieważnienia certyfikatu nie posiada aktywnego w ramach danej polityki certyfikacji klucza podpisującego, a następnie złoży wniosek o aktualizację, to wniosek ten musi uzyskać potwierdzenie wystawione przez operatora punktu rejestracji lub operatora Centrum Certyfikacji. Identyfikacja i uwierzytelnienie subskrybenta może przebiegać analogicznie jak w przypadku rejestracji początkowej (patrz rozdz. 3.1) lub może być oparty na uprzednio dostarczonych dokumentach.

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

3.4. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

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

W przypadku pierwszej z dróg postępowania subskrybent musi złożyć uwierzytelniony wniosek o unieważnienie certyfikatu. Uwierzytelnienie wniosku przez subskrybenta polega na złożeniu pod nim podpisu cyfrowego lub podaniu uzgodnionego wcześniej hasła na witrynie WWW.

Procedurze postępowania za pośrednictwem punktu rejestracji powinien poddać się subskrybent, który jednocześnie zgubił (został mu skradziony, itp.) aktywny klucz prywatny oraz sekret unieważniania certyfikatów. Wniosek o unieważnienie musi zostać poświadczony przez punkt rejestracji lub operatora CERTUM. Poświadczenie to nie musi mieć postaci elektronicznej.

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

Identyfikacja i uwierzytelnienie subskrybenta w punkcie rejestracji przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz. 3.1) lub tak jak w przypadku aktualizacji kluczy (patrz rozdz. 3.2.1). Uwierzytelnienie subskrybenta w urzędzie certyfikacji polega na zweryfikowaniu autentyczności wniosku lub osoby występującej z żądaniem unieważnienia certyfikatu.

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

4.Wymagania funkcjonalne

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

CERTUM udostępnia następujące podstawowe usługi: rejestracja, certyfikacja, recertyfikacja, aktualizacja kluczy, modyfikacja certyfikatu oraz unieważnienie certyfikatu.

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

Wniosek w miejsce klucza publicznego może zawierać żądanie subskrybenta wygenerowania w jego imieniu pary kluczy asymetrycznych. Może to być realizowane w punkcie rejestracji lub urzędzie certyfikacji. Po wygenerowaniu klucze są w sposób bezpieczny przekazywane subskrybentowi.

4.1. Składanie wniosków

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

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

Wnioski dostarczane są za pośrednictwem protokołów sieciowych takich jak: HTTP, S/MIME lub TCP/IP lub w postaci nieelktronicznej – np. Zamówień (dotyczy jedynie przypadków, gdy certyfikaty wydawane są na kartach kryptograficznych) .

CERTUM wydaje certyfikaty na podstawie złożonego żądania o rejestrację, recertyfikację, aktualizację kluczy lub modyfikację certyfikatu.

4.1.1. Wniosek o rejestrację

Wniosek o rejestrację składany jest pośrednio w punkcie rejestracji lub bezpośrednio w urzędzie certyfikacji i powinien zawierać informacje przedstawione poniżej:

- nazwa pełna instytucji lub nazwisko i imię subskrybenta lub administratora,

- nazwę wyróżnioną DN,
- identyfikatory NIP lub REGON/PESEL,
- adres siedziby lub adres zamieszkania subskrybenta (województwo, kod pocztowy, miejscowość, gmina, powiat, ulica, nr domu, nr lokalu, numer faksu),
- wnioskowany typ certyfikatu,
- identyfikator polityki certyfikacji, według której ma zostać wystawiony certyfikat,
- adres poczty elektronicznej (e-mail),
- klucz publiczny, który ma być poddany certyfikacji.

W zależności od zawartości certyfikatu oraz jego klasy, niektóre z wymienionych powyżej danych mogą być opcjonalne.

Po uwierzytelnieniu tożsamości subskrybenta (patrz rozdz. 3.1.7, 3.1.8 i 3.1.9) składającego wniosek o rejestrację oraz otrzymaniu potwierdzenia wystawionego przez punkt rejestracji wniosek jest przesyłany do urzędu certyfikacji.

4.1.2. Wniosek o recertyfikację, aktualizację kluczy, certyfikację lub modyfikację certyfikatu

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

- bezpośrednio po unieważnieniu jakiegokolwiek certyfikatu,
- ubieganiu się o certyfikat, który ma być wystawiany zgodnie z inną polityką certyfikacji niż certyfikaty będące aktualnie w posiadaniu subskrybenta,
- na wyraźne żądanie operatora urzędu certyfikacji.

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

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

- nazwę wyróżnioną DN wnioskodawcy (subskrybenta),
- wnioskowany typ certyfikatu,
- identyfikator polityki certyfikacji według której ma zostać wystawiony certyfikat,
- klucz publiczny (poprzednio używany w przypadku recertyfikacji i modyfikacji certyfikatu lub nowy w przypadku aktualizacji kluczy), który ma być poddany certyfikacji.

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

Po uwierzytelnieniu tożsamości subskrybenta (patrz rozdz. 3.1.7, 3.1.8 i 3.1.9) składającego wniosek o rejestrację oraz otrzymaniu potwierdzenia wystawionego przez punkt rejestracji wniosek jest przesyłany do urzędu certyfikacji.

4.1.3. Wniosek o unieważnienie lub zawieszenie

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

- braku aktualnie ważnego klucza prywatnego do realizacji podpisu cyfrowego,
- na wyraźne żądanie operatora urzędu certyfikacji.

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

Informacje podawane w elektronicznym wniosku o unieważnienie lub zawieszenie certyfikatu:

- nazwa wyróżniona DN wnioskodawcy (subskrybenta),
- lista certyfikatów do unieważnienia lub zawieszenia, zawierająca pary: numer seryjny certyfikatu, przyczyna unieważnienia.

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

Wniosek o unieważnienie może być przekazany w postaci elektronicznej z uwierzytelnieniem, w postaci papierowej (faks, list, itp.) lub ustnej (telefon). Szczegółowe wymagania w tym zakresie prezentowane są w dokumencie Instrukcji weryfikacji tożsamości.

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

4.2. Przetwarzanie wniosków

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

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

Złożenie wniosku w trybie *off-line* wymaga osobistego stawienia się subskrybenta, uprawnionego przedstawiciela organizacji w punkcie rejestracji lub urzędzie certyfikacji, przedstawiciela urzędu certyfikacji w siedzibie subskrybenta lub dostarczenia wierzytelnych danych służących do uzyskania certyfikatu do przedstawiciela CERTUM. Uwierzytelnienie wykonywane jest zgodnie z zasadami opisanymi w dokumencie Instrukcja weryfikacji tożsamości. Dla wniosków złożonych w trybie *off-line* CERTUM może utworzyć dedykowane procesy uzyskiwana certyfikatów lub wydać certyfikaty na kartach kryptograficznych.

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

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

- **skrzynki poświadczania żądań**, jeśli wniosek wymaga wystawienia potwierdzenia przez punkt rejestracji,
- **skrzynki żądań**, jeśli wniosek nie wymaga wystawienia potwierdzenia przez punkt rejestracji.

Obie skrzynki są pod pełną kontrolą urzędu certyfikacji.

Wnioski przetwarzane na podstawie zgłoszeń w trybie *off-line*, po ich pozytywnym zweryfikowaniu przez operatora punktu rejestracji lub operatora certyfikacji, przekazywane są najczęściej do **skrzynki żądań**.

4.2.1. Przetwarzanie wniosków w punkcie rejestracji

Każdy wniosek, który został skierowany do skrzynki poświadczania żądań lub złożony w punkcie rejestracji w postaci papierowej przetwarzany jest następująco:

- operator urzędu pobiera wniosek subskrybenta (papierowy lub elektroniczny ze skrzynki poświadczania żądań),
- weryfikuje zawarte w nim dane, m.in. dane osobowe subskrybenta (patrz procedura identyfikacji i uwierzytelnienia subskrybenta opisana w rozdz. 3.1.8) oraz jeśli występuje, to sprawdza także dowód posiadania klucza prywatnego (rozdz. 3.1.6),
- jeśli weryfikacja wniosku przebiegnie pozytywnie, to operator poświadcza (podpisuje) żądanie; jeśli oryginalny wniosek zawiera błędne dane, to wniosek jest odrzucany,
- poświadczony wniosek przesyłany jest do skrzynki żądań urzędu certyfikacji,
- w punkcie rejestracji mogą być weryfikowane także inne dane, które nie wchodzą w skład wniosku, a które wymagane są przez CERTUM do prowadzenia działalności biznesowej.

4.2.2. Przetwarzanie wniosków w urzędzie certyfikacji

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

- wiąże wniosek z bazą danych zarejestrowanych subskrybentów,
- weryfikuje uwierzytelnienia wniosku (podpis cyfrowy lub kod uwierzytelniający),
- weryfikuje formalną poprawność wniosku (składni i zawartości),
- sprawdza czy subskrybent jest uprawniony do wystawienia przysłanego typu wniosku oraz zawartej w nim treści,
- wszystkie czynności odnotowuje w bazie danych i rejestrach czynności.

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

4.3. Wydanie certyfikatu

Urząd certyfikacji, po otrzymaniu odpowiedniego wniosku oraz po pomyślnym przetworzeniu go (patrz rozdz. 4.2) **wydaje certyfikat**. Certyfikat uważa się za ważny (o statusie aktywny lub gotowy) od momentu zaakceptowania go przez subskrybenta (patrz rozdz. 4.4). Okresy ważności wydawanego certyfikatu zależą od typu certyfikatu oraz kategorii subskrybenta i są zgodne z okresami podanymi w Tab.6.6.

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

- przetworzony wniosek subskrybenta przesyłany jest na serwer wystawiania certyfikatów,
- jeśli wniosek zawiera żądanie wygenerowania pary kluczy, to serwer zleca to zadanie sprzętowemu generatorowi kluczy spełniającemu wymagania minimum FIPS-140 Level 2,
- testowana jest jakość dostarczonych lub wygenerowanych przez urząd certyfikacji kluczy publicznych,
- w przypadku pomyślnego zakończenia wszystkich procedur, serwer wystawia certyfikat i zleca jego podpisanie sprzętowemu modułowi kryptograficznemu; certyfikat zapisywany jest w bazach danych urzędu certyfikacji,
- urząd certyfikacji przygotowuje odpowiedź, zawierającą wydany certyfikat (jeśli został wystawiony) i wysyła go subskrybentowi; certyfikat nie jest publikowany w repozytorium (nawet, jeśli subskrybent wyraził na to zgodę) do czasu otrzymania od subskrybenta potwierdzenia akceptacji certyfikatu w formie jawnej lub domniemanej (rozdz. 4.4).

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

Drugi z mechanizmów polega na wydaniu certyfikatu i po zapisaniu go (zwykle tam, gdzie znajduje się klucz prywatny) na kryptograficznej karcie elektronicznej i przesłaniu pocztą na adres subskrybenta (PIN przesyłany jest w oddzielnej kopercie).

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

CERTUM publikuje certyfikat w repozytorium dopiero po zaakceptowaniu certyfikatu przez subskrybenta (patrz rozdz. 4.4).

4.3.1. Okres oczekiwania na wydanie certyfikatu

Urząd certyfikacji powinien dołożyć wszelkich starań, aby od momentu otrzymania wniosku o rejestrację i certyfikację, certyfikację lub aktualizację (kluczy lub certyfikatu)

przeprowadzić jego weryfikację oraz wydać certyfikat w czasie nie dłuższym niż ten, który podano w Tab.4.1.

Tab.4.1 Maksymalne okresy oczekiwania na wydanie certyfikatu

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

Podane okresy zależą głównie od kompletności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy CERTUM a wnioskodawcą.

4.3.2. Odmowa wydania certyfikatu

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

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

- subskrybent nie jest w stanie udowodnić swojego prawa do posługiwania się proponowanym identyfikatorem (nazwa **DN**),
- istnieje podejrzenie lub pewność, że subskrybent sfałszował lub podał nieprawdziwe dane,
- subskrybent w sposób szczególnie uciążliwy dla CERTUM angażuje jego zasoby oraz moce obliczeniowe, np. wysyłając zbyt dużą jak na jego potrzeby liczbę wniosków,
- z innych nie wymienionych powyżej przyczyn.

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

4.4. Akceptacja certyfikatu

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

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

- podanie PIN-u, dzięki któremu następuje instalacja certyfikatu za pośrednictwem strony WWW (https://www.certum.pl),
- brak w tym okresie unieważnienia certyfikatu.

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

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

Akceptacja certyfikatu jest także jednoznaczna z oświadczeniem subskrybenta, że zanim użył certyfikatu w dowolnej operacji kryptograficznej, dokładnie zapoznał się z zasadami wydawania certyfikatów, opisanych w niniejszym dokumencie.

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

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

4.5. Stosowanie kluczy oraz certyfikatów

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

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

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

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**),
- tylko po zweryfikowaniu ich statusu (patrz rozdz. 4.9) oraz wiarygodności podpisu urzędu certyfikacji, który wystawił certyfikat,
- w przypadku klucza publicznego do wymiany kluczy, szyfrowania danych lub uzgadniania kluczy tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu strona ufająca także nie może używać tego typu kluczy publicznych.

4.6. Recertyfikacja

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

4.7. Certyfikacja i aktualizacja kluczy

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

- **certyfikacja kluczy** nie jest związana z żadnym ważnym certyfikatem i jest stosowna przez subskrybentów wtedy, gdy zachodzi potrzeba uzyskania jednego lub więcej (zwykle dodatkowych) certyfikatów dowolnego typu, niekoniecznie wystawionych w ramach tej samej polityki certyfikacji,
- **aktualizacja kluczy** dotyczy zawsze ściśle określonego, wskazanego we wniosku certyfikatu; z tego powodu nowy certyfikat posiada identyczną treść jak związany z nim certyfikat; jedyne różnice to: nowy klucz publiczny, nowy numer seryjny certyfikatu, nowy okres ważności certyfikatu oraz nowy podpis urzędu certyfikacji; aktualizacja kluczy może również nosić nazwę odnowienia certyfikatu.

Wniosek o aktualizację kluczy złożony przez subskrybenta może dotyczyć tylko:

- certyfikatu, który nie został wcześniej unieważniony,

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

- nie posiada aktualnego i ważnego klucza prywatnego do realizacji podpisów;
- chce uzyskać dodatkowy certyfikat tego samego lub innego typu, ale tylko w ramach polityki certyfikacji, zgodnie z którą został mu wydany przynajmniej jeden certyfikat;
- subskrybent nie posiada żadnego ważnego certyfikatu wystawionego według jednej z polityk zdefiniowanych w niniejszym Kodeksie Postępowania Certyfikacyjnego.

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

Uwierzytelnienie wniosków o aktualizację kluczy i certyfikację realizowane jest w zgodnie z zasadami opisanymi w dokumencie Instrukcja weryfikacji tożsamości.

Procedura przetwarzania wniosku o aktualizację certyfikatu i certyfikację jest zgodna z procedurami opisanymi w rozdz. 4.2 i 4.3. W wyniku realizacji tej ostatniej procedury:

- subskrybent jest powiadamiany o wystawieniu nowego certyfikatu o nowym numerze seryjnym,
- subskrybent powinien przesłać urzędowi certyfikacji uwierzytelnione potwierdzenie akceptacji certyfikatu,
- nowy certyfikat jest publikowany w repozytorium.

Procedurze certyfikacji i aktualizacji klucza mogą podlegać także certyfikaty urzędów certyfikacji.

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

4.8. Modyfikacja certyfikatu

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

Modyfikacja certyfikatu:

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

Modyfikacja certyfikatu traktowana jest i przetwarzana analogicznie jak aktualizacja kluczy (odnowienie), w przypadku gdy zmianie ulegają dane o mniejszym poziomie wrażliwości, np.:

- adres email
- adres subskrybenta

lub jak certyfikacja kluczy, w przypadku gdy zmianie ulegają dane o wyższym poziomie wrażliwości.

Jeśli procedura modyfikacji certyfikatu zakończy się pomyślnie, to certyfikat który był przedmiotem modyfikacji może zostać unieważniony i umieszczany na liście CRL. Jako przyczynę unieważnienia podaje się określenie ***modyfikacja***[25] *(ang. affiliationChanged) oznaczające, że (1) unieważniony certyfikat został zastąpiony innym, w którym zostały zmodyfikowane niektóre dane, np. nazwa subskrybenta, oraz (2) informujące strony ufające, że nie ma powodów, aby uważać, iż klucz prywatny związany z certyfikatem został ujawniony.*

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

4.9. Unieważnienie i zawieszenie certyfikatu

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

Zawieszenie certyfikatów dokonywane jest jedynie w zamkniętych systemach korporacyjnych afiliowanych przy CERTUM.

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

---

[25] W tym przypadku domyślnie chodzi o zastąpienie certyfikatu

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

Niniejszy rozdział określa warunki, które muszą być spełnione lub zaistnieć, aby urząd certyfikacji miał podstawy do unieważnienia lub zawieszenia certyfikatu. Mimo, iż zawieszenie certyfikatu jest szczególną formą unieważnienia, dalej będziemy rozróżniać te dwa pojęcia dla podkreślenia istotnej różnicy pomiędzy nimi: zawieszenie certyfikatu można anulować, unieważnienie - nie.

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

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

4.9.1. Okoliczności unieważnienia certyfikatu

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

Unieważnianie certyfikatu może mieć miejsce w następujących okolicznościach:

- gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się,
- ilekroć klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub nośnik na którym jest przechowywany jest lub istnieje uzasadnione podejrzenie, że będzie ujawniony[26]; procedura unieważniania certyfikatu jest wówczas przeprowadzana na wniosek subskrybenta,
- subskrybent rezygnuje z umowy zawartej z Unizeto Technologies S.A. (wówczas operacja ta jest ściśle związana z unieważnieniem rejestracji subskrybenta w punkcie rejestracji); jeśli subskrybent nie wystąpi z takim wnioskiem sam, prawo takie przysługuje urzędowi certyfikacji lub przedstawicielowi instytucji, której pracownikiem jest subskrybent,
- na każde żądanie subskrybenta wskazanego w certyfikacie,
- przez wystawcę certyfikatu, tzn. przez CERTUM, np. wskutek nieprzestrzegania przez subskrybenta zaakceptowanej Polityki Certyfikacji lub postanowień innych dokumentów sygnowanych przez urząd certyfikacji,

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

- w przypadku zakończenia działalności przez urząd certyfikacji unieważnia się wszystkie certyfikaty wydane przez ten urząd przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego urzędu certyfikacji,
- subskrybent nie wywiązuje się z zobowiązań płatniczych za usługi świadczone przez urząd certyfikacji, lub innych zobowiązań które podjął na rzecz CERTUM,
- klucz prywatny lub bezpieczeństwo systemu komputerowego urzędu certyfikacji zostały ujawnione w sposób, który bezpośrednio zagraża wiarygodności certyfikatów,
- subskrybent, będący pracownikiem organizacji, po rozwiązaniu z nim umowy o pracę nie oddał kryptograficznej karty elektronicznej, na której przechowywany był certyfikat i komplementarny z nim klucz prywatny,
- inne przyczyny opóźniających lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałych wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

Z wnioskiem o unieważnienie można występować (patrz rozdz. 3.4) za pośrednictwem punktu rejestracji (wymaga to skontaktowania się subskrybenta z punktem rejestracji) lub bezpośrednio do urzędu certyfikacji (wniosek może być uwierzytelniony przy pomocy podpisu). W pierwszym przypadku podpisany przez punkt rejestracji wniosek o unieważnienie certyfikatu lub dokument papierowy odsyłany jest do urzędu certyfikacji, w drugim zaś – subskrybent sam uwierzytelnia wniosek o unieważnienie i bezpośrednio wysyła go do urzędu certyfikacji.

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

4.9.2. Kto może żądać unieważnienia certyfikatu

Następujące podmioty mogą zgłaszać żądanie unieważnienia certyfikatu subskrybenta:

- subskrybent będący podmiotem unieważnianego certyfikatu,
- autoryzowany przedstawiciel urzędu certyfikacji (w przypadku CERTUM rolę taką pełni inspektor bezpieczeństwa),
- zamawiający[27], np. pracodawca subskrybenta; subskrybent musi być o tym fakcie niezwłocznie poinformowany,
- operator punktu rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej unieważnienie certyfikatu.

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

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

---

[27] Patrz **Słownik pojęć**

- sprawdza, czy dany wnioskodawca może żądać unieważnienia certyfikatu (np. występuje jako zamawiający),
- wysyła powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

Każdy wniosek może być przekazany:

- bezpośrednio do urzędu certyfikacji w postaci wniosku elektronicznego z potwierdzeniem lub bez potwierdzenia punktu rejestracji,
- bezpośrednio lub pośrednio (za pośrednictwem innych punktów rejestracji) do głównego punktu rejestracji w postaci wniosku nieelektronicznego (dokument papierowy, faks, telefon, itp.).

4.9.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na trzy sposoby:

- **pierwszy sposób** polega na przesłaniu do urzędu certyfikacji elektronicznego wniosku o unieważnienie, podpisanego aktualnym kluczem prywatnym lub autoryzowanego przy pomocy hasła; unieważnienia tego typu można dokonać jedynie na wniosek subskrybenta (dowolny podmiot, posiadacz unieważnianego certyfikatu),
- **drugi sposób** wymaga przesłania do urzędu certyfikacji elektronicznego wniosku o unieważnienie, potwierdzonego przy pomocy podpisu cyfrowego przez urząd rejestracji; dotyczy to przypadków, gdy (a) subskrybent zgubił, został mu skradziony klucz prywatny lub nie posiada hasła, (b) unieważnienia zażądał sponsor subskrybenta, autoryzowany przedstawiciel urzędu certyfikacji lub punktu rejestracji, jeśli tylko istnieją podstawy do zażądania unieważnienia certyfikatu subskrybenta,
- **trzeci sposób** polega na tym, że uwierzytelniony wniosek nieelektroniczny (dokument papierowy, faks lub telefon) można przekazać do Głównego Punktu Rejestracji; uwierzytelnienie wniosku papierowego (w tym faksu) opisane jest w dokumencie Instrukcja weryfikacji tożsamości.

We wszystkich przypadkach urząd certyfikacji – po pozytywnej weryfikacji wniosku – **unieważnia** certyfikat. Informacja o unieważnionym lub zawieszonym certyfikacie umieszczana jest na liście **CRL** (patrz rozdz. 7.2), wydawanej przez urząd certyfikacji.

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

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

Procedura unieważnienia certyfikatu przebiega następująco:

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

telefonicznie, faksem lub w trakcie osobistej wizyty wnioskodawcy u upoważnionego przedstawiciela urzędu certyfikacji (lub odwrotnie);

- jeśli wniosek jest wiarygodny, to urząd certyfikacji umieszcza informację o unieważnionym lub zawieszonym certyfikacie na liście certyfikatów unieważnionych (CRL) wraz z informacją o przyczynie unieważnienia lub informacją o zawieszeniu certyfikatu (patrz rozdz. 7.2.1);
- przekazuje, drogą elektroniczną lub zwykłą pocztą, stronie ubiegającej się o unieważnienie certyfikatu zaświadczenie unieważnienia certyfikatu lub decyzję odmowną wraz ze wskazaniem przyczyny odmowy,
- dodatkowo, w przypadku gdy strona wnioskująca o unieważnienie certyfikatu nie jest podmiotem tego certyfikatu, to urząd certyfikacji musi wysłać powiadomienie do tego podmiotu o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

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

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

4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

CERTUM gwarantuje, że maksymalne okresy zwłoki[28] w przetwarzaniu wniosków o unieważnienie certyfikatów:

- przesyłanych w postaci elektronicznej (i we właściwym formacie) lub przekazywane telefonicznie,
- przesyłanych w formie papierowej, od momentu dotarcia wniosku papierowego do CERTUM,

są zgodne z okresami podanymi w Tab.4.2.

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

Tab.4.2 Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

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

Wnioski o unieważnienie certyfikatów zgłaszane przez urzędy certyfikacji do wystawców tych certyfikatów rozpatrywane są w ciągu 1 godziny od otrzymania wniosku, niezależnie od polityk certyfikacji, według których były wystawione.

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 (patrz rozdz. 4.9.9).

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

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

4.9.5. Okoliczności zawieszenia certyfikatu

Zawieszeniu mogą podlegać jedynie certyfikatu urzędu certyfikacji. Zawieszenie może mieć miejsce jedynie w przypadku zmian w politykach certyfikacji, zakończeniu świadczenia usług przez CERTUM lub uzasadnionych podejrzeniach co do bezpieczeństwa kluczy urzędu.

4.9.6. Kto może żądać zawieszenia certyfikatu

Z uwagi na fakt, że zawieszeniu mogą podlegać jedynie certyfikaty urzędu, żądanie zawieszenia może być zgłaszane jedynie przez Inspektora bezpieczeństwa w porozumieniu z Kierownikiem CERTUM lub Dyrektorem właściwym dla usług certyfikacyjnych.

4.9.7. Procedura zawieszenia i odwieszania certyfikatu

Zawieszenie certyfikatu urzędu wymaga formalnego wniosku Inspektora Bezpieczeństwa potwierdzonego przez Kierownika CERTUM lub Dyrektora właściwego dla usług certyfikacyjnych.

4.9.8. Ograniczenia okresu/zwłoki zawieszenia certyfikatu

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

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

4.9.9. Częstotliwość publikowania list CRL

Każdy z urzędów certyfikacji funkcjonujący w ramach CERTUM wydaje oddzielną listę certyfikatów unieważnionych.

Wszystkie listy uaktualniane są nie rzadziej niż raz w miesiącu[29], jeśli w tym czasie nie został unieważniony żaden nowy certyfikat. Nowa lista CRL publikowana jest jednak w repozytorium po każdym unieważnieniu certyfikatu. Lista CRL urzędu Certum CA publikowana jest nie rzadziej niż raz na 5 lat, chyba, że w tym czasie nastąpi odwołanie certyfikatu jednego z urzędów afiliowanych przy Certum CA.

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

4.9.10. 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.

Weryfikację stanu certyfikatów strona ufająca może oprzeć na listach CRL tylko w tych przypadkach, gdy proponowane przez CERTUM okresy odnowienia list CRL nie niosą ryzyka znaczących strat w działalności prowadzonej przez stronę ufającą. W przypadkach przeciwnych, strona ufająca powinna skontaktować się (telefonicznie, faksem) z urzędem wydającym certyfikaty lub skorzystać z elektronicznej usługi weryfikacji stanu certyfikatu w trybie *on-line* (rozdz. 4.9.11).

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

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

W przypadkach, gdy certyfikat unieważniono, podając jako przyczynę:

```
affiliationChanged   - zamiana danych (afiliacji) subskrybenta,
superseded           - zastąpienie (odnowienie) klucza,
removeFromCRL[30]    - certyfikat wycofany z listy CRL (odwieszony),
```

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

---

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

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

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

CERTUM udostępnia usługę weryfikacji certyfikatu w czasie rzeczywistym. Usługa tego typu realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 2560[31]. Protokół OCSP umożliwia uzyskiwanie częstszych informacji o unieważnieniu certyfikatu w porównaniu z przypadkiem posługiwania się jedynie listami certyfikatów unieważnionych (CRL).

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

- **poprawny** (*ang. good*) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny[32],
- **unieważniony** (*ang. revoked*) – oznacza, że certyfikat został unieważniony,
- **nieznany** (*ang. unknown*) – oznacza, że weryfikowany certyfikat nie został wydany przez jeden z urzędów afiliowanych przy Certum CA.

Usługa OCSP udostępniana jest wszystkim subskrybentom oraz stronom ufającym, którzy akceptują warunki świadczenia usług opisane w niniejszym dokumencie.

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

4.9.12. Obowiązek sprawdzania unieważnień w trybie on-line

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

4.9.13. Inne dostępne formy ogłaszania unieważnień certyfikatów

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

---

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

32 Patrz **Słownik pojęć**.

4.9.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów

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

4.9.15. Specjalne obowiązki w przypadku naruszenia ochrony klucza

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

4.9.16. Unieważnienie lub zawieszenie certyfikatu urzędu certyfikacji

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

- urząd certyfikacji jest przekonany, że dane zawarte w certyfikacie urzędu któremu wystawił certyfikat są fałszywe,
- klucz prywatny urzędu certyfikacji lub jego system komputerowy zostały ujawnione w sposób mający wpływ na pewność wydawanych przez niego certyfikatów,
- urząd certyfikacji naruszył zasady niniejszego Kodeksu Postępowania Certyfikacyjnego.

4.10. Rejestrowanie zdarzeń oraz procedury audytu

W celu nadzoru nad sprawnym działaniem systemu CERTUM, rozliczania użytkowników oraz personelu CERTUM ze swoich działań, rejestrowane są wszystkie te zdarzenia występujące w systemie, które maja istotny wpływ na bezpieczeństwo funkcjonowania CERTUM.

Wymaga się, aby każda ze stron – w jakikolwiek sposób związana ze świadczeniem usług certyfikacyjnych – dokonywała rejestracji informacji i zarządzała nią adekwatnie do pełnionych obowiązków. Zapisy zarejestrowanej informacji tworzą tzw. rejestrach zdarzeń i muszą być tak przechowywane, aby umożliwiały stronom dostęp do odpowiedniej i niezbędnej w danej chwili informacji, a także towarzyszyły przy rozstrzyganiu sporów pomiędzy stronami oraz pozwalały na wykrywanie prób włamań do systemu CERTUM. Rejestrowane zdarzenia podlegają procedurom kopiowania. Kopie przechowywane są poza siedzibą CERTUM.

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

W systemie CERTUM inspektor bezpieczeństwa zobowiązany jest do regularnego sprawdzania zgodności wdrożonych mechanizmów z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego, a także do oceny efektywności istniejących procedur bezpieczeństwa.

4.10.1. Typy rejestrowanych zdarzeń

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa CERTUM rejestrowane są w rejestrach zdarzeń oraz archiwizowane. Archiwa mogą być szyfrowane i w celu zapobieżenia modyfikacjom zapisywane na nośnikach jednokrotnego zapisu.

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

- **systemowe** – rekord wpisu zawiera informacje o żądaniu klienta i odpowiedzi serwera (lub odwrotnie) na poziomie protokołu sieciowego (np. http, https, tcp, itp.); rejestracji podlega adres IP hosta lub serwera, wykonywana operacja (np. wyszukiwanie, edycja, zapis, itp.) oraz jej wynik (np. liczba wpisów do bazy),
- **błędy** – w rekordzie zapisywane są informacje o błędach na poziomie protokołów sieciowych oraz na poziomie modułów oprogramowania,
- **audyt** – rekord wpisu zawiera wszystkie wiadomości związane z usługami certyfikacyjnymi, np. żądanie rejestracji i certyfikacji, żądanie aktualizacji kluczy, potwierdzenia akceptacji certyfikatów, publikowanie certyfikatów i list CRL, itp.

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

Rekordy zdarzeń rejestrowane automatycznie lub ręcznie w rejestrach zdarzeń zawierają:

- typ zdarzenia,
- identyfikator zdarzenia,
- datę i czas wystąpienia zdarzenia,
- identyfikator lub inne dane pozwalające na określenie osoby odpowiedzialnej za zaistniałe zdarzenia,
- określenie czy zdarzenie dotyczy operacji zakończonej sukcesem, czy błędem,

Rejestrowane zdarzenia obejmują:

- alarmy generowane przez firewall i IDS,
- czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów oraz innymi usługami świadczonymi przez organ wydający certyfikaty,
- wszelkie modyfikacje struktury sprzętowej i programowej,
- modyfikacje sieci i połączeń,
- fizyczne wejścia do obszarów zastrzeżonych oraz ich naruszenia,
- zmiany haseł, PIN-ów, uprawnień oraz ról personelu,
- udane i nieudane próby dostępu do oprogramowania serwerów CERTUM oraz jego baz danych,
- generowanie kluczy dla potrzeb urzędu certyfikacji, jak również innych stron, np. punktów rejestracji,

- wszystkie otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej; obowiązek rejestrowania tego typu zdarzeń spoczywa nie tylko na urzędzie certyfikacji, ale także na punktach rejestracji,
- historia tworzenia kopii bezpieczeństwa oraz archiwizowania rekordów informacyjnych oraz baz danych.

Szczegółowa lista rejestrowanych zdarzeń zależna jest od poziomu wiarygodności (nazwy polityki certyfikacji) certyfikatów wystawianych lub potwierdzanych przez określony urząd certyfikacji lub punkt rejestracji.

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

Dostęp do zapisów rejestrowanych zdarzeń (logów) posiadają jedynie inspektor bezpieczeństwa, administrator systemu oraz inspektor ds. audytu (patrz rozdz. 5.2.1).

4.10.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów)

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

4.10.3. Okres przechowywania zapisów rejestrowanych zdarzeń

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

Zarchiwizowane zdarzenia przechowywane są przez okres min. 5 lat.

4.10.4. Ochrona zapisów rejestrowanych zdarzeń

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

Rejestr zdarzeń może być przeglądany jedynie przez **inspektora bezpieczeństwa**, **administratora systemu** oraz **inspektora ds. audytu**. Dostęp do rejestru jest tak skonfigurowany, że:

- tylko osoby upoważnione, tj. audytorzy oraz osoby występujące w jednej z trzech wymienionych powyżej ról mają prawo czytania rekordów z rejestrów zdarzeń,
- tylko inspektor bezpieczeństwa może archiwizować i usuwać, po zarchiwizowaniu, z systemu pliki zawierające zarejestrowane zdarzenia,

- możliwe jest wykrycie każdego naruszenia jego integralności; daje to możliwość upewnienia się, że rekordy nie zawierają luk lub sfałszowanych wpisów,
- żaden podmiot nie posiada prawa modyfikowania jego zawartości.

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

4.10.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury bezpieczeństwa CERTUM wymagają, aby rejestry zdarzeń oraz zapisy zdarzeń powstałe w czasie przeglądania w tych rejestrów przez inspektora bezpieczeństwa, administratora systemu lub inspektora ds. audytu, takie jak czynności wykonywane na rejestrach, zestawienia zbiorcze, analizy, statystyki, wykryte zagrożenia, itp., były kopiowane przynajmniej raz w miesiącu. Kopie te przechowywane są w ośrodku głównym i zapasowym CERTUM. Kopie mogą być oznaczone znacznikiem czasu.

4.10.6. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

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

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

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

4.10.7. Oszacowanie podatności na zagrożenia

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

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

4.11. Archiwizowanie danych

Wymaga się, aby archiwizacji podlegały wszystkie dane i pliki dotyczące rejestrowanych danych o zabezpieczeniach systemu, danych o wnioskach napływających od subskrybentów, informacje o subskrybentach, generowane certyfikaty i listy CRL, historie kluczy, którymi

posługują się urzędy certyfikacji oraz punkty rejestracji, a także pełna korespondencja prowadzona wewnątrz CERTUM oraz z subskrybentami. Archiwizacji podlegają również dokumenty i dane użyte w procesie uwierzytelniania tożsamości. Z dokumentów można usunąć cześć danych (wizerunek, stan cywilny i rysopis), nie wymaganych bezpośrednio w procesie certyfikacji. Dane w postaci papierowej przetwarzane są do postaci elektronicznej i również podlegają archiwizacji.

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

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

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

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

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

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

4.11.1. Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące dane:

- dane z przeglądu i oceny (z audytu) zabezpieczeń logicznych i fizycznych systemu komputerowego urzędu certyfikacji, punktu rejestracji oraz repozytorium,
- otrzymywane wnioski oraz wydawane decyzje, mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub wiadomości elektronicznej,
- baza danych subskrybentów,
- baza danych certyfikatów,
- wydane listy CRL,
- historia kluczy urzędu certyfikacji, od ich wygenerowania do zniszczenia włącznie,
- historia kluczy subskrybentów, od ich wygenerowania do zniszczenia włącznie, jeśli klucze te są archiwizowane przez subskrybenta w urzędzie certyfikacji,
- wewnętrzna i zewnętrzna korespondencja (papierowa i elektroniczna) CERTUM z subskrybentami oraz ufającymi stronami przy operacjach zawieszania i odwieszania certyfikatów,

- dokumenty i dane użyte w procesie uwierzytelnianie tożsamości.

4.11.2. Częstotliwość archiwizowania danych

Archiwizacja realizowana jest kilkupoziomowo w następujących odstępach czasowych:

- baza danych certyfikatów oraz danych o subskrybentach przez okres trzech lat (od momentu wydania certyfikatu) znajduje się na nośnikach CERTUM, duplikowanych przez macierze dyskowe. Przez okres następnych trzech lat dane te są przechowywane na taśmach magnetycznych lub płytach DVD, ale nadal są dostępne na bieżąco (w trybie *on-line*). W siódmym roku (po upływie sześciu lat od wydania certyfikatu) wszystkie dane o subskrybencie oraz jego certyfikat składowane są na płycie DVD i od tego momentu mogą być dostępne tylko w trybie *off-line*,
- listy CRL, korespondencja elektroniczna oraz wnioski przychodzące od subskrybentów oraz wydane decyzje archiwizowane są w taki sam sposób i z taką samą częstotliwością, jak w przypadku bazy danych certyfikatów oraz danych o subskrybentach.

4.11.3. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej i papierowej), opisane w rozdz. 4.11.1 przechowywane są przez minimalny okres 25 lat. Po upływie przyjętego okresu archiwizacji dane mogą być zniszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany jest ze szczególną starannością.

4.11.4. Procedury tworzenia kopii zapasowych

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

- dyski instalacyjne z oprogramowaniem systemowym, m.in. systemami operacyjnymi,
- dyski instalacyjne z aplikacjami urzędów certyfikacji i punktów rejestracji
- dyski instalacyjne serwera WWW i repozytorium,
- historie kluczy urzędów, certyfikatów i list CRL,
- dane z repozytorium,
- dane o subskrybentach oraz personelu CERTUM,
- rejestry zdarzeń.

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

- **gorąca rezerwa** – codziennie są tworzone kopie baz danych, które mogą być w razie konieczności wykorzystane przy odtworzeniu utraconych danych,
- **cotygodniowe kopie zapasowe** – tworzone są w ośrodku podstawowym i mogą być w razie konieczności wykorzystane do odtworzenia utraconych danych oraz odtworzenia konfiguracji sprzętu i oprogramowania; kopia powinna objąć pełny, aktualny stan systemu CERTUM, odtworzenie funkcji urzędu w pełnym zakresie ośrodek osiąga w ciągu maksymalnie 48 godzin.

Szczegółowe procedury tworzenia kopii zapasowych oraz odtwarzania po awariach opisane są w dokumentacji infrastruktury technicznej. Dokumentacja ma status „niejawny" i udostępniany jest tylko upoważnionemu do tego personelowi oraz audytorom.

4.11.5. Wymaganie znakowania archiwizowanych danych znacznikiem czasu

Zaleca się, aby archiwizowane dane oznaczane były znacznikiem czasu, tworzonym przez wiarygodny organ znacznika czasu (TSA), posiadający certyfikat wydany przez operacyjny urząd certyfikacji afiliowany przy **Certum CA**.

4.11.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

W celu sprawdzenia integralności zarchiwizowane dane mogą być okresowo weryfikowane oraz porównywane z danymi oryginalnymi (jeśli jeszcze funkcjonują w systemie). Czynność ta może być przeprowadzona tylko pod kontrolą inspektora bezpieczeństwa i powinna być odnotowywana w rejestrze zdarzeń.

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

4.12. Zmiana klucza

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

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

Każda zmiana kluczy urzędów certyfikacji anonsowana jest odpowiednio wcześniej za pośrednictwem serwisów WWW, publikacji nowych kluczy w oprogramowaniu, np. przeglądarki internetowe, programy pocztowe, itp. Dodatkowo, w przypadku zmiany kluczy przez urząd certyfikacji **Certum CA** informacja o tym fakcie może być publikowana w środkach masowego przekazu w tygodniu poprzedzającym koniec okresu ważności klucza prywatnego.

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

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

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

Rozdział ten zawiera opis procedur postępowania, realizowanych przez CERTUM w wypadkach szczególnych (także klęsk żywiołowych) w celu przywrócenia gwarantowanego

poziomu usług. Procedury te realizowane są według opracowanego planu podnoszenia systemu po katastrofie (*ang. disaster recovery plan*).

4.13.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Polityka bezpieczeństwa, realizowana przez CERTUM bierze pod uwagę następujące zagrożenia, mające wpływ na dostępność i ciągłość świadczonych usług:

- fizyczne uszkodzenie systemu komputerowego CERTUM, w tym także sieci - obejmuje to przypadki uszkodzenia powstałe wskutek wypadków losowych,
- awarie oprogramowania pociągające za sobą utratę dostępu do danych - awarie tego typu dotyczą systemu operacyjnego, oprogramowania użytkowego oraz działania oprogramowania złośliwego, np. wirusów, robaków, koni trojańskich,
- utratę istotnych z punktu widzenia interesów CERTUM usług sieciowych - związane jest to w pierwszym rzędzie z zasilaniem oraz połączeniami telekomunikacyjnymi,
- awaria tej części sieci internetowej, za pośrednictwem której CERTUM udostępnia swoje usługi - awaria taka oznacza zablokowanie i w istocie odmowę (niezamierzoną) świadczenia usług.

Aby zapobiec lub ograniczyć skutki wymienionych zagrożeń, polityka bezpieczeństwa CERTUM obejmuje następujące zagadnienia:

- **Plan odtwarzania systemu po katastrofie.** Wszyscy subskrybenci oraz strony ufające są jak najszybciej i w sposób najbardziej odpowiedni do zaistniałej sytuacji powiadamiani o każdej poważnej awarii lub katastrofie, dotyczącej dowolnego komponentu systemu komputerowego i sieci. Plan odtwarzania systemu obejmuje szereg procedur, które są realizowane w momencie, gdy dowolna część systemu ulegnie skompromitowaniu (uszkodzeniu, ujawnieniu, itp.). Wykonywane są działania:
    - tworzone i konserwowane są kopie obrazu dysków każdego z serwerów oraz stacji roboczej systemu CERTUM; każda kopia przechowywana jest w zarówno w siedzibie, jak i w bezpiecznym pomieszczeniu poza siedzibą CERTUM,
    - okresowo, zgodnie z procedurami opisanymi w rozdz. 4.11.4 tworzone są kopie baz danych zawierające wszystkie zgłoszone żądania ze strony subskrybentów, wydane, aktualizowane i unieważnione certyfikaty; najbardziej aktualne kopie przechowywane są w bezpiecznym miejscu w siedzibie jak i poza siedzibą CERTUM,
    - okresowo, zgodnie z procedurami opisanymi w rozdz. 4.11.4 tworzone są kopie każdego z serwerów zawierające pełne kopie serwerów, wszystkie zgłoszone żądania ze strony subskrybentów, zapisy rejestrowanych zdarzeń (logi), wydane, aktualizowane i unieważnione certyfikaty; najbardziej aktualne kopie przechowywane są w bezpiecznym miejscu poza siedzibą CERTUM,
    - klucze CERTUM, rozproszone zgodnie z zasadami sekretów współdzielonych przechowywane są przez zaufane osoby, w miejscach tylko im znanych;
    - wymiana komputera jest wykonywana tak, aby możliwe było odtworzenie obrazu dysku, w oparciu o najbardziej aktualne dane oraz klucze (dotyczy to serwera podpisującego),

- proces odtwarzania systemu po katastrofie testowany jest na każdym elemencie systemu co najmniej raz w roku i jest częścią procedur audytu wewnętrznego.

- **Kontrolowanie zmian.** W systemie docelowym instalacja uaktualnionych wersji oprogramowania możliwa jest tylko i wyłącznie po przeprowadzeniu na systemie modelowym intensywnych testów, wykonywanych według ściśle opracowanych procedur. Wszystkie zmiany dokonywane w systemie wymagają akceptacji inspektora bezpieczeństwa CERTUM. Jeśli mimo stosowania się do tej procedury wdrożone nowe elementy spowodują awarię systemu docelowego, opracowane plany odtwarzania systemu po katastrofie pozwalają na powrót do stanu sprzed awarii.

- **System zapasowy.** W przypadku awarii uniemożliwiającej funkcjonowanie CERTUM w ciągu maksymalnie 24 godzin zostanie uruchomiony ośrodek zapasowy, który przejmie do czasu uruchomienia głównego ośrodka CERTUM podstawowe funkcje urzędów certyfikacji. Z uwagi na regularne tworzenie kopii zapasowych, archiwizację, gromadzenie nieprzetworzonych przesyłek oraz redundancję sprzętowo-programową w przypadku awarii uniemożliwiającej funkcjonowanie CERTUM możliwe jest:
  - uruchomienie ośrodka zapasowego pozwalającego na uruchomienie CERTUM,
  - przetworzenie wszystkich zgromadzonych i nieprzetworzonych żądań unieważnienia certyfikatów,
  - do czasu regeneracji i ponownego uruchomienia ośrodka głównego - przetwarzanie na bieżąco przychodzących wiadomości od użytkowników.

- **System tworzenia kopii zapasowych.** System CERTUM korzysta z oprogramowania tworzącego kopie zapasowe z danych, które w każdej chwili umożliwiają ich odtworzenie oraz obsługę audytu. Kopie zapasowe oraz archiwa tworzone są ze wszystkich danych, mających istotny wpływ na bezpieczeństwo i normalne funkcjonowanie CERTUM. Kopie tworzone są okresowo i zapisywane na taśmach, archiwa zaś na płytach CD-ROM. Kopie zapasowe mogą być chronione przy pomocy hasła, płyty CD-ROM są szyfrowane i mogą być oznaczane czasem. Kopie danych i ich archiwa przechowywane są poza miejscem lokalizacji głównego systemu przetwarzającego.

- **Usługi szczególne.** W celu zapobieżenia czasowemu zanikowi zasilania i zapewnienia ciągłości usług stosuje się zasilanie awaryjne (UPS-y). Urządzenia UPS sprawdzane są co 6 miesięcy.

4.13.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

W przypadku ujawnienia lub podejrzenia ujawnienia kluczy prywatnych urzędów certyfikacji, funkcjonujących w ramach CERTUM podjęte zostaną następujące kroki:

- urząd certyfikacji generuje nową parę kluczy i tworzy nowy certyfikat,
- w trybie natychmiastowym zostaną zawiadomieni o tym fakcie wszyscy użytkownicy certyfikatów za pośrednictwem komunikatu w środkach masowego przekazu oraz za pośrednictwem poczty elektronicznej,
- skompromitowany certyfikat znajdzie się na liście certyfikatów unieważnionych z podaniem przyczyny unieważnienia,

- unieważnione i umieszczone na liście certyfikatów unieważnionych wraz z podaniem odpowiedniej przyczyny unieważnienia zostaną także wszystkie certyfikaty znajdujące się w ścieżce certyfikacji skompromitowanego certyfikatu,
- wygenerowane zostaną nowe certyfikaty użytkowników,
- nowe certyfikaty użytkowników zostaną przesłane do użytkowników bez obciążania ich kosztami za powyższą operację.

4.13.3. Spójność zabezpieczeń po katastrofach

Po każdym przywróceniu systemu po katastrofie do normalnego stanu inspektor bezpieczeństwa lub administrator systemu wykonuje następujące czynności:

- zmienia wszystkie poprzednio stosowane hasła,
- usuwa i ponownie określa wszystkie upoważnienia dostępu do zasobów systemu,
- zmienia wszystkie kody oraz numery PIN związane z fizycznym dostępem do pomieszczeń oraz elementów systemu,
- jeśli usunięcie awarii wymagało ponownego zainstalowania systemu operacyjnego oraz użytkowego, zmienia wszystkie adresy IP elementów systemu oraz jego podsieci,
- dokonuje przeglądu analizy przyczyn i aktualizacji planów, polityki bezpieczeństwa sieci CERTUM oraz fizycznego dostępu do pomieszczeń i elementów systemu,
- zawiadomić wszystkich użytkowników o wznowieniu działalności systemu.

4.14. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Przedstawione poniżej obowiązki urzędu certyfikacji mają na uwadze redukcję wpływu skutków podjęcia przez ten urząd decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym wszystkich subskrybentów, urzędu który akredytował likwidowany urząd certyfikacji (jeśli taki istnieje) oraz przekazania odpowiedzialności - na drodze odpowiednich umów z innymi urzędami certyfikacji - za obsługę swoich subskrybentów, zarządzanie bazami danych oraz innymi zasobami.

4.14.1. Wymagania związane z przekazaniem obowiązków

Zanim urząd certyfikacji wstrzyma swoją działalność zobowiązany jest do:

- powiadomienia urzędu, który wydał mu certyfikat o swoim zamiarze zaprzestania działalności jako autoryzowanego urzędu certyfikacji; zawiadomienie takie powinno być złożone co najmniej na 90 dni przed planowanym zakończeniem działalności;
- zawiadomienia (co najmniej na 90 dni wcześniej) wszystkich subskrybentów, którzy posiadają jeszcze ważny, wydany przez siebie certyfikat, o zamiarze zakończenia działalności,
- unieważnienia wszystkich certyfikatów, które pozostały aktywne w dniu upłynięcia deklarowanego terminu zakończenia działalności niezależnie od tego czy subskrybent złożył stosowny wniosek o unieważnienie, czy też nie,

- poinformowania wszystkich subskrybentów związanych z urzędem certyfikacji o zaprzestaniu działalności,
- uczynienia wszystkiego co możliwe, aby zaprzestanie działalności urzędu spowodowało jak najmniejsze szkody w działalności subskrybentów oraz osób prawnych, zaangażowanych w proces ciągłego weryfikowania podpisów cyfrowych (będących jeszcze w obiegu) przy pomocy kluczy publicznych, poświadczonych certyfikatami wydanymi przez likwidowany urząd certyfikacji,
- zwrotu subskrybentowi (lub jego sponsorowi) kosztów wydanego certyfikatu, proporcjonalnie do pozostałego okresu ważności wydanego certyfikatu.

4.14.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji

W celu zapewnienia ciągłości usług certyfikacyjnych świadczonych subskrybentom, likwidowany urząd certyfikacji może zawrzeć z innym urzędem tego typu umowę, dotyczącą ponownego wydania pozostających jeszcze w obiegu certyfikatów subskrybentów likwidowanego urzędu certyfikacji.

Wydając ponownie certyfikat następca likwidowanego urzędu certyfikacji przejmuje na siebie prawa i obowiązki likwidowanego urzędu certyfikacji w zakresie zarządzania certyfikatami pozostającymi w obiegu.

Archiwum kończącego działalność urzędu certyfikacji musi być przekazane głównemu urzędowi certyfikacji **Certum CA** (w przypadku zaprzestania działalności przez **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV**, **Certum Partners**) lub instytucji, z którą zawarta została odpowiednia umowa (w przypadku zaprzestania działalności przez **Certum CA**).

5.Zabezpieczenia fizyczne, organizacyjne oraz personelu

W rozdziale opisano ogólne 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.

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. W zapisach zdarzeń (logach systemowych) rejestrowane jest każde wejście i wyjście. Testowana jest stabilność zasilania, temperatura oraz wilgotność.

5.1.1.1. Miejsce lokalizacji oraz budynek

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

5.1.1.2. Dostęp fizyczny

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.

Siedziba Unizeto Technologies S.A. jest publicznie dostępna w każdy dzień roboczy w godzinach pracy w firmie. W pozostałym czasie (w tym w dni nierobocze) w budynku mogą przebywać tylko osoby znane ochronie z imienia i nazwiska oraz posiadające pozwolenie Dyrekcji Unizeto Technologies S.A.

Goście odwiedzający pomieszczenia zajmowane przez CERTUM mogą poruszać się po tych pomieszczeniach jedynie wraz z personelem CERTUM.

Pomieszczenia CERTUM dzielą się na:

- pomieszczenie systemu komputerowego,
- pomieszczenie operatorsko - administracyjne.

Pomieszczenie systemu komputerowego wyposażone jest w nadzorowany system zabezpieczeń, zbudowany w oparciu o czujniki ruchu, przeciwpożarowe oraz przeciwpowodziowe. Dostęp do pomieszczenia posiadają tylko osoby upoważnione, tzn. zaufany personel CERTUM oraz Unizeto Technologies S.A. Nadzorowanie praw dostępu realizowane jest w oparciu o posiadane przez nich karty mikroprocesorowe oraz system kontroli dostępu, którego końcówki zamontowane są przy wejściu do pomieszczeń. Każde wejście i wyjście odnotowywane jest w

logach systemowych. Obecność innych osób (np. audytorów lub pracowników serwisu sprzętowego) wymaga obecności uprawnionego członka personelu oraz zgody Kierownika CERTUM.

Dostęp do pomieszczenia operatorsko-administracyjnego chroniony jest za pomocą kart mikroprocesorowych oraz systemu kontroli dostępu. Ponieważ wszystkie informacje wrażliwe przechowywane są w sejfach trwale związanych z podłożem, do których dostęp jest możliwy jedynie przy użyciu dwóch kluczy (zasada dwóch par oczu), zaś dostęp do terminali operatorskich i administracyjnych wymaga uprzedniego uwierzytelnienia, zastosowane zabezpieczenie fizyczne uważa się za wystarczające. Klucze do pomieszczenia są pobierane tylko przez upoważnione do tego osoby. W pomieszczeniu mogą przebywać jedynie pracownicy CERTUM oraz inne uprawnione osoby, przy czym osoby te nie mogą w pomieszczeniu przebywać pojedynczo. Jedyne odstępstwo od tej zasady dotyczy pracowników, którzy pełnią w CERTUM rolę sklasyfikowaną jako **zaufana**.

5.1.1.3. Zasilanie oraz klimatyzacja

W przypadku zaniku zasilania zainstalowane podstawowego system przechodzi na zasilanie awaryjne (UPS i/lub generatory).

Środowisko pracy w pomieszczeniu systemu komputerowego kontrolowane jest w sposób ciągły i niezależny od innych pomieszczeń.

Wszystkie pomieszczenia są klimatyzowane.

5.1.1.4. Zagrożenie zalaniem

W pomieszczeniu systemu komputerowego zainstalowane są czujniki wilgotności oraz wykrywające obecność wody. Czujniki te sprzęgnięte są z systemem ochrony całego budynku Unizeto Technologies S.A. O zagrożeniach informowana jest obsługa portierska, która w zależności od sytuacji zawiadamia odpowiednie służby miejskie, inspektora bezpieczeństwa oraz jednego z administratorów systemu.

5.1.1.5. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej zainstalowany w siedzibie firmy Unizeto Technologies S.A., spełnia wymogi stosownych przepisów i norm przeciwpożarowych. W pomieszczeniach serwerowi zainstalowano urządzenia gaśnicze (gazowe), które załączają się automatycznie w przypadku wykrycia pożaru w chronionym obszarze.

5.1.1.6. Nośniki informacji

W zależności od stopnia wrażliwości informacji nośniki, na których przechowywane są archiwa oraz bieżące kopie danych składowane są w sejfach ognioodpornych zlokalizowanych w pomieszczeniach operatorsko-administracyjnych oraz pomieszczeniu systemu komputerowego. Dostęp do sejfu możliwy jest jedynie przy użyciu dwóch kluczy będących w posiadaniu autoryzowanych osób. Kopie stosownych dokumentów oraz kopie zapasowe i archiwalne są składowane również w ośrodku zapasowym, w sejfach ognioodpornych, trwale związanych z podłożem.

5.1.1.7. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo CERTUM po upływie okresu przechowywania (patrz rozdz. 4.11) niszczone są

w specjalnych urządzeniach niszczących. W przypadku kluczy kryptograficznych oraz numerów PIN lub PUK nośniki, na których informacje te były przechowywane są niszczone w urządzeniach klasy DIN-3 (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji i ich ponowne użycie do tych samych lub innych celów).

5.1.1.8. Przechowywanie kopii bezpieczeństwa

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. Umożliwia to awaryjne odtworzenie kluczowych funkcji CERTUM w ciągu maksimum 48 godzin (w siedzibie głównej lub w ośrodku zapasowym).

5.1.2. Bezpieczeństwo punktów rejestracji

Komputery rejestrujące wnioski subskrybentów oraz wydające im potwierdzenia znajdują się w specjalnie przeznaczonym do tego celu pomieszczeniu oraz pracują w trybie *on-line* (muszą być włączone w sieć). Dostęp do nich jest fizycznie chroniony przed nieupoważnionymi osobami. Do ich obsługi dopuszczone są jedynie upoważnione do tego osoby.

5.1.2.1. Miejsce lokalizacji oraz budynek

Punkty rejestracji Centrum Certyfikacji zlokalizowane są w następujących miejscach:

- Główny Punkt Rejestracji (GPR) - w pomieszczeniu operatorsko-administracyjnym CERTUM (patrz rozdz. 5.1.1.1),
- lokalizacja innych punktów rejestracji dostępna jest w repozytorium i za pośrednictwem poczty elektronicznej: info@certum.pl.

5.1.2.2. Dostęp fizyczny

Dostęp do Głównego Punktu Rejestracji musi być zgodny z wymogami rozdz. 5.1.1.2. W przypadku pozostałych typów punktów rejestracji nie narzuca się w tym zakresie żadnych dodatkowych wymagań. Zaleca się jedynie, aby pomieszczenie punktu rejestracji było pomieszczeniem wydzielonym i wyposażonych z urządzenia zapewniające bezpieczne przechowywanie danych i dokumentów. Dostęp do niego powinien być kontrolowany i ograniczony tylko do grona osób związanych z funkcjonowaniem punktu rejestracji (operatorów punktów rejestracji, administratorów systemu) oraz ich klientów.

5.1.2.3. Zasilanie oraz klimatyzacja

Pomieszczenie Głównego Punktu Rejestracji jest włączone w system zasilania awaryjnego Unizeto. Klimatyzacja nie jest wymagana. Na pozostałe punkty rejestracji nie nakłada się wymagań odnośnie awaryjnych systemów zasilania oraz klimatyzacji.

5.1.2.4. Zagrożenie wodne

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

5.1.2.5. Ochrona przeciwpożarowa

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

5.1.2.6. Nośniki informacji

Nośniki informacji, na których przechowywane są archiwa, bieżące kopie danych, oraz dokumenty papierowe składowane są w sejfach zlokalizowanych w pomieszczeniu Głównego Punktu Rejestracji.

5.1.2.7. Niszczenie informacji

Po upływie okresu przechowywania (patrz rozdz. 4.11.3) papierowe oraz elektroniczne nośniki, zawierające informacje poufne lub sekretne są niszczone w specjalnych urządzeniach niszczących.

W przypadku kluczy kryptograficznych oraz numerów PIN lub PUK nośniki, na których informacje te były przechowywane niszczone są w urządzeniach klasy DIN-3 (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji i ich ponowne użycie do tych samych lub innych celów). Sprzętowe urządzenia kryptograficzne (moduły) są zerowane zgodnie z dokumentacją producenta. Zerowanie urządzeń ma miejsce również w momencie oddawania modułu do serwisu.

5.1.2.8. Przechowywanie kopii bezpieczeństwa

Przechowywane kopie bezpieczeństwa powinny być w sejfach i zapewniać wymóg dostępu dwuosobowego.

Zaleca się przechowywanie poza punktem rejestracji archiwów oraz bieżących kopii informacji przetworzonej przez system komputerowy.

5.1.3. Bezpieczeństwo subskrybenta

Subskrybent powinien chronić swoje hasło dostępu do systemu lub osobiste numery identyfikacyjne (PIN i PUK). Jeżeli używane hasło lub PIN / PUK są trudne do zapamiętania, mogą zostać zapisane jednak pod warunkiem przechowywania ich w sejfie, do którego dostęp mają tylko upoważnione osoby lub zaszyfrowane algorytmem znanym właścicielowi danego numeru PIN / PUK.

Użytkownik certyfikatu nie powinien pozostawiać bez opieki stacji roboczej oraz zainstalowanego na nim oprogramowania w momencie, gdy znajduje się ona w stanie kryptograficznie niezabezpieczonym, tzn. zostało wprowadzone hasło, PIN lub załadowany do obszaru kryptograficznego klucz prywatny.

Hasło używane do zabezpieczania nośnika wraz ze znajdującym się na nim kluczem prywatnym użytkownika nie mogą być przechowywane w tym samym miejscu, w którym znajduje się nośnik.

5.2. Zabezpieczenia organizacyjne

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w CERTUM. Opisano także odpowiedzialność związaną z każdą pełnioną rolą.

5.2.1. Zaufane role

5.2.1.1. Zaufane role w CERTUM

W CERTUM określono następujące zaufane role, które mogą być pełnione przez jedną lub więcej osób:

- **członek Zespołu ds. Rozwoju Usług PKI** – określa kierunki rozwoju CERTUM, wdraża oraz zarządza Polityką Certyfikacji, a także Kodeksem Postępowania Certyfikacyjnego,
- **kierownik CERTUM** – odpowiada za prawidłowe funkcjonowanie CERTUM,
- **inspektor bezpieczeństwa** – nadzoruje wdrożenie i stosowanie wszystkich procedur bezpiecznej eksploatacji systemów teleinformatycznych, stosowanych przy świadczeniu usług, kieruje administratorami systemu, inicjuje i nadzoruje proces generowania kluczy oraz sekretów współdzielonych, przydziela uprawnienia w zakresie zabezpieczeń oraz prawa dostępu użytkownikom, dokonuje przeglądu zapisów, nadzoruje prace serwisowe,
- **operator systemu** – wykonuje stałą obsługę systemu informatycznego, w tym także kopie zapasowe, lokuje kopie archiwów oraz bieżące kopie bezpieczeństwa poza siedzibą CERTUM,
- **inspektor ds. rejestracji** – weryfikuje tożsamość subskrybenta oraz poprawność złożonego przez niego wniosku, zatwierdza przygotowane zgłoszenia certyfikacyjne,
- **administrator systemu** – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, wstępnie konfiguruje system oraz sieć, zarządza publicznie dostępnymi katalogami używanymi przez CERTUM,
- **programista aplikacji** – tworzy mechanizmy obsługi procesu certyfikacji oraz stron WWW,
- **inspektor ds. audytu** – odpowiada za przegląd, archiwizowanie i zarządzanie rejestrami zdarzeń (w tym w szczególności sprawdzanie ich integralności) oraz prowadzenie audytów wewnętrznych pod kątem zgodności funkcjonowania urzędów certyfikacji zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego; odpowiedzialność ta rozciąga się także na wszystkie punkty rejestracji, funkcjonujące w ramach CERTUM.

Przedstawiony podział ról zapobiega nadużyciom przy korzystaniu z systemu CERTUM. Każdemu z użytkowników przydzielono tylko takie prawa, które wynikają z pełnionej przez niego roli i ponoszonej z tego tytułu odpowiedzialności.

Wymienione role mogą być łączone w ograniczonym zakresie, kształtowane w inny sposób lub pozbawiane klauzuli poufności. Łączeniu nie podlegają jednak role inspektora bezpieczeństwa z rolami administratora systemu lub operatora systemu oraz role inspektora ds. audytu z rolami inspektora bezpieczeństwa, inspektora ds. rejestracji, administratora systemu czy operatora systemu.

Dostęp do oprogramowania nadzorującego operacje realizowane przez CERTUM posiadają tylko te osoby, których odpowiedzialność i obowiązki wynikają z pełnionych przez nie ról administratora systemu.

5.2.1.2. Zaufane role w punkcie rejestracji

CERTUM musi być pewne, że obsługa punktu rejestracji rozumie swoją odpowiedzialność wynikającą z konieczności rzetelnej identyfikacji oraz uwierzytelniania subskrybentów. Z tego powodu w punkcie rejestracji wyróżnia się minimum trzy zaufane role:

- **administrator systemu** – instaluje sprzęt oraz oprogramowanie systemu operacyjnego, instaluje oprogramowanie, konfiguruje system i aplikacje, uaktywnia i konfiguruje zabezpieczenia, zakłada konta i hasła operatorom, tworzy kopie bezpieczeństwa i archiwizuje informacje, przegląda zapisy zdarzeń (logi) oraz (razem z operatorem punktu rejestracji) na polecenie inspektora bezpieczeństwa niszczy zbędną informację,
- **inspektor ds. rejestracji** – weryfikuje tożsamość subskrybenta oraz poprawność złożonego przez niego wniosku, potwierdza wnioski i przekazuje je do urzędu certyfikacji, pośredniczy w tworzeniu certyfikatu, wysyłając informację z wniosków do urzędu certyfikacji, zawiera umowy z subskrybentami na świadczenie usług przez urząd certyfikacji, archiwizuje w postaci papierowej wnioski i wydane potwierdzenia.
- **agent punktu rejestracji –** odpowiada za sprawne działanie punktu systemu rejestracji; jego rola polega na zapewnieniu finansowania pracowników, zarządzaniu pracą operatora i administratora systemu, rozstrzyganiu sporów, podejmowaniu decyzji, wynikających z realizowanych przez punkt rejestracji czynności.

5.2.1.3. Zaufane role u subskrybenta

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

5.2.2. Liczba osób wymaganych do realizacji zadania

Operacją, którą wymaga zachowania szczególnej ostrożności jest proces generowania kluczy, używanych przez urząd certyfikacji do podpisywania certyfikatów i list CRL. Przy ich generowaniu muszą być osoby, pełniące role:

- inspektora bezpieczeństwa,
- operatora modułu kryptograficznego,
- posiadaczy sekretów współdzielonych,
- sprawozdawcy,
- obserwatorzy – (opcjonalnie) np. przedstawiciele audytora.

We wszystkich pozostałych przypadkach role wydzielone w CERTUM mogą być wykonywane przez pojedyncze przypisane do tej roli osoby.

5.2.3. Identyfikacja oraz uwierzytelnianie ról

Personel CERTUM jest poddawany procedurze identyfikacji oraz uwierzytelniania w następujących przypadkach:

- umieszczania na liście osób posiadających dostęp do pomieszczeń CERTUM,
- umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci CERTUM,
- wydawania poświadczenia upoważniającego do wykonywania przypisanej roli,

- przydzielania konta oraz hasła w systemie komputerowym CERTUM.

Każde z powyższych poświadczeń oraz przypisanych kont:

- musi być unikalne i bezpośrednio przypisane konkretnej osobie,
- nie może być współdzielone z innymi osobami,
- musi być ograniczone do funkcji (wynikających z roli pełnionej przez określoną osobę) realizowanych tylko za pośrednictwem dostępnego oprogramowania systemu CERTUM, systemu operacyjnego oraz kontroli proceduralnych.

Operacje wykonywane w CERTUM, które wymagają dostępu poprzez sieć współdzieloną są zabezpieczone dzięki wprowadzonym mechanizmom silnego uwierzytelniania oraz szyfrowaniu przesyłanej informacji.

5.3. Personel

CERTUM musi mieć pewność, że osoby wykonujące swoje obowiązki wynikające z funkcji realizowanych przez urząd certyfikacji lub punkt rejestracji:

- posiadają minimum wykształcenie średnie,
- zawarły umowę o pracę lub inną umowę cywilno-prawną precyzującą rolę, którą mają pełnić oraz określa wynikające z niej prawa i obowiązki,
- przeszły niezbędne przeszkolenie z zakresu obowiązków, które będą wykonywały,
- zostały przeszkolone w zakresie ochrony danych osobowych,
- w umowie lub regulaminie zawarto 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 urzędzie certyfikacji lub punkcie rejestracji musi przejść cykl szkoleń dotyczących:

- zasad Polityki Certyfikacji,
- zasad Kodeksu Postępowania Certyfikacyjnego,
- zasad zawartych w dokumentacji, przypisanej roli, którą dana osoba pełni,
- zasad i mechanizmów zabezpieczeń stosowanych w urzędzie certyfikacji oraz punktach rejestracji,
- oprogramowania systemu komputerowego urzędu certyfikacji oraz punktu rejestracji,
- obowiązków, które będą pełniły lub aktualnie pełnią,
- procedur realizowanych po awariach lub katastrofach systemu urzędu certyfikacji.

Po zakończeniu szkolenia jego uczestnicy podpisują dokument potwierdzający zapoznanie się z przedstawioną dokumentacją oraz akceptację wynikających z nich ograniczeń.

5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione w rozdz. 5.3.1 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu CERTUM lub punktów rejestracji, bądź zostały opublikowane nowe wersje Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego..

5.3.3. Rotacja stanowisk

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

5.3.4. Sankcje z tytułu nieuprawnionych działań

W przypadku wykrycia nieuprawnionego działania lub podejrzenia o takie działanie administrator systemu w porozumieniu z inspektorem bezpieczeństwa (w przypadku pracowników CERTUM) lub tylko administrator systemu (w przypadku pracowników punktu rejestracji) może sprawcy takiego zdarzenia zawiesić dostęp do systemu CERTUM lub punktu rejestracji. Dalsze postępowanie przeprowadzane jest w porozumieniu z kierownictwem CERTUM.

5.3.5. Pracownicy kontraktowi

Pracownicy kontraktowi (serwis zewnętrzny, wykonawcy podsystemów i oprogramowania, producenci, itp.) poddawani są takiej samej procedurze, jak stali pracownicy CERTUM i punktu rejestracji (patrz rozdz. 5.3.1, 5.3.2 i 5.3.3). Dodatkowo pracownicy kontraktowi podczas przebywania na terenie CERTUM lub punktu rejestracji muszą zawsze znajdować się w towarzystwie pracownika urzędu certyfikacji lub punktu rejestracji.

5.3.6. Dokumentacja przekazana personelowi

Kierownictwo CERTUM, jak również agent punktu rejestracji muszą umożliwić swojemu personelowi dostęp do następujących dokumentów:

- Polityki Certyfikacji,
- Kodeksu Postępowania Certyfikacyjnego,
- wzory umów oraz stosowanych formularzy wniosków,
- niezbędne wyciągi z dokumentacji (właściwej dla pełnionej roli), w tym procedur awaryjnych,
- zakresu obowiązków i uprawnień wynikających z pełnionej roli.

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych urzędów certyfikacji, punktów rejestracji oraz użytkownika, 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.

Urząd certyfikacji **Certum CA** posiada przynajmniej jeden autocertyfikat. Klucz prywatny, komplementarny z zawartym w autocertyfikacie kluczem publicznym, stosowany jest jedynie do podpisywania certyfikatów kluczy publicznych urzędów certyfikacji **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV** i **Certum Partners oraz innych utworzonych na podstawie niniejszego dokumentu urzędów certyfikacji** (np. dla świadczenia usług niezaprzeczalności) oraz wystawienia listy certyfikatów unieważnionych (CRL) i tzw. certyfikatów operacyjnych urzędu certyfikacji, koniecznych do funkcjonowania urzędu. Podobne zastosowania znajdują klucze prywatne, będące w posiadaniu każdego z urzędów certyfikacji **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV**, **Certum Partners** i komplementarne z odpowiednimi kluczami publicznymi zawartymi w certyfikatach wystawionych przez **Certum CA** każdemu z tych urzędów.

Klucze będące w posiadaniu każdego z urzędów certyfikacji powinny umożliwić im:

- podpisywanie certyfikatów i list CRL (klucz publiczny związany z kluczem prywatnym uwierzytelniony jest w postaci autocertyfikatu – przypadek **Certum CA** lub certyfikatu – przypadek **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV**, **Certum Partners**);
- podpisywanie wiadomości, wymienianych z subskrybentami oraz punktami rejestracji (klucz operacyjny);
- do uzgadniania kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem a otoczeniem (klucz operacyjny).

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

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędu certyfikacji **Certum CA**, urzędów pośrednich **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV** i **Certum Partners** oraz urzędów dla usług niezaprzeczalności generowane są w siedzibie CERTUM w obecności wybranej, przeszkolonej grupy zaufanych osób (w grupie tej muszą znajdować się także inspektor bezpieczeństwa i administrator systemu). Taka grupa osób konieczna jest tylko w przypadku generowania kluczy do podpisywania certyfikatów i list CRL.

Klucze urzędów certyfikacji funkcjonujących w ramach CERTUM generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu kryptograficznego, spełniającego wymagania klasy FIPS 140-2 Level 3 lub wyżej.

Klucze urzędów generowane są zgodnie z przyjętą w CERTUM procedurą generowania kluczy. Czynności wykonywane w trakcie generowania każdej pary kluczy są rejestrowane, datowane i podpisywane przez każdą uczestniczącą w procedurze osobę. Zapisy te są przechowywane dla potrzeb audytu oraz bieżących przeglądów systemu.

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

Każdy z subskrybentów z zasady samodzielnie generuje dla swoich potrzeb każdą parę kluczy lub może to zadanie zlecić urzędowi certyfikacji (tylko w przypadku uzyskania certyfikatu na karcie kryptograficznej).

CERTUM może na żądanie subskrybenta lub operatora punktu rejestracji wygenerować klucze i w bezpieczny sposób dostarczyć je wnioskodawcom. Do generowania kluczy używany jest w takich przypadkach sprzętowy moduł kryptograficzny, spełniający wymagania klasy FIPS 140-2 Level 2 lub wyżej (patrz rozdz. 6.1.2).

6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji Certum CA

Procedura generowania początkowych kluczy **Certum CA** wykorzystywana jest podczas pierwszego inicjowania pracy systemu CERTUM lub w przypadku gdy istnieje podejrzenie, że któryś z kolejnych kluczy urzędu certyfikacji został ujawniony. Polega ona na:

- bezpiecznym wygenerowaniu głównej pary kluczy do podpisu certyfikatów i list CRL - główna para kluczy ma postać $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(1)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(1)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzeniu autocertyfikatu klucza publicznego $\mathbf{K_{GPK(1)}}$.

Po wygenerowaniu pary kluczy do podpisu certyfikatów i list CRL, rozproszeniu klucza prywatnego i uaktywnieniu go w sprzętowym module kryptograficznym, klucze te mogą być wykorzystywane w operacjach kryptograficznych do momentu utraty ważności lub ich ujawnienia.

6.1.1.2. Procedury aktualizacji kluczy Certum CA

Klucze **Certum CA** mają skończony okres życia, po którego upływie muszą zostać uaktualnione.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do podpisywania certyfikatów i list CRL. Polega ona na wydaniu przez **Certum CA** specjalnych certyfikatów ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym stary autocertyfikat **Certum CA**, na bezpieczne przejście do pracy z nowym autocertyfikatem, zaś nowym użytkownikom końcowym posiadającym nowy autocertyfikat na bezpieczne pozyskanie starego autocertyfikatu, umożliwiającego weryfikację istniejących danych (patrz RFC 2510).

Aby uzyskać wspomniany wyżej efekt **Certum CA** musi stosować procedurę, która po wygenerowaniu nowej pary kluczy zabezpieczy (uwiarygodni) nowy klucz publiczny przy pomocy starego (poprzednio stosowanego) klucza prywatnego i odwrotnie, stary klucz publiczny zabezpieczony zostanie przy pomocy nowego klucza prywatnego. Oznacza to, że w momencie uaktualniania autocertyfikatu urzędu certyfikacji **Certum CA**, oprócz nowego autocertyfikatu zostaną utworzone dwa dodatkowe certyfikaty. Łącznie istnieją cztery certyfikaty do podpisywania certyfikatów i list CRL: stary **autocertyfikat StaryStarym** (stary klucz publiczny podpisany starym kluczem prywatnym), nowy **autocertyfikat NowyNowym** (nowy klucz publiczny podpisany nowym kluczem prywatnym), **autocertyfikat StaryNowym** (stary klucz publiczny podpisany nowym kluczem prywatnym) oraz **autocertyfikat NowyStarym** (nowy klucz publiczny podpisany starym kluczem prywatnym).

Procedura aktualizacji nowej pary kluczy **Certum CA**, przeznaczonej do podpisywania certyfikatów i list CRL przebiega następująco:

- Generowanie nowej, kolejnej i-tej głównej pary kluczy $\mathbf{GPK_{(i)}=\{K^{-1}_{GPK(i)}, K_{GPK(i)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(i)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(i)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową).
- Utworzenie autocertyfikatu zawierającego nowy klucz publiczny **Certum CA**, podpisany przy pomocy starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ (**autocertyfikat NowyStarym**).
- Deaktywacja starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ i aktywacja nowego klucza prywatnego $\mathbf{K^{1}_{GPK(I)}}$ – w sprzętowym module kryptograficznym znajduje się nowy klucz prywatny do podpisywania certyfikatów i list CRL.
- Utworzenie autocertyfikatu zawierającego stary klucz publiczny Certum CA, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(I)}}$ (**autocertyfikat StaryNowym**).
- Utworzenie autocertyfikatu zawierającego nowy klucz publiczny **Certum CA**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(I)}}$ (**autocertyfikat NowyNowym**).
- Opublikowanie utworzonych certyfikatów w repozytorium, rozesłanie informacji o nowych certyfikatach.

Po wygenerowaniu i uaktywnieniu nowego klucza prywatnego (może to nastąpić w dowolnym momencie okresu ważności starego autocertyfikatu), urząd **Certum CA** podpisuje certyfikaty pośrednie tylko przy pomocy nowego klucza prywatnego.

Stary klucz publiczny (stary autocertyfikat) jest w użyciu aż do momentu, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego autocertyfikatu (nowego klucza publicznego) **Certum CA** (powinno to nastąpić najpóźniej w momencie upływu okresu ważności starego autocertyfikatu).

Początek i koniec okresu ważności **autocertyfikatu StaryNowym** pokrywa się z początkiem i końcem okresu ważności starego autocertyfikatu.

Okres ważności **autocertyfikatu NowyStarym** rozpoczyna się w momencie wygenerowania nowej pary kluczy i kończy w chwili, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego autocertyfikatu (nowego klucza publicznego) **Certum CA** (powinno to nastąpić najpóźniej w momencie upływu okresu ważności starego autocertyfikatu).

Okres ważności **autocertyfikatu NowyNowym** rozpoczyna się w chwili wygenerowania nowej pary kluczy, zaś kończy się przynajmniej 180 dni po następnej przewidywanej chwili generowania kolejnej pary kluczy. Wymóg ten oznacza, że urząd certyfikacji **Certum CA**

zaprzestaje używać klucza prywatnego do podpisywania certyfikatów i list CRL przynajmniej na 180 dni przed datą upływu aktualności autocertyfikatu, z którym klucz prywatny jest związany.

6.1.1.3. Procedury aktualizacji kluczy urzędów certyfikacji podległych Certum CA

Procedury aktualizacji pośrednich kluczy urzędów **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV** i **Certum Partners** realizowane są podobnie jak w przypadku aktualizacji kluczy urzędu **Certum CA** (patrz rozdz. 6.1.1.2), poza jednym wyjątkiem: **certyfikat NowyNowym** wystawiany jest przez urząd **Certum CA**.

6.1.1.4. Procedury recertyfikacji kluczy Certum CA i innych urzędów certyfikacji

Certyfikaty urzędu certyfikacji **Certum CA** oraz innych urzędów mogą być recertyfikowane. Realizowane jest to tylko w przypadkach opisanych w rozdz. 3.2.2. Przed wydaniem nowego certyfikatu urząd certyfikacji ocenia, czy długość klucza gwarantuje mu dalsze bezpieczeństwo w okresie, na który przedłużany jest certyfikat.

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

Klucze subskrybentów generowane są przez nich samych lub mogą być generowane przez urząd certyfikacji w tokenie (np. kryptograficznej karcie elektronicznej) lub na dyskietce (tylko **Certum Level I**, w tym przypadku klucze są szyfrowane i zapisywane w formacie PKCS#12) i przekazywane subskrybentowi osobiście lub pocztą kurierską; dane do uaktywnienia karty (m.in. PIN/PUK) lub odszyfrowania kluczy (hasło) podane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji.

CERTUM gwarantuje, że procedury stosowane w urzędzie w żadnym momencie po wygenerowaniu na żądanie subskrybenta klucza prywatnego nie pozwalają na użycie go do realizacji podpisu cyfrowego ani też nie stwarzają warunków, które umożliwią zrealizowanie takiego podpisu innemu podmiotowi, poza właścicielem tego klucza.

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

Subskrybenci oraz operatorzy punktów rejestracji dostarczają wygenerowane przez siebie klucze publiczne w postaci żądań elektronicznych, których format musi być zgodny z realizowanymi przez urząd certyfikacji, punkt rejestracji oraz subskrybenta protokołami PKCS#10 *Certification Request Syntax*[33] (CRS).

W chwili obecnej CERTUM akceptuje jedynie żądania nadsyłane w formacie PKCS#10 Certification Request Syntax (CRS) oraz Netscape SPKAC (ang. Signed Public Key and Challenge).

Żądania wysyłane do urzędu certyfikacji mogą w niektórych przypadkach wymagać potwierdzenia w punkcie rejestracji (patrz rozdz. 3 i 4).

---

[33] RFC 2314 (CRS): B. Kaliski *PKCS #10: Certification Request Syntax, Version 1.5*, March 1998

Dostarczenie kluczy publicznych staje się zbędne przypadku, gdy klucze na żądanie zostały wygenerowane przez ten urząd certyfikacji, który dla wygenerowanego klucza publicznego wystawia jednocześnie certyfikat.

6.1.4. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

Klucze publiczne urzędu wydającego certyfikaty rozpowszechniane są tylko w formie certyfikatów zgodnych z zaleceniem ITU-T X.509 v.3, przy czym w przypadku urzędu certyfikacji **Certum CA** certyfikat ma postać autocertyfikatu.

Urzędy certyfikacji CERTUM rozpowszechniają swoje certyfikaty dwoma sposobami:

- umieszczają w ogólnie dostępnym repozytorium CERTUM w Internecie pod adresem: http://www.certum.pl
- dystrybuowane są za pomocą dedykowanego oprogramowaniem (np. przeglądarki internetowe, programy pocztowe, itp.), które umożliwia korzystanie z usług CERTUM.

W przypadku aktualizacji kluczy urzędów certyfikacji CERTUM w repozytorium umieszczane są wszystkie dodatkowe autocertyfikaty lub certyfikaty, powstałe w wyniku realizacji procedury opisanej w rozdz. 6.1.1.

6.1.5. Długości kluczy

Długości kluczy używanych przez CERTUM przez operatorów punktów rejestracji oraz użytkowników końcowych (subskrybentów) podano w Tab.6.1.

Tab.6.1 Stosowane klucze i ich długości

Typ właściciela klucza	Główny rodzaj zastosowania klucza		
	RSA do podpisu certyfikatów, CRL oraz poświadczeń	RSA do podpisu wiadomości i wymiany kluczy	Diffie-Hellman
Certum CA	2048 bitów	–	–
Certum Level I	1024 bity	–	–
Certum Level II	1024 bity	–	–
Certum Level III	1024 bity	–	–
Certum Level IV	1024 bity	–	–
Certum Partners	1024 bity	–	–
Certum Notary Authority	2048 bitów	–	–
Certum Validation Service	2048 bitów	–	–
Certum Time-Stamping Authority	2048 bitów	–	–
Osoby fizyczne i prawne oraz urządzenia tych osób (subskrybenci)	–	Definiowane przez użytkownika	–

6.1.6. Parametry generowania klucza publicznego

Niniejszy Kodeks Postępowania Certyfikacyjnego nie nakłada żadnych wymagań w tym zakresie. Zaleca się jednak, aby w przypadku generowania kluczy RSA i DSA spełnione były minimalne wymagania określone w *„Algorithms and Parameters for Secure Electronic Signatures”* [25].

6.1.7. Weryfikacja jakości klucza publicznego

Za jakość wygenerowanego klucza oraz jego weryfikację odpowiedzialność ponoszą ich twórcy. Wymaga się, aby weryfikacji poddano:

- zdolność do realizacji operacji szyfrowania i deszyfrowania, w tym podpisu cyfrowego i jego weryfikacji,
- proces generowania klucza, który powinien bazować na silnych kryptograficznie generatorach liczb losowych, najlepiej opartych na fizycznych źródłach szumu,
- odporność na znane ataki (dotyczy to algorytmów kryptograficznych RSA i DH).

Dodatkowo każdy urząd certyfikacji, po otrzymaniu lub wygenerowaniu (na żądanie subskrybenta) klucza publicznego poddaje go odpowiednim testom na zgodność z ograniczeniami nałożonymi przez Kodeks Postępowania Certyfikacyjnego (m.in. długość modułu oraz eksponenta).

Weryfikacja jakości parametrów klucza, obejmująca m.in. testy pierwszości w przypadku liczb pierwszych powinna być obligatoryjna w przypadku centralnego generowania kluczy i realizowana wg zaleceń określonych w *„Algorithms and Parameters for Secure Electronic Signatures”* [25].

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

W przypadku urzędów certyfikacji klucze generowane są przy pomocy sprzętowych modułów kryptograficznych, zgodnych z wymaganiami opisanymi w rozdz. 6.2.1.

W przypadku subskrybentów dopuszcza się zarówno sprzętowe, jak i programowe generowanie kluczy (rozdz. 6.2.1).

Tab.6.2 Sposób generowania kluczy subskrybenta

Nazwa polityki certyfikacji	Sposób generowania kluczy
Certum Level I	Sprzętowy lub programowy
Certum Level II	Sprzętowy lub programowy
Certum Level III	Sprzętowy lub programowy
Certum Level IV	Sprzętowy lub programowy
Certum Partners	Sprzętowy

6.1.9. Zastosowania kluczy

Sposób użycia klucza określony jest w polu **KeyUsage** (patrz rozdz. 7.1.1.2) rozszerzeń standardowych certyfikatu zgodnego z X.509 v3. Pole to jednak nie musi być obligatoryjnie weryfikowane przez aplikacje, które korzystają z tego certyfikatu.

Użycie poszczególnych bitów w polu **KeyUsage** musi być zgodne z następującymi zasadami (ustawiony bit oznacza odpowiednio):

a) **digitalSignature**: przeznaczenie certyfikatu do weryfikacji podpisu cyfrowego, złożonego w innych celach niż określone w pkt. b), f) i g);

b) **nonRepudiation**: przeznaczenie certyfikatu dla zapewnienia usługi niezaprzeczalności przez osoby fizyczne, ale jednocześnie dla innego celu niż określony w pkt. f) i g). Bit **nonRepudiation** może być ustawiony tylko w certyfikatach kluczy publicznych użytkowników służących do weryfikacji podpisów cyfrowych i nie może być łączony z innymi przeznaczeniami, w tym w szczególności o których mowa w pkt. c) - e) związanymi z zapewnieniem poufności;

c) **keyEncipherment**: do szyfrowania kluczy algorytmów symetrycznych zapewniających poufność danych;

d) **dataEncipherment**: do szyfrowania danych użytkownika, innych niż określone w pkt. c) i e);

e) **keyAgreement**: do protokołów uzgadniania klucza;

f) **keyCertSign**: klucz publiczny jest używany do weryfikacji podpisów cyfrowych w certyfikatach i zaświadczeniach certyfikacyjnych wydanych przez podmiot świadczący usługi certyfikacyjne;

g) **cRLSign**: klucz publiczny jest używany do weryfikacji podpisów cyfrowych w listach unieważnionych i zawieszonych certyfikatów wydanych przez podmiot świadczący usługi certyfikacyjne;

h) **encipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do szyfrowania danych w protokołach uzgadniania klucza;

i) **decipherOnly**: może być użyty tylko z bitem **keyAgreement** do wskazania, że służy tylko do odszyfrowania danych w protokołach uzgadniania klucza.

W przypadku certyfikatów wydanych według polityk **Certum Level I**, **Certum Level II**, **Certum Level III** i **Certum Level IV** dopuszcza się stosowanie jednego klucza zarówno w operacjach realizacji podpisu cyfrowego (bit **digitalSignature**), jak i też szyfrowania danych (bit **dataEncipherment**). Dzięki temu możliwe jest użycie tego typu certyfikatu np. w aplikacjach bazujących na protokole *Secure Multipurpose Internet Mail Extensions (S/MIME).*

Certyfikaty używane jednocześnie do podpisywania i szyfrowania mogą być wydawane jedynie subskrybentom. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie do weryfikacji podpisów cyfrowych, poza przypadkami wyraźnie określonymi w niniejszym Kodeksie Postępowania Certyfikacyjnego.

6.2. Ochrona klucza prywatnego

Każdy subskrybent, a także operatorzy urzędów certyfikacji i punktów rejestracji generują oraz przechowują swój klucz prywatny, wykorzystując w tym celu wiarygodny system tak, aby zapobiec jego utracie, ujawnieniu, modyfikacji lub nieautoryzowanemu użyciu. Urząd certyfikacji (patrz rodz.6.1.1), który generuje parę kluczy w imieniu subskrybenta, musi przekazać go w sposób bezpieczny oraz pouczyć subskrybenta o zasadach ochrony klucza prywatnego (patrz rozdz. 6.1.2).

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji są zgodne z wymaganiami normy FIPS 140-2. W przypadku używania przez subskrybenta sprzętowej ochrony klucza prywatnego zaleca się, aby spełniał on wymagania FIPS 140-2 lub ITSEC (*ITSEC v 1.2 wydany przez Komisję Europejską, Dyrektoriat XIII/F, w 1991 r.*).

Tab. 6.3 Minimalne wymagania nakładane na moduł kryptograficzny

Typ podmiotu certyfikatu	Wykorzystywany moduł kryptograficzny
Urząd certyfikacji Certum CA	Sprzętowy FIPS 140-2 Level 3 i wyżej
Urząd certyfikacji Certum Level I	Sprzętowy FIPS 140-2 Level 2 i wyżej
Urząd certyfikacji Certum Level II	Sprzętowy FIPS 140-2 Level 2 i wyżej
Urząd certyfikacji Certum Level III	Sprzętowy FIPS 140-2 Level 2 i wyżej
Urząd certyfikacji Certum Level IV	Sprzętowy FIPS 140-2 Level 2 i wyżej
Urząd certyfikacji Certum Partners	Sprzętowy FIPS 140-2 Level 2 i wyżej
Urząd znacznika czasu Certum Time-Stmaping Authority	Sprzętowy FIPS 140-2 Level 2 i wyżej
Urząd weryfikacji statusu certyfikatów Certum Validation Service	Sprzętowy FIPS 140-2 Level 2 i wyżej
Urząd DVCS Certum Notary Authority	Sprzętowy FIPS 140-2 Level 2 i wyżej
Osoba fizyczna i prawna lub urządzenie tej osoby (subskrybenci)	–
Punkt rejestracji	Sprzętowy FIPS 140-2 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 prywatne wszystkich urzędów certyfikacji CERTUM stosowane do realizacji podpisów certyfikatów i list CRL oraz innych operacji kryptograficznych, np. szyfrowanie wiadomości.

W CERTUM dopuszcza się bezpośrednią i pośrednią metodę podziału klucza prywatnego. W przypadku zastosowania metody bezpośredniej podziałowi na części poddawany jest klucz prywatny, z kolei w przypadku metody pośredniej podziałowi na części podlega kluczy symetryczny, którego wcześniej użyto do zaszyfrowania klucza prywatnego.

W obu przypadkach klucze (odpowiednio asymetryczny lub symetryczny) dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Tab.6.4.

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

Tab.6.4 Podział i dystrybucja sekretów współdzielonych

Nazwa podmiotu świadczącego usługi certyfikacyjne	Liczba sekretów współdzielonych wymagana do odtworzenia klucza	Całkowita liczba sekretów
Certum CA	3	5
Certum Level I	2	3
Certum Level II	2	3
Certum Level III	2	3
Certum Level IV	2	3
Certum Partners	2	3
Certum Time-Stamping Authority	2	3
Certum Validation Service	2	3
Certum Notary Authority	2	3

Procedura przekazania sekretów musi przewidywać udział posiadacza sekretu w procesie generowania kluczy i ich podziału, obejmować akceptację przekazanego sekretu, akceptację odpowiedzialności za przechowywany sekret oraz określać warunki i zasady udostępniania sekretu współdzielonego upoważnionym do tego osobom.

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

Każdy posiadacz sekretu współdzielonego, zanim wejdzie w jego posiadanie, powinien osobiście obserwować tworzenie, weryfikację poprawności utworzenia sekretu oraz jego dystrybucję. Każda część sekretu musi być przekazana posiadaczowi sekretu współdzielonego na karcie elektronicznej, chronionej tylko jemu znanym numerem PIN. Fakt otrzymania sekretu oraz zgodność sposobu jego utworzenia z zasadami niniejszego dokumentu posiadacz sekretu potwierdza własnoręcznym podpisem, złożonym na odpowiednim formularzu, którego kopia przekazywana jest urzędowi certyfikacji.

6.2.2.2. Zabezpieczenie sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien chronić go przed ujawnieniem. Z wyjątkami, opisanymi dalej, posiadacz sekretu współdzielonego deklaruje, że:

- nie ujawni, nie skopiuje, nie udostępni stronom trzecim, ani też nie użyje sekretu w sposób nieautoryzowany,
- nie wyjawi (bezpośrednio lub pośrednio), że jest posiadaczem sekretu współdzielonego,
- nie będzie przechowywał sekretu współdzielonego w miejscu, które uniemożliwi odzyskanie sekretu w przypadku, gdy posiadacz sekretu będzie poza miejscem normalnego pobytu lub będzie nieosiągalny.

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien udostępniać współdzielony sekret autoryzowanym osobom (wyszczególnionym w formularzu, podpisanym przez posiadacza w

momencie powierzania sekretu) tylko po uprzedniej autoryzacji czynności przekazania sekretu. Fakt ten powinien zostać odnotowany w systemie zabezpieczeń w postaci odpowiedniego wpisu do rejestru zdarzeń.

W sytuacjach klęsk żywiołowych (deklarowanych wcześniej przez wydawcę sekretu współdzielonego), posiadacz sekretu współdzielonego powinien zgłosić się do ośrodka zapasowego CERTUM, zgodnie z instrukcją otrzymaną od wydawcy sekretu. Zanim posiadacz sekretu współdzielonego stawi się w żądane miejsce powinien uzyskać od wydawcy sekretu uwierzytelnione potwierdzenie zaistniałego faktu oraz polecenie udania się w zalecane miejsce. Do ośrodka zapasowego sekret współdzielony powinien zostać dostarczony osobiście w sposób, który umożliwi użycie go w przypadku klęski żywiołowej w procedurze powrotu urzędu certyfikacji do stanu normalnego.

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien wykonywać swoje obowiązki zgodnie z postanowieniami niniejszego dokumentu oraz w sposób odpowiedzialny i rozważny we wszystkich możliwych sytuacjach. Powinien on poinformować wydawcę sekretu współdzielonego o zgubieniu, kradzieży, niewłaściwym ujawnieniu lub naruszeniu ochrony sekretu, natychmiast po zorientowaniu się, że fakt taki miał miejsce. Posiadacz sekretu współdzielonego nie odpowiada za zaniedbanie swoich obowiązków wskutek przyczyn, które były poza kontrolą posiadacza sekretu, ale ponosi odpowiedzialność za niewłaściwe ujawnienie sekretu lub zaniedbanie obowiązku poinformowania wydawcy sekretów współdzielonych o niewłaściwym ujawnieniu lub naruszenia ochrony sekretu, wynikające z własnego błędu, w tym z zaniedbania lub lekkomyślności.

6.2.3. Deponowanie klucza prywatnego

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

Kopie prywatnych kluczy subskrybentów mogą być jednak archiwizowane w urzędzie certyfikacji lub u subskrybenta i następnie odzyskiwane. Może to być robione na dwa sposoby:

- subskrybent może wygenerować klucz symetryczny, zaszyfrować nim klucz prywatny i przekazać urzędowi certyfikacji albo zaszyfrowany klucz prywatny (klucz symetryczny przechowuje subskrybent) albo w bezpieczny sposób klucz symetryczny (zaszyfrowany klucz prywatny przechowywany jest u subskrybenta),
- subskrybent w bezpieczny sposób przesyła klucz prywatny do urzędu certyfikacji, gdzie jest on deponowany w skarbcu elektronicznym (*ang. Electronic Vault*).

Jeśli subskrybent chce odzyskać złożoną w urzędzie certyfikacji kopię klucza prywatnego, to żąda:

- w pierwszym przypadku przysłania albo zaszyfrowanego klucza prywatnego (klucz deszyfrujący posiada subskrybent) albo klucza deszyfrującego (zaszyfrowana kopia klucza prywatnego jest w posiadaniu subskrybenta), zaś
- w drugim bezpiecznego przekazania subskrybentowi zarchiwizowanego w urzędzie certyfikacji klucza prywatnego.

6.2.4. Kopie zapasowe klucza prywatnego

Urzędy certyfikacji funkcjonujące w ramach CERTUM tworzą kopie swoich kluczy prywatnych. Kopie te wykorzystywane są w przypadku potrzeby realizacji normalnej lub awaryjnej (np. po wystąpieniu klęski żywiołowej) procedury odzyskiwania kluczy.

W zależności od zastosowanej metody podziału klucza na części (odpowiednio bezpośredniej lub pośredniej, patrz rozdz. 6.2.2) kopie klucza prywatnego przechowywane są w częściach lub w całości (po zaszyfrowaniu kluczem symetrycznym). Skopiowane klucze przechowywane są wewnątrz sprzętowych modułów kryptograficznych. Moduł kryptograficzny stosowany do przechowywania kluczy prywatnych spełnia wymagania przedstawione w rozdz. 6.2.1. Kopia klucza prywatnego wprowadzana jest z kolei do modułu kryptograficznego zgodnie z procedurą opisaną w rozdz. 6.2.6.

Sekrety współdzielone, kopie klucza szyfrującego sekrety, jak też chroniące je numery PIN przechowywane są w różnych, fizycznie chronionych, miejscach. W żadnym z tych miejsc nie jest przechowywany taki zestaw kart oraz numerów PIN, który umożliwia odtworzenie klucza urzędu certyfikacji.

Urzędy CERTUM nie przechowują kopii kluczy prywatnych operatorów punktów rejestracji. Kopie kluczy subskrybentów tworzone są jedynie na ich żądanie i zgodnie z metodami opisanymi w rozdz. 6.2.3.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędów certyfikacji stosowane do realizacji podpisów cyfrowych są archiwizowane przynajmniej 5 lat od chwili zaprzestania wykonywania przy ich użyciu operacji podpisywania. Analogiczne sytuacja ma miejsce po upływie okresu ważności komplementarnego z kluczem prywatnym certyfikatu lub po jego unieważnieniu.

Klucze prywatne urzędów certyfikacji stosowane w operacjach uzgadniania lub szyfrowania kluczy muszą być archiwizowane po utracie okresu ważności odpowiadającego im certyfikatu lub po jego unieważnieniu przez okres dłuższy niż 5 lat. Archiwizowane klucze są dostępne przez 25 lat, z tego przez okres 15 lat muszą być dostępne w trybie *on-line*.

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,
- może być konieczne przeniesienie klucza prywatnego z modułu operacyjnego, wykorzystywanego codziennie przez podmiot do innego modułu; sytuacja taka może wystąpić np. w przypadku defektu modułu lub konieczności jego zniszczenia.

Wprowadzanie klucza prywatnego do modułu kryptograficznego jest operacją krytyczną. Z tego względu w trakcie jej realizacji stosowane są takie środki i procedury, które zapobiegają ujawnieniu klucza, jego modyfikacji lub podstawienia.

W CERTUM stosuje się dwie metody zapewnienia integralności ładowanemu kluczowi:

- po pierwsze, jeśli klucz występuje w całości, to nie jest on nigdy dostępny poza modułem w postaci jawnej; oznacza to, że w momencie wygenerowania klucza i

konieczności załadowania go do innego modułu, klucz ten jest szyfrowany przy pomocy klucza tajnego; klucz tajny jest tak przechowywany, że nigdy osoba do tego nieupoważniona nie jest w posiadaniu obu tych informacji jednocześnie,

- po drugie, jeśli klucz lub chroniące go hasło przechowywane są w częściach, to dzięki ładowaniu kolejnych fragmentów sam moduł jest w stanie zweryfikować potencjalne próby ataków lub oszustw.

Wprowadzenie klucza prywatnego do obszaru sprzętowego modułu kryptograficznego któregokolwiek z urzędów certyfikacji wymaga odtworzenia klucza z kart w obecności wymaganej w tym celu liczby posiadaczy sekretów współdzielonych lub kart administratorskich chroniących moduł z kluczami (patrz rozdz. 6.2.2). Ponieważ każdy urząd certyfikacji może posiadać także zaszyfrowane kopie kluczy prywatnych (rozdz. 6.2.4), stąd klucze te można w takiej postaci przenosić także pomiędzy modułami kryptograficznymi.

Klucz prywatny operatora punktu rejestracji występuje zawsze tylko w jednym egzemplarzu (brak kopii) i z tego powodu nie jest wymagana operacja wprowadzania klucza do modułu kryptograficznego.

Z kolei zainstalowanie klucza prywatnego w module kryptograficznym subskrybenta końcowego może wymagać załadowania go z posiadanego nośnika, np. plik chroniony hasłem na dyskietce (operację tę może wykonać tylko sam subskrybent).

6.2.7. Metody aktywacji klucza prywatnego

Metody aktywacji kluczy prywatnych, będących w posiadaniu różnych uczestników i użytkowników systemu CERTUM odnoszą się do sposobów uaktywniania kluczy przed każdym ich użyciem lub przed rozpoczęciem każdej sesji (np. połączenia internetowego), w trakcie której klucze te są stosowane. Raz uaktywniony klucz prywatny jest gotowy do użycia aż do momentu jego dezaktywacji.

Przebieg procedur aktywacji (i dezaktywacji) klucza prywatnego jest uzależniony od typu podmiotu, w którego posiadaniu jest klucz (użytkownik końcowy, punkt rejestracji, urząd certyfikacji, urządzenia, itp.), ważności danych, które są chronione przy pomocy tego klucza oraz tego czy klucz po uaktywnieniu pozostaje aktywny tylko na czas wykonania jednej operacji z użyciem klucza, jednej sesji lub na czas nieokreślony.

Wszystkie klucze prywatne urzędów certyfikacji 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 podpisujące operatorów punktów rejestracji stosowane do podpisywania informacji są uaktywniane dopiero po uwierzytelnieniu operatora (podaniu numeru PIN) i tylko na czas wykonania pojedynczej operacji kryptograficznej z użyciem tego klucza. Po zakończeniu wykonywania operacji klucz prywatny jest automatycznie dezaktywowany i musi być ponownie uaktywniany przed wykonaniem kolejnej operacji. Inne klucze prywatne, np. używane do uwierzytelnienia aplikacji punktu rejestracji lub utworzenia szyfrowanego połączenia sieciowego uaktywniane są automatycznie na okres trwania sesji, natychmiast po uwierzytelnieniu operatora. Zakończenie sesji dezaktywuje wszystkie uaktywnione wcześniej klucze prywatne.

Aktywacja kluczy prywatnych subskrybentów realizowana jest podobnie jak w przypadku kluczy operatorów punktów rejestracji, niezależnie od tego czy klucze przechowywane są na karcie elektronicznej, czy też w postaci zaszyfrowanej na dyskietce lub innym nośniku.

6.2.8. Metody dezaktywacji klucza prywatnego

Metody dezaktywacji kluczy prywatnych odnoszą się do sposobów dezaktywowania kluczy po każdym ich użyciu lub po zakończeniu każdej sesji (np. połączenia internetowego) w trakcie której klucze te są stosowane.

W przypadku kluczy subskrybenta lub operatora punktu rejestracji dezaktywowanie kluczy podpisujących następuje natychmiast po zrealizowaniu podpisu cyfrowego lub po zakończeniu sesji (np. wylogowania się z aplikacji). Jeśli w trakcie wykonywania operacji kryptograficznych klucz prywatny znajdował się w pamięci operacyjnej aplikacji, to aplikacja musi zadbać o to, aby niemożliwe było nieautoryzowane odtworzenie klucza prywatnego.

W przypadku CERTUM dezaktywowanie kluczy jest wykonane 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.

6.2.9. Metody niszczenia klucza prywatnego

Niszczenie kluczy subskrybentów lub operatorów punktu rejestracji polega odpowiednio na ich bezpiecznym wymazaniu z nośnika (z dyskietki, karty elektronicznej, pamięci operacyjnej, sprzętowego modułu kryptograficznego, itp.), zniszczeniu nośnika kluczy (np. karty elektronicznej) lub przynajmniej przejęcie nad nim kontroli w przypadku, gdy mechanizmy karty nie zezwalają na definitywne usunięcie z niej informacji o kluczu prywatnym.

Niszczenie klucza prywatnego urzędów certyfikacji oznacza fizyczne zniszczenie kart elektronicznych i/lub innych nośników, na których są przechowywane kopie lub archiwizowane sekrety współdzielone. Każde zniszczenie klucza prywatnego jest odnotowywane w rejestrze zdarzeń.

6.3. Inne aspekty zarządzania kluczami

Pozostałe wymagania tego rozdziału dotyczą procedury archiwizowania kluczy publicznych oraz okresów ważności kluczy publicznych i prywatnych wszystkich subskrybentów, w tym także urzędów certyfikacji.

6.3.1. Archiwizacja kluczy publicznych

Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów cyfrowych już po usunięciu certyfikatu z repozytorium (patrz rozdz. 2.6). Jest to szczególnie ważne w przypadku świadczenia usług niezaprzeczalności, takich jak np. usługa znacznika czasu lub usługa weryfikacji statusu certyfikatu.

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

Każdy z urzędów wydających certyfikaty przechowuje klucze publiczne tych subskrybentów, którym wydał je w postaci certyfikatów. Własne klucze publiczne urzędu certyfikacji archiwizowane są razem w sposób przedstawiony w rozdz. 6.2.5.

Certyfikaty mogą być także archiwizowane lokalnie przez subskrybentów, zwłaszcza w przypadkach, gdy wymagają tego używane przez nich aplikacje, np. poczta elektroniczna.

Archiwa kluczy publicznych powinny być chronione w taki sposób, aby możliwe było zapobieganie nieautoryzowanemu dodawaniu kluczy do archiwum, kasowaniu lub modyfikacji. Tego typu ochronę osiąga się dzięki uwierzytelnianiu podmiotów archiwizujących oraz autoryzowaniu ich żądań.

W systemie CERTUM archiwizowane są tylko klucze używane do weryfikacji podpisów cyfrowych. Każdy inny typ klucza publicznego (np. klucz używany do szyfrowania wiadomości) jest natychmiast niszczony po usunięciu go z repozytorium.

Inspektor bezpieczeństwa dokonuje raz na kwartał audytu archiwum kluczy, sprawdzając jego integralność. Sprawdzenie to ma na celu upewnienie się, że archiwum nie zawiera luk i że certyfikaty w nim przechowywane nie zostały zmodyfikowane. Mechanizmy zapewniające integralność archiwum biorą pod uwagę fakt, iż okres przechowywania archiwum może być większy, aniżeli odporność na złamanie kluczy użytych do ich budowy.

Klucze publiczne przechowywane są w archiwum kluczy publicznych przez okres 25 lat (patrz także rozdz. 4.11).

Każde zarchiwizowanie lub zniszczenie klucza publicznego jest odnotowywane w rejestrze zdarzeń.

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole **validity** każdego certyfikatu klucza publicznego (patrz rozdz. 7.1). Okres ważności klucza prywatnego może być krótszy niż okres ważności certyfikatu lub zaświadczenia certyfikacyjnego (wynika to z możliwości zaprzestania używania klucza w dowolnym momencie).

Standardowe maksymalne okresy ważności certyfikatów urzędów certyfikacji podane są w Tab.6.5, zaś certyfikatów subskrybentów w Tab.6.6.

Okresy ważności certyfikatu i tym samym klucza prywatnego mogą ulec skróceniu w wyniku zawieszenia lub unieważnienia kluczy.

Początkowa data ważności certyfikatu pokrywa się z datą jego wydania. Nie dopuszcza się, aby data ta ulokowana była w przeszłości ani w przyszłości.

Tab.6.5 Maksymalne okresy ważności certyfikatów urzędów

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza	
		RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokenów
Certum CA	klucz publiczny	25 lat	–
	klucz prywatny	15 lat	–
Certum Level I	klucz publiczny	10 lat	–
	klucz prywatny	9 lat	–
Certum Level II	klucz publiczny	10 lat	–
	klucz prywatny	9 lat	–
Certum Level III	klucz publiczny	10 lat	–
	klucz prywatny	8 lat	–
Certum Level IV	klucz publiczny	10 lat	–
	klucz prywatny	8 lat	–
Certum Partners	klucz publiczny	10 lat	–
	klucz prywatny	5 lat	–
Certum Time-Stamping Authority	klucz publiczny	–	10 lat
	klucz prywatny	–	10 lat
Certum Validation Service	klucz publiczny	–	10 lat
	klucz prywatny	–	10 lat
Certum Notary Authority	klucz publiczny	–	10 lat
	klucz prywatny	–	10 lat

Każdy z użytkowników, w tym przede wszystkim urzędy certyfikacji, może w dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji podpisów, mimo że certyfikat jest nadal aktualnie ważny. Urząd certyfikacji jest jednak zobowiązany do poinformowania o tym fakcie (związanym ze zmianą kluczy) swoich subskrybentów.

Tab.6.6 Maksymalne okresy ważności certyfikatów subskrybentów

Typ właściciela klucza	Nazwa polityki certyfikacji	Główny rodzaj zastosowania klucza		
		RSA do podpisu wiadomości	RSA do wymiany kluczy	Diffie-Hellman
Osoby fizyczne oraz urządzenia osób fizycznych	Certum Level I	min. 3 miesiące	min. 3 miesiące	min. 3 miesiące
	Certum Level II	1 rok	1 rok	1 rok
	Certum Level III	2 lata	2 lata	2 lata
	Certum Level IV	2 lata	2 lata	2 lata
Osoby prawne oraz urządzenia osób prawnych	Certum Level I	min. 3 miesiące	min. 3 miesiące	min. 3 miesiące
	Certum Level II	1 rok	1 rok	1 rok
	Certum Level III	2 lata	2 lata	2 lata
	Certum Level IV	2 lata	2 lata	2 lata
	Certum Partners	–	5 lat	–

6.4. Dane aktywujące

Dane aktywujące stosowane są do uaktywniania kluczy prywatnych stosowanych przez punkty rejestracji, urzędy certyfikacji oraz subskrybentów. Najczęściej używane są na etapie uwierzytelnienia podmiotu i kontroli dostępu do klucza prywatnego.

6.4.1. Generowanie danych aktywujących i ich instalowanie

Dane aktywujące używane są w dwóch podstawowych przypadkach:

- jako element jedno- lub dwuczynnikowej procedury uwierzytelniania (tzw. frazy uwierzytelniania, np. hasła, numery PIN, itp.),
- jako część sekretu współdzielonego, który po zainstalowaniu w systemie umożliwią odtworzenie klucza lub kluczy kryptograficznych.

Operatorzy punktów rejestracji, urzędów certyfikacji oraz inne osoby pełniące role określone w rozdz. 5.2 posługują się hasłami odpornymi na ataki brutalne (zwane także wyczerpującymi). Zaleca się, aby w podobny sposób tworzone były hasła subskrybentów.

W przypadku aktywacji kluczy prywatnych zaleca się stosowanie dwuczynnikowych procedur uwierzytelniania, np. token kryptograficzny (w tym także kryptograficzna karta elektroniczna) i fraza uwierzytelniania lub token kryptograficzny i biometria (np. odcisk palca).

Frazy uwierzytelnienia, o których była mowa powyżej, powinny być generowane zgodnie z wymaganiami określonymi w FIPS 112.

Sekrety współdzielone używane do ochrony kluczy prywatnych urzędów certyfikacji generowane są zgodnie z wymaganiami określonymi w rozdz. 6.2 i zapisywane w tokenach kryptograficznych. Tokeny chronione są numerem PIN, którego procedura tworzenia jest zgodna z FIPS 12. Sekrety współdzielone stają się danymi aktywacyjnymi dopiero po ich uaktywnieniu, tj. prawidłowym podaniu numeru PIN chroniącego token.

6.4.2. Ochrona danych aktywujących

Ochrona danych aktywujących obejmuje takie metody kontroli danych aktywujących, które zapobiegają ich ujawnieniu. Metody kontroli ochrony danych aktywujących zależą z jednej strony od tego czy są to frazy uwierzytelniania, z drugiej zaś strony od tego czy kontrola ta sprawowana jest na podstawie podziału na części (sekrety współdzielone) klucza prywatnego lub też aktywujących go danych.

W przypadku ochrony fraz uwierzytelniania należy stosować się do zaleceń określonych w FIPS 112, z kolei przy ochronie sekretów współdzielonych do zaleceń FIPS 140.

Zaleca się, aby dane aktywujące stosowane do uaktywniania kluczy prywatnych były chronione przy zastosowaniu mechanizmów kryptograficznych oraz fizycznej kontroli dostępu. Dane aktywujące powinny być danymi biometrycznymi lub pamiętanymi (nie zapisywanymi) przez podmiot uwierzytelniany. Jeśli dane aktywujące są zapisywane, to ich poziom zabezpieczenia powinien być taki sam jak danych, do których ochrony użyto tokena kryptograficznego. Kilkakrotne nieudane próby dostępu do takiego modułu powinny prowadzić do zablokowania tokena. Zapisywane dane aktywujące nie są nigdy przechowywane razem z tokenem kryptograficznym.

6.4.3. Inne problemy związane z danymi aktywującymi

Dane aktywujące przechowywane są zawsze tylko w jednej kopii. Jedynym odstępstwem od tej zasady są numery PIN, chroniące dostęp do sekretów współdzielonych – każdy posiadacz sekretu może stworzyć kopie numeru PIN i przechowywać w innym miejscu niż sekret współdzielony.

Dane aktywujące chroniące dostęp do kluczy prywatnych zapisanych w tokenach kryptograficznych mogą być okresowo zmieniane.

Dane aktywujące mogą podlegać archiwizacji.

6.5. Zabezpieczenia systemu komputerowego

Zadania punktów rejestracji i urzędów certyfikacji funkcjonujących w ramach systemu CERTUM realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzących system, który spełnia wymagania określone w dokumencie *Information Technology Security Evaluation Criteria*[34] (ITSEC), przynajmniej na poziomie E3.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

Wymagania techniczne określone w niniejszym rozdziale odnoszą się do kontroli zabezpieczeń pojedynczego komputera oraz zainstalowanego na nim oprogramowania, używanego w systemie CERTUM. Funkcje zabezpieczające systemy komputerowe są realizowane na poziomie systemu operacyjnego, aplikacji oraz zabezpieczeń fizycznych.

Komputery funkcjonujące w urzędach certyfikacji oraz w powiązanych z nimi komponentach (np. punktach rejestracji) wyposażone są w następujące funkcje zabezpieczające:

- obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),

[34] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

- uznaniową kontrolę dostępu,
- możliwość prowadzenia audytu zabezpieczeń,
- komputery udostępniane są tylko personelowi, który pełni zaufane role w CERTUM,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
- archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
- bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
- mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

Ocena zabezpieczeń systemów komputerów prowadzona jest zgodnie wytycznymi zawartymi w *Information Technology Security Evaluation Cryteria* (ITSEC) i dotyczącymi zabezpieczeń poziomu E4.

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe CERTUM spełniają wymagania określone w *Information Technology Security Evaluation Cryteria* (ITSEC). Zostało to potwierdzone przez niezależnego audytora, oceniającego funkcjonowanie systemu CERTUM na podstawie kryteriów określonych w *WebTrust Principles and Criteria for Certification Authorities*.

6.6. Kontrola techniczna

6.6.1. Kontrola zmian systemu

Aplikacje stosowane w systemie CERTUM są projektowane i implementowane przez Unizeto Technologies S.A. Wszystkie aplikacje są rozwijane i uaktualniane za pośrednictwem systemu Concurrent Versions System (CVS). W systemie CVS tworzona jest również dokumentacja systemu.

Rejestrowane i monitorowane są również wymiany sprzętu w systemie. W szczególności mechanizmy te zapewniają, że:

- sprzęt dostarczany jest w sposób, który umożliwia prześledzenie całej drogi przebytej przez sprzęt od dostawcy do miejsca zainstalowania,
- dostawa sprzętu na wymianę jest realizowana w taki sam sposób jak dostawa sprzętu oryginalnego; sama wymiana jest dokonywana przez zaufany i przeszkolony personel.

6.6.2. Kontrola zarządzania bezpieczeństwem

Kontrola zarządzania bezpieczeństwem ma na celu takie nadzorowanie funkcjonowania systemu CERTUM, która daje pewność, że system ten pracuje prawidłowo i jego funkcje są zgodne z zaplanowaną i zrealizowaną konfiguracją.

Aktualna konfiguracja systemu CERTUM, jak również dowolne modyfikacje i aktualizacje tego systemu są dokumentowane i kontrolowane. Zastosowane w systemie CERTUM mechanizmy pozwalają na ciągłą weryfikację integralności oprogramowania, kontrolę ich wersji, a także uwierzytelnianie i weryfikowanie źródła pochodzenia.

6.6.3. Ocena cyklu życia zabezpieczeń

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

6.7. 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.

Pierwszy segment zawiera serwer WWW oraz serwer SMTP (łącznie – repozytorium systemu), natomiast drugi segment wydzieloną, oddzieloną logicznie część wewnętrzną obsługującą właściwy proces certyfikacji (zawiera ona m.in. serwer certyfikujący oraz serwer bazy danych).

CERTUM posiada drugą podsieć spełniającą rolę systemu modelowego, wykorzystywanego w pracach projektowych oraz do testów.

System komputerowy CERTUM zabezpieczony jest przed atakiem typu odmowa usługi oraz chroniony jest przez system wykrywania intruzów. Mechanizmy ochrony zbudowane są w oparciu o zaporę sieciową (*ang. firewall*) oraz filtrowanie ruchu w routerach i serwisach PROXY.

Zabezpieczenia zapór sieciowych akceptują jedynie wiadomości przysyłane i wysyłane w oparciu o protokoły: http, https, NTP, POP3 oraz SMTP. Zapisy zdarzeń (logi) rejestrowane przez rejestry systemowe umożliwiają nadzorowanie przypadków niewłaściwego korzystania z usług świadczonych przez CERTUM.

Szczegółowy opis konfiguracji sieci CERTUM oraz jej zabezpieczeń zawarty jest w dokumentacji infrastruktury technicznej systemu. Dokument ma status „niejawny" i udostępniany jest tylko upoważnionym osobom.

6.8. Kontrola wytwarzania modułu kryptograficznego

Kontrola wytwarzania modułu kryptograficznego obejmuje wymagania nakładane na proces projektowania, produkcji i dostarczania modułów kryptograficznych. CERTUM nie definiuje własnych wymagań w tym zakresie. Akceptuje jednak tylko takie moduły kryptograficzne, które spełniają wymagania określone w rozdz. 6.2.

6.9. Znaczniki czasu jako element bezpieczeństwa

Wnioski tworzone w ramach protokołu CMP lub CRS (rozdz. 6.1.3) nie wymagają znakowania wiarygodnym czasem. W przypadku innych wiadomości przesyłanych pomiędzy urzędem certyfikacji, punktem rejestracji i subskrybentem zaleca się stosować znaczniki czasu.

Znaczniki czasu tworzone w ramach systemu CERTUM są zgodne z zaleceniem RFC 3161 oraz Microsoft Authenticode™. Znaczniki czasu wydawane są zgodnie z Polityką Urzędu Znacznika Czasu (dokument jest dostępny *on-line* w repozytorium).

7. Profile certyfikatów, listy CRL, token znacznika czasu i statusu certyfikatu

Profile certyfikatów oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3, zaś tokena statusu certyfikatu z RFC 2560 oraz tokena znacznika z RFC 3161 (patrz także *ETSI Time stamping profile, TS 101 861 v1.2.1*). Przedstawione poniżej informacje określają znaczenie poszczególnych pól certyfikatu, list CRL, tokena znacznika czasu i tokena statusu certyfikatu, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek CERTUM.

7.1. Struktura certyfikatów

Certyfikat według normy X.509 v.3 jest sekwencją trzech pól, z których pierwsze zawiera treść certyfikatu (**tbsCertificate**), drugie – informację o typie algorytmu użytego do podpisania certyfikatu (**signatureAlgorithm**), zaś trzecie – podpis cyfrowy, składany na certyfikacie przez urząd certyfikacji (**signatureValue**).

7.1.1. Treść certyfikatu

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

Rozszerzenia zdefiniowane w certyfikatach zgodnych z rekomendacją X.509 v.3 umożliwiają przypisanie dodatkowych atrybutów subskrybentowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną strukturą certyfikatów. Certyfikaty zgodne z rekomendacją X.509 v.3 pozwalają także definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

7.1.1.1. Pola podstawowe

CERTUM obsługuje następujące pola podstawowe certyfikatu:

- **Version**: wersję trzecią (X.509 v.3) formatu certyfikatu;
- **SerialNumber**: numer seryjny certyfikatu, unikalny w ramach domeny urzędu certyfikacji;
- **Signature Algorithm**: identyfikator algorytmu stosowanego przez urząd certyfikacji wydający certyfikaty do podpisania certyfikatu;
- **Issuer**: nazwa wyróżniająca (DN) urzędu certyfikacji;
- **Validity**: data ważności certyfikatu określona przez początek (**notBefore**) oraz koniec (**notAfter**) ważności certyfikatu;
- **Subject**: nazwę wyróżniająca (DN) subskrybenta, otrzymującego certyfikat;

- **SubjectPublicKeyInfo**: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

W certyfikatach wydawanych przez CERTUM wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab.7.1.

Tab.7.1 Profil podstawowych pól certyfikatu

Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	Version 3	
Serial Number (numer seryjny)	Unikalne wartości we wszystkich certyfikatach wydawanych przez urzędy certyfikacji CERTUM.	
Signature Algorithm (algorytm podpisu)	md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) lub sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (wystawca, nazwa DN)	Common Name (CN) =	Certum {CA,Level{I,II,III,IV},Partners}
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar CERTUM 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). Zegar CERTUM jest znany jako ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Subject (podmiot, nazwa DN)	Nazwa DN jest zgodna z wymaganiami X.501. Wszystkie atrybuty tego pola są opcjonalne, z wyjątkiem pól: emailAddress (w przypadku certyfikatów subskrybenta), organizationName (w przypadku certyfikatów urzędów certyfikacji i podmiotów świadczących usługi niezaprzeczalności), commonName (w przypadku certyfikatów serwerów), unstructured{Address or Name} (w przypadku certyfikatów VPN), które są obligatoryjne.	
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.	

7.1.1.2. Pola rozszerzeń standardowych

Funkcja każdego z rozszerzeń określona jest przez standardową wartość związanego z nim identyfikatora obiektu (**OBJECT IDENTIFIER**). Rozszerzenie, w zależności od opcji wybranej przez organ wydający certyfikat, może być **krytyczne** lub **niekrytyczne**. Jeśli rozszerzenie oznaczone jest jako krytyczne, to aplikacja bazująca na certyfikatach musi odrzucić każdy certyfikat, w którym po napotkaniu krytycznego rozszerzenia nie będzie w stanie go rozpoznać. Z kolei każde niekrytyczne rozszerzenie może być ignorowane.

CERTUM obsługuje następujące pola rozszerzeń podstawowych certyfikatu:

- **AuthorityKeyIdentifier**: identyfikator certyfikatu klucza publicznego urzędu certyfikacji komplementarnego z tym kluczem prywatnym, przy pomocy którego urząd certyfikacji podpisał wydany certyfikat – **rozszerzenie nie jest krytyczne**;
- **SubjectKeyIdentifier**: identyfikator klucza podmiotu – **rozszerzenie nie jest krytyczne**;
- **KeyUsage**: dozwolone użycie klucza – **rozszerzenie może być krytyczne**. Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do szyfrowania danych, klucz do podpisu cyfrowego, itp. (patrz niżej)

```
digitalSignature          (0), -- klucz do realizacji podpisu cyfrowego
nonRepudiation            (1), -- klucz związany z realizacją usług
                               -- niezaprzeczalności
keyEncipherment           (2), -- klucz do wymiany kluczy
dataEncipherment          (3), -- klucz do szyfrowania danych
keyAgreement              (4), -- klucz do uzgadniania kluczy
keyCertSign               (5), -- klucz do podpisywania certyfikatów
cRLSign                   (6), -- klucz do podpisywania list CRL
encipherOnly              (7), -- klucz tylko do szyfrowania
decipherOnly              (8)  -- klucz tylko do deszyfrowania
```

- **ExtKeyUsage**: sprecyzowanie (ograniczenie) użycia klucza – **rozszerzenie może być krytyczne**. Pole to określa jeden lub więcej obszarów, w uzupełnieniu podstawowego zastosowania określonego przez pole **keyUsage**, w obrębie których może być stosowany certyfikat. Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**. CERTUM wydaje certyfikaty, które mogą zawierać jedną z poniższych wartości lub ich kombinację:

```
serverAuth       - uwierzytelnianie TLS Web serwera; bity pola keyUsage,
                   które są zgodne z tym polem: digitalSignature,
                   keyEncipherment lub keyAgreement
clientAuth       - uwierzytelnianie TLS Web klient; bity pola keyUsage,
                   które są zgodne z tym polem: digitalSignature
                   i/lub keyAgreement
codeSigning      - podpisywanie ładowalnego kodu wykonywalnego;
                   bity pola keyUsage, które są zgodne z tym polem:
                   digitalSignature
emailProtection  - ochrona E-mail; bity pola keyUsage, które są zgodne
                   z tym polem: digitalSignature, nonRepudiation i/lub
                   (keyEncipherment lub keyAgreement)
ipsecEndSystem   - ochrona protokołu IPSEC
ipsecTunnel      - tryb tunelowania protokołu IPSEC
ipsecUser        - ochrona protokołu IP w aplikacjach użytkownika
timeStamping     - wiązanie wartości skrótu z czasem z wcześniej
                   uzgodnionego wiarygodnego źródła czasu; bity pola
                   keyUsage, które są zgodne z tym polem:
                   digitalSignature i/lub nonRepudiation
OCSPSigning      - oznacza prawo do wystawiania w imieniu CA poświadczeń
                   statusu certyfikatu; bity pola keyUsage, które są
                   zgodne z tym polem: digitalSignature i/lub
                   nonRepudiation
dvcs             - wystawianie poświadczeń przez urząd notarialny w
                   oparciu o protokół DVCS; bity pola keyUsage, które są
                   zgodne z tym polem: digitalSignature, nonRepudiation,
                   keyCertSign, cRLSign
```

- **CertificatePolicies**: informacja typu **PolicyInformation** (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez dany organ wydający certyfikaty – **rozszerzenie nie jest krytyczne**

Tab.7.2 Identyfikatory polityk i ich opisy

Identyfikator polityki	Opis polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-I(1)[35]	Identyfikuje politykę certyfikacji o nazwie Certum Level I.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-II(2)	Identyfikuje politykę certyfikacji o nazwie Certum Level II.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-III(3)	Identyfikuje politykę certyfikacji o nazwie Certum Level III.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-IV(4)	Identyfikuje politykę certyfikacji o nazwie Certum Level IV.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-tsa(5)	Identyfikuje politykę oznaczania czasem o nazwie Certum Time-Stamping Authority.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-dvcs(6)	Identyfikuje politykę usług notarialnych o nazwie Certum Notary Authority.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-rfc-3125-signature(7)	Identyfikuje politykę podpisu elektronicznego RFC 3125/RFC 3126 o nazwie Certum Electronic Signature Policy.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-dstamp(8)	Identyfikuje politykę usług o nazwie Certum Digital Stamp.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-partners(9)	Identyfikuje politykę certyfikacji urzędów o nazwie Certum Partners.

W certyfikatach wydawanych przez urzędy certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 3280.

- **PolicyMapping**: odwzorowanie polityki – **rozszerzenie nie jest krytyczne**; pole to zawiera jedną lub więcej par OID, które określają równoważność polityki wydawcy z polityką podmiotu;
- **IssuerAlternativeName**: alternatywna nazwa wydawcy certyfikatu – **rozszerzenie nie jest krytyczne**;
- **SubjectAlternativeName**: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**;

[35] Dla CERTUM świadczącego niekwalifikowane usługi certyfikacyjn został przydzielony identyfikator obiektu o postaci: {iso(1) member-body(2) pl(616) organization(1) unizeto(113527) ccert(2) certum(2)}.

- **BasicContraints**: więzy podstawowe - **rozszerzenie jest krytyczne w certyfikatach urzędów certyfikacji i może być niekrytyczne w certyfikatach subskrybentów**. Rozszerzenie umożliwia określenie czy podmiot certyfikatu jest urzędem certyfikacji (pole **cA**) oraz ile maksymalnie (przy założeniu hierarchicznego uporządkowania urzędów certyfikacji) może być urzędów certyfikacji na ścieżce prowadzącej od rozpatrywanego urzędu certyfikacji do subskrybenta końcowego (pole **pathLength**);
- **CRLDistributionPoints**: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**. Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL, wydaną przez **cRLIssuer**;
- **SubjectDirectoryAttributes**: atrybuty katalogu podmiotu - **rozszerzenie nie jest krytyczne**; pole zawiera dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**; w rozszerzeniu tym występują atrybuty, które nie należą do elementów wchodzących w skład nazwy DN podmiotu;
- **AuthorityInfoAccessSyntax**: dostęp do informacji urzędu certyfikacji - **rozszerzenie nie jest krytyczne**; pole wskazuje, w jaki sposób udostępniane są informacje i usługi przez wystawcę certyfikatu, w którego certyfikacie to rozszerzenie występuje;
- **BiometricSyntax**: informacje o cechach biometrycznych podmiotu certyfikatu - **rozszerzenie nie jest krytyczne**; dostępne są dwa typy informacji biometrycznej: podpis odręczny oraz zdjęcie; w certyfikacie umieszczany jest jedynie skrót z cechy biometrycznej; wartość skrótu umieszczana jest w polu **biometricDataHash**, zaś identyfikator funkcji skrótu przy pomocy której policzono tę wartość w polu **hashAlgorithm**; pełna informacja biometryczna o podmiocie (jego wzorzec biometryczny) przechowywana jest w bazie danych, której adres URI podany jest w polu **sourceDataUri**. Efektywne wykorzystanie informacji biometrycznej umieszczonej w certyfikacie (skrót) możliwe jest jedynie w przypadku, gdy nastąpi porównanie wzorca zawartego w bazie (informacja pełna) ze skrótem odczytanym z certyfikatu.

7.1.2. Rozszerzenia a typy wydawanych certyfikatów

Certyfikaty wydawane przez urzędy CERTUM mogą zawierać różne kombinacje rozszerzeń wymienionych w rozdz. 7.1.1.2. Ich dobór jest uzależniony głównie od zastosowania certyfikatu oraz tego, komu jest wydawany.

7.1.2.1. Certyfikaty pośrednich urzędów certyfikacji

Autocertyfikat urzędu certyfikacji **Certum CA** oraz certyfikaty podległych mu urzędów certyfikacji **Certum Level I**, **Certum Level II**, **Certum Level III**, **Certum Level IV** i **Certum Partners** mogą zawierać rozszerzenia określone w Tab.7.3.

Tab.7.3 Rozszerzenia w certyfikatach urzędów certyfikacji

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji={brak,1,2,...}	Krytyczne

7.1.2.2. Certyfikaty do uwierzytelniania serwerów

Certyfikaty wydawane przez urzędy certyfikacji na potrzeby uwierzytelniania serwerów (w tym także certyfikaty stosowane w serwisach bezprzewodowych i OFX) oraz domen sieciowych (w tym certyfikaty Wildcard) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.4.

Tab.7.4 Rozszerzenia w certyfikatach do uwierzytelniania serwerów

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage (użycie klucza)	Klucz do podpisu (digitalSignature), bit 0 Klucz do szyfrowania (keyEncipherment), bit 2	Niekrytyczne
Extended Key Usage (rozszerzone użycie klucza)	Server Authentication Client Authentication Netscape SGC Microsoft SGC	Niekrytyczne
Certificate Template Name (zidentyfikowana nazwa certyfikatu)	(1.3.6.14.1.311.20.2): Domain Controller	Niekrytyczne
Netscape Cert Type	SSL Server, bit 1	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	OtherName: 1.3.6.1.4.1.311.25.1=Unikalny ID Kontrolera Domeny DNS.1: Pełna nazwa DNS serwisu (FQDN) DNS.2: Alternatywna nazwa serwisu (opcja)	Niekrytyczne
CRL Distribution Points (punkty dystrybucji listy CRL)	URI: http://crl.certum.pl/class{1,2,3,4}.crl URI: ldap://directory.certum.pl/C=PL,O=Unizeto Sp. z o.o.,CN=Certum Level I,II,III,IV},/?certificaterevocationlist	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityki: 1.2.616.1.113527.2.2.{1,2,3,4} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): zależy od typu certyfikatu. Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Niekrytyczne

7.1.2.3. Certyfikaty do uwierzytelniania kodu oprogramowania

Certyfikaty wydawane przez urzędy certyfikacji do uwierzytelniania kodu oprogramowania (w tym także formularzy oraz kanałów kryptograficznych) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.5.

Tab.7.5 Rozszerzenia w certyfikatach do uwierzytelniania kodu oprogramowania

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage (użycie klucza)	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Niekrytyczne
Extended Key Usage (rozszerzone użycie klucza)	Code Signing	Niekrytyczne
Netscape Cert Type (typ certyfikatu w Netscape)	Object Signing, bit 3	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	URI: http://www.customer-site.somwhere.pl	Niekrytyczne
CRL Distribution Points (punkty dystrybucji listy CRL)	URI: http://crl.certum.pl/class{1,3}.crl URI: ldap://directory.certum.pl/C=PL,O=Unizeto Sp. z o.o.,CN=Certum Level I,III},/?certificaterevocationlist	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityki: 1.2.616.1.113527.2.2.{1,3} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): zależy od typu certyfikatu. Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Niekrytyczne

7.1.2.4. Certyfikaty osób fizycznych

Certyfikaty wydawane osobom fizycznym (w tym także certyfikaty na potrzeby systemów szyfrowania plików EFS i elektronicznej wymiany dokumentów EDI, certyfikaty kwalifikowane w sensie normy RFC 3039 zawierające informacje biometryczne oraz certyfikaty jako silne identyfikatory w sieci Internet, tzw. Strong Internet ID's) mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.6.

Tab.7.6 Rozszerzenia w certyfikatach osób fizycznych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage (użycie klucza)	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1 Szyfrowanie kluczem (keyEncipherment), bit 2 Szyfrowanie danych (dataEncipherment), bit 3	Niekrytyczne
Extended Key Usage (rozszerzone użycie klucza)	Encrypted File System TLS Client Authentication Email Protection Smart Card Logon (1.3.6.1.4.1.311.20.2.2)	Niekrytyczne
Certificate Template Name (zidentyfikowana nazwa certyfikatu)	(1.3.6.14.1.311.20.2): Smart Card User Smart Card Logon	Niekrytyczne
Certificate Template Name (1.3.6.14.1.311.20.2)	Smart Card User Smart Card Logon	Niekrytyczne
Netscape Cert Type (typ certyfikatu w Netscape)	SSL Client, bit 0 S/MIME, bit 2	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	OtherName: UPN: customer@somewhere.pl (OID: 1.3.6.1.4.1.311.20.2.3) Email: customer@somewhere-in-world.com	Niekrytyczne
CRL Distribution Points (punkty dystrybucji listy CRL)	URI: http://crl.certum.pl/class{1,2,3,4}.crl URI: ldap://directory.certum.pl/C=PL,O=Unizeto Sp. z o.o.,CN=Certum Level I,II,III,IV},/? certificaterevocationlist	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	OCSP: http://ocsp.certum.pl	Niekrytyczne
Biometric Info (informacje biometryczne)	Zdjęcie podmiotu, DNA, wzór siatkówki oka, odcisk palca, bit 0 Wzór podpisu odręcznego podmiotu, bit 1 URI: lokalizacja danych biometrycznych	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityki: 1.2.616.1.113527.2.2.{1,2,3,4} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): zależy od typu certyfikatu. Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Niekrytyczne

7.1.2.5. Certyfikaty dla potrzeb budowania prywatnych sieci wirtualnych (VPN)

Certyfikaty umożliwiające budowanie sieci VPN mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.7.

Tab.7.7 Rozszerzenia w certyfikatach VPN

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage (użycie klucza)	Podpisy cyfrowe (digital signature), bit 0 Szyfrowanie kluczem (keyEncipherment), bit 2	Niekrytyczne
Extended Key Usage (rozszerzone użycie klucza)	IPsec Client IPsec Tunnel IPsec End System	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	DNS: pełna nazwa domeny (FQDN) routera VPN IP: Adres IP Routera VPN	Niekrytyczne
CRL Distribution Points (punkty dystrybucji listy CRL)	URI: http://crl.certum.pl/class{1,2,3,4}.crl URI: ldap://directory.certum.pl/C=PL,O=Unizeto Sp. z o.o.,CN=Certum Level I,II,III,IV},/? certificaterevocationlist	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityki: 1.2.616.1.113527.2.2.{1,,2,3,4} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): zależy od typu certyfikatu. Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Niekrytyczne

7.1.2.6. Certyfikaty wzajemne i certyfikaty dla potrzeb usług niezaprzeczalności

Certyfikaty wzajemne i certyfikaty dla potrzeb usług niezaprzeczalności mogą zawierać rozszerzenia wyspecyfikowane w Tab.7.8.

Tab.7.8 Rozszerzenia w certyfikatach wzajemnych i dla potrzeb usług niezaprzeczalności

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji={brak,1,2,...}	Niekrytyczne
Key Usage (użycie klucza)	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Niekrytyczne
Extended Key Usage (rozszerzone użycie klucza)	Validation Authority (OCSP) Time-Stamp Authority (TSA) Notary Authority (DVCS)	Niekrytyczne
CRL Distribution Points (punkty dystrybucji listy CRL)	URI: http://crl.certum.pl/{class1, partners}.crl URI: ldap://directory.certum.pl/C=PL,O=Unizeto Sp. z o.o.,CN=Certum Level I, Certum Partners},/?certificaterevocationlist	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	URI: http://www.customer-service.somwhere Lokalizacja serwisu klienta	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	OCSP: http://ocsp.certum.pl	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityki: 1.2.616.1.113527.2.2.{1,8} KPC: http://www.certum.pl/CPS Numer wiadomości (notice number): zależy od typu certyfikatu. Organizacja: Unizeto Sp. z o.o. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Niekrytyczne

7.1.3. Typ stosowanego algorytmu podpisu cyfrowego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji podpisu cyfrowego, składanego przez urząd certyfikacji na certyfikacie. W przypadku CERTUM stosowany jest algorytm RSA w kombinacji z funkcją skrótu MD5, SHA-1, SHA-256 lub SHA-512.

7.1.4. Pole podpisu cyfrowego

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

7.2. Profil listy certyfikatów unieważnionych (CRL)

Lista certyfikatów unieważnionych (CRL) składa się z ciągu trzech pól. Pierwsze pole (**tbsCertList**) zawiera informacje o unieważnionych certyfikatach, drugie i trzecie pole (**signatureAlgorithm** oraz **signatureValue**) – odpowiednio informację o typie algorytmu

użytego do podpisania listy oraz podpis cyfrowy, składany na certyfikacie przez urząd certyfikacji. Znaczenie dwóch ostatnich pól jest dokładnie takie samo jak w przypadku certyfikatu.

Pole informacyjne **tbsCertList** jest sekwencją pól obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty oraz rozszerzenia listy CRL.

Na treść pól obowiązkowych oraz opcjonalnych listy CRL składają się następujące pola:

- **Version**: wersja formatu listy CRL;
- **Signature**: Pole to zawiera identyfikator algorytmu stosowanego przez urząd certyfikacji do podpisania listy **CRL**; urzędy CERTUM podpisują listy CRL przy użyciu algorytmu **sha1WithRSAEncryption**;
- **Issuer**: nazwa urzędu certyfikacji wydającego listę CRL; każdy urząd CERTUM wystawia własną listę certyfikatów unieważnionych; wymóg ten dotyczy następujących urzędów: **Certum CA**, **Certum Level I**, **Certum Level II, Certum Level III**, **Certum Level IV** i **Certum Partners**;
- **ThisUpdate**: data publikacji listy CRL;
- **NextUpdate**: zapowiedź daty następnej publikacji listy CRL; jeśli pole wystąpi, wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy (publikacja może nastąpić wcześniej);
- **RevokedCertificates**: lista unieważnionych certyfikatów (pole puste w przypadku braku unieważnionych certyfikatów); informacja ta składa się z trzech podpól:

```
userCertificate     - numer seryjny unieważnianego certyfikatu
revocationDate      - data unieważnienia certyfikatu
crlEntryExtensions  - rozszerzony dostęp do listy CRL (zawiera
                      dodatkowe informacje o unieważnionych
                      certyfikatach - opcjonalnie)
```

- **crlExtensions**: poszerzone informacje o liście CRL (pole opcjonalne). Spośród wielu rozszerzeń najbardziej istotne są dwa, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL (pole **AuthorityKeyIdentifier**, patrz także rozdz. 7.1.1.2), zaś drugie (pole **cRLNumber**) - zawiera monotonicznie zwiększany numer listy CRL, wydawanej przez urząd certyfikacji (dzięki temu rozszerzeniu użytkownik listy jest w stanie określić, kiedy jakiś CRL zastąpił inny CRL).

7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL

Funkcje oraz sens rozszerzeń są takie same jak w przypadku rozszerzeń certyfikatu (patrz rozdz. 7.1.1.2). Obsługiwane przez CERTUM rozszerzenia dostępu do listy CRL (**crlEntryExtensions**) zawierają następujące pola:

- **ReasonCode**: kod przyczyny unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie przyczyny unieważnienia certyfikatu. Dopuszcza się następujące przyczyny unieważnienia:

```
unspecified          – nieokreślona (nieznana);
keyCompromise        – ujawnienie klucza;
cACompromise         – ujawnienie klucza urzędu certyfikacji;
affiliationChanged   – zamiana danych (afiliacji) subskrybenta;
superseded           – zastąpienie certyfikatu (recertyfikacja);
cessationOfOperation – zaprzestanie operacji z wykorzystaniem klucza;
certificateHold      – zawieszenie certyfikatu;
removeFromCRL        – certyfikat wycofany z listy CRL;
```

```
privilegeWithdrawn   - certyfikat został unieważniony z powodu zmiany
                       danych zawartych w certyfikacie, określających
                       rolę właściciela certyfikatu; powód unieważnienia
                       nie wyklucza, że ma miejsce kompromitacja lub
                       podejrzenie kompromitacji danych służących do
                       składania podpisu elektronicznego właściciela;
aaCompromise         - dotyczy certyfikatu atrybutów i ma znaczenie
                       identyczne jak wyżej;
```

- **HoldInstructionCode**: kod czynności po zawieszeniu certyfikatu. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które definiuje zarejestrowany identyfikator instrukcji, określającej działanie jakie powinno zostać podjęte po napotkaniu certyfikatu na liście CRL z adnotacją o przyczynie unieważnienia: certyfikat zawieszony (**certificateHold**). Jeśli aplikacja napotka kod **id-holdinstruction-callissuer** powinna poinformować użytkownika o konieczności skontaktowania się z CERTUM w celu wyjaśnienia przyczyn zawieszenia certyfikatu lub musi odrzucić certyfikat (uznać go za nieważny). W przypadku napotkania z kolei kodu **id-holdinstruction-reject** należy obligatoryjnie odrzucić rozpatrywany certyfikat. Kod **id-holdinstruction-none** jest semantycznie równoważny pominięciu rozszerzenia **holdInstructionCode**; stosowanie tego rodzaju kodu w listach CRL wydawanych przez CERTUM jest zabronione;
- **InvalidityDate**: data unieważnienia. Pole jest **niekrytycznym rozszerzeniem** dostępu do CRL, które umożliwia określenie daty faktycznego lub przypuszczalnego skompromitowania klucza lub wystąpienia innej przyczyny.

7.2.2. Certyfikaty unieważnione a listy CRL

Certyfikaty unieważnione pozostają na listach certyfikatów unieważnionych (wydawanych przez urzędy certyfikacji CERTUM) przez okres 25 lat, licząc od daty pierwszego umieszczenia certyfikatu na liście. Zasada ta dotyczy także unieważnionych certyfikatów urzędów certyfikacji: certyfikaty muszą być umieszczane na kolejnych listach CRL publikowanych przez wydawcę unieważnionego certyfikatu (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium innego, np. nadrzędnego organu wydającego certyfikaty (patrz także rozdz. 4.14).

Przedstawionej powyżej zasada nie stosuje się do unieważnionych certyfikatów klasy Certum Level I. Zalecane jest, aby certyfikaty te z chwilą ich przeterminowania usuwane były z listy certyfikatów unieważnionych.

7.3. Profil tokena znacznika czasu

Urząd znacznika czasu **Certum Time-Stamping Authority (TSA)** poświadcza elektronicznie wystawiane przez siebie tokeny znaczników czasu przy pomocy jednego lub większej liczby kluczy prywatnych zarezerwowanych specjalnie do tego celu. Zgodnie z zaleceniem RFC 3280 komplementarne z nimi certyfikaty kluczy publicznych urzędów zawierają pole precyzujące zawężenie dopuszczalnego zastosowania klucza (**ExtKeyUsageSyntax**) zaznaczone jako **krytyczne**. Oznacza to, że certyfikat może być używane przez urząd znacznika czasu tylko do realizacji poświadczeń elektronicznych w wystawianych przez siebie znacznikach czasu.

Certyfikat urzędu TSA zawiera informację o sposobie kontaktowania się z urzędem. Informacja ta zawarta jest w polu rozszerzenia prywatnego i ma postać (**AuthorityInfoAccessSyntax**) oraz pole to jest oznaczone jako niekrytyczne.

Profil podstawowych pól certyfikatu urzędu znacznika czasu jest przedstawiony w Tab.28.

Tab.28 Profil podstawowych pól certyfikatu urzędu TSA

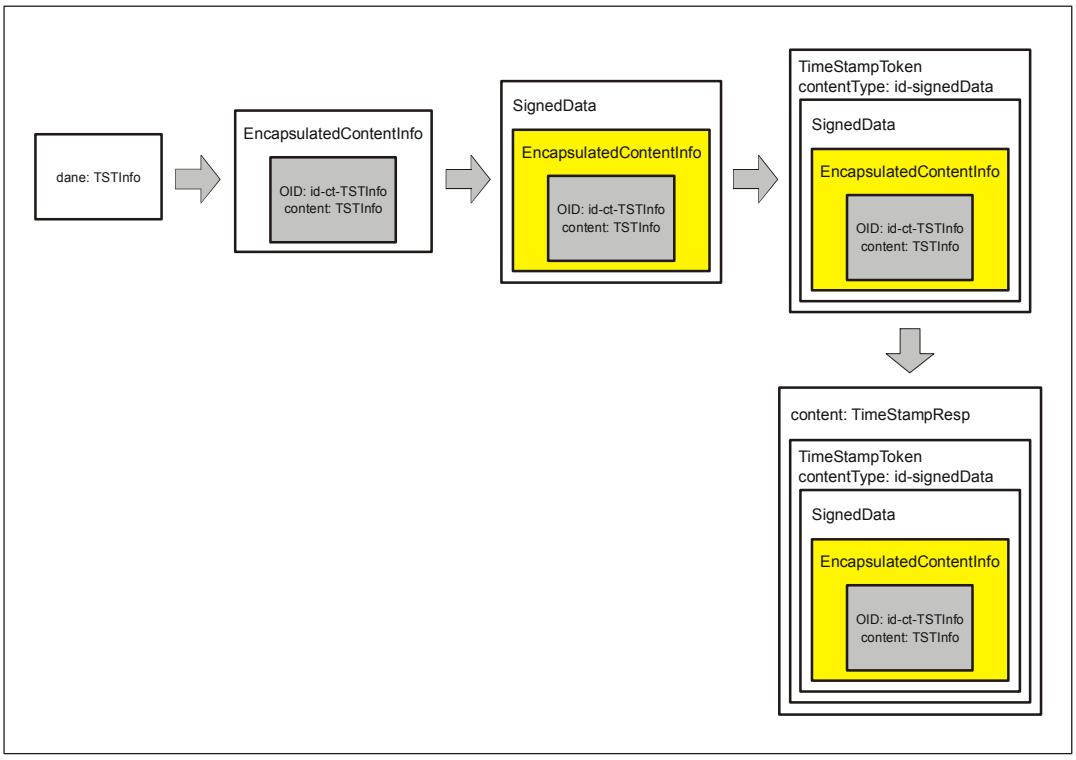
Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	Version 3	
Serial Numer (numer seryjny)	Unikalne wartości we wszystkich certyfikatach wydawanych przez urząd certyfikacji,	
Signature Algorithm (algorytm podpisu)	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (wystawca, nazwa DN)	Common Name (CN) =	Certum CA
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Zegar CERTUM 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). Zegar CERTUM jest znany jako ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Subject (podmiot, nazwa DN)	Common Name (CN) =	Certum Time-Stamping Authority
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
Subject Public Key Info (klucz publiczny podmiotu)	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 3280 zawiera informacje o kluczu publicznym RSA (identyfikatorze klucza, wartości klucza publicznego)	
Signature (podpis)	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 3280.	
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Niekrytyczne
Key Usage (użycie klucza)	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Niekrytyczne
Extended Key Usage (rozszerzone użycie klucza)	Time Stamping Authority (TSA)	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	URI: http://time.certum.pl Lokalizacja serwisu klienta	Niekrytyczne

Token znacznika czasu wystawiony przez urząd znacznika czasu Certum Time-Stamping Authority zawiera (patrz rys.10) w sobie informację o znaczniku czasu (struktura **TSTInfo**), umieszczoną w strukturze **SignedData** (patrz RFC 2630), podpisanej przez urząd znacznika i zagnieżdżonej w strukturze **ContentInfo** (patrz RFC 2630).

Odpowiedź w notacji ASN.1 na żądanie wydania tokena znacznika czasu ma więc postać:

```
TimeStampResp ::= SEQUENCE {
    status          PKIStatusInfo,
    timeStampToken  TimeStampToken OPTIONAL
}
```

Pole statusu odpowiedzi **PKIStatusInfo** umożliwia przekazywanie żądającemu wydania tokena znacznika czasu informacji o wystąpieniu lub nie wystąpieniu błędów zawartych w żądaniu. Jeśli kod błędu jest równy zero lub jeden, to oznacza to, iż odpowiedź zawiera token znacznika czasu. W każdym innym przypadku odpowiedź nie zawiera tokena znacznika czasu, zaś powód ze względu na który nie wydano tokena znacznika czasu określony jest w polu **failInfo** struktury **PKIStatusInfo**.



Rys.10 Kapsułkowanie odpowiedzi żądania utworzenia znacznika czasu

Struktura PKIStatusInfo ma następującą postać:

```
PKIStatusInfo ::= SEQUENCE {
    status          PKIStatus,
    statusString    PKIFreeText     OPTIONAL,
    failInfo        PKIFailureInfo OPTIONAL
}
```

Znaczenie pól:

- **status** zawiera informację o statusie odpowiedzi; za RFC 3161 przyjęto następujące wartości:

```
PKIStatus :: INTEGER {
    granted                 (0),
      -- otrzymałeś dokładnie to o co prosiłeś, tzn. TimeStampToken
    grantedWithMode         (1),
      -- odpowiedź jest zbliżona do tego czego żądałeś (TimeStampToken);
      -- żądający jest odpowiedzialny za sprawdzenie różnic
    rejection               (2),
      -- nie otrzymałeś odpowiedzi, więcej informacji w załączonej
      -- wiadomości
    waiting                 (3)
      -- zadanie nie zostało jeszcze przetworzone, oczekuj
      -- wiadomości później
    revocationWarning       (4)
      -- wiadomość ta zawiera ostrzeżenie, że zbliża się unieważnienie
    revocationNotification (5)
      -- potwierdzenie, że nastąpiło unieważnienie
}
```

- **statusString** może być wykorzystane do przesyłania żądającemu wiadomości w formie czytelnej (w dowolnym języku). Kod tego języka określony jest przy pomocy odpowiedniego znacznika, określonego w RFC 1766.

```
PKIFreeText ::= SEQUENCE SIZE (1..512) OF UTF8String
    -- tekst kodowany jest jako UTF-8 string (uwaga: każdy UTF8String
    -- powinien zawierać znacznik (tag) języka wg RFC 1766/2044,
    -- określający język, w którym zapisany jest tekst
```

- **failInfo** stosowane jest w przypadku konieczności dokładniejszego opisu przyczyny błędu (przyczyny nie wystawienia tokena znacznika czasu).

```
PKIFailureInfo ::= BIT STRING (
    badAlg               (0),
      -- nieznany lub nieobsługiwany identyfikator algorytmu
    badMessageCheck      (1),
      -- błąd integralności danych (np. błąd weryfikacji podpisu)
    badRequest           (2),
      -- niedozwolona lub nieobsługiwana transakcja (żądanie)
    badCertId            (4),
      -- do żądania nie dołączono właściwego certyfikatu (-ów)
    badDataFormat        (5),
      -- dostarczone dane mają zły format
    wrongAuthority       (6),
      -- organ wskazywany w żądaniu jako właściwy do wydania odpowiedzi
      -- nie jest tym, który otrzymał to żądanie
    inccorectData        (7),
      -- dane podane przez żądającego są niewłaściwe właściwy do wydania
      -- odpowiedzi
    missingTimeStamp     (8),
      -- brak znacznika czasu mimo iż powinien znajdować się w żądaniu
    timeNotAvailable     (14),
      -- źródło czasu TSA jest niedostępne
    unacceptedPolicy     (15),
      -- żądana polityka TSA nie jest polityką obowiązująca w TSA
    unacceptedExtension  (16),
      -- występujące w żądaniu rozszerzenie nie jest wspierane przez TSA
    addInfoNotAvailable  (17),
      -- żądanie dodatkowej informacji jest niezrozumiałe
      -- lub jest niedostępne
    systemFailure        (25),
      -- żądanie nie może być przetworzone ze względu na awarię sprzętu
}
```

Format ogólnego tokena znacznika czasu TimeStampToken jest zgodny z formatem ContentInfo:

```
TimeStampToken ::= ContentInfo
```

Token znacznika czasu nie może zawierać żadnych innych poświadczeń elektronicznych poza poświadczeniem urzędu znacznika czasu. Identyfikator certyfikatu urzędu znacznika czasu musi być uważany za atrybut podpisany i umieszczony w obszarze pola **signedAttributes** struktury **SignedData**.

Część informacyjna tokena zawarta jest w strukturze **TSTInfo**, wypełniającej pole **eContent** struktury **EncapsulatedContentInfo** (patrz RFC 2630). Typ pola **eContent**, określony przez pole **eContentType** w przypadku **TSTinfo** jest zdefiniowany następująco:

```
id-ct-TSTInfo  OBJECT IDENTIFIER ::= { iso(1) member-body(2) us(840)
                         rsadsi(113549) pkcs(1) pkcs-9(9) smime(16) ct(1) 4}
```

Zawartość informacyjna tokena znacznika czasu ma postać:

```
-- OBJECT IDENTIFIER (id-ct-TSTInfo)
TSTInfo ::= SEQUENCE  {
    version              INTEGER  { v1(1) },
    policy               TSAPolicyId,
    messageImprint       MessageImprint,
    serialNumber         INTEGER,
    genTime              GeneralizedTime,
    accuracy             Accuracy OPTIONAL,
```

```
    ordering              BOOLEAN DEFAULT FALSE,
    nonce                 INTEGER OPTIONAL,
    tsa                [0] GeneralName OPTIONAL,
    extensions         [1] IMPLICIT Extensions OPTIONAL
}
```

Znaczenie ważniejszych pól **TSRInfo** jest następujące:

- **policy** musi wystąpić i musi określać politykę zgodnie z którą wydawane są tokeny znacznika czasu przez urząd znacznika czasu; w przypadku urzędu **Certum Time-Stamping Authority** identyfikator polityki według której wystawiane są tokeny znacznika czasu ma wartość:

Identyfikator polityki	Nazwa polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-tsa(5)	Certum Time-Stamping Authority Identyfikuje politykę certyfikacji, według której wydawane są tokeny znacznika czasu

- **messageImprint** zawiera informację przesłaną przez żądającego, która została oznaczona znacznikiem czasu;
- **serialNumber** określa numer seryjny tokena znacznika czasu wystawionego przez dany urząd znacznika czasu. Numer seryjny musi zawierać ściśle rosnące wartości całkowite;
- pole **genTime** oznacza datę oraz czas wystawienia przez urząd znacznika czasu z dokładnością do 1 sekundy;
- pole **accuracy** określa dokładność z jaką generowany jest czas przez urząd znacznika czasu (urząd Certum Time-Stamping Authority generuje czas z dokładnością większą niż 1 sekunda). W przypadku, gdy pole jest pominięte, domyślnie przyjmuje się dokładność jednej sekundy;
- jeśli pole **ordering** nie występuje lub jego wartość ustawiona została na FALSE, to pole **genTime** pokazuje jedynie czas utworzenia znacznika czasu przez urząd znacznika czasu. W tym przypadku uporządkowanie dwóch tokenów znacznika czasu wydanych przez ten sam lub różne urzędy znacznika czasu jest możliwe jedynie wtedy, gdy różnica pomiędzy **genTime** pierwszego tokena, a **genTime** drugiego tokena jest większa od sum pól określających dokładności każdego z tokenów; jeśli pole **ordering** występuje i jego wartość ustawiona została na TRUE, to każdy token znacznika czasu wydany przez ten sam urząd znacznika czasu może być tylko na podstawie znajomości pola **genTime**, niezależnie od dokładności pomiaru czasu. Urząd znacznika czasu Certum Time-Stamping Authority zawsze ustawia wartość tego pola na FALSE;
- **nonce** pole musi wystąpić, jeśli wystąpiło w żądaniu przesłanym przez subskrybenta i musi mieć taką samą wartość;
- pole **tsa** służy do identyfikacji nazwy urzędu znacznika czasu. Jeśli występuje, musi odpowiadać nazwie podmiotu zawartej w certyfikacie wydanemu urzędowi znacznika czasu przez Certum CA i wykorzystywanym w procesie weryfikacji tokena.

Ze strukturą TimeStampToken związany jest zbiór atrybutów, które są podpisywane. W tokenie znacznika czasu występują przynajmniej następujące atrybuty:

1. Atrybut typu zawartości

```
Nazwa:      id-contentType
OID:        { iso(1) member-body(2)
                     us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
```

```
Składnia:   id-ct-TSTInfo
wartości:   wartość id-ct-TSTInfo jest ponowiona tylko raz
```

2. Atrybut skrótu wiadomości

```
Nazwa:      id-messageDigest
OID:        { iso(1) member-body(2)
                        us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
Składnia:   MessageDigest
wartości:   wartość typu MessageDigest jest ponowiona tylko raz

--skrót z pola eContent struktury EncapsulatedContentInfo
MessageDigest ::= Digest
Digest ::= OCTET STRING (SIZE(1..20))
```

3. Atrybut certyfikatu podpisującego

```
Nazwa:      id-aa-signingCertificate
OID:        { iso(1)
       member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
       smime(16) id-aa(2) 12 }
Składnia:   SigningCertificate
wartości:   wartość typu SigningCertificate jest ponowiona tylko raz

-- Podpisany atrybut certyfikatu
SigningCertificate ::= SEQUENCE {
    certs     SEQUENCE OF ESSCertID,
    policies  SEQUENCE OF PolicyInformation OPTIONAL
}

ESSCertID ::= SEQUENCE{
    CertHash       Hash,
    IsssuerSerial  IssuerSerial OPTIONAL
}

Hash ::= OCTET STRING -- SHA1 skrót z całego certyfikatu

IssuerSerial ::= SEQUENCE {
    Issuer         GeneralNames,
    SerialNumber   CertificateSerialNumber
}

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

7.4. Profil tokena statusu certyfikatu

Protokół weryfikacji statusu certyfikatu w trybie *on-line* (OCSP) jest stosowany przez urzędy certyfikacji i umożliwia określenie stanu certyfikatu.

Usługa weryfikacji statusu certyfikatu jest świadczona przez CERTUM w imieniu wszystkich działających w jego ramach urzędów certyfikacji. Serwer OCSP, który wystawia poświadczenia o statusie certyfikatu, posługuje się specjalną parą kluczy, przeznaczoną jedynie do tego celu.

Certyfikat serwera weryfikacji statusu certyfikatu musi zawierać w swojej treści rozszerzenie o nazwie **extKeyUsage**, określone w RFC 3280. Rozszerzenie to powinno być zaznaczone jako **krytyczne** i oznacza, że urząd certyfikacji wystawiając certyfikat serwerowi OCSP poświadcza swoim podpisem fakt oddelegowania mu prawa wystawiania w jego imieniu poświadczeń o statusie certyfikatów klientów danego urzędu.

Certyfikat może zawierać także informację o sposobie kontaktowania się z serwerem urzędu weryfikacji statusu certyfikatu. Informacja ta zawarta jest w polu rozszerzenia **AuthorityInfoAccessSyntax** (patrz rozdz. 7.1.1.2).

7.4.1. Numer wersji

Serwer weryfikacji statusu certyfikatu funkcjonujący w ramach systemu CERTUM wystawia tokeny o statusie certyfikatu zgodnie z normą RFC 2560. Z tego powodu jedynym dozwolonym numerem wersji jest 0 (odpowiada to wersji v1).

7.4.2. Informacja o statusie certyfikatu

Informacja o statusie certyfikatu umieszczana jest w polu **certStatus** struktury **SingleResponse**. Może ona przyjmować jedną z trzech dozwolonych wartości, zdefiniowanych w rozdz. 4.9.11. W przypadku, gdy serwer zwróci status **poprawny**, to podmiot żądający informacji o statusie certyfikatu powinien sprawdzić dodatkowo rozszerzenie **CertHash** zawarte w odpowiedzi (patrz rozdz. 7.4.4) w celu przekonania się, że weryfikowany certyfikat został opublikowany przez wystawcę oraz rozszerzenie **ArchveCutoff**, którego wartość jest lewostronnym przedziałem czasu począwszy, od którego serwer OCSP weryfikował status certyfikatu (wartość prawostronnego przedziału czasu określona jest przez moment wystawienia poświadczenia weryfikacji statusu certyfikatu, określony w polu **producedAt**). Pozytywny wynik tych weryfikacji pozwala na uzyskanie tzw. **pozytywnego potwierdzenia** statusu certyfikatu.

7.4.3. Obsługiwane rozszerzenia standardowe

Zgodnie z RFC 2560 serwer weryfikacji statusu certyfikatu obsługuje następujące rozszerzenia:

- Frazę (*ang. nonce*), która wiąże żądanie z odpowiedzią i zapobiega atakowi powtórzeniowemu. Wartość frazy umieszcza się w polu **requestExtensions** żądania **OCSPRequest** oraz powtarza w polu **responseExtensions** odpowiedzi **OCSPResponse**.
- W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, w odpowiedzi umieszczane są dane identyfikacyjne tej listy. Informacja o liście CRL zawiera adres URL listy CRL, jej numer oraz czas jej utworzenia. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.
- W przypadku, gdy weryfikowany certyfikat występuje na liście CRL, dodatkowo w odpowiedzi należy umieścić wszystkie trzy rozszerzenia listy CRL, opisane w rozdz. 7.2.1. Informacje te umieszczane są w polu **singleExtensions** struktury **SingleResponse**.
- Typy odpowiedzi akceptowane przez podmiot (dokładniej, działające w jego aplikacji) wysyłający żądanie weryfikacji statusu do serwera OCSP. Rozszerzenie to określa deklarowane typy odpowiedzi, które rozumie aplikacja. Informacja o akceptowanych typach odpowiedzi (m.in. **id-pkix-ocsp-basic**) umieszczana jest w żądaniu w rozszerzeniu **AcceptableResponses**.
- **Graniczna data archiwizacji** dotyczy daty, do której włącznie przechowywane są w archiwum CERTUM informacje o statusie certyfikatów (rozszerzenie **ArchiveCutoff**). Umieszczenie tej informacji w odpowiedzi przez serwer weryfikacji statusu certyfikatu oznacza, że serwer ten posiada informacje o unieważnieniach certyfikatów także wtedy, gdy same certyfikaty są już przeterminowane. Tego typu informacja dostarcza dowodu na to czy podpis cyfrowy związany z weryfikowanym certyfikatem był lub nie był ważny w momencie wystawienia odpowiedzi przez serwer OCSP, nawet jeśli w tym momencie certyfikat był już przeterminowany. Ponieważ informacje o statusie certyfikatów są dostępne w trybie *on-line* przez okres 15 lat (patrz rozdz. 6.2.5), to

wartość granicznej daty archiwizacji jest różnicą pomiędzy datą wystawienia poświadczenia o statusie certyfikatu a okresem przechowania informacji o unieważnieniach certyfikatów przez serwer OCSP.

Każdy odbiorca poświadczenia wystawionego przez serwer OCSP musi być w stanie obsłużyć standardowy typ odpowiedzi o identyfikatorze **id-pkix-ocsp-basic**.

7.4.4. Obsługiwane rozszerzenia prywatne

Jeśli w odpowiedzi na żądanie wysłane do serwera urzędu weryfikacji statusu certyfikatu podmiot otrzyma poświadczenie zawierające status **poprawny**, to bez posiadania dodatkowych informacji nie musi to oznaczać, że certyfikat był kiedykolwiek wystawiony lub też że moment utworzenia odpowiedzi zawiera się w okresie ważności tego certyfikatu. Drugi z problemów można rozwiązać dzięki umieszczeniu w odpowiedzi rozszerzenia **graniczna data archiwizacji** (**ArchieveCutoff**), opisanego w rozdz. 7.4.3.

Rozwiązanie pierwszego z problemów jest możliwe dzięki wprowadzeniu do zaświadczeń wystawianych przez serwer urzędu weryfikacji statusu certyfikatu rozszerzenia prywatnego **CertHash**.

Rozszerzenie **CertHash** jest oznaczone jako **niekrytyczne**. Opisująca je struktura danych oraz jej identyfikator mają postać:

```
id-ccert-CertHash           OBJECT IDENTIFIER ::= { id-ccert-ext 4}
CertHash ::= SEQUENCE {
    hashAlgorithm   DigestAlgorithmIdentifier,
    hashedCert      OCTET STRING
}

id-unizeto                  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
                              organization(1) id-unizeto(113527)}
id-ccert-ext                OBJECT IDENTIFIER ::= { id-ccert(2) 0}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier
AlgorithmIdentifier ::= SEQUENCE {
    algorithm               OBJECT IDENTIFIER,
    parameters              ANY DEFINED BY algorithm OPTIONAL
}
```

Pole **hashAlgorithm** określa identyfikator silnej funkcji skrótu. Oznacza to, że funkcja skrótu powinna być funkcją jednokierunkową, odporną na kolizje (np. SHA-1).

Wartość pola **hashedCert** zawiera skrót z certyfikatu, którego aktualny status jest umieszczony w odpowiedzi serwera OCSP. Wielkość tego pola zależy od typu zastosowanej funkcji skrótu.

Innym rozszerzeniem prywatnym obsługiwanym przez CERTUM jest rozszerzenie **CertumDigitalStamp** i jest oznaczone jako **niekrytyczne**. Opisująca je struktura danych oraz jej identyfikator mają postać:

```
CertumDigitalStamp::= SEQUENCE {
      type       CDStampType,
      issuerInfo GeneralNames,
      stampInfo  UTF8String (SIZE (128)),
      currency   Iso4217AlphaCurrencyCode,
      amount     INTEGER,
      exponent   INTEGER} -- value = amount * 10^exponent
```

Rozszerzenie to jest wykorzystywane przy elektronicznych znaczkach opłatowych.

7.4.5. Oświadczenie wystawcy tokena weryfikacji statusu certyfikatu

Aktualna wersja serwera urzędu weryfikacji statusu certyfikatu CERTUM nie umieszcza w odpowiedzi rozszerzeń ***CertHash*** *oraz* ***ArchiveCutoff****. CERTUM oświadcza jednak, że otrzymany w odpowiedzi status certyfikatu* ***poprawny*** *oznacza, że certyfikat ten był wydany przez (dowolny) urząd certyfikacji oraz, że nie był on nigdy unieważniony w okresie ostatnich 15 lat. Jeśli certyfikat był unieważniony w okresie ostatnich 15 lat, to serwer OCSP zwraca status* ***unieważniony*** *oraz podaje datę unieważnienia.*

8. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego obowiązuje (posiada status aktualny) do czasu opublikowania i zatwierdzenia nowej wersji (patrz rozdz. 8.3). Nowa wersja opracowywana jest przez Zespół ds. Rozwoju Usług PKI i ze statusem **w ankiecie** przekazana do ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety, nowa wersja Kodeksu Postępowania Certyfikacyjnego przekazywana jest do zatwierdzenia. W czasie trwania procedury zatwierdzania nowa wersja dokumentu posiada status – **w zatwierdzeniu,** a po zakończeniu procedury osiąga status – **aktualny**.

Oprócz wersji istnieją także wydania Kodeksu Postępowania Certyfikacyjnego, które posiadają takie same statusy jak wersja. Nowe wydanie Kodeksu Postępowania Certyfikacyjnego opatrzone jest zmiennym numerem umieszczanym po numerze wersji, oddzielonym znakiem kropki, aktualnego Kodeksu Postępowania Certyfikacyjnego.

Decyzję o zakwalifikowaniu zmian w Kodeksie Postępowania Certyfikacyjnego dotyczących wersji lub wydania podejmuje Zespół ds. Rozwoju Usług PKI.

Przedstawione poniżej dalsze zasady administrowania Kodeksem Postępowania Certyfikacyjnego obowiązują podczas wprowadzania zmian w Polityce Certyfikacji.

Subskrybenci zobowiązani są stosować się wyłącznie do aktualnie obowiązującej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.

8.1. Procedura wprowadzania zmian

Zmiany w Kodeksie Postępowania Certyfikacyjnego mogą być wynikiem zauważonych błędów, uaktualnień oraz sugestii zainteresowanych stron. Propozycje zmian mogą być nadsyłane zwykłą pocztą lub elektroniczną na adresy kontaktowe CERTUM. Propozycje zmian powinny opisywać ich zakres, uzasadnienie oraz adres kontaktowy autora wprowadzenia zmian.

Podmioty mające prawo zgłaszać propozycję wprowadzania zmian do istniejącego Kodeksu Postępowania Certyfikacyjnego:

- zamawiający,
- instytucje audytujące,
- instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Kodeks Postępowania Certyfikacyjnego jest sprzeczny z zasadami prawnymi obowiązującymi w Rzeczypospolitej Polskiej oraz może działać na niekorzyść subskrybenta,
- inspektor bezpieczeństwa, administrator systemu oraz inni pracownicy CERTUM,
- Zespół ds. Rozwoju Usług PKI,
- subskrybenci CERTUM,
- eksperci z zakresu zabezpieczeń systemów informatycznych.

Po wprowadzeniu każdej zmiany uaktualniana jest data opublikowania Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego oraz modyfikowany jest identyfikator dokumentu, numer jego wersji lub wydania.

Wprowadzane zmiany można ogólnie podzielić na dwie kategorie:

- zmiany niewymagające informowania subskrybentów o modyfikacjach,
- zmiany wymagające informowania (zwykle odpowiednio wczesnego) subskrybentów o modyfikacjach.

8.1.1. Zmiany niewymagające informowania

Jedynymi zmianami, które według Kodeksu Postępowania Certyfikacyjnego nie wymagają wcześniejszego informowania subskrybentów są zmiany wynikające z wprowadzenia korekt edycyjnych, zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie dokumentem, zmiany niemające rzeczywistego wpływu na znaczącą grupę użytkowników. Wprowadzone zmiany nie podlegają procedurze zatwierdzania i zmienia się jedynie wydanie Kodeksu Postępowania Certyfikacyjnego.

8.1.2. Zmiany wymagające informowania

8.1.2.1. Lista elementów

Po uprzednim poinformowaniu subskrybentów, zmianom mogą podlegać dowolne elementy Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich istotnych, rozważanych przez Zespół ds. Rozwoju Usług PKI zmianach w dokumencie jest przesyłana wszystkim zainteresowanym stronom w postaci informacji o miejscu dostępu nowej wersji Kodeksu Postępowania Certyfikacyjnego o statusie **w ankiecie**. Propozycje zmian mogą być otwarcie publikowane w repozytorium CERTUM oraz rozsyłane pocztą elektroniczną. Do nowego Kodeksu Postępowania Certyfikacyjnego dołączona jest także informacja o wprowadzonych zmianach.

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. Rozwoju Usług PKI. Jeśli w wyniku nadesłanych komentarzy Zespół ds. Rozwoju Usług PKI dokonał **istotnych modyfikacji** w proponowanych zmianach, modyfikacje te muszą być ponownie opublikowane i poddane ocenie. W pozostałych przypadkach, nowa wersja Kodeksu Postępowania Certyfikacyjnego przyjmuje status **w zatwierdzeniu** i poddana jest procedurze zatwierdzenia (rozdz. 8.3)

Zespół ds. Rozwoju Usług PKI może w pełni akceptować zgłaszane uwagi, akceptować ze zmianami lub odrzucać je po upływie terminu nadsyłania odpowiedzi na rozesłaną i opublikowaną ankietę.

8.1.2.3. Zmiany wymagające nowego identyfikatora

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników usług certyfikacyjnych, Zespół ds. Rozwoju Usług PKI może przydzielić zmodyfikowanemu dokumentowi nowy identyfikator (OBJECT IDENTIFIER). Zmianie mogą ulec także identyfikatory polityk certyfikacji, według której są świadczone usługi certyfikacyjne. Powyższy przypadek może mieć miejsce po zmianie następujących jego elementów:

- poszerzeniu grona użytkowników certyfikatów na obszary związane np. z elektronicznymi płatnościami, wymianę informacji wewnątrz banków oraz pomiędzy bankami, itp.,
- wprowadzeniu nowych typów certyfikatów,
- dopuszczeniu w systemie certyfikacji wzajemnej pomiędzy organami wydającymi certyfikaty,
- istotnej zmiany zawartości i interpretacji pól certyfikatu oraz list CRL, np. zmiana znaczenia pól z niekrytycznych na krytyczne lub odwrotnie,
- wdrożeniu w ramach CERTUM usługi zawieszania i odwieszania certyfikatu.

8.2. Publikacja

8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego

Publicznie nie są dostępne zastosowane zabezpieczenia systemu komputerowego, procedury oraz mechanizmy uwierzytelniania, a także te elementy, których ujawnienie może osłabić zabezpieczenia oraz zasugerować ataki na nie. W szczególności nie ujawnia się:

- zastosowanych platform sprzętowo-programowych,
- szczegółów użytej konfiguracji sprzętowej,
- planu odtwarzania systemu po awariach i katastrofach,
- miejsc przechowywania kluczy CERTUM i chroniących je sekretów współdzielonych oraz numerów PIN do nich,
- listy osób posiadających sekrety współdzielone,
- przedsięwziętych sposobów ochrony personelu,
- zabezpieczeń sieci,
- procedur logowania się do systemu.

Nie publikowane elementy udostępniane są inspektorowi bezpieczeństwa, administratorowi systemu oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie CERTUM w specjalnie przeznaczonym do tego celu pomieszczeniu.

8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego

Kopia Kodeksu Postępowania Certyfikacyjnego dostępna jest w formie elektronicznej:

- na stronie WWW pod adresem: http://www.certum.pl
- via e-mail o adresie: info@certum.pl

W repozytorium oraz za pośrednictwem strony WWW dostępne są zawsze trzy wersje (jeśli jest to możliwe) Kodeksu Postępowania Certyfikacyjnego: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz. 8.3). W przypadku zmiany wydania Kodeksu Postępowania Certyfikacyjnego nie jest konieczne publikowanie poprzedniego wydania.

Za pośrednictwem tych samych adresów zaleca się udostępnienie także dokumentu, opisującego istotne różnice pomiędzy aktualnym (jeszcze obowiązującym) a Kodeksem Postępowania Certyfikacyjnego poddanym procedurze zatwierdzania.

8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego

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

Historia dokumentu

Historia zmian dokumentu		
V 1.0	15 kwietnia 2000 r.	Szkic dokumentu do dyskusji
V 1.33	12 marca 2002 r.	Pełna wersja dokumentu. Dokument zatwierdzony
V 2.0	15 lipca 2002 r.	Zdefiniowanie dodatkowych typów certyfikatów. Modyfikacje procedur certyfikacji, doprecyzowanie profilu certyfikatów i list CRL. Przeredagowano rozdz.3, 4, 6.1, 2.6, 6.2-6.9 i 7. Zatwierdzenie dokumentu.
V 2.1	01 lutego 2005 r.	Zdefiniowanie dodatkowych typów certyfikatów. Zmodyfikowano rozdziały dotyczące procesów odnowienia i recertyfikacji kluczy kryptograficznych. Wprowadzono zapisy o możliwości stosowania nowych rozszerzeń w certyfikatach. Poprawiono szereg błędów interpunkcyjnych oraz wprowadzono modyfikację rozdziału traktującego o weryfikacji podmiotu w procesie certyfikacji. Wprowadzono dodatkowo szereg drobnych poprawek w celu zachowania spójności treści niniejszego dokumentu.
V 2.2	09 maja 2005 r.	Zmiana formy prawnej spółki, przekształcenie Unizeto Sp. z o.o. w Unizeto Technologies S.A.
V 2.3	26 października 2005 r.	Zmiana nazwy własnej jednostki i logo z Unizeto CERTUM – Centrum Certyfikacji na CERTUM – Powszechne Centrum Certyfikacji
V 2.4	19 maja 2006 r.	Usunięcie informacji o poprzedniej formie prawnej firmy. Przeniesienie szczegółów dotyczących dokumentów wymaganych do wydania certyfikatu do osobnego dokumentu. Usunięcie informacji o zawieszeniu certyfikatów. Dodanie informacji o składowaniu kopii danych użytych do weryfikacji tożsamości. Poprawki edycyjne i usuwające nieścisłości z angielską wersją językową.
V 2.5	12 maja 2008 r.	Zmiany edytorskie oraz dostosowanie wersji językowej polskiej i angielskiej.

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

KPC Kodeks Postępowania Certyfikacyjnego

KRIO Krajowy Rejestr Identyfikatorów Obiektów

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

PC Polityka Certyfikacji

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

PR Punkt Rejestracji

PSE osobiste bezpieczne środowisko (*ang. personal security environment*)

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*)

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

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.

Autocertyfikat – dowolny certyfikat klucza publicznego przeznaczony do weryfikacji podpisu złożonego na certyfikacie, w którym podpis da się zweryfikować przy pomocy klucza publicznego zwartego w polu **subjectKeyInfo**, zawartości pól **issuer** oraz **subject** są takie same, zaś pole **cA** rozszerzenia **BasicConstrains** ustawione jest na **true**.

Bezpieczna ścieżka (*ang. trusted path*) – łącze zapewniające wymianę informacji związanych z uwierzytelnieniem użytkownika komputera, aplikacji lub innego urządzenia (np. kryptograficznej karty elektronicznej), zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

Certyfikat (certyfikat klucza publicznego) – elektroniczne zaświadczenie które zawiera co najmniej nazwę lub identyfikator urzędu certyfikacji, identyfikator subskrybenta, jego klucz publiczny, okres ważności certyfikatu, numer seryjny certyfikatu oraz jest podpisane przez urząd certyfikacji.

UWAGA: Certyfikat może znajdować się w jednym z trzech podstawowych stanów (patrz Stany klucza kryptograficznego): w oczekiwaniu na aktywność, aktywny i uśpiony.

Certyfikat 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.

Certyfikat wzajemny (*ang. cross-certificate*) – jest to taki certyfikat klucza publicznego wydany urzędowi certyfikacji, w którym nazwy wystawcy i podmiotu tego certyfikatu są różne, klucz publiczny zawarty w certyfikacie może być używany jedynie do weryfikacji podpisów oraz wyraźnie jest zaznaczone, że certyfikat należy do urzędu certyfikacji.

Certyfikacja wzajemna (*ang. cross-certification*) – procedura wydawania certyfikatu przez urząd certyfikacji innemu urzędowi certyfikacji, który nie pozostaje z urzędem wydającym certyfikat w relacji bezpośredniego podporządkowania lub jest mu bezpośrednio podporządkowany. Zwykle certyfikat wzajemny wydawany jest w celu uproszczenia budowy i weryfikacji ścieżek certyfikatów, złożonych z certyfikatów wydawanych przez różne urzędu certyfikacji. Wydanie certyfikatów wzajemnych może być, ale nie jest to konieczne, realizowane na zasadzie wzajemności: tj. dwa urzędy certyfikacji wydają sobie nawzajem certyfikaty wzajemne.

Dane do audytu – chronologiczne zapisy aktywności w systemie pozwalające na zrekonstruowanie i analizowanie sekwencji zdarzeń oraz zmian, z którymi związane jest zarejestrowane zdarzenie.

Dostęp – zdolność do korzystania z dowolnego zasobu systemu informacyjnego.

Dowód posiadania klucza prywatnego (POP, *ang. proof of possesion*) – informacja przekazana przez nadawcę do odbiorcy w takiej postaci, która umożliwia odbiorcy zweryfikowanie ważności powiązania istniejącego pomiędzy nadawcą a kluczem prywatnym, którym jest w stanie posłużyć się lub posługuje się; sposób przeprowadzenia dowodu jest uzależniony zwykle od rodzaju zastosowania pary kluczy; np. w przypadku kluczy podpisujących wystarczy, aby subskrybent przedłożył podpisany tekst (pozytywnie zakończona weryfikacja podpisu stanowi dowód posiadania klucza prywatnego), z kolei w przypadku kluczy szyfrujących subskrybent musi być w stanie odszyfrować informację zaszyfrowaną przy użyciu należącego do niego klucza publicznego. W CERTUM weryfikacja powiązań pomiędzy parami kluczy stosowanych do podpisu i szyfrowania realizowana jest tylko przez punkty rejestracji i urzędy certyfikacji.

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 ze sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych, które dzięki współpracy realizują oraz udostępniają usługi certyfikacyjne, w tym 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.

Klucz tajny – klucz wykorzystywany w symetrycznych technikach kryptograficznych i stosowany jedynie przez zbiór określonych subskrybentów.

UWAGA: Klucz tajny jest przeznaczony do stosowania przez bardzo mały zbiór korespondentów do szyfrowania i deszyfrowania danych.

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

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

Lista certyfikatów unieważnionych (CRL, *ang. Certificate Revocation List*) – lista podpisana cyfrowo przez urząd certyfikacji zawierająca 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, realizujący 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.

Naruszenie (np. danych) – ujawnienie informacji nieuprawnionym osobom lub taka ingerencja naruszająca politykę bezpieczeństwa systemu, w wyniku której wystąpi nieuprawnione (zamierzone lub niezamierzone) ujawnienie, modyfikacja, zniszczenie lub udostępnienie dowolnego obiektu.

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

Obiekt – jednostka do której dostęp jest kontrolowany, np. plik, program, obszar w pamięci głównej; gromadzone i utrzymywane dane osobowe (PN-2000:2002).

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

Podpis cyfrowy – przekształcenie kryptograficzne jednostki danych, umożliwiające odbiorcy danych sprawdzenie pochodzenia i integralności jednostki danych oraz ochronę nadawcy i odbiorcy jednostki danych przed sfałszowaniem przez odbiorcę; asymetryczne podpisy cyfrowe mogą być generowane przez jeden podmiot przy zastosowaniu klucza prywatnego i algorytmu asymetrycznego, np. RSA.

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.

Procedura postępowania w sytuacji awaryjnej – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu jeśli wystąpi sytuacja nadzwyczajna, lecz przewidywana.

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.).

PUK (*ang. Personal Unblocking Key*) – kod służący do odblokowania karty kryptograficznej oraz zmiany kodu PIN.

Punkt Rejestracji (PR) – miejsce, gdzie świadczone są usługi w zakresie weryfikacji i potwierdzania tożsamości osób ubiegających się o certyfikat, 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.

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

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.

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

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

Subskrybent – jednostka (osoba fizyczna, osoba prawna, jednostka organizacyjna nie posiadająca osobowości prawnej, urządzenie, które jest pod opieką tych osób lub jednostki organizacyjnej), która jest podmiotem wymienionym lub zidentyfikowanym w certyfikacie wydanym tej jednostce, posiada klucz prywatny, który odpowiada kluczowi publicznemu zawartemu w certyfikacie oraz sama nie wydaje certyfikatów innym stronom.

System informacyjny – całość infrastruktury, organizacja, personel oraz komponenty służące do gromadzenia, przetwarzania, przechowywania, przesyłania, prezentowania, rozgłaszania i zarządzanie informacją.

Ścieżka certyfikacji – uporządkowany ciąg certyfikatów, prowadzący od certyfikatu **punktu zaufania**, wybranego przez weryfikującego, aż do weryfikowanego certyfikatu, utworzony w celu weryfikacji certyfikatu. Ścieżka certyfikacji spełnia następujące warunki:

- dla każdego certyfikatu Cert(x) należącego do ścieżki certyfikacji {Cert(1), Cert(2), ..., Cert(n-1)} podmiot certyfikatu Cert(x) jest wydawcą certyfikatu Cert(x+1),
- certyfikat Cert(1) jest wydany przez urząd certyfikacji (**punkt zaufania**), któremu ufa weryfikator,
- Cert(n) jest weryfikowanym certyfikatem.

Z każdą ścieżką certyfikacji można związać jedną lub więcej polityk certyfikacji lub też taka polityka może nie istnieć. Polityki przypisane określonej ścieżce certyfikacji są częścią wspólną (iloczynem) zbiorów polityk, których identyfikatory są zawarte w każdym certyfikacie, należącym do ścieżki certyfikacji i zdefiniowane w ich rozszerzeniu **certificatePolicies**.

Token – element danych stosowany w wymianach pomiędzy stronami zawierający informację, która została przekształcona z wykorzystaniem technik kryptograficznych. Token może być podpisany przez operatora punktu rejestracji i wykorzystany do uwierzytelnienia jego nadawcy w trakcie kontaktów z urzędem certyfikacji.

Token statusu certyfikatu – dane w postaci elektronicznej, które zawierają informacje o aktualnym statusie certyfikatu, ścieżki certyfikacji, do której należy określony certyfikat oraz inne informacje przydatne podczas weryfikacji, poświadczone elektronicznie przez urząd weryfikacji statusu certyfikatu.

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.

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 m.in. szyfrowania lub podpisu. Unieważniony certyfikat umieszczany jest na liście certyfikatów unieważnionych (CRL).

CERTUM – jednostka usługowa Unizeto Technologies S.A. świadcząca niekwalifikowane i kwalifikowane usługi certyfikacyjnych (urząd certyfikacji).

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 weryfikacji statusu certyfikatu – zaufana trzecia strona, która dostarcza stronie ufającej mechanizm weryfikacji wiarygodności certyfikatu lub zaświadczenia certyfikacyjnego podmiotu, jak również udostępnia dodatkowe informacje o atrybutach tego certyfikatu lub zaświadczenia certyfikacyjnego.

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

Uwierzytelniać – potwierdzać deklarowaną tożsamość podmiotu.

Uwierzytelnienie – mechanizm zabezpieczeń, którego zadaniem jest zapewnienie wiarygodności przesyłanych danych, wiadomości lub nadawcy, albo mechanizmy weryfikowania autoryzacji osoby przed otrzymaniem przez nią określonych kategorii informacji.

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

Weryfikacja podpisu – ma na celu określenie, czy 1) podpis cyfrowy 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.

Zamawiający – osoba lub instytucja, która w imieniu subskrybenta finansuje usługi certyfikacyjne świadczone przez organ wydający certyfikaty. Sponsor jest właścicielem certyfikatu i przysługuje mu prawo do zgłoszenia jego unieważnienia w przypadkach przewidzianych w Kodeksie Postępowania Certyfikacyjnego.

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).

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.

X.500 – norma międzynarodowa określająca protokół dostępu do katalogu DAP (*ang. Directory Access Protocol*), oraz protokół usług katalogowych DSP (*ang. Directory Service Protocol*).

Literatura

[1] ITU-T Recommendation X.509 – *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, June 1997 (odpowiednik ISO/IEC 9594-8)

[2] ITU-T Recommendation X.520 – *Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types*, 1993

[3] *CARAT Guidelines – Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*, National Automated Clearing House Association (NACHA), The Internet Council CARAT Task Force, v.1.0, Draft September 21, 1998

[4] *VeriSign CPS – VeriSign Certification Practice Statement*, ver.2.0, August 31, 2001, http://www.verisign.com

[5] *ARINC Digital Signature Service (ADSS) – Certification Practice Statement (CPS),* ver.2.0, August 6, 1998

[6] ISO/IEC JTC 1/SC27 N691 *Guidelines on the Use and Management of Trusted Third Party Services*, August 1993

[7] RFC 822 D.Crocker – *Standard for the format of ARPA Internet text messages*, August 1982

[8] RFC 1738 T.Berners-Lee, L.Masinter, M.McCahill – *Uniform Resource Locators (URL),* December 1994

[9] RFC 1778 T.Howes, S.Kille, W.Yeong, C.Robbins *The String Representation of Standard Attribute Syntaxes*, March 1995

[10] RFC 2247 S.Kille, M.Wahl, A.Grimstad, R.Huber, S.Sataluri – *Using Domains in LDAP/X.500 Distinguished Names*, January 1998

[11] RFC 3280 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile*, 2002

[12] Steven Castell *Trusted Third Party Services – User Requirements for Trusted Third Party Services*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, July 29, 1993

[13] Steven Castell *Trusted Third Party Services - Functional model*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, December 13, 1993

[14] *Ustawa z dnia 22 stycznia 1999 O ochronie informacji niejawnych*, Dziennik Ustaw Rzeczpospolitej Polskiej, Nr.11, Warszawa, 8 lutego 1999 r.

[15] Simson Garfinkel, Gene Spafford *Bezpieczeństwo w Unixie i internecie*, Wyd. RM, Warszawa 1997

[16] S.Chkhani, W.*Ford Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, RFC 2527, March, 1999

[17] S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. *Wu Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, July 12, 2001, < draft-ietf-pkix-ipki-new-rfc2527-00.txt >

[18] European Telecommunications Standards Institute *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456 V1.1.1 (2000-12)

[19] *Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure* (Working Draft), v.2.0 August 1998

[20] RFC 3161 *Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP), PKIX Working Group*, January 2001

[21] *PKI Assessment Guidelines - Guidelines to Help Assess and Facilitate Interoperable Trustworthy Public Key Infrastructures, PAG v0.30*, Public Draft for Comment, June 18, 2001, Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law, American Bar Association,

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

[23] CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*, CEN (European Committee for Standardization) November 2001,

[24] *Digital Signature Standard*, FIPS 186-2 NIST (Jan. 2000)

[25] *EESSI-SG Algorithms and Parameters for Secure Electronic Signatures*, 19 October 2001

[26] FIPS 112 *Password Usage*, 30 May 1985, http://csrs.nist.gov/fips/