Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM

Wersja 5.1
Data: 07 Marca 2018
Status: archiwalny

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia
Certum - Powszechne Centrum Certyfikacji
ul. Bajeczna 13
71-838 Szczecin
http://www.certum.pl

Klauzula: Prawa Autorskie

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, 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 w ramach tzw. ***niekwalifikowanych usług CERTUM****. Procedura definiowania i aktualizowania zarówno Polityki Certyfikacji, jak również Kodeksu Postępowania Certyfikacyjnego jest zgodna z regułami opisanymi w rozdz. 9.12.*

Kodeks Postępowania Certyfikacyjnego opisuje zbiór polityk 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 3647 *Certificate Policy and Certification Practice Statement Framework*.

Firma Asseco Data Systems S.A. (Spółka przejmująca) w ramach połączenia ze Spółką Unizeto Technologies S.A. (Spółka przejmowana), dokonanego na podstawie art. 492 § 1 pkt 1 ustawy z dnia 15 września 2000 r. Kodeks spółek handlowych (t.j. Dz.U. z 2013 r. poz. 1030 z późn. zm., dalej "Ksh"), polegającego na przeniesieniu całego majątki Spółki przejmowanej na Spółkę przejmującą, wstąpiła we wszelkie prawa i obowiązki Spółki Unizeto Technologies S.A. (sukcesja generalna - art. 494 § 1 Ksh).

W związku z przeniesieniem całego majątku Spółki Unizeto Technologies S.A. na Spółkę Asseco Data Systems S.A. oświadczamy, że Spółka Asseco Data System S.A. zobowiązuje się do utrzymywania zaświadczenia certyfikacyjnego wydanego na Spółkę Unizeto Technologies S.A. do czasu wygaśnięcia ostatniego certyfikatu wydanego przez Spółkę Unizeto Technologies S.A. w ramach posiadanego zaświadczenia certyfikacyjnego.

---

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

[2] Patrz **Słownik pojęć**

[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 danych certyfikatów.

[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.

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 świadczone są w ramach **usług niekwalifikowanych CERTUM** z dwoma oddzielnymi domenami certyfikacji: **certum** z wydzielonym głównym urzędem certyfikacji **Certum CA** oraz **ctnDomena** z wydzielonymi głównymi urzędami certyfikacji **Certum Trusted Network CA**, **Certum Trusted Network CA 2**[6] oraz **Certum Trusted Network CA EC**. Główne urzędy certyfikacji obu domen same sobie wystawią tzw. autocertyfikat[7] i są niezależne od siebie. Hierarchicznie poniżej głównych urzędów certyfikacji znajdują się podległe im pośrednie urzędy certyfikacji.

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** lub domeny **ctnDomena**.

Certyfikaty wydawane przez CERTUM w ramach domen **certum** i **ctnDomena** zawierają identyfikatory polityk certyfikacji[8], 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. 7.1.6) każdego certyfikatu wydawanego przez CERTUM.

Z Kodeksem Postępowania Certyfikacyjnego związane są inne dodatkowe dokumenty, które wykorzystywane są w systemie CERTUM i regulują jego funkcjonowanie (patrz Tab. 1.1). Dokumenty te mają różny status. Najczęściej jednak ze względu na wagę zawartych w nich informacji oraz bezpieczeństwo systemu nie są publicznie udostępniane.

---

[6] Wszystkie informacje w niniejszym dokumencie odnoszące się do urzędu Certum Trusted Network CA dotyczą także urzędu Certum Trusted Network CA 2

[7] **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).

[8] 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. 1.1 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.	Dokumentacja personelu. Zakres obowiązków i odpowiedzialności.	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
4.	Dokumentacja Głównego Punktu Rejestracji.	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
5.	Dokumentacja infrastruktury technicznej.	Niejawny	Lokalnie - tylko uprawnione osoby oraz audytor
6.	Dokumentacja zarządzania ciągłością działalności systemu.	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 Kodeksowi Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci **Kodeks Postępowania Certyfikacyjnego Niekwalifikowanych Usług CERTUM**. Dokument ten jest dostępny w postaci elektronicznej w repozytorium o adresie http://www.certum.pl,

Z dokumentem Kodeksu Postępowania Certyfikacyjnego związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113527.2.2.0.1.5.1):

```
id-ccert-kpc-v3_0  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(5) 1}
```

w którym dwie ostatnie wartości liczbowe odnoszą się do aktualnej **wersji** i **wydania** 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.

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 z domeny **certum**, urzędów certyfikacji z domeny **ctnDomena** a także 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 nieposiadającym 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

Głównymi urzędami certyfikacji dla domeny **są:**

- urząd certyfikacji **Certum CA**,
- urząd certyfikacji **Certum Trusted Network CA**,
- urząd certyfikacji **Certum Trusted Network CA 2** oraz
- urząd certyfikacji **Certum Trusted Network CA EC**,

którym podlegają wszystkie pośrednie urzędy certyfikacji.

W chwili obowiązywania niniejszego Kodeksu Postępowania Certyfikacyjnego urzędy **Certum Trusted Network CA 2** oraz **Certum Trusted Network CA EC** nie świadczą usług certyfikacyjnych.

1.3.1.1. Główne urzędy certyfikacji

Główne urzędy certyfikacji CERTUM mogą rejestrować i wydawać certyfikaty tylko pośrednim urzędom certyfikacji oraz urzędom wystawiającym elektroniczne poświadczenia niezaprzeczalności.

Urzędy **Certum CA, Certum Trusted Network CA EC**, **Certum Trusted Network CA oraz Certum Trusted Network CA 2** działają w oparciu o wystawione przez siebie autocertyfikaty. W autocertyfikatach nie umieszcza się rozszerzenia **certificatePolicies**, co należy interpretować jako brak ograniczeń na zbiór ścieżek certyfikacji[9], do których można dołączać certyfikat urzędu głównego.

[9] Patrz **Słownik pojęć**

Urzędy certyfikacji **Certum CA, Certum Trusted Network CA, Certum Trusted Network CA 2** oraz **Certum Trusted Network CA EC** świadczą usługi certyfikacyjne dla:

- samych siebie (wystawia i aktualizuje autocertyfikaty),
- urzędów pośrednich,
- 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 wystawiają certyfikaty subskrybentom zgodnie z politykami, których identyfikatory podane są w Tab.1.2.

Nazwa pośredniego urzędu certyfikacji	Identyfikator polityki certyfikacji
Certum Level I CA	1.2.616.1.113527.2.2.1
Certum Level II CA	1.2.616.1.113527.2.2.2
Certum Level III CA	1.2.616.1.113527.2.2.3
Certum Level IV CA	1.2.616.1.113527.2.2.4
Certum Global Services CA	2.5.29.32.0 (**anyPolicy**)[10] lub 1.2.616.1.113527.2.2.9[11]
Certum Extended Validation CA, Certum Extended Validation CA SHA2	1.2.616.1.113527.2.5.1.1
Certum Organization Validation CA SHA2	1.2.616.1.113527.2.5.1.2
Certum Digital Identification CA SHA2	1.2.616.1.113527.2.5.1.6.11 1.2.616.1.113527.2.5.1.6.12 1.2.616.1.113527.2.5.1.6.13 1.2.616.1.113527.2.5.1.6.14
Certum Domain Validation CA SHA2	1.2.616.1.113527.2.5.1.3
Certum Code Signing CA, Certum Code Signing CA SHA2	1.2.616.1.113527.2.5.1.4, 2.23.140.1.4.1
Certum Extended Validation Code Signing CA SHA2	1.2.616.1.113527.2.5.1.7 2.23.140.1.3
Certum Class 1 CA, Certum Class 1 CA SHA2	1.2.616.1.113527.2.5.1.5
WoSign EV SSL CA WoSign OV SSL CA WoSign Code Signing CA WoSign DV SSL CA	1.2.616.1.113527.2.5.1.13.1 1.2.616.1.113527.2.5.1.12.2 1.2.616.1.113527.2.5.1.14.4 1.2.616.1.113527.2.5.1.15.3 2.23.140.1.2.1
Yandex CA	1.2.616.1.113527.2.5.1.10.2
Certum Global Services CA SHA2	1.2.616.1.113527.2.5.1.9
GIS CA	1.2.616.1.113527.2.5.1.9.1.3
nazwaSSL	1.2.616.1.113527.2.5.1.9.2.3
Shoper® SSL	1.2.616.1.113527.2.5.1.9.3.3
SpaceSSL CA	1.2.616.1.113527.2.5.1.9.4.3
www.lh.pl	1.2.616.1.113527.2.5.1.9.5.3
Certyfikat SSL	1.2.616.1.113527.2.5.1.9.6.3
4fastssl.com	1.2.616.1.113527.2.5.1.9.7.3
TrustAsia DV SSL CA - C3	1.2.616.1.113527.2.5.1.9.8.3
TrustAsia OV SSL CA - C3	1.2.616.1.113527.2.5.1.9.9.2
TrustAsia EV SSL CA - C3	1.2.616.1.113527.2.5.1.9.10.1
TrustOcean Certification Authority	1.2.616.1.113527.2.5.1.9.11.3, 1.2.616.1.113527.2.5.1.9.11.2
GDCA TrustAUTH R4 DV SSL CA G2	1.2.616.1.113527.2.5.1.9.12.3
GDCA TrustAUTH R4 OV SSL CA G2	1.2.616.1.113527.2.5.1.9.13.2
GDCA TrustAUTH R4 EV SSL CA G2	1.2.616.1.113527.2.5.1.9.14.1
GoGetSSL Domain Validation CA SHA2	1.2.616.1.113527.2.5.1.9.15.3

[10] Urzędy certyfikacji **Certum Global Services CA** oraz **Certum Global Services CA SHA2** wpisują do certyfikatów wydanych akredytowanym przez siebie urzędom certyfikacji identyfikator polityki certyfikacji o wartości 2.5.29.32.0 (**anyPolicy**). Z kolei wszystkie certyfikaty znajdujące się w ścieżce certyfikacji pomiędzy certyfikatem akredytowanego urzędu, a certyfikatem użytkownika końcowego włącznie muszą zawierać identyfikator polityki certyfikacji utworzony na bazie węzła drzewa identyfikatorów o wartości 1.2.616.1.113527.2.2.9. Przykładem takiego identyfikatora polityki jest polityka o wartości 1.2.616.1.113527.2.2.9.1. W szczególnych przypadkach CERTUM może wydać certyfikat akredytowanym przez siebie urzędom certyfikacji spod głównego root'a z domeny ctnDomena.

[11] Według tej polityki certyfikacji urzędy certyfikacji **Certum Global Services CA oraz Certum Global Services CA SHA2** wydają certyfikaty wszystkim innym urzędom nie będącym urzędami certyfikacji.

GoGetSSL Business Validation CA SHA2	1.2.616.1.113527.2.5.1.9.16.2
GoGetSSL Extended Validation CA SHA2	1.2.616.1.113527.2.5.1.9.17.1

W certyfikatach wystawianych pośrednim urzędom oraz certyfikatach innych urzędów i podmiotów umieszcza się rozszerzenia ***certificatePolicies****.*

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

Innym urzędom certyfikacji certyfikaty mogą wystawiać tylko następujące urzędy pośrednie: ***Certum Level I CA*** *i* ***Certum Class 1 CA SHA2*** *(testowe urzędy certyfikacji) oraz* ***Certum Global Services CA*** *i* ***Certum Global Services CA SHA2*** *(komercyjne urzędy certyfikacji). Zawsze jednak certyfikaty wydawane innym urzędom certyfikacji podlegają wyłącznej kontroli CERTUM. Także wydawanie certyfikatów subskrybentom przez urzędy, którym wydano zaświadczenia odbywa się wyłącznie pod kontrolą CERTUM. Żaden z urzędów pośrednich, którym wydano certyfikaty nie może pełnić roli Punktu Rejestracji ani samodzielnie wydawać certyfikatów użytkownikom końcowym.*

Z CERTUM ściśle współpracuje Główny Punkt Rejestracji oraz Punkty Rejestracji, które 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;
- innych urzędów certyfikacji (dotyczy to tylko pośrednich urzędów **Certum Level I CA, Certum Class 1 CA SHA2**, **Certum Global Services CA** oraz **Certum Global Services CA SHA2**).

1.3.2. Punkty Rejestracji

Główny Punkt Rejestracji przyjmuje, weryfikuje i następnie aprobuje lub odrzuca – 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 oraz zademonstrowania przez subskrybenta kontroli nad certyfikowaną Nazwą Wyróżnioną) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Główny Punkt Rejestracji może 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 Główny Punkt Rejestracji sprawdza tylko prawidłowość podanego adresu email. Najdokładniejsza weryfikacja może z kolei wymagać osobistego stawienia się subskrybenta w punkcie Rejestracji i przedłożenia stosownych dokumentów. Oznacza to, że weryfikacja może być realizowana albo całkowicie automatycznie, albo ręcznie przez operatora Głównego Punktu Rejestracji.

Główny Punkt Rejestracji działa z upoważnienia odpowiedniego urzędu certyfikacji należącego do domeny **certum** lub **ctnDomena** w zakresie weryfikacji tożsamości aktualnego lub przyszłego subskrybenta oraz weryfikacji uprawnień subskrybenta do Nazwy Wyróżnionej.

W przypadku Punktów Rejestracji zarządzanych przez podmioty inne niż Asseco Data Systems S.A. (zewnętrzne Punkty Rejestracji), szczegółowy zakres obowiązków Punktów Rejestracji i jego operatorów może być określony poprzez osobną umowę zawartą pomiędzy Asseco Data Systems 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 niniejszym Kodeksie Postępowania Certyfikacyjnego.

Lista aktualnie akredytowanych przez GPR Punktów Rejestracji dostępna jest w repozytorium pod adresem: http://www.certum.pl

Podstawowa różnica pomiędzy Głównym Punktem Rejestracji oraz zewnętrznymi Punktami Rejestracji polega na tym, że zewnętrzne Punkty Rejestracji nie mogą – w przeciwieństwie do Głównego Punktu Rejestracji – akredytować innych Punktów Rejestracji, rejestrować nowych urzędów certyfikacji oraz nie posiadają uprawnień do weryfikowania żądań certyfikacyjnych subskrybentów w zakresie walidacji Nazw Wyróżnionych.

Główny Punkt Rejestracji 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 Głównym Punkcie Rejestracji. Dodatkowo Główny Punkt Rejestracji 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. 1.5.2.

1.3.3. Subskrybenci

Subskrybentami CERTUM mogą być dowolne osoby fizyczne, prawne lub podmioty nieposiadające osobowości prawnej oraz urządzenia będące pod ich kontrolą, którego identyfikator umieszczany jest w polu podmiot (ang. Subject) certyfikatu lub innych poświadczeń wydawanych przez CERTUM.

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 typach. Subskrybent powinien zdecydować, jaki typ certyfikatu jest najodpowiedniejszy do jego potrzeb (patrz rozdz. 1.4).

1.3.4. Strony ufające

Stroną ufającą, korzystającą z usług CERTUM, jest dowolny podmiot, który podejmuje decyzję o akceptacji certyfikatu lub innego poświadczenia wydanego przez CERTUM 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**.

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.

1.3.5. Inne strony

W ramach CERTUM działają także podmioty, które świadczą usługi uzupełniające podstawowe usługi wydawania i unieważniania certyfikatów.

1.3.5.1. Urząd znacznika czasu

Elementem infrastruktury **CERTUM** jest urząd znacznika czasu **Certum EV TSA SHA2**, który działa w domenie certyfikacji **ctnDomena**.

Urząd znacznika czasu wydaje znaczniki czasu zgodnie z RFC 3161 lub zaleceniami ETSI[12]. Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony oraz poświadczany jest wyłącznie za pomocą klucza prywatnego wytworzonego specjalnie dla usługi znakowania czasem.

Tab. 1.3 Identyfikator polityki certyfikacji umieszczany przez **Certum EV TSA SHA2** w tokenach znacznika czasu

Nazwa tokena	Identyfikator polityki certyfikacji	Zgodność z wymaganiami
Token znacznika czasu	1.2.616.1.113527.2.5.1.11	RFC 3161 ETSI TS 101 861, Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates, Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,

Znaczniki czasu, wydawane zgodnie z polityką określoną w Tab. 1.4, znajdują zastosowanie przede wszystkim do zabezpieczania długookresowych podpisów cyfrowych[13] oraz transakcji zawieranych w sieci globalnej.

Urząd znacznika czasu **Certum EV TSA SHA2** przy świadczeniu usług znacznika czasu stosuje rozwiązania zapewniające synchronizację z międzynarodowym wzorcem czasu (Coordinated Universal Time – UTC), z dokładnością większą niż 1 sekunda.

1.3.5.2. Urząd weryfikacji statusu certyfikatu

CERTUM oprócz standardowego sposobu weryfikacji statusu certyfikatów w oparciu o pobieranie listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu

12 ETSI TS 101 861 *Time stamping profile*, August 2001

13 IETF RFC 3126 *Electronic Signature Formats for long term electronic signatures*, September 2001

certyfikatu w trybie *on-line* (OCSP). Usługa ta świadczona jest przez grupę urzędów weryfikacji statusu certyfikatu o wspólnej nazwie **Certum Validation Service**. Każdy urząd certyfikacji w domenach **certum** oraz **ctnDomena** posiada własny, dedykowany urząd weryfikacji.

Wszystkie urzędy weryfikacji statusu certyfikatu pracują w trybie **autoryzowany responder** (ang. Authorized Responder).

1.4. Zakres stosowania certyfikatów

Certyfikaty umożliwiają, posługującym się nimi podmiotom, wzajemną identyfikację oraz mogą służyć do zabezpieczania elektronicznej wymiany informacji. Zakres stosowania certyfikatów określa obszary tzw. Dozwolonego użycia certyfikatu. Obszar ten określa naturę (charakter) zastosowania certyfikatu (poufność, integralność lub 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[14] powinny zostać oszacowane przez subskrybenta. Urzędy certyfikacji CERTUM wydają certyfikaty w trzech klasach o różnym poziomie wiarygodności. Poziom wiarygodności dla poszczególnych klas został opisany w Polityce Certyfikacji Niekwalifikowanych Usług CERTUM.

Za określenie poziomu wiarygodności certyfikatu, przydatnego do określonego zastosowania, odpowiada strona ufająca lub sam subskrybent. Strony te na podstawie różnych istotnych czynników ryzyka powinny 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 PCC jest członkiem CAB/Forum i świadczy swoje usługi zgodnie z wymaganiami aktualnych obowiązujących wersji następujących dokumentów:

- **Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates**,
- **Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates** oraz
- **Guidelines For The Issuance And Management Of Extended Validation Certificates.**

W przypadku jakichkolwiek rozbieżności pomiędzy niniejszym dokumentem a wymaganiami CAB/Forum, wymagania te mają pierwszeństwo nad niniejszym dokumentem.

Ponadto, od dnia 01.02.2017 wszystkie usługi związane z wydawaniem, unieważnianiem i obsługą certyfikatów przeznaczonych do podpisywania kodu, świadczone są zgodnie z wymaganiami **Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates**.

CERTUM wydaje także certyfikaty zgodnie z polityką **Certum Global Services CA** oraz **Certum Global Services CA SHA2**. Certyfikaty te wydawane są zgodnie z zasadami określonymi dla danych typów certyfikatów.

---

14 Patrz **Słownik pojęć**

1.4.1. Typy certyfikatów i zalecane obszary ich zastosowań

CERTUM wydaje następujące podstawowe typy certyfikatów, określających jednocześnie obszary ich zastosowania. Są to:

a) **certyfikaty osobiste** – umożliwiają szyfrowanie i podpisywanie poczty elektronicznej oraz znajdują zastosowanie w zabezpieczaniu dokumentów elektronicznych (poczta elektroniczna wg standardu S/MIME lub PGP),

b) **certyfikaty SSL i EV SSL do uwierzytelnienia serwisów lub serwerów** – stosowane przez globalne oraz ekstranetowe serwisy usługowe pracujące w osłonie protokołu SSL/TLS/WTLS,

c) **certyfikaty SSL do uwierzytelniania subskrybentów** (osób prawnych i fizycznych, urządzeń) – stosowane m.in. w protokołach SSL/TLS/WTLS,

d) **certyfikaty do poświadczania statusu certyfikatów** – wydawane są na serwery działające zgodnie z protokołem OCSP i wystawiające tokeny aktualnego statusu weryfikowanego certyfikatu,

e) **certyfikaty do szyfrowania** – umożliwiają zabezpieczanie plików, katalogów oraz systemów plików,

f) **certyfikaty do zabezpieczania kodu** – certyfikaty przeznaczone dla programistów służące do zabezpieczania oprogramowania przed sfałszowaniem,

g) **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 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,

h) **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.

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

- prawidłowo zarządzają kluczami publicznymi i prywatnymi, ich przesyłaniem oraz używaniem,
- certyfikaty oraz związane z nimi klucze prywatne 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.

CERTUM oferuje swoim klientom certyfikaty we wszystkich rodzajach zastosowań opisanych wyżej.

Tab. 1.4 Grupy certyfikatów wydawane przez pośrednie urzędy 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 podpisów na wystawianych certyfikatach i listach CRL, wymiany kluczy, uzgadniania kluczy, świadczenia usług niezaprzeczalności (patrz rozszerzenie certyfikatu **keyUsage**)

Certyfikaty	Urząd Certyfikacji
Certyfikaty testowe	Certum Level I CA, Certum Class 1 CA, Certum Class 1 CA SHA 2,
Certyfikaty ID z walidacją adresu email	Certum Level II CA, Certum Domain Validation CA SHA2
Certyfikaty ID z walidacją danych DN	Certum Level IV CA, Certum Digital Identification CA SHA2, Certum Organization Validation CA SHA2
Certyfikaty SSL DV	Certum Level II CA, Certum Domain Validation CA SHA2
Certyfikaty SSL OV	Certum Level IV CA, Certum Organization Validation CA SHA2
Certyfikaty SSL EV	Certum Extended Validation CA, Certum Extended Validation CA SHA2
Certyfikaty Code Signing	Certum Code Signing CA, Certum Code Signing CA SHA2
Certyfikaty EV Code Signing	Certum Extended Validation Code Signing CA SHA2
Certyfikaty VPN oraz IPSec Client	Certum Level II CA, Certum Level IV CA,
Certyfikaty partnerskie	Certum Global Services CA, Certum Global Services CA SHA2

1.4.2. Nierekomendowane zastosowania certyfikatów

Zabrania się używania certyfikatów CERTUM niezgodnie z ich deklarowanym przeznaczeniem oraz w aplikacjach, które nie spełniają wymagań określonych w rozdz. 1.4.1. W szczególności certyfikaty urzędów certyfikacji oraz innych urzędów świadczących usługi certyfikacyjne mogą być stosowane przez te urzędy tylko w kontekście funkcji, które mają prawo realizować. Dodatkowo certyfikaty subskrybentów (poza certyfikatami wydawanymi w ramach polityki certyfikacji Certum Global Services CA oraz Certum Global Services CA SHA2) nie mogą być stosowane w roli certyfikatów urzędów certyfikacji, tzn. nie można ich używać do weryfikowania certyfikatów urzędów certyfikacji oraz certyfikatów innych podmiotów świadczących usługi certyfikacyjnych.

1.5. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego obowiązuje (posiada status aktualny) do czasu opublikowania i zatwierdzenia nowej wersji (patrz rozdz. 9.10). Nowa wersja opracowywana jest przez pracowników CERTUM 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 (patrz 1.2).

Subskrybenci zobowiązani są stosować się wyłącznie do aktualnie obowiązującej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego.

Dalsze zasady administrowania Kodeksem Postępowania Certyfikacyjnego przedstawiono w rozdz. 9.10.

1.5.1. Organizacja odpowiedzialna za administrowanie dokumentem

Asseco Data Systems S.A
ul. Podolska 21
81-321 Gdynia
Polska

1.5.2. Kontakt

Asseco Data Systems S.A.
CERTUM – Powszechne Centrum Certyfikacji
71-838 Szczecin, ul. Bajeczna 13
Polska
E-mail: info@certum.pl
Numer telefonu: +48 91 4801 340

1.5.3. Podmioty określające aktualność zasad określonych w dokumencie

Za ocenę aktualności i przydatności niniejszego Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji oraz innych dokumentów dotyczących usług PKI, świadczonych przez CERTUM, a także za zgodność między wymienionymi dokumentami, odpowiada zespół CERTUM. Wszelkie zapytania i uwagi związane z zawartością wymienionych dokumentów powinny być kierowane pod adres podany w rozdz. 1.5.2).

1.5.4. 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. 9.10), nie wpłyną istotne zastrzeżenia odnośnie ich merytorycznej zawartości, nowa wersja dokumentu o statusie **w zatwierdzeniu** jest publikowana w repozytorium i staje się obowiązującą wykładnią Kodeksu Postępowania Certyfikacyjnego, respektowaną przez wszystkich subskrybentów CERTUM i przyjmuje status **aktualny**.

Decyzję o opublikowaniu nowej wersji Kodeksu Postępowania Certyfikacyjnego podejmuje osoba zarządzająca PCC CERTUM.

1.6. Definicje i używane skróty

Definicje oraz skróty używane w niniejszym dokumencie znajdują się na końcu niniejszego dokumentu.

2. Odpowiedzialność za publikację i repozytorium

2.1. Repozytorium

Repozytorium jest zbiorem publicznie dostępnych katalogów zarządzanych i kontrolowanych przez CERTUM.

Na potrzeby usług niekwalifikowanych CERTUM funkcjonuje tylko jedno repozytorium, wspólne dla użytkowników obu domen certyfikacji ***certum*** *i* ***ctnDomena*** *oraz dla wszystkich urzędów certyfikacji działających w ich obrębie lub z nimi powiązanych.*

Wspólne repozytorium CERTUM:

- zapewnia, że wszystkie certyfikaty opublikowane w repozytorium należą do subskrybentów wskazanych w certyfikacie oraz że subskrybenci ci zaakceptowali certyfikat zgodnie z wymaganiami przedstawionymi w rozdz. 4.4,
- terminowo publikuje i archiwizuje certyfikaty urzędów certyfikacji, Punktów Rejestracji, należących do obu domen certyfikacji oraz certyfikaty subskrybentów, po uprzednim uzyskaniu na to ich zgody,
- publikuje i archiwizuje Politykę Certyfikacji, Kodeks Postępowania Certyfikacyjnego oraz wzory umów zawieranych z subskrybentami,
- udostępnia informacje o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL), serwer OCSP lub zapytania kierowane za pośrednictwem protokołu HTTP,
- zapewnia urzędom certyfikacji, Punktom Rejestracji, subskrybentom oraz stronom ufającym gwarancję, ciągłego dostępu do informacji zgromadzonej w repozytorium, 7 dni w tygodniu przez 24 godziny
- szybko i zgodnie z okresami określonymi w niniejszym dokumencie publikuje listy CRL oraz inne informacje,
- zapewnia bezpieczny i kontrolowany dostęp 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.

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

2.2. Informacje publikowane w repozytorium

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

Informacje dostępne są w repozytorium to:

- certyfikaty wszystkich 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,
- aktualna i poprzednie wersje Polityki Certyfikacji,
- aktualna i poprzednie wersje Kodeksy Postępowania Certyfikacyjnego,
- Polityka Certyfikacji lub Kodeksy Postępowania Certyfikacyjnego posiadające status w zatwierdzeniu,
- wzory umów z subskrybentami,
- 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 za pośrednictwem serwera WWW (adres http://www.certum.pl) oraz mogą być udostępniane dodatkowo za pośrednictwem serwisów usług katalogowych (adres 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 za pośrednictwem strony WWW (adres http://www.certum.pl) lub usługi OCSP (adres: http://ocsp.certum.pl).

2.3. Częstotliwość publikowania

Wymienione poniżej publikacje CERTUM są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego – patrz rozdz. 9.12;
- certyfikaty urzędów certyfikacji funkcjonujących w ramach CERTUM – każdorazowo, gdy nastąpi wydanie 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. 4.9.7;
- raporty z audytu dokonywanego przez upoważnioną instytucję – każdorazowo, po otrzymaniu go przez CERTUM;
- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.4. 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.

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, które 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. Nadawanie nazw

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.

W przypadku certyfikatów wydawanych na potrzeby uwierzytelniania serwerów, CERTUM posiada automatyczne procedury, które uniemożliwiają wydanie użytkowi końcowemu certyfikatu typu Wildcard, który zwierałby wieloznacznik (*) w miejscu poprzedzającym bezpośrednio nazwę domeny najwyższego poziomu.

W przypadku wniosków certyfikacyjnych dotyczących nazw domenowych zawierających znaki spoza notacji ASCI (ang. Internationalized Domain Name) CERTUM, w celu zapobieżenia próbom fałszowania nazw domenowych (ang. Homographic spoofing), weryfikuje właściciela certyfikowanej domeny oraz stosuje niezautomatyzowane procedury umożliwiające wykrycie ryzyka fałszerstwa.

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 17 oraz schematami nazewniczymi stosowanymi przez protokół LDAP (patrz RFC 1778).

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. 7.1 (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 5280 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 UN **– nazwa routera lub urządzenia sieciowego,**
- pola D – dodatkowa nazwa wyróżniająca subskrybenta.

Zgodnie z wymaganiami **Guidelines for the Issuance and Management of Extended Validation Certificates** w certyfikatach EV SSL umieszczane są dodatkowe atrybuty nazwy wyróżnionej DN.

Nazwa wyróżniona subskrybenta musi zostać zweryfikowana przez Punkt Rejestracji oraz zaakceptowana przez urząd certyfikacji.

3.1.3. Anonimowość subskrybentów

CERTUM nie wystawia certyfikatów oraz innych poświadczeń zapewniających anonimowość danych subskrybenta (np. pseudonimem).

3.1.4. 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.

3.1.5. 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** i domenie **ctnDomena**) numer seryjny. Stanowi on

wyróżnik certyfikatu, który wraz z nazwą wyróżnioną DN precyzyjnie i unikalnie określa właściwego subskrybenta.

3.1.6. Rozpoznawanie, uwierzytelnianie oraz rola znaków towarowych

CERTUM nie umieszcza w certyfikatach znaków towarowych. Jednocześnie zabrania się używania we wnioskach nazw, które nie są własnością subskrybenta. W przypadku, gdy we wniosku o wystawienie certyfikatu występują informacje o takim charakterze, to wnioskodawca jest obowiązany do dołączenia dokumentów potwierdzających posiadane prawa własności.

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.

3.2. Rejestracja

Rejestracja subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składający wniosek o rejestrację nie posiada żadnego **ważnego certyfikatu**[16] 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 do Punktu Rejestracji dowód posiadania klucza prywatnego (patrz rozdz.3.2.1); opcjonalnie subskrybent może zlecić wygenerowanie pary kluczy urzędowi certyfikacji,,
- 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 Asseco Data Systems S.A. na świadczenie usług przez CERTUM.

16 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.

3.2.1. Dowód posiadania klucza prywatnego

Podstawowy dowód posiadania klucza prywatnego ma postać podpisu cyfrowego składanego na żądaniach rejestracji i modyfikacji danych oraz na żądaniach aktualizacji kluczy/certyfikatu, dostarczanych do Punktu Rejestracji lub bezpośrednio do urzędu certyfikacji.

Za dowód posiadania klucza prywatnego uznaje się żądanie certyfikacyjne (ang. Certificate Signing Request) w formacie PKCS#10 lub SPKAC (ang. Signed Public Key and Challenge).

3.2.2. Uwierzytelnienie tożsamości osób prawnych

CERTUM musi zweryfikować, że dana organizacja, której nazwa znajdzie się w treści certyfikatu istniała faktycznie w momencie wydawania certyfikatu.

Weryfikację wykonuje się w oparciu o niezależne od CERTUM **kwalifikowane źródła informacji** m. in. publicznie dostępne rejestry przedsiębiorstw/organizacji.

CERTUM zobowiązane 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 kwalifikowanych 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) muszą potwierdzić:

- nazwę subskrybenta certyfikatu,
- faktyczne istnienie osoby prawnej reprezentowanej w certyfikacie,
- dane adresowe subskrybenta certyfikatu
- prawo subskrybenta lub administratora do występowania w imieniu jednostki lub osoby prawnej,
- w przypadku certyfikatów SSL operator Punktu Rejestracji może sprawdzić rejestrację domeny w publicznie dostępnych serwisach WHOIS.

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 przedstawicielem.

Jeśli we wniosku certyfikacyjnym znajduje się kod kraju (countryName), wówczas CERTUM weryfikuje kraj wnioskodawcy na podstawie najwyższej krajowej domeny będącej częścią certyfikowanej nazwy domenowej.

Szczegółowe wymagania dotyczące dokumentów oraz potwierdzania danych opisano na stronach www.certum.pl.

Punkt Rejestracji zobligowany jest do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku. W przypadku certyfikatów EV SSL oraz EV Code Signing stosowane są dodatkowe procedury zgodne z wymaganiami ***Guidelines for the Issuance and Management of Extended Validation Certificates*** oraz ***Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates****.W przypadku certyfikatów służących do zabezpieczania poczty elektronicznej oprócz uwierzytelnienia na podstawie przesłanych dokumentów Punkt Rejestracji żąda weryfikacji adresu email. Czynność ta polega na odebraniu przez subskrybenta danych uwierzytelniających wysłanych przez CERTUM na adres wskazany w żądaniu certyfikacyjnym.*

W przypadku certyfikatów wystawionych dla urządzeń, weryfikacja może odbywać się poprzez sprawdzenie dostępu do domeny znajdującej się w żądaniu przesłanym przez Subskrybenta. Weryfikacja ta polega na umieszczeniu przez subskrybenta na serwerze docelowym elementu wskazanego przez CERTUM lub na udzieleniu przez subskrybenta odpowiedzi na wiadomość email wysłaną przez CERTUM na ustalony adres w domenie wskazanej w żądaniu przesłanym przez subskrybenta.

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.

3.2.3. 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. Weryfikacja adresu e- mail przeprowadzana jest analogicznie jak punkcie 3.2.2.

3.2.4. Dane subskrybenta niepodlegające weryfikacji

CERTUM weryfikuje wszystkie informacje zawarte w nazwie wyróżnionej podmiotu certyfikatu

3.2.5. Weryfikacja uprawnień

W przypadku, gdy wniosek certyfikacyjny zawiera nazwę organizacji (atrybut O), to należy to interpretować jako afiliację osoby fizycznej składającej wniosek lub uprawnienie (autoryzację) tej osoby do działania w imieniu organizacji. Oznacza to jednocześnie, że CERTUM weryfikuje, czy osoba fizyczna, która złożyła wniosek certyfikacyjny była w momencie wystawienia certyfikatu pracownikiem organizacji lub jej współpracownikiem i ma prawo do działania w imieniu organizacji; zakres tych uprawnień oraz okres ich ważności może być regulowany przez oddzielne przepisy lub stronę ufającą dokonującą weryfikacji tych uprawnień w momencie weryfikowania podpisu cyfrowego lub deszyfrowania otrzymanego dokumentu i znajduje się poza zakresem odpowiedzialności CERTUM; dane osoby fizycznej i jej uprawnienia CERTUM sprawdza w oparciu o dostępne zapisy lub bazy, kontakt telefoniczny lub e-mailowy z organizacją, której pracownikiem lub współpracownikiem jest osoba fizyczna.

3.2.6. Weryfikacja nazw domenowych

W przypadku certyfikatów SSL, CERTUM zawsze weryfikuje czy wnioskodawca jest uprawniony do posługiwania się nazwą (nazwami) domenową lub posiada nad nią kontrolę. Weryfikacja wykonywana jest przynajmniej jedną z następujących metod:

- przez umieszczenie pliku o określonej nazwie w katalogu /.well-known/pki-validation,
- przez umieszczenie określonych danych w rekordzie TXT domeny,
- potwierdzając dane kontaktowe zamieszczone w bazie WHOIS lub bezpośrednio kontaktując się z rejestratorem domeny lub otrzymując Dokument Potwierdzający prawo subskrybenta do domeny – wyłącznie jeśli zweryfikowana została tożsamość oraz uprawnienia subskrybenta zgodnie z rozdziałem 3.2.2
- otrzymując pozytywną informację zwrotną na wiadomość wysłaną na jeden z następujących adresów email: webmaster@domain.com, postmaster@domain.com, admin@domain.com, administrator@domain.com, hostmaster@domain.com.

CERTUM korzysta wyłącznie ze źródeł WHOIS zaakceptowanych przez IANA oraz ICANN.

3.2.7. Kryteria interoperacyjności

CERTUM może akredytować lub być akredytowane przez zewnętrzne podmioty świadczące usługi certyfikacyjne. Akredytacja odbywa się na wniosek zainteresowanego podmiotu, po spełnieniu poniższych warunków:

- podmiot zewnętrzny świadczy usługi certyfikacyjne zgodnie z Polityką Certyfikacji i Kodeksem Postępowania Certyfikacyjnego; oba dokumenty nie mogą być sprzeczne z niniejszym dokumentem w zakresie świadczonej lub świadczonych usług;
- system teleinformatyczny oraz struktura organizacyjna wnioskodawcy uzyska pozytywną opinię upoważnionej komórki CERTUM lub innego audytor akceptowanego przez CERTUM,
- usługa lub usługi świadczone przez akredytowany podmiot zapewniają interoperacyjność z odpowiednimi usługami świadczonymi przez CERTUM,
- zostanie zawarta umowa pomiędzy CERTUM i akredytowanym podmiotem, regulująca wzajemne relacje biznesowe, prawa i obowiązki.

Akredytowane podmioty otrzymują certyfikat na świadczenie odpowiedniej usługi wystawione przez urzędy certyfikacji **Certum Global Services CA** oraz **Certum Global Services CA SHA2.** Certyfikat ten może być unieważniony, jeśli coroczny audyt

przeprowadzony przez upoważnioną komórkę CERTUM lub innego audytora akceptowanego przez CERTUM wykaże rażące zaniedbania akredytowanego podmiotu i które nie zostaną usunięte w okresie wskazanym przez audytora.

W ramach wsparcia użytkowników podpisujących aplikacje wykonywane w trybie jądra systemu (ang. kernel mode) w systemach Microsoft Windows, urząd certyfikacji Certum Trusted Network został certyfikowany przez urząd certyfikacji Microsoft Code Verification Root. Certyfikat wzajemny **(*ang. cross-certificate*)** dostępny jest w repozytorium.

3.3. Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy

W przypadku, gdy subskrybent posiada ważny certyfikat (taki, który nie jest ani przeterminowany ani też unieważniony), to może wystąpić o wydanie nowego certyfikatu. Nowy certyfikat może być wydany dla nowej pary kluczy, wygenerowanej przez subskrybenta lub CERTUM (tzw. **Aktualizacja klucza**) lub aktualnej pary kluczy (tzw. **Recertyfikacja**). CERTUM dopuszcza także modyfikację certyfikatu w wyniku, której zmianie podlegają dane subskrybenta umieszczane w certyfikacie oraz klucz publiczny (dokładniej – para kluczy subskrybenta, patrz rozdz. 3.3.1.3 i 4.8).

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.

Aktualizacja kluczy, recertyfikacja lub modyfikacja certyfikatu może odbywać się za pośrednictwem strony WWW udostępnionej przez CERTUM.

3.3.1. Identyfikacja i uwierzytelnienie w przypadku standardowej aktualizacji kluczy

3.3.1.1. 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, inną datą początku ważności oraz nowym podpisem urzędu certyfikacji (szczegóły patrz rozdz. 4.7).

Jeśli subskrybent prześle prawidłowo wypełniony i podpisany cyfrowo wniosek lub dostarczy poprawne hasło, to w przypadku aktualizacji kluczy proces wydawania nowego certyfikatu może odbywać się automatycznie, o ile wydawany certyfikat jest tego samego typu co

nieprzeterminowany i nieunieważniony certyfikat aktualnie posiadany przez subskrybenta oraz jest wydawany w ramach tej samej polityki certyfikacji.

Aktualizacja kluczy w trybie automatycznym jest możliwa w okresie 30 dni od daty początku ważności certyfikatu. Nowo wydany certyfikat zachowuje datę końca ważności poprzedniego certyfikatu.

W innych przypadkach weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest na podstawie dokumentów dostarczonych do aktualizowanego (odnawianego) certyfikatu.

3.3.1.2. 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.

Żądania recertyfikacji mogą być obsługiwane w trybie automatycznym. Recertyfikacja w trybie automatycznym jest możliwa w okresie 30 dni od daty początku ważności certyfikatu. Nowo wydany certyfikat zachowuje datę końca ważności poprzedniego certyfikatu.

3.3.1.3. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza utworzenie nowego certyfikatu na podstawie certyfikatu, który jest aktualnie w posiadaniu subskrybenta. Nowy certyfikat posiada ten sam 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).

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.

3.3.2. Identyfikacja i uwierzytelnienie w przypadku żądania aktualizacji kluczy po ich 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 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. Identyfikacja i uwierzytelnienie w przypadku żądania unieważnienia 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 lub tak jak w przypadku aktualizacji kluczy (patrz rozdz. 3.3.1.1). 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 rozdz. 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 subskrybentów składane są 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: HTTPS, S/MIME lub TCP/IP lub w postaci nieelektronicznej np. zamówień.

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

4.1.1. Kto może składać wnioski o wydanie certyfikatu?

Z wnioskami o wydanie certyfikatu może występować każdy podmiot należący do jednej z poniższych kategorii:

- osoba fizyczna, która jest lub będzie podmiotem certyfikatu,
- uprawniony przedstawiciel osoby prawnej lub instytucji nieposiadającej osobowości prawnej, nazywany zamawiającym,

- uprawniony przedstawiciel urzędu certyfikacji z domeny **certum**, **ctnDomena** lub zewnętrznego podmiotu świadczącego usługi certyfikacyjne (akredytowanego przez CERTUM),
- uprawniony przedstawiciel Głównego Punktu Rejestracji (GPR) lub Punktu Rejestracji (PR).

CERUM nie wydaje certyfikatów podmiotom wykonującym działalność gospodarczą w państwach, z którym prawo Rzeczpospolitej Polskiej zabrania prowadzenia wymiany handlowej.

Zgodnie z wymaganiami **Guidelines for the Issuance and Management of Extended Validation Certificates** oraz **Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates**, certyfikaty EV SSL oraz EV Code Signing mogą być wydawane jedynie organizacjom i przedsiębiorstwom posiadającym osobowość prawną, przedsiębiorstwom i organizacjom nieposiadającym osobowości prawnej a także podmiotom administracji publicznej oraz organizacjom międzynarodowym o charakterze niekomercyjnym. CERTUM nie wydaje certyfikatów EV SSL oraz EV Code Signing osobom fizycznym.

Przed wydaniem certyfikatu uwierzytelniania witryn internetowych CERTUM porównuje dane z wniosku certyfikacyjnego z wewnętrzną listą unieważnionych certyfikatów oraz odrzuconych wniosków certyfikacyjnych. Jeśli już raz certyfikat został unieważniony lub CERTUM odrzuciło dany wniosek certyfikacyjny ze względu na bezpieczeństwo użytkowników, aplikacja o nowy certyfikat może zostać odrzucona.

4.1.2. Proces składania wniosków i związane z tym obowiązki

4.1.2.1. Certyfikaty subskrybentów

Wszyscy subskrybenci certyfikatów i użytkownicy końcowi (w tym także podmioty świadczące usługi certyfikacyjne nie polegające na wydawaniu i unieważnianiu certyfikatów) powinni zaakceptować zobowiązania i gwarancje określone w Warunkach Użytkowania lub Umowie z Subskrybentem (patrz 9.6.3) oraz poddać się procesowi rejestracji, który wymaga wykonania następujących czynności:

- złożenia wniosku, wypełnionego zgodnie z określonymi dla niego zasadami oraz zawierającego prawdziwe i poprawne informacje,
- samodzielnego wygenerowania lub zlecenia CERTUM wygenerowania pary kluczy,
- w przypadku samodzielnego wygenerowania pary kluczy dostarczenie klucza publicznego bezpośrednio do CERTUM lub za pośrednictwem wybranego Punktu Rejestracji pracującego na rzecz CERTUM, a także udowodnienie posiadania klucza prywatnego odpowiadającego przekazanemu kluczowi publicznemu (patrz rozdz. 3.2.1).

4.1.2.2. Certyfikaty urzędów certyfikacji i Punktów Rejestracji

Te urzędy certyfikacji oraz Punkty Rejestracji, które świadczą usługi na rzecz lub z upoważnienia CERTUM oraz nie są jednostkami organizacyjnymi CERTUM muszą wcześniej zawrzeć odpowiednią umowę z CERTUM. Umowa ta, oprócz praw i obowiązków obu stron, określa tożsamość osób oraz ich upoważnienia do reprezentowania obu stron w okresie realizacji umowy. Upoważniona, przez wnioskodawcę, osoba lub osoby powinny m.in. określić przed wydaniem certyfikatu urzędowi certyfikacji lub Punktowi Rejestracji właściwą nazwę wyróżnioną podmiotu certyfikatu.

Klucze i certyfikaty urzędów certyfikacji mogą być generowane tylko podczas ceremonii generowania kluczy, w której udział muszą brać obligatoryjne upoważnieni przedstawiciele CERTUM.

Po zawarciu umowy z Punktem Rejestracji, certyfikaty mogą być wydawane uprawnionym osobom fizycznym oraz urządzeniom tego Punktu Rejestracji niezbędnym podczas świadczenia usług na rzecz CERTUM.

4.1.2.3. Wniosek certyfikacyjny

Wniosek certyfikacyjny 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/KRS 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. 3.2.2, 3.2.3) składającego wniosek certyfikacyjny oraz otrzymaniu potwierdzenia wystawionego przez Punkt Rejestracji wniosek jest przesyłany do urzędu certyfikacji.

4.1.2.4. Wniosek o recertyfikację, aktualizację kluczy lub modyfikację certyfikatu

Wniosek należący do tej grupy wniosków składany jest przez subskrybenta w punkcie Rejestracji lub bezpośrednio w urzędzie certyfikacji.

Wniosek o recertyfikację, aktualizację kluczy lub modyfikację 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. 3.2.2, 3.2.3) składającego wniosek o rejestrację oraz otrzymaniu potwierdzenia wystawionego przez Punkt Rejestracji wniosek jest przesyłany do urzędu certyfikacji.

4.1.2.5. Wniosek o unieważnienie

Wniosek o unieważnienie certyfikatu składany jest przez subskrybenta w Punkcie Rejestracji lub bezpośrednio w urzędzie certyfikacji.

Szczegółowe wymagania w tym zakresie prezentowane są w rozdziale 4.9.3.

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 grupowo. 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 wypełnia – zgodnie z zawartymi tam instrukcjami – właściwy formularz wniosku certyfikacyjnego i wysyła go do urzędu certyfikacji. W przypadku wniosków, które zawierają dane możliwe do weryfikacji w trybie challenge-response (w przypadku wniosków na certyfikaty, które zawierają wyłącznie adres email lub wyłącznie adres domeny) wnioski są przetwarzane automatycznie, zaś w pozostałych przypadkach ręcznie - jeśli wniosek wymaga porównania zawartych w nim danych z dostarczonymi do CERTUM dokumentami. Wniosek o wydanie certyfikatu przetwarzany jest automatycznie, jeśli do zweryfikowania zawartych w nim informacji wystarczą bazy 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 uwierzytelnionych danych służących do uzyskania certyfikatu do przedstawiciela CERTUM. Uwierzytelnienie wykonywane jest zgodnie z zasadami opisanymi na stronach www.certum.pl. 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 grupowe. Wnioski takie są potwierdzane przez operatora urzędu certyfikacji lub Punktu Rejestracji i przetwarzane zbiorczo.

4.2.1. Realizacja funkcji identyfikacji i uwierzytelniania

Funkcje identyfikacji i uwierzytelniania wszystkich wymaganych danych subskrybenta są realizowane przez Główny Punkt Rejestracji oraz współpracujące Punkty Rejestracji zgodnie z warunkami określonymi w rozdz. 1.3.2.

4.2.2. Przyjęcie lub odrzucenie wniosku

4.2.2.1. Procedura przyjęcia wniosku w Punkcie Rejestracji

Każdy wniosek, który został skierowany do urzędu certyfikacji lub złożony w Punkcie Rejestracji przetwarzany jest następująco:

- operator pobiera wniosek subskrybenta (papierowy lub elektroniczny),
- operator sprawdza, czy subskrybent wniósł opłatę za rozpatrzenie wniosku o wydanie certyfikatu, o ile taka opłata jest przewidziana w cenniku CERTUM; w przypadku braku takiej opłaty, wniosek jest odrzucany,
- operator weryfikuje zawarte w nim dane, m.in. dane osobowe subskrybenta (patrz procedura identyfikacji i uwierzytelnienia subskrybenta opisana w rozdz. 3.2.2, 3.2.3),dla certyfikatów wydanych do dnia 28 lutego 2018 CERTUM może korzystać, w

celu weryfikacji wniosku certyfikacyjnego, z informacji i dokumentów wymaganych zgodnie z rozdz. 3.2, które zostały pozyskane przez CERTUM nie dalej jak 39 miesięcy przed wydaniem certyfikatu,

- dla certyfikatów uwierzytelnienia witryn internetowych (z wyjątkiem certyfikatów Premium EV SSL) wydawanych od dnia 1 marca 2018 CERTUM może korzystać, w celu weryfikacji wniosku certyfikacyjnego, z informacji i dokumentów wymaganych zgodnie z rozdz. 3.2, które zostały pozyskane przez CERTUM nie dalej jak 825 dni przed wydaniem certyfikatu,
- dla certyfikatów Premium EV SSL CERTUM może korzystać, w celu weryfikacji wniosku certyfikacyjnego, z informacji i dokumentów wymaganych zgodnie z rozdz. 3.2, które zostały pozyskane przez CERTUM nie dalej jak 13 miesięcy przed wydaniem certyfikatu,
- jeśli weryfikacja wniosku przebiegnie pozytywnie, to operator poświadcza żądanie; jeśli oryginalny wniosek zawiera błędne dane, to wniosek jest odrzucany lub poddawany jest korekcie,
- na podstawie poświadczonego wniosku wydawany jest certyfikat,
- 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.

4.2.2.2. 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),
- wniosek certyfikacyjny zawiera nazwę domenową z rodzaju nowych domen funkcjonalnych (ang. new gTLDs), jeśli nie jest ona dodana do aktualnej listy publicznych sufiksów DNS (ang. Public Suffix List),
- 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,
- subskrybent nie wniósł opłaty za wydanie certyfikatu, o ile taka opłata jest przewidziana w cenniku CERTUM,
- z innych nie wymienionych powyżej przyczyn.

Subskrybenci, których wnioski o wydanie certyfikatu zostały odrzucony, mogą ponownie starać się o wydanie certyfikatu składając nowy wniosek.

4.2.3. Okres oczekiwania na przetworzenie wniosku

CERTUM dokłada wszelkich starań, aby od momentu otrzymania wniosku certyfikacyjnego, wniosku o modyfikację certyfikatu lub wniosku o aktualizację lub recertyfikację kluczy przeprowadzić jego weryfikację oraz wydać certyfikat w czasie nie dłuższym niż 7 dni.

Czas oczekiwania zależy głównie od typu certyfikatu, kompletności dostarczonego wniosku, ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy CERTUM a wnioskodawcą lub wynikają z warunków umowy zawartej z subskrybentem.

4.2.4. Przetwarzanie rekordów autoryzujących urzędy certyfikacji

Podczas wydawania certyfikatów CERTUM sprawdza rekordy DNS autoryzujące urzędy certyfikacji (ang. Certification Authority Authorization (CAA)). CERTUM akceptuje następujące nazwy w rekordach CAA:

- `certum.pl`
- `certum.eu`
- `yandex.ru`

Rekord CAA o nazwie `certum.pl` wskazujący na CERTUM jako urząd certyfikacji upoważniony do wydania certyfikatu przyjmuje postać:

- dla standardowych certyfikatów SSL:

```
nazwa domeny IN CAA 0 issue "certum.pl"
```

- dla certyfikatów wildcard:

```
nazwa domeny  IN CAA 0 issuewild "certum.pl"
```

4.3. Wydanie certyfikatu

4.3.1. Czynności urzędu certyfikacji wykonywane podczas wydawania certyfikatu

Urząd certyfikacji, po otrzymaniu odpowiedniego wniosku oraz po pomyślnym przetworzeniu go (patrz rozdz. 4.2) wydaje certyfikat.

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

- każdy wniosek certyfikacyjny jest rejestrowany oraz weryfikowany w Głównym Punkcie Rejestracji,
- dostęp do kont operatorskich Głównego Punktu Rejestracji posiadają wyłącznie osoby pełniące zaufane role. Korzystanie z kont zabezpieczone jest wielopoziomowym uwierzytelnieniem i umożliwia przetwarzanie wniosków certyfikacyjnych włącznie z możliwością skierowania ich do serwera urzędu certyfikacji,
- przetworzone przez Główny Punkt Rejestracji wnioski subskrybenta przesyłane są na serwer wystawiania certyfikatów,
- 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 140-2 Level 3,
- 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 udostępnia go subskrybentowi.

4.3.2. Informowanie subskrybenta o wydaniu certyfikatu

Urząd certyfikacji CERTUM stosuje dwa podstawowe mechanizmy informowania subskrybenta o wydaniu 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).

4.4. Akceptacja certyfikatu

4.4.1. Potwierdzenie akceptacji 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). Jeśli w ciągu 7 dniu od daty otrzymania certyfikatu subskrybent nie poinformuje CERTUM, że nie akceptuje certyfikatu lub jeśli w tym okresie nie unieważni go, wówczas taki certyfikat uważa się za ważny.

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 Asseco Data Systems 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. 4.9.9).

4.4.2. Publikowanie certyfikatu przez urząd certyfikacji

Każdy wydany i zaakceptowany certyfikat publikowany jest w repozytorium CERTUM.

4.4.3. Informowanie o wydaniu certyfikatu innych podmiotów

O wydaniu certyfikatu CETUM może informować Punkt Rejestracji, który potwierdził dane zawarte we wniosku subskrybenta, a także informować zamawiającego, jeśli certyfikat został wydany w oparciu o zawartą z nim umowę.

4.5. Stosowanie kluczy oraz certyfikatów

4.5.1. Stosowanie kluczy i certyfikatu przez subskrybenta

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 Asseco Data Systems S.A.,
- tylko w okresie ich ważności (nie dotyczy to certyfikatów do weryfikacji podpisów cyfrowych),
- tylko do momentu unieważnienia certyfikatu.

4.5.2. Stosowanie kluczy i certyfikatu przez stronę ufającą

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 w ramach tego samego konta użytkownika.

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 stosowana 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, nowa data początku ważności certyfikatu oraz nowy podpis urzędu certyfikacji; aktualizacja kluczy może również nosić nazwę odnowienia certyfikatu.

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

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

4.7.1. Okoliczności certyfikacji i aktualizacji kluczy

Aktualizacja kluczy 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.

4.7.2. Kto może żądać certyfikacji nowej pary kluczy

Certyfikacja lub aktualizacja kluczy odbywa się tylko na żądanie subskrybenta lub uprawnionego przedstawiciela zamawiającego (osoby prawnej lub jednostki organizacyjnej nie posiadającej osobowości prawnej) i musi być poprzedzona złożeniem odpowiedniego wniosku.

4.7.3. Przetwarzanie wniosku o certyfikację i aktualizacje kluczy

Uwierzytelnienie wniosków o aktualizację kluczy i certyfikację realizowane jest w zgodnie z zasadami opisanymi na stronach www.certum.pl .

Procedura przetwarzania wniosku o aktualizację certyfikatu i certyfikację jest zgodna z procedurami opisanymi w rozdz. 4.2 i 4.3.

4.7.4. Informowanie o wydaniu nowego certyfikatu

Patrz także rozdz. 4.3.2.

4.7.5. Potwierdzenie akceptacji nowego certyfikatu

Patrz także rozdz. 4.4.1.

4.7.6. Publikowanie nowego certyfikatu

Patrz także rozdz. 4.4.2

4.7.7. Informowanie o wydaniu certyfikatu innych podmiotów

Patrz także rozdz. 4.4.3

4.8. Modyfikacja certyfikatu

4.8.1. Okoliczności modyfikacji 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 inne niż klucz publiczny.

CERTUM traktuje modyfikację certyfikatu w taki sam sposób jak wydanie nowego certyfikatu

CERTUM może zmodyfikować certyfikat, który został odnowiony, lub którego klucze zostały wcześniej zaktualizowane. Oryginalny certyfikat może zostać unieważniony po zakończeniu procesu modyfikacji certyfikatu.

4.8.2. Kto może żądać modyfikacji certyfikatu?

Szczegóły, patrz rozdz. 4.1.1.

4.8.3. Przetwarzanie wniosku o modyfikację certyfikatu

Szczegóły, patrz rozdz. 4.2.

4.8.4. Informowanie o wydaniu zmodyfikowanego certyfikatu

Patrz rozdz. 4.3.2.

4.8.5. Potwierdzenie akceptacji zmodyfikowanego certyfikatu

Patrz rozdz. 4.4.1.

4.8.6. Publikowanie zmodyfikowanego certyfikatu

Patrz rozdz. 4.4.2.

4.8.7. Informowanie o wydaniu certyfikatu innych podmiotów

Patrz także rozdz. 4.4.3.

4.9. Unieważnienie i zawieszenie certyfikatu

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

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

Unieważnienie 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 certyfikatu.

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, 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.

CERTUM unieważnia certyfikat subskrybenta w następujących okolicznościach:

- gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się,
- gdy subskrybent powiadomi CERTUM, że wniosek certyfikacyjny, na podstawie którego wydano certyfikat, nie został autoryzowany przez podmiot certyfikatu,
- gdy technologie zabezpieczeń kryptograficznych zdezaktualizują się, co może uczynić certyfikat subskrybenta podatnym na zagrożenia (np. zawartość lub format certyfikatu przedstawia ryzyko nieakceptowane przez strony ufające lub dostawców oprogramowania),
- gdy CERTUM otrzyma dowody na nieuprawnione lub niedozwolone użycie certyfikatu,
- gdy CERTUM otrzyma dowody na to, że używanie przez subskrybenta nazwy domenowej lub adresu IP nie jest legalne,
- ilekroć klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub nośnik na którym jest przechowywany jest lub istnieje uzasadnione podejrzenie, że będzie ujawniony[17]
- subskrybent rezygnuje z umowy zawartej z Asseco Data Systems 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, w tym także podmiotu świadczącego usługi certyfikacyjne oraz Punktu Rejestracji,
- .wskutek nieprzestrzegania przez subskrybenta zaakceptowanej Polityki Certyfikacji oraz Kodeksu Postępowania Certyfikacyjnego lub postanowień innych dokumentów, przywołanych w niniejszym dokumencie, których wymagań subskrybent certyfikatu zobowiązuje się przestrzegać,[18]

---

[17] 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.

[18] Przede wszystkim wymagania:

- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,
- Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates,
- Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates oraz
- Guidelines For The Issuance And Management Of Extended Validation Certificates

- 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 opóźniające 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.

Powyższe okoliczności mogą decydować także o unieważnieniu certyfikatu EV SSL.

Certyfikat urzędu certyfikacji może zostać unieważniony 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.

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 lub innych danych uwierzytelniających). 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. 3.2.2 lub 3.2.3.

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); dotyczy to w szczególności przypadku unieważniania certyfikatu urzędu certyfikacji, wystawionego przez urząd, który reprezentuje ten autoryzowany przedstawiciel,
- zamawiający[19], np. pracodawca subskrybenta; subskrybent musi być o tym fakcie niezwłocznie poinformowany,

19 Patrz **Słownik pojęć**

- operator Punktu Rejestracji, który może wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli jest w posiadaniu informacji, uzasadniającej unieważnienie certyfikatu.
- każda strona ufająca, dostawca oprogramowania lub jakakolwiek strona trzecia jest uprawniona do poinformowania CERTUM o możliwej potrzebie unieważnienia 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:

- 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

4.9.3.1. Procedura unieważniania certyfikatu użytkownika końcowego

Unieważnienie certyfikatu można realizować na trzy sposoby:

- pierwszy sposób polega na przesłaniu do urzędu certyfikacji elektronicznego wniosku o unieważnienie autoryzowanego przy pomocy hasła; unieważnienia tego typu subskrybent wykonuje samodzielnie,
- drugi sposób wymaga przesłania do urzędu certyfikacji elektronicznego wniosku o unieważnienie, potwierdzonego przy pomocy podpisu cyfrowego przez subskrybenta lub Punkt Rejestracji; dotyczy to przypadków, gdy (a) subskrybent utracił jednocześnie klucz prywatny oraz hasło, (b) unieważnienia zażądał zamawiający certyfikat, autoryzowany przedstawiciel urzędu certyfikacji lub Punktu Rejestracji, jeśli tylko istnieją podstawy do zażądania unieważnienia certyfikatu subskrybenta,
- trzeci sposób polega na tym, żezgłoszenia może dokonać każda zainteresowana strona wysyłając tradycyjnym listem poleconym pismo z wnioskiem o unieważnienie, podpisane przez subskrybenta lub osobę upoważnioną lub wysyłając żądanie elektroniczne – za pośrednictwem formularza dostępnego na stronie internetowej certum.pl w zakładce Wsparcie Techniczne. .

We wszystkich przypadkach urząd certyfikacji – po pozytywnej weryfikacji wniosku – unieważnia certyfikat. Informacja o unieważnionym certyfikacie umieszczana jest na liście CRL (patrz rozdz. 0), 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 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 certyfikacie na liście certyfikatów unieważnionych (CRL) wraz z informacją o przyczynie unieważnienia (patrz rozdz. 7.2.2);
- 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 zamawiającego certyfikat 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.

4.9.3.2. Procedura unieważniania certyfikatu urzędu certyfikacji lub Punktu Rejestracji

Podmiot świadczący usługi certyfikacyjne (w tym przede wszystkim urząd certyfikacji) lub Punkt Rejestracji żądający unieważnienia swojego certyfikatu zobowiązany jest przekazać taki wniosek bezpośrednio do CERTUM. Każde uprawnione żądanie unieważnienia jest realizowane przez CERTUM bez zbędnej zwłoki.

O unieważnienie certyfikatu podmiotu świadczącego usługi certyfikacyjne lub Punkt Rejestracji może występować także CERTUM (patrz rozdz. 4.9.2).

4.9.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

CERTUM gwarantuje maksymalny 24-godzinny okresy zwłoki[20] 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.

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. Dla polityk certyfikacji Certum Level I CA, Certum Class 1 CA oraz Certum Class 1 CA SHA2 CERTUM nie ma obowiązku unieważnienia certyfikatu.

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. 4.9.8).

W momencie unieważnienia certyfikatu automatycznie o tym fakcie są informowani operatorzy Punktów Rejestracji oraz zainteresowani subskrybenci.

4.9.5. Maksymalny dopuszczalny czas przetwarzania wniosku o unieważnienie

Wniosek o unieważnienie certyfikatu przetwarzany jest przez CERTUM bez zbędnej zwłoki.

4.9.6. Obowiązek sprawdzania unieważnień przez stronę ufającą

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. 4.9.10).

Adresy URL Punktów dystrybucji list CRL dostępne są w publicznym repozytorium pod adresem http://www.certum.pl.

4.9.7. Częstotliwość publikowania list CRL

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

---

20 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).

Wszystkie listy uaktualniane są nie rzadziej niż raz w tygodniu[21], jeśli w tym czasie nie został unieważniony żaden nowy certyfikat. Nowa lista CRL publikowana jest jednak w repozytorium po każdym unieważnieniu certyfikatu.

Listy CRL urzędów głównych **Certum CA**, **Certum Trusted Network CA, Certum Trusted Network CA 2 oraz Certum Trusted Network CA EC** publikowane są nie rzadziej niż raz na rok, chyba, że w tym czasie nastąpi odwołanie certyfikatu jednego z urzędów afiliowanych przy jednym z urzędów głównych.

4.9.8. Maksymalne opóźnienie w publikowaniu CRL

Każda lista CRL jest publikowana bez zbędnej zwłoki natychmiast po jej utworzeniu (zwykle odbywa się to automatycznie w ciągu paru minut).

4.9.9. 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 RFC6960. Protokół OCSP umożliwia uzyskiwanie informacji o statusie certyfikatu bez potrzeby pobierania oraz sprawdzania całej listy 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 (**good**) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny[22],
- unieważniony (**revoked**) – oznacza, że certyfikat został unieważniony,
- nieznany (**unknown**) – oznacza, że weryfikowany certyfikat nie został wydany przez jeden z urzędów afiliowanych przy Certum CA lub Certum Trusted Network CA.

Serwis OCSP generuje odpowiedź bazując na bazie danych. Ważność odpowiedzi OCSP wynosi 7 dni. W celu zachowania odpowiedniej wydajności systemu odpowiedzi OCSP są cachowane przez ustalony czas (najczęściej nie większy niż kilka godzin). Aby wymusić aktualną odpowiedź OCSP należy użyć przełącznika *-nonce* w zapytaniu kierowanym do serwera OCSP.

4.9.10. Obowiązek sprawdzania unieważnień w trybie on-line

Strony ufające muszą sprawdzać informacje dotyczące statusu certyfikatu, któremu ufają. W przeciwnym razie wszystkie gwarancje udzielane przez CERTUM staja się nieważne.

W przypadku certyfikatów subskrybentów CERTUM aktualizuje informacje dostarczane za pośrednictwem protokołu OCSP co kilka minut. Maksymalny okres ważności odpowiedzi OCSP wynosi 7 dni.

W przypadku certyfikatów urzędów pośrednich CERTUM aktualizuje informacje dostarczane za pośrednictwem protokołu OCSP przynajmniej raz w roku oraz maksymalnie do 24 godzin po unieważnieniu certyfikatu pośredniego.

---

21 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 urzędów wydających certyfikaty końcowe standardowa wartość tego pola (zapowiedź publikacji) wynosi 10 dni. .

22 Patrz **Słownik pojęć**.

4.9.11. Inne dostępne formy ogłaszania unieważnień certyfikatów

Nie dotyczy.

4.9.12. Specjalne obowiązki w przypadku naruszenia ochrony klucza

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.

CERTUM stosuje wszelkie dostępne środki w celu niezwłocznego poinformowania o tym fakcie stron ufających, odwołujących się do informacji zgromadzonej w repozytorium zarządzanego przez CERTUM.

4.9.13. Okoliczności zawieszenia certyfikatu

CERTUM nie świadczy usługi zawieszenia certyfikatu.

4.9.14. Kto może żądać zawieszenia certyfikatu

Nie dotyczy

4.9.15. Procedura zawieszenia i odwieszania certyfikatu

Nie dotyczy.

4.9.16. Ograniczenia okresu/zwłoki zawieszenia certyfikatu

Nie dotyczy.

4.10. Usługi weryfikacji statusu certyfikatu

4.10.1. Charakterystyki operacyjne

Informację o statusie certyfikatów wydanych przez CERTUM można uzyskać w oparciu listy CRL publikowane na stronie internetowej CERTUM oraz za pośrednictwem usługi OCSP.

Numer seryjny unieważnionego certyfikatu pozostaje na liście CRL do końca okresu ważności unieważnionego certyfikatu.

4.10.2. Dostępność usługi

Usługi weryfikacji statusu certyfikatu są dostępne w reżimie 24/7 (bez żadnych planowanych przerw eksploatacyjnych).

4.10.3. Cechy opcjonalne

Usługa weryfikacji statusu certyfikatów w trybie on-line (OCSP) nie jest udostępniana dla wszystkich typów certyfikatów oraz wszystkich stron ufających.

Adres URL usługi OCSP jest zwykle umieszczany w certyfikatach wydawanych subskrybentom. W takim przypadku oznacza to, że usługa OCSP jest dostępna dla tego certyfikatu.

Usługa OCSP jest obligatoryjnie świadczona dla wszystkich certyfikatów sub-CA (patrz rozdz. 0), SSL oraz EV SSL wydanych przez CERTUM.

4.11. Zakończenie subskrypcji

O zakończeniu z korzystania z usług certyfikacyjnych przez subskrybenta należy mówić w następujących przypadkach, gdy:

- minął okres ważności certyfikatu subskrybenta, zaś subskrybent nie podjął działań mających na celu aktualizację jego klucza, recertyfikację lub modyfikację,
- unieważniono certyfikat subskrybenta i nie został on zastąpiony przez inny certyfikat,

4.12. Deponowanie i odtwarzanie klucza

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).

5. Zabezpieczenia techniczne, organizacyjne i operacyjne

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

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.

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.

5.1.1. Miejsce lokalizacji oraz budynki

Centrum Certyfikacji CERTUM mieści się w budynkach Asseco Data Systems S.A., znajdujących się w Szczecinie przy ul. Bajecznej 13 oraz przy ul. Królowej Korony Polskiej 21. Lokalizacja Punktów Rejestracji dostępna jest w repozytorium i za pośrednictwem poczty elektronicznej: info@certum.pl.

5.1.2. Dostęp fizyczny

Fizyczny dostęp do budynków oraz pomieszczeń CERTUM jest kontrolowany oraz nadzorowany przez zintegrowany system alarmowy. Ochrona fizyczna budynków funkcjonuje 24 godziny na dobę. 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 Asseco Data Systems S.A. 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 osoby zarządzającej PCC CERTUM.

Dostęp do pomieszczenia operatorsko-administracyjnego chroniony jest za pomocą kart mikroprocesorowych oraz systemu kontroli dostępu. W pomieszczeniu mogą przebywać jedynie pracownicy CERTUM oraz inne uprawnione osoby, przy czym osoby te nie mogą w pomieszczeniu przebywać samodzielnie. Jedyne odstępstwo od tej zasady dotyczy pracowników, którzy pełnią w CERTUM rolę sklasyfikowaną jako zaufana.

Dostęp do Głównego Punktu Rejestracji jest zgodny z wymogami określonymi na początku tego rozdziału. W przypadku pozostałych typów Punktów Rejestracji nie narzuca się 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.

5.1.3. 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.

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

5.1.4. Zagrożenie powodziowe

W pomieszczeniu systemu komputerowego zainstalowane są czujniki wilgotności oraz wykrywające obecność wody. Czujniki te sprzęgnięte są z systemem ochrony budynków przy ul. Królowej Korony Polskiej 21 oraz Bajecznej 13 w Szczecinie. O zagrożeniach informowana jest obsługa portierska, która w zależności od sytuacji zawiadamia odpowiednie służby miejskie, inspektora bezpieczeństwa oraz jednego z administratorów systemu.

5.1.5. Ochrona przeciwpożarowa

System ochrony przeciwpożarowej zainstalowany w budynkach firmy przy ul. Królowej Korony Polskiej 21 oraz Bajecznej 13 w Szczecinie 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.

5.1.6. Nośniki informacji

W Centrum Certyfikacji, 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.

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

5.1.7. Niszczenie zbędnych nośników i informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo CERTUM po upływie okresu przechowywania (patrz rozdz. 6.2.5) 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). Sprzętowe urządzenia kryptograficzne (moduły) są zerowane zgodnie z dokumentacją producenta. Zerowanie urządzeń ma miejsce również w momencie oddawania modułu do serwisu.

5.1.8. 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 krytycznych danych systemowych, dzienniki zdarzeń na potrzeby audytu, wrażliwe informacje przetworzone 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).

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.

5.2. 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

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

- osoba zarządzająca PCC CERTUM – odpowiada za prawidłowe funkcjonowanie CERTUM, określa kierunki rozwoju CERTUM, wdraża oraz zarządza Polityką Certyfikacji, a także Kodeksem Postępowania Certyfikacyjnego
- 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,
- 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.

5.2.1.1. 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.

5.2.2. Liczba osób wymaganych podczas realizacji zadania

Operacją, którą wymaga zachowania szczególnej ostrożności jest proces generowania i odtwarzania 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,**
- **obserwatorzy – (opcjonalnie) np. przedstawiciele audytora.**

5.2.3. Identyfikacja oraz uwierzytelnianie każdej roli

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.

5.2.4. Role, które nie mogą być łączone

Przedstawiony w rozdz. 5.2.1 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 zaufania. 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.

5.3. Nadzorowanie personelu

Personel CERTUM zatrudniany na stanowiska związane z pełnieniem zaufanych ról musi posiadać udokumentowane przygotowanie oraz doświadczenie, które daje gwarancje kompetentnego i odpowiedniego wypełniana swoich przyszłych obowiązków. W przypadkach, gdy jest to wymagane, to osoba zatrudniana do obsługi świadczeń certyfikacyjnych na rzecz instytucji rządowych powinna posiadać certyfikat bezpieczeństwa wydany przez administratora bezpieczeństwa Asseco Data Systems S.A lub Agencję Bezpieczeństwa Wewnętrznego.

Kontrola przygotowania zawodowego każdej osoby pełniącej dowolna z zaufanych ról w CERTUM jest powtarzane przynajmniej raz na 5 lat.

5.3.1. Kwalifikacje, doświadczenie oraz upoważnienia

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.

5.3.2. Procedura weryfikacji przygotowania

Kontrola przygotowania do pracy na danym stanowisku wiążącym się z pełnieniem zaufanej roli przeprowadzana jest w stosunku do każdego nowego pracownika, przed

dopuszczeniem go do wykonywania obowiązków i poprzedzona jest stosownym szkoleniem. Kontrola przygotowania obejmuje:

- potwierdzenie przebiegu poprzedniego zatrudnienia,
- sprawdzenie referencji i uprawnień zawodowych,
- potwierdzenie poziomu wykształcenia odpowiedniego do pełnienia zaufanej roli,
- sprawdzenie informacji o niekaralności,
- sprawdzenie informacji w Krajowym Rejestrze Dłużników,
- sprawdzenie numeru PESEL.

W przypadku braku dostępności niektórych informacji (np. ze względu na obowiązujące prawo), CERTUM może stosować inne – dozwolone prawem – techniki, które pozwolą na uzyskanie informacji podobnych do wyżej wymienionych.

CERTUM może odrzucić kandydaturę na stanowisko związane z pełnieniem zaufanej roli lub podjąć działania przeciwko osobie już zatrudnionej na takim stanowisku w przypadku stwierdzenia m.in. następujących faktów:

- wprowadzenie w błąd przez kandydata do pełnienia zaufanej roli lub osobę pełniącą już taka rolę,
- wysoce niekorzystne lub mało wiarygodne referencje i uprawnienia zawodowe,
- kryminalnej przeszłości kandydata lub osoby już zatrudnionej potwierdzonej prawomocnym wyrokiem,
- braku wiarygodności finansowej.

W przypadku stwierdzenia któregokolwiek z powyższych faktów, dalsze czynności prowadzone są zgodnie z procedurami bezpieczeństwa Asseco Data Systems S.A oraz obowiązującym prawem.

5.3.3. 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.

5.3.4. Częstotliwość powtarzania szkoleń oraz wymagania

Szkolenia wymienione w rozdz. 5.3.3 muszą być powtarzane lub uzupełniane zawsze wtedy, gdy nastąpiły istotne zmiany w funkcjonowaniu CERTUM lub Punktów Rejestracji.

5.3.5. Częstotliwość rotacji stanowisk i jej kolejność

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

5.3.6. 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.

5.3.7. Pracownicy kontraktowi

Pracownicy kontraktowi lub konsultanci mogą pełnić zaufane role, wymienione w rozdz. 5.2.1. W takich przypadkach podlegają oni tym samym wymaganiom stosowanym wobec pracowników CERTUM zatrudnionych na porównywalnych stanowiskach.

Pracownik kontraktowy lub konsultant, który nie dostarczył kompletu wymaganych informacji o przygotowaniu do pełnienie jednej za zaufanych ról lub nie przeszedł pomyślnie kontroli przygotowania (patrz rozdz. 5.3.2) musi zawsze podczas przebywania na terenie CERTUM lub Punktu Rejestracji znajdować się cały czas w towarzystwie pracownika urzędu certyfikacji lub Punktu Rejestracji, pełniącego zaufaną rolę w CERTUM lub w punkcie Rejestracji.

5.3.8. Dokumentacja przekazana personelowi

Kierownictwo CERTUM, jak również kierownik Punktu Rejestracji muszą umożliwić swojemu personelowi dostęp do następujących dokumentów:

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

5.4. Procedury rejestrowania zdarzeń oraz 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.

5.4.1. 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.

Szczegółowa lista rejestrowanych zdarzeń zależna jest od polityki certyfikacji certyfikatów wystawianych lub potwierdzanych przez określony urząd certyfikacji lub Punkt Rejestracji zawsze jednak obejmuje następujące zdarzenia:

- Zdarzenia związane z cyklem życia kluczy kryptograficznych urzędów certyfikacji CERTUM:
  - generowanie, odtwarzanie, kopiowanie, archiwizowanie oraz niszczenie kluczy,
  - zdarzenia związane z cyklem życia urządzeń kryptograficznych.
- Zdarzenia związane z cyklem życia kluczy kryptograficznych subskrybentów
  - wnioski certyfikacyjne oraz wnioski o unieważnienie certyfikatu,
  - wszystkie czynności wykonywane w ramach weryfikacji wniosku certyfikacyjnego,
  - data, czas, numer telefonu oraz dane osoby, z którą CERTUM kontaktuje się w celu prowadzenia weryfikacji wniosku certyfikacyjnego,
  - akceptacja lub odrzucenie wniosku certyfikacyjnego,
  - wydanie certyfikatu,
  - generowanie list CRL oraz odpowiedzi OCSP.
- Zdarzenia bezpieczeństwa:

- udane oraz nieudane próby dostępu do systemów CERTUM,
- wszelkie działania podejmowane w związku z bezpieczeństwem systemów CERTUM,
- zmiany profili bezpieczeństwa
- awarie systemu, sprzętu oraz pozostałe anomalie,
- działanie zapór (firewall) oraz urządzeń sieciowych,
- wejścia i wyjścia z obiektów i pomieszczeń CERTUM

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).

5.4.2. Częstotliwość przetwarzania zapisów rejestrowanych zdarzeń (logów)

Zapisy zarejestrowanych zdarzeń powinny być przeglądane szczegółowo przynajmniej raz w miesiącu. Wszystkie zauważone istotne zdarzenia muszą być wyjaśnione i opisane w 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.

5.4.3. Okres przechowywania zapisów rejestrowanych zdarzeń

Rejestry zdarzeń utrzymywane są przez okres min. 7 lat.

5.4.4. Ochrona zapisów zdarzeń na potrzeby audytu

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. 5.4.3).

5.4.5. Procedury tworzenia kopii zapisów zdarzeń na potrzeby audytu

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.

5.4.6. System gromadzenia danych na potrzeby audytu (wewnętrzny a zewnętrzny)

Aplikacje, komponenty i oprogramowanie sieciowe oraz systemy operacyjne wykorzystywane w systemach CERTUM generują w sposób automatyczny informacje o zdarzeniach na potrzeby audytu. Informacje o tego typu zdarzeniach są także wprowadzane ręcznie przez personel CERTUM.

5.4.7. 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.

W przypadku zarejestrowania zdarzenia przez system gromadzenia zdarzeń na potrzeby audytu nie jest wymagane poinformowanie o tym fakcie osoby fizycznej, organizacji lub aplikacji, która to zdarzenie spowodowała. O zdarzeniach tego typu, mające 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.

5.4.8. Oszacowanie podatności na zagrożenia

Niniejszy Kodeks Postępowania Certyfikacyjnego wymaga przeprowadzenia przez urząd wydający certyfikaty (także urzędy podległe **Certum Global Services CA** oraz **Certum Global Services CA SHA2**), związany z nim Główny Punkt Rejestracji oraz pozostałe 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.

CERTUM prowadzi ewidencję oraz klasyfikuje wszystkie posiadane aktywa zgodnie z normą PN-ISO/IEC 27001:2014. Niniejszy Kodeks Postępowania Certyfikacyjnego wymaga przeprowadzenia przez CERTUM analizy podatności na zagrożenia wszystkich posiadanych aktywów, w tym w szczególności oprogramowania oraz systemu komputerowego. Wymogi te mogą być także określone przez zewnętrzną instytucję, uprawnioną do przeprowadzania audytu w CERTUM.

Analiza ryzyka dla CERTUM prowadzona jest przynajmniej raz w roku lub przy wprowadzaniu nowych usług, dużych zmian w systemach CERTUM lub w wyniku incydentu bezpieczeństwa.

Aktywa CERTUM oraz Polityka Bezpieczeństwa Informacji, która jest elementem wdrożonego w Asseco Data Systems S.A. Zintegrowanego Systemu Zarządzania podlega corocznym przeglądom i akceptacji Dyrektora CERTUM.

Zgodnie z procedurą zarządzania ryzykiem każda z analiz ryzyka rozpoczyna się określeniem i weryfikacją listy aktywów.

Lista aktywów wysyłana jest do weryfikacji do zespołu prowadzącego analizę. Zweryfikowane listy przesyłane są do menadżera analizy, który konsoliduje otrzymane informacji i tworzy aktualną listę aktywów.

Proces szacowania ryzyka przeprowadzony jest:

- Jeśli powstanie nowa grupa informacji,
- Jeśli pojawią się nowe aktywa,
- Jeśli pojawi się nowe zagrożenie/ryzyko,
- Jeśli rozpocznie się nowy cykl analizy, czyli najpóźniej w 11 miesięcy po zakończeniu poprzedniej analizy.

Ryzyka o poziomie niskim akceptowane są przez Dyrektora CERTUM. Dla stwierdzonych zagrożeń powyżej akceptowalnego poziomu, tworzone są plany postępowania z ryzykiem, które także wymagają akceptacji dyrektora CERTUM.

5.5. Zapisy archiwalne

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 on-line może zastępować archiwum off-line.

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.

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

5.5.1. 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 lub papierową, które nadeszły od subskrybenta lub zostały mu przekazane w formie dokumentu papierowego, 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,
- dokumenty i dane użyte w procesie uwierzytelnianie tożsamości.

5.5.2. Okres przechowywania danych w archiwum

CERTUM przechowuje pełną dokumentację (w formie elektronicznej i papierowej) dotyczącą złożonych wniosków certyfikacyjnych oraz wydanych i unieważnionych certyfikatów przez okres przynajmniej siedmiu lat od czasu gdy certyfikat, którego dane dotyczą, utracił ważność.

Po upływie przyjętego okresu archiwizacji dane mogą być zniszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany jest ze szczególną starannością.

5.5.3. Ochrona archiwum

Dostęp do archiwum mają tylko uprawnione osoby pełniące zaufane role w CERTUM. Archiwum jest przechowywane w systemie, który spełnia wymagania określone w CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements*. System ten zapewnia ochronę archiwum przed nieuprawnionym przeglądaniem, modyfikowaniem, usuwaniem lub manipulowaniem. Nośniki, na których przechowywane są archiwa oraz aplikacje do przetwarzania archiwów muszą być utrzymywane w takim stanie, aby zapewnić deklarowany okres dostępu do archiwów (rozdz. 5.5.2).

5.5.4. 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.

5.5.5. 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**.

5.5.6. System gromadzenia danych archiwalnych (wewnętrzny a zewnętrzny)

System gromadzenia archiwów jest wewnętrznym systemem CERTUM. Wyjątkiem od tej zasady są zewnętrzne archiwa prowadzone przez zewnętrzne Punkty Rejestracji świadczące usługi na rzecz CERTUM. Dane w zewnętrznych archiwach muszą być przechowywane przede wszystkim na potrzeby audytów przeprowadzanych przez CERTUM lub wskazane przez CERTUM jednostki audytujące.

5.5.7. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

Dostęp do archiwum mają jedynie osoby pełniące zaufane role w CERTUM i jest możliwy dopiero po pomyślnie zakończonej autoryzacji (tj. uwierzytelnieniu osoby oraz potwierdzeniu jej praw dostępu).

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. Weryfikowanie integralności danych archiwalnych odbywa się także zawsze podczas ich odtwarzania w systemie.

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

5.6. 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 4210, a także rozdz. 6.1.1.1).

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 główne

urzędy certyfikacji 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. 6.1.

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

5.7. 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).

5.7.1. Procedury obsługi incydentów i reagowania na zagrożenia

Sposób obsługi incydentów i reagowania na zagrożenia regulują procedury objęte Planem Ciągłości Działania CERTUM. Przynajmniej raz w roku CERTUM testuje skuteczność procedur objętych Planem Ciągłości Działania (ang. Bussiness Continuity Plan).

Plan Ciągłości Działania CERTUM zawiera:

- Przyczyny uruchomienia planu.
- Procedury reagowania w sytuacjach awaryjnych.
- Plany awaryjne.
- Procedury przywracania procesów CERTUM.
- Harmonogram utrzymania Planu.
- Wymagania wobec pracowników CERTUM dotyczące ich świadomości i umiejętności realizowania Planu.
- Dopuszczalny czas odtworzenia krytycznych procesów CERTUM (ang. RTO - recovery time objective)
- Plan utrzymania lub terminowego odtworzenia działalności biznesowej CERTUM.
- Wymagania dotyczące przechowywania w ośrodku zapasowym tzw. materiału kryptograficznego (np. bezpieczne urządzenia kryptograficzne, karty kryptograficzne zawierające współdzielone klucze urzędów certyfikacji)
- Warunki, dla których można określić akceptowalny okres przerwy w działaniu oraz okres niezbędny do odtworzenia danego systemu CERTUM.
- Częstotliwość wykonywania kopii zapasowych kluczowych aplikacji oraz informacji biznesowych.
- Odległość między ośrodkami przetwarzania CERTUM (głównym i zapasowym).
- Procedury zabezpieczania aktywów CERTUM w okresie pomiędzy następującą katastrofą i przed przywróceniem bezpieczeństwa.

5.7.2. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

Wszystkie informacje o przypadkach uszkodzenia zasobów obliczeniowych, oprogramowania lub danych przekazywane są inspektorowi bezpieczeństwa, który zleca podjęcie działań zgodnie z opracowanymi procedurami. Procedury te mają na celu analizę natężenia ataku, zbadanie incydentu, zminimalizowanie jego skutków oraz wyeliminowanie go w przyszłości. O ile jest to konieczne podjęte muszą być czynności przewidziane na przypadek ujawnienia klucza urzędu CERTUM lub uruchomienie procedur związanych z planem odtwarzania systemu po katastrofie.

5.7.3. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych podmiotu działającego w ramach CERTUM

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.

Powyższe czynności realizowane są zgodnie z planem opracowanym przez zespół ds. zapobiegania incydentom, w skład którego wchodzi osoba zarządzająca PCC CERTUM, inspektor bezpieczeństwa, administratorzy bezpieczeństwa oraz inni niezbędni pracownicy CERTUM, wskazani przez osobę zarządzającą PCC CERTUM. Opracowany plan musi zostać zatwierdzony przez członka Zarządu Asseco Data Systems S.A.

5.7.4. Zapewnienie ciągłości działania po katastrofach

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. 5.5.4 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. 5.5.4 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. 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.

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.

5.8. Zakończenie działalności urzędu certyfikacji lub Punktu Rejestracji

Przedstawione poniżej obowiązki urzędu certyfikacji lub Punktu Rejestracji mają na uwadze redukcję skutków podjęcia przez ten urząd lub Punkt 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.

5.8.1. 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 oraz Punktów Rejestracji 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 zamawiającemu) kosztów wydanego certyfikatu, proporcjonalnie do pozostałego okresu ważności wydanego certyfikatu.

Jeśli decyzja o zaprzestaniu działalności dotyczy tylko Punktu Rejestracji, to Punkt jest zobowiązany do:

- powiadomienia urzędu lub urzędów certyfikacji, na rzecz którego lub których świadczy usługi weryfikacji tożsamości subskrybentów o zamiarze zaprzestania działalności jako autoryzowanego Punktu Rejestracji; zawiadomienie takie powinno być złożone co najmniej na 90 dni przed planowanym zakończeniem działalności;
- przekazania dokumentacji dotyczącej subskrybentów, w tym archiwum i danych na potrzeby audytu właściwym urzędom certyfikacji.

Warunki zaprzestania działalności Punktu Rejestracji są szczegółowo określane w procedurach działania Punktów Rejestracji.

5.8.2. 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 pośredniego urzędu certyfikacji musi być przekazane głównemu urzędowi certyfikacji lub instytucji, z którą zawarta została odpowiednia umowa (w przypadku zaprzestania działalności przez **urzędy główne CERTUM**).

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych urzędów certyfikacji, Głównego Punktu Rejestracji, Punktów Rejestracji oraz użytkownika, wraz z towarzyszącymi temu uwarunkowaniami technicznymi.

Zapisy dotyczące certyfikatu **Certum Trusted Network CA** mają zastosowanie dla pozostałych certyfikatów z tej samej domeny: **Certum Trusted Network CA 2** oraz **Certum Trusted Network CA EC**.

6.1. Generowanie pary kluczy i jej instalowanie

6.1.1. Generowanie pary kluczy

Procedury zarządzania kluczami dotyczą bezpiecznego przechowywania i używania kluczy, będących pod kontrolą ich właścicieli. Szczególnej uwagi wymaga generowanie i ochrona par kluczy prywatnych głównych urzędów certyfikacji CERTUM, od których zależy bezpieczeństwo funkcjonowania całego systemu certyfikowania kluczy publicznych.

Urzędy główne CERTUM posiadają przynajmniej jeden autocertyfikat. Klucz prywatny, komplementarny z zawartym w autocertyfikacie kluczem publicznym, stosowany jest przez te urzędy jedynie do podpisywania certyfikatów kluczy publicznych pośrednich urzędów certyfikacji, wystawienia list certyfikatów unieważnionych (CRL) oraz tzw. Certyfikatów operacyjnych urzędów certyfikacji, koniecznych do prawidłowego funkcjonowania obu urzędów.

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

- podpisywanie certyfikatów i list CRL;
- podpisywanie wiadomości, wymienianych z subskrybentami oraz Punktami Rejestracji (klucz operacyjny);
- uzgadnianie kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem a otoczeniem (klucz operacyjny).

Klucze głównych urzędów certyfikacji, urzędów pośrednich 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.

Dodatkowo, w trakcie generowania kluczy głównych urzędów CERTUM (Root CA), świadkiem tego zdarzenia musi być kwalifikowany audytor zewnętrzny. Audytor potwierdza, że ceremonia generowania kluczy przebiegała zgodnie z przyjętą przez CERTUM procedurą oraz zastosowano środki gwarantujące integralność i poufność wygenerowanych kluczy.

Tworzenie kluczy urzędów certyfikacji CERTUM odbywa się w specjalnie do tego przystosowanym pomieszczeniu ekranującym promieniowanie elektromagnetyczne 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.

6.1.1.1. Procedury aktualizacji kluczy urzędów głównych CERTUM

Klucze urzędów głównych CERTUM mają skończony okres życia, po którego upływie muszą zostać uaktualnione.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do podpisywania certyfikatów i list CRL. Polega ona na wydaniu przez jeden z **urzędów głównych CERTUM** (w momencie aktualizowania kluczy) specjalnych certyfikatów ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym **stary autocertyfikat urzędu głównego**, 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 4210).

Aby uzyskać wspomniany wyżej efekt CERTUM stosuje 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 głównego CERTUM**, oprócz nowego autocertyfikatu zostaną utworzone dwa dodatkowe certyfikaty. Łącznie istnieją cztery certyfikaty do weryfikowania certyfikatów i list CRL: **stary autocertyfikat StaryStarym** (stary klucz publiczny podpisany starym kluczem prywatnym), **nowy autocertyfikat NowyNowym** (nowy klucz publiczny podpisany nowym kluczem prywatnym), **nowy certyfikat StaryNowym** (stary klucz publiczny podpisany nowym kluczem prywatnym) oraz **nowy certyfikat NowyStarym** (nowy klucz publiczny podpisany starym kluczem prywatnym).

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

- Generowanie nowej, kolejnej i-tej głównej pary kluczy $GPK_{(i,CA)}=\{K^{-1}_{GPK(i,CA)}, K_{GPK(i,CA)}\}$, gdzie $K^{-1}_{GPK(i,CA)}$ – klucz prywatny, $K_{GPK(i,CA)}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową).
- Utworzenie certyfikatu zawierającego nowy klucz publiczny **urzędu głównego CERTUM**, podpisany za pomocą starego klucza prywatnego $K^{-1}_{GPK(i-1,CA)}$ (certyfikat NowyStarym).
- Deaktywacja starego klucza prywatnego $K^{-1}_{GPK(i-1,CA)}$ i aktywacja nowego klucza prywatnego $K^{1}_{GPK(i,CA)}$ – w sprzętowym module kryptograficznym znajduje się nowy klucz prywatny do podpisywania certyfikatów i list CRL.
- Utworzenie certyfikatu zawierającego stary klucz publiczny **urzędu głównego CERTUM**, podpisany za pomocą nowego klucza prywatnego $K^{1}_{GPK(i,CA)}$ (certyfikat StaryNowym).
- Utworzenie autocertyfikatu zawierającego nowy klucz publiczny **urzędu głównego CERTUM**, podpisany za pomocą nowego klucza prywatnego $K^{1}_{GPK(i,CA)}$ (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 główny CERTUM**

podpisuje certyfikaty urzędów pośrednich oraz listy CRL tylko za pomocą 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) **urzędu głównego CERTUM** (powinno to nastąpić najpóźniej w momencie upływu okresu ważności starego autocertyfikatu).

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

Okres ważności certyfikatu 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) **urzędu głównego CERTUM** (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 główny CERTUM** 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.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

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

W przypadku certyfikatów przeznaczonych do stosowania przy podpisywaniu kodu subskrybenci zobowiązani są do generowania i ochrony kluczy wyłącznie na nośniku zewnętrznym. CERTUM rekomenduje stosowanie w tym celu oferowanych przez siebie kart kryptograficznych spełniających kryteria FIPS 140 Level 2.

CERTUM zaleca, aby w przypadku certyfikatów ID użytkownik samodzielnie generował klucze prywatne oraz przechowywał je wraz z certyfikatem na karcie kryptograficznej dostarczonej przez CERTUM. Stosowanie kart kryptograficznych gwarantuje bezpieczeństwo posiadanego klucza prywatnego.

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. Dostarczanie 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 protokołami PKCS#10 Certification Request Syntax[23] (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).

[23] 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 v3, przy czym w przypadku urzędu certyfikacji **Certum CA**, **Certum Trusted Network CA EC**, **Certum Trusted Network CA** oraz **Certum Trusted Network CA 2** 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 większość urzędów certyfikacji CERTUM wynoszą 2048 bitów. Klucze o długości 4096 bitów stosowane są przez urząd **Certum Trusted Network CA 2**. Z kolei klucz urzędu **Certum Trusted Network CA EC** posiada długość 521 bitów i szyfrowany jest algorytmem ECDH_P521. Długość kluczy w certyfikatach wykorzystywanych przez operatorów Punktów Rejestracji oraz użytkowników końcowych (subskrybentów) definiowana jest przez użytkownika (2048 bitów lub więcej).

6.1.6. Parametry generowania klucza publicznego oraz weryfikacja jakości

CERTUM przestrzega wymagań określonych w „rekomendacji NIST SP 800-89.

W przypadku generowania kluczy przez CERTUM stosuje parametry kluczy zgodne z FIPS 186. W przypadku weryfikacji kluczy subskrybentów, CERTUM sprawdza ich jakość zawsze przed wydaniem certyfikatu. Tzw. "słabe klucze" są rozpoznawane i nie zostają dopuszczone do certyfikacji. Nie dopuszcza się do wydania certyfikatu, którego klucze nie spełniają wymagań specyfikacji opisanej w rozdziale 6.1.6 Baseline Requirements.

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 algorytmu kryptograficznego RSA).

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 NIST SP 800-89.

6.1.7. Zastosowania kluczy (zgodnie z zawartością pola użycie klucza wg X.509 v3)

Sposób użycia klucza określony jest w polu **keyUsage** 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 zasadami przedstawionymi w RFC 5280.

Certyfikaty używane jednocześnie do podpisywania i szyfrowania mogą być wydawane jedynie subskrybentom.

Klucze prywatne głównych urzędów certyfikacji CERTUM nie są stosowane do podpisywania certyfikatów z wyjątkiem następujących przypadków:

- w samo podpisanym certyfikacie głównego urzędu certyfikacji,
- do podpisania certyfikatu pośredniego urzędu certyfikacji oraz certyfikatu wzajemnego,
- do podpisania certyfikatu infrastruktury (np. certyfikaty dla urządzeń CERTUM)
- do podpisania certyfikatów respondera OCSP.

6.2. Ochrona klucza prywatnego i nadzorowanie mechanizmów modułu kryptograficznego

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).

CERTUM stosuje fizyczne i logiczne zabezpieczenia, aby zapobiec nieautoryzowanemu wydaniu certyfikatu. Ochrona klucza prywatnego CERTUM - jeśli klucz znajduje się poza systemem lub urządzeniem CERTUM - MUSI składać się z jego fizycznego bezpieczeństwa, zaszyfrowania lub połączenia obydwu tych metod, zaimplementowanych w sposób uniemożliwiający ujawnienie klucza prywatnego.

CERTUM szyfruje swój klucz prywatny za pomocą algorytmu i klucza, które zgodnie ze współczesnym stanem wiedzy są w stanie wytrzymać ataki kryptoanalityczne biorąc pod uwagę ich okres ważności.

6.2.1. Standardy modułu kryptograficznego oraz jego nadzorowania

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji są zgodne z wymaganiami normy FIPS 140-2 Level 3 lub wyżej. W przypadku używania przez subskrybenta sprzętowej ochrony klucza prywatnego zaleca się, aby spełniał on wymagania FIPS 140-2 Level 2 i wyższe.

6.2.2. Podział klucza prywatnego na części (typu m z n)

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. Wartość progowa umożliwiająca odtworzenie klucza oraz liczba podziałów klucza na sekrety współdzielone wynosi 3 z 5.

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

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.

6.2.3. Deponowanie klucza prywatnego

Patrz rozdz. 4.12.

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.

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. 4.12.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne wszystkich urzędów certyfikacji CERTUM archiwizowane są wyłącznie przez CERTUM.

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.

CERTUM nie archiwizuje kopii kluczy prywatnych należących do subskrybentów i Punktów Rejestracji.

6.2.6. Wprowadzanie lub pobieranie 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 lub jego modyfikacji. Klucze prywatne wszystkich pośrednich urzędów certyfikacji pozostają pod wyłączną kontrolą CERTUM.

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.

6.2.7. Przechowywanie klucza prywatnego w module kryptograficznym

Sprzętowe moduły kryptograficzne używane przez urzędy certyfikacji CERTUM są zgodne z wymaganiami normy FIPS 140-2 Level 3 lub wyżej. Niezależnie od formy przechowywania klucz prywatny nie jest dostępny z zewnątrz modułu kryptograficznego dla nieuprawnionych podmiotów.

6.2.8. 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 w pliku.

6.2.9. 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.

6.2.10. Metoda niszczenia klucza prywatnego

Niszczenie kluczy subskrybentów lub operatorów Punktu Rejestracji polega odpowiednio na ich bezpiecznym wymazaniu z nośnika (z dysku, 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.

6.2.11. Ocena modułu kryptograficznego

Patrz rozdz. 6.2.1.

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. Archiwizowanie kluczy publicznych

Archiwizowanie kluczy publicznych ma na celu stworzenie możliwości weryfikacji podpisów cyfrowych już po usunięciu certyfikatu z repozytorium (patrz rozdz. 2). 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.

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.

Klucze publiczne przechowywane są w archiwum kluczy publicznych przez okres 25 lat (patrz także rozdz. 5.5).

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).

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

Tab.6.1 Maksymalne okresy ważności certyfikatów urzędów

Typ właściciela klucza i rodzaj klucza	Główny rodzaj zastosowania klucza	
	Certyfikaty i listy CRL	Tokeny

Certum CA	klucz publiczny	25 lat	–
	klucz prywatny	15 lat	–
Certum CA EC	klucz publiczny	35 lat	–
	klucz prywatny	25 lat	–
Certum Trusted Network CA	klucz publiczny	25 lat	–
	klucz prywatny	15 lat	–
Certum Trusted Network CA 2	klucz publiczny	35 lat	--
	klucz prywatny	25 lat	--
Certum Level I CA	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–
Certum Level II CA	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–
Certum Level III CA	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–
Certum Level IV CA	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–

Certum Domain Validation CA SHA2	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	
Certum Organization Validation CA SHA2	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	
Certum Digital Identification CA SHA2	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–
Certum Extended Validation CA	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–
Certum Extended Validation CA SHA2	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	
Certum Code Signing CA	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–
Certum Code Signing CA SHA2	klucz publiczny	15 lat	–
	klucz prywatny	12 lat	–
Certum Extended Validation Code Signing CA SHA2	klucz publiczny	14	–
	klucz prywatny	11	–
Certum Class 1 CA	klucz publiczny	15 lat	–
	klucz prywatny	14 lat	–
Certum Class 1 CA SHA2	klucz publiczny	15 lat	–
	klucz prywatny	14 lat	
Certum Global Services CA	klucz publiczny	15 lat	–
	klucz prywatny	5 lat	–
Certum Global Services CA SHA2	klucz publiczny	15 lat	–
	klucz prywatny	5 lat	
Certum EV TSA SHA2	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.

Klucze urzędu walidacji statusu certyfikatów podpisywane przez urzędy pośrednie nie podlegają powyższym zasadom.

Maksymalny okres ważności certyfikatów subskrybentów uzależniony jest od zastosowania danego certyfikatu:

- Maksymalny okres ważności dla certyfikatów zabezpieczających pocztę elektroniczną wynosi 1095 dni
- Maksymalny okres ważności dla certyfikatów do podpisywania kodu wynosi 1095 dni.
- Maksymalny okres ważności dla certyfikatów do uwierzytelniania witryn internetowych wynosi 730 dni.

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. 5.2.1 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 NIST SP 800-63 i FIPS 180-3.

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 zaleceniami przedstawionymi w NIST SP 800-63. 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 aspekty 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. Nadzorowanie bezpieczeństwa 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 CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements* przynajmniej dla poziomu EAL3 wg ISO/IEC 15408-3:1999 *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements*.

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),
- 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.

CERTUM wymusza uwierzytelnianie wieloskładnikowe użytkownika pracującego na dowolnym koncie, z którego można bezpośrednio spowodować wydanie certyfikatu..

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe CERTUM spełniają wymagania nakładane na podmioty świadczące usługi niekwalifikowane określone w CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements*. Zostało to potwierdzone przez niezależnego audytora, oceniającego funkcjonowanie systemu CERTUM na podstawie kryteriów określonych w WebTrust Principles and Criteria for Certification Authorities.

6.6. Cykl życia zabezpieczeń technicznych

6.6.1. Nadzorowanie rozwoju systemu

Aplikacje stosowane w systemie CERTUM są projektowane i implementowane przez Asseco Data Systems S.A.

Wymiana sprzętu w systemie jest rejestrowana i monitorowana. W szczególności:

- 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.

Nadzorowanie 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.

6.6.2. Nadzorowanie zarządzania bezpieczeństwem

Nadzorowanie procesów 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. Nadzorowanie cyklu życia zabezpieczeń

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

6.7. Nadzorowanie zabezpieczeń 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. 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. Znakowanie czasem

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 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, CRL, OCSP i innych tokenów

Profile certyfikatów oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3, tokena statusu certyfikatu z RFC 2560, zaś 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. Profil certyfikatu

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).

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

Certyfikaty CERTUM zawierają co najmniej następujące pola podstawowe:

- **Version**: wersję trzecią (X.509 v.3) formatu certyfikatu;
- **SerialNumber**: numer seryjny certyfikatu, unikalny w ramach domeny urzędu certyfikacji (CERTUM wykorzystuje kryptograficzny generator liczb pseudolosowych do tworzenia niesekwencyjnych numerów seryjnych certyfikatów (liczby dodatnie większe od zera), które zawierają wielkość co najmniej 64 bitów);
- **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,
- **Signature**: podpis generowany i kodowany zgodnie z RFC 5280.

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)	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) sha384WithRSAEncryption (OID: 1.2.840.113549.1.1.12) sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)	
Issuer (wystawca, nazwa DN)	Common Name (CN) =	Odpowiednia nazwa root'a
	Organization (O) =	**Unizeto Sp. Z o.o. (stara nazwa) Unizeto Technologies S.A.**
	Organization Unit (OU) =	**Certum Certification Authority** (tylko w przypadku certyfikatów z domeny ctnDomena)
	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: mailAddress (w przypadku certyfikatów subskrybenta), organizationName (w przypadku certyfikatów urzędów certyfikacji i podmiotów świadczących usługi niezaprzeczalności), subjectAltName (w przypadku certyfikatów serwerów: zawiera wszystkie nazwy domenowe lub adresy IP), commonName (w przypadku certyfikatów serwerów: zawiera jeden z adresów IP lub jedną z nazw domenowych umieszczonych w polu subjectAltName), 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 5280 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 5280.	

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. Numer wersji

Wszystkie certyfikaty CERTUM są wydawane zgodnie z wersją trzecią (X.509 v.3).

7.1.2. Rozszerzenia certyfikatów

Wartości rozszerzeń tworzone są zgodnie z RFC 5280. 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. Wymagania nakładane na rozszerzenia certyfikatu EV SSL opisane są w ***Guidelines for the issuance and Management of Extended Validation Certificates***.

Certyfikaty główne CERTUM (Root CA):

basicConstraints (critical) – cA True
keyUsage (critical) – keyCertSign, cRLSign
certificatePolicies – not present
extendedKeyUsage – not present
cRLDistributionPoints – not present
authorityInformationAccess – not present

Certyfikaty pośrednie CERTUM (Subordinate CA):

basicConstraints (critical) – cA True
keyUsage (critical) – keyCertSign, cRLSign
certificatePolicies – anyPolicy
extendedKeyUsage – not present
cRLDistributionPoints – present
authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2

Certyfikaty subskrybentów CERTUM:

basicConstraints (critical) – cA False
keyUsage (critical) –

- digitalSignature (certyfikaty do zabezpieczenia poczty elektronicznej, certyfikaty do podpisywania kodu, certyfikaty uwierzytelniania witryn internetowych)
- keyEncipherment (certyfikaty do zabezpieczenia poczty elektronicznej)
- Non Repudiation (certyfikaty do zabezpieczenia poczty elektronicznej)
- Key Encipherment (certyfikaty do zabezpieczenia poczty elektronicznej, certyfikaty uwierzytelniania witryn internetowych)
- Data Encipherment (certyfikaty do zabezpieczenia poczty elektronicznej)

certificatePolicies – patrz. 1.3.1.2
extendedKeyUsage –

- serverAuth (certyfikaty uwierzytelniania witryn internetowych),
- clientAuth (certyfikaty uwierzytelniania witryn internetowych, certyfikaty do zabezpieczenia poczty elektronicznej)
- codeSigning (certyfikaty do podpisywania kodu)
- Kernel Mode Code Signing (certyfikaty do podpisywania kodu)
- emailProtection (certyfikaty do zabezpieczenia poczty elektronicznej)

cRLDistributionPoints – present
authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2

7.1.3. Identyfikatory algorytmów

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 jedną następujących funkcją skrótu SHA-1, SHA-256, SHA-384 lub SHA-512:

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2)
                           us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2)
                           us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2)
                           us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption  OBJECT IDENTIFIER  ::=  { iso(1) member-body(2)
                           us(840) rsadsi(113549) pkcs(1) pkcs-1(1)  13 }
```

W przypadku certyfikatów uwierzytelniania witryn internetowych CERTUM stosuje wyłącznie algorytmy SHA-256 i wyższe.

7.1.4. Formy nazw

CERTUM wydaje certyfikaty zawierające nazwę wystawcy i podmiotu tworzone zgodnie z zasadami opisanymi w rozdz. 3.1.1.

7.1.5. Ograniczenia nakładane na nazwy

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

7.1.6. Identyfikatory polityk certyfikacji

Polityka certyfikacji zawiera informację typu **policyInformation** (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez dany organ wydający certyfikaty – rozszerzenie nie jest krytyczne.

W certyfikatach wydawanych przez urzędy certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 5280.

7.1.7. Stosowanie rozszerzenia określającego ograniczenia nakładane na politykę

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

7.1.8. Składnia i semantyka kwalifikatorów polityki

W większości przypadków certyfikaty wydawane przez CERTUM zawierają dwa kwalifikatory polityki certyfikacji, umieszczane w rozszerzeniu policyInformation. Pierwszy z kwalifikatorów zawiera wskazanie na Kodeks Postępowania Certyfikacyjnego (ang. CPS Pointer). Z kolei drugi z kwalifikatorów – kwalifikator notki adresowanej do strony ufającej – zawiera numer notki oraz jej treść. Numer notki określa jednoznacznie typ certyfikatu wystawianego w ramach określonej polityki certyfikacji, zaś treść notki – zawiera komercyjną nazwę typu certyfikatu (patrz Tab. 1.4).

7.1.9. Przetwarzanie semantyki krytycznych rozszerzeń polityki certyfikacji

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

7.2. Profil listy 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.

Tab.7.2 Profil podstawowych pól i rozszerzeń CRL

Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	Version 3	
Signature Algorithm (algorytm podpisu)	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11) sha384WithRSAEncryption (OID: 1.2.840.113549.1.1.12) sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)	
Issuer (wystawca, nazwa DN)	Common Name (CN) =	Odpowiednia nazwa root'a
	Organization (O) =	**Unizeto Sp. z o.o.** (w domenie **certum**) lub **Unizeto Technologies S.A.** (w domenie **ctnDomena**)
	Organization Unit (OU) =	**Certum Certification Authority** (tylko w przypadku certyfikatów z domeny ctnDomena)
	Countm.in.(C) =	PL
thisUpdate	Data i czas wydania listy CRL.	
nextUpdate	Data i czas wydania kolejnej listy CRL.	
revokedCertificates:	Każdy zapis dotyczący certyfikatu zawiera następujące pola: • userCertif–cate - numer seryjny unieważnianego certyfikatu, • revocatio–Date - data unieważnienia certyfikatu, • crlEntryExten–ions - rozszerzony dostęp do listy CRL (zawiera dodatkowe informacje o unieważnionych certyfik–tach - opcjonalnie), • CRLReason (zawiera informacje o przyczynie unieważnienia certyf–katu - opcjonalnie) Informacje o w/w polach zapisano w kolejnych trzech wierszach niniejszej tabeli.	
userCertificate	Numer seryjny certyfikatu, który uległ unieważnieniu.	
revocationDate	Data i czas unieważnienia certyfikatu.	
CRLReason	Przyczyna unieważnienia certyfikatu. Dopuszczalne wartości pola określono w rozdziale 7.2.2.	
Extensions	Zbiór rozszerzeń określających dodatkowe informacje związane z wykorzystaniem certyfikatu. Pełen zbiór dopuszczalnych rozszerzeń znajduje się w rozdziale 7.2.1.	
Signature (podpis)	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 5280.	

7.2.1. Numer wersji

Wersje publikowanych przez CERTUM list CRL różnią się w zależności od urzędów certyfikacji, których dotyczą. Listy CRL urzędów głównych oraz urzędów pośrednich, dla których nie wydaje się już certyfikatów, zgodne są z formatem wersji pierwszej (X.509 v.1). Natomiast listy CRL odnoszące się do certyfikatów pośrednich, które zastąpiły urzędy, dla których nie wydaje się już certyfikatów, zgodne są z formatem wersji drugiej (X.509 v.2).

7.2.2. Rozszerzenia CRL oraz rozszerzenia dostępu do listy CRL

Spośród wielu rozszerzeń CRL najbardziej istotne są dwa, z których pierwsze umożliwia identyfikację klucza publicznego, odpowiadającego kluczowi prywatnemu, zastosowanemu do podpisania listy CRL (pole **authorityKeyIdentifier**)), 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). Funkcje oraz sens rozszerzeń są takie same jak w przypadku rozszerzeń certyfikatu (patrz rozdz. 7.1.2).

7.3. Profil tokena statusu certyfikatu (token OCSP)

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 każdy z urzędów certyfikacji CERTUM. Każdy 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 5280. 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**.

Zgodnie z RFC 2560 (*X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP*, June 1999) poświadczenia statusu certyfikatów wydawane mogą być w trzech trybach:

- w trybie **lokalnym** przez ten urząd certyfikacji, który wydał weryfikowany certyfikat; poświadczenie jest podpisywane za pomocą tego samego klucza prywatnego , który został użyty do podpisania weryfikowanego certyfikatu,
- w trybie **zaufany responder** (ang. Trusted Responder); żądający ufają certyfikatowi klucza publicznego tego respondera;
- w trybie **autoryzowany responder** (ang. Authorized Responder); poświadczenia są weryfikowane za pomocą specjalnie oznaczonego certyfikatu klucza publicznego wydanego bezpośrednio przez urząd certyfikacji urzędowi weryfikacji statusu certyfikatu OCSP, który może wystawiać takie poświadczenia w imieniu urzędu, ale **tylko dla certyfikatów wydanych przez ten urząd**.

Certyfikat urzędu weryfikacji statusu certyfikatu, wydającego zaświadczenia w trybie **autoryzowany responder** musi zawierać rozszerzenie **extendedKeyUsage** z wpisaną wartością *id-kp-OCSPSigning*.

Wszystkie urzędy OCSP, wystawiające poświadczenia statusu certyfikatów, działające w strukturze CERTUM, pracują w trybie **autoryzowany responder**.

7.3.1. 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).

7.3.2. Rozszerzenia OCSP

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 swojej ważności.

Zgodnie z RFC 6960 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. 7.2.2. 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**.

Każdy odbiorca poświadczenia wystawionego przez serwer OCSP musi być w stanie obsłużyć standardowy typ odpowiedzi o identyfikatorze *id-pkix-ocsp-basic*.

7.4. Inne profile

7.4.1. Profil tokena znacznika czasu (token TST)

Urząd znacznika czasu **Certum EV TSA SHA2** 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 5280 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.

Tab.7.3 Wymagania nakładane na urzędy weryfikacji statusu certyfikatu pracujące w strukturze CERTUM

Nazwa urzędu TSA	OID polityki znakowania czasem	Zgodność z wymaganiami	Źródło czasu
Certum Time Stamping Authority (Certum EV TSA SHA2)	iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum-tsa(5) 1 11	RFC 3161 ETSI TS 101 861, Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates	Zewnętrzne źródło czasu klasy STRATUM 1 + NTP

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.

Token znacznika czasu wystawiony przez urząd znacznika czasu **Certum EV TSA SHA2** zawiera w sobie informację o znaczniku czasu (struktura TSTInfo), umieszczoną w strukturze SignedData (zgodnie z RFC 2630), podpisaną przez urząd znacznika i zagnieżdżoną w strukturze ContentInfo (patrz RFC 2630).

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**.

7.4.1.1. Numer wersji

Urząd znacznika czasu **Certum EV TSA SHA2** wystawia tokeny znacznika czasu zgodnie z normą RFC 3161 lub ETSI TS 101 861. Z tego powodu jedynym dozwolonym numerem wersji jest 1 (odpowiada to wersji v1).

7.4.1.2. Rozszerzenia znacznika czasu

Tokeny znacznika czasu wystawiane przez urząd znacznika czasu **Certum EV TSA SHA2** nie zawierają żadnych rozszerzeń.

8. Audyt zgodności i inne oceny

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** oraz **Certum Trusted Network CA**, Punkty Rejestracji oraz inne elementy infrastruktury klucza publicznego, m.in. serwer OCSP.

Audyt CERTUM może być prowadzony przez komórki wewnętrzne Asseco Data Systems S.A. (audyt wewnętrzny) oraz przez jednostki organizacyjne niezależne od Asseco Data Systems S.A (audyt zewnętrzny). W obu przypadkach audyt jest prowadzony na wniosek i pod nadzorem inspektora bezpieczeństwa (patrz rozdz. 5.2.1).

8.1. Częstotliwość i okoliczności audytu

W przypadku certyfikatów uwierzytelniania witryn internetowych oraz certyfikatów do podpisywania kodu audyt wewnętrzny odbywa się co kwartał i obejmuje trzy procent losowo wybranych certyfikatów wydanych od dnia zakończenia poprzedniego audytu.

W przypadku certyfikatów wydanych przez pośrednie urzędy certyfikacji dedykowane Partnerom CERTUM audyt wewnętrzny odbywa się co miesiąc i obejmuje pięć procent losowo wybranych certyfikatów wydanych od dnia zakończenia poprzedniego audytu.

CERTUM corocznie poddaje się audytom zgodności z wymaganiami **AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria** oraz **AICPA/CICA WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria**.

8.2. 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 Asseco Data Systems S.A.

8.3. Związek audytora z audytowaną jednostką

Patrz rozdz. 8.2.

8.4. Zagadnienia objęte audytem

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*.

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.

8.5. Działania podejmowane 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.

8.6. Informowanie o wynikach audytu

Raport z audytu, w możliwie szczegółowej postaci wraz z opinią instytucji audytującej, publikowany w repozytorium.

9. Inne kwestie biznesowe i prawne

9.1. 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 Asseco Data Systems S.A., na podstawie faktury lub zamówienia.

9.1.1. Opłaty za wydanie certyfikatu lub recertyfikację

CERTUM pobiera opłaty za wydanie i recertyfikację.

Ze względu na odmienność procedur wydawania certyfikatu i recertyfikacji opłaty realizowane według jednego z wymienionych powyżej modeli 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 zwłaszcza w przypadku recertyfikacji (można pominąć koszty identyfikacji i uwierzytelnienia subskrybenta oraz wydania karty).

9.1.2. 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 CA.

9.1.3. Opłaty za unieważnienie lub 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.

9.1.4. Opłaty za inne usługi

CERTUM może pobierać opłaty za inne usługi niż te wymienione w rozdz. 9.1.1-9.1.3. 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.

9.1.5. 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.

9.2. Odpowiedzialność finansowa

Odpowiedzialność Asseco Data Systems S.A. za pośrednictwem swojej jednostki organizacyjnej, działającej pod nazwą CERTUM PCC (dalej: 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.

CERTUM ponosi odpowiedzialność za zaistnienie sytuacji wymienionych w punkcie 9.9 niniejszego Kodeksu Postępowania Certyfikacyjnego.

CERTUM odpowiada finansowo wobec Subskrybentów usług certyfikacyjnych oraz **stron ufających będących beneficjentami gwarancji**. Podmioty te nazywane będą dalej podmiotami będącymi beneficjentami gwarancji.

CERTUM nie ponosi odpowiedzialności finansowej zdefiniowanej w niniejszym dokumencie wobec innych osób trzecich, nieujętych w punkcie 9.2 niniejszego Kodeksu Postępowania Certyfikacyjnego.

Odpowiedzialność finansowa CERTUM występuje wobec podmiotów będących beneficjentami gwarancji tylko wówczas, jeśli szkody wystąpią z winy CERTUM lub z winy stron, z którymi Asseco Data Systems S.A ma tak zawarte umowy, że wina ta przenosi się na CERTUM.

W przypadku wystąpienia szkody podmiot będący beneficjentem gwarancji musi zgłosić jej wystąpienie w ciągu 30 dni od jej zajścia. W przypadku zgłoszenie wystąpienia szkody w terminie późniejszym CERTUM nie ma obowiązku rozpatrzenia danej szkody.

CERTUM ponosi odpowiedzialność finansową wobec podmiotów będących beneficjentami gwarancji tylko jeżeli szkoda wystąpiła w okresie ważności certyfikatu, którego dotyczy.

W przypadku potwierdzenia przez pracowników CERTUM wystąpienia szkody, Asseco Data Systems S.A. zobowiązuje się do wypłacenia odszkodowania. Wysokość odszkodowania dla pojedynczego podmiotu będącego beneficjentem gwarancji w ramach jednej zgłoszonej szkody dla danego typu certyfikatu wydanego według określonej polityki certyfikacji, nie może być wyższa niż limit gwarancji finansowej dla pojedynczej szkody określony w Tab. 9.1. Wielkość wypłaconego odszkodowania nie będzie wyższa niż udowodniona przez podmiot będący beneficjentem gwarancji wartość szkody.

Asseco Data Systems S.A. zobowiązuje się dla wszystkich przypadków wystąpienia szkody wypłacić łączne odszkodowanie do wysokości łącznego limitu gwarancji finansowej określonej w Tab. 9.1 w stosunku do jednego certyfikatu w trakcie całego okresu jego ważności, łącznie dla wszystkich podmiotów będących beneficjentami gwarancji.

Asseco Data Systems S.A. wypłaca odszkodowania wobec zgłoszonych szkód według kolejności zgłoszenia wystąpienia szkody przez podmioty będące beneficjentami gwarancji. W przypadku osiągnięcia limitu gwarancji finansowej, Asseco Data Systems S.A. nie ma obowiązku wypłacania dalszych odszkodowań wobec kolejnych zgłoszonych szkód przez kolejne podmioty będące beneficjentami gwarancji dla danego certyfikatu.

9.2.1. Zakres ubezpieczenia

CERTUM posiada ciągle aktualne ubezpieczenie, które swoim zakresem obejmuje błędy i przeoczenia spowodowane przez personel CERTUM. Jednocześnie zaleca się subskrybentom i stronom ufającym, aby (zwłaszcza osoby prawne) korzystały dostępnych na rynku ubezpieczeń od ryzyka biznesowego, o ile chcą posiadać wyższy poziom ubezpieczenia niż ten gwarantowany przez CERTUM.

Ubezpieczenia, które swoim zakresem obejmują błędy i przeoczenia spowodowane przez personel, muszą mieć także wszystkie podmioty świadczące usługi certyfikacyjne akredytowane przez CERTUM.

9.2.2. Inne aktywa

CERTUM oraz każdy podmiot świadczący usługi certyfikacyjne akredytowany przez CERTUM posiadają wystarczające środki finansowe niezbędne do prowadzenia działalności oraz wywiązywania się ze swoich obowiązków i z gwarancji zapewnionych subskrybentom i stronom ufającym.

9.2.3. Rozszerzony zakres gwarancji

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

9.3. Poufność informacji biznesowej

Asseco Data Systems 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.

Asseco Data Systems 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.

9.3.1. Zakres poufności informacji

Asseco Data Systems 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[24], 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 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);

[24] 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.

- 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. 9.3.2 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.

Asseco Data Systems 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.

9.3.2. Informacje znajdujące się poza zakresem poufności informacji

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 urzędy wydające certyfikaty zgodnie z opisem przedstawionym w rozdz. 7.1. 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 w procesie rejestracji.

Wymienione poniżej informacje 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.

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.

9.3.3. Obowiązek ochrony poufności informacji

CERTUM chroni prywatne informacje przed ujawnieniem i udostępnieniem stronom trzecim.

9.4. Prywatność informacji osobowych

9.4.1. Zasady prywatności

Dane prywatne przekazywane do CERTUM przez subskrybentów są objęte ochroną określoną przez Ustawę o ochronie danych osobowych. Zakres danych osobowych gromadzonych i przetwarzanych przez CERTUM odpowiada celom, do których dane te są potrzebne. Zgoda subskrybenta/przedstawiciela organizacji na przetwarzanie jego danych osobowych jest zawarta w umowie oświadczenie usług certyfikacyjnych i jest obowiązkowa.

Dane prywatne są wykorzystywane tylko w związku ze świadczeniem usług certyfikacyjnych.

Dane prywatne chronione są zgodnie z zasadami ochrony prywatności zawartymi w polityce bezpieczeństwa Asseco Data Systems S.A.

9.4.2. Informacje uważane za prywatne

Dowolna informacja dotycząca subskrybenta, która nie jest publicznie udostępniana w wydanym certyfikacie, w repozytorium i w listach CRL jest uważana za informację prywatną.

9.4.3. Informacja nieuważana za prywatną

Wszystkie informacje udostępniane publicznie certyfikacie nie są uważane za informacje prywatne, o ile reguła ta nie narusza wymagań wynikających z Ustawy o ochronie danych osobowych.

9.4.4. Odpowiedzialność za ochronę informacji prywatnej

Każdy pracownik lub użytkownik CERTUM, który uzyskał dostęp do informacji prywatnej musi chronić ją przed ujawnieniem i udostępnieniem stronom trzecim. Niezależnie od tego, przekazanie dostępu do informacji prywatnej musi być zgodne z wymaganiami Ustawy o ochronie danych osobowych.

9.4.5. Zastrzeżenia i zezwolenie na użycie informacji prywatnej

O ile inaczej nie postawiono w niniejszym Kodeksie Postępowania Certyfikacyjnego, w odnośnych zasadach prywatności lub umowie, informacje prywatne nie mogą być wykorzystywane bez zgody strony, której ta informacja dotyczy.

Zastrzeżenia i zezwolenia nie mogą naruszać wymagań zawartych w Ustawie o ochronie danych osobowych.

9.4.6. Udostępnianie informacji zgodnie z nakazem sądowym lub administracyjnym

Informacje poufne/prywatne mogą zostać udostępniona na żądanie organów sądowych lub administracyjnych, ale tylko i wyłącznie po spełnieniu wszystkich wymagań stawianych przez obowiązujące na terenie Rzeczypospolitej Polskiej akty prawne.

9.4.7. Inne okoliczności ujawniania informacji

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

9.5. Prawo do własności intelektualnej

Wszystkie używane przez Asseco Data Systems 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, o ile regulują to odpowiednie zapisy umowy z subskrybentami lub przepisy prawa, wynikające z Ustawy z dnia 4 lutego 1994 r. o prawie autorskim i prawach pokrewnych.

Szczegółowe zasady ochrony praw do własności intelektualnej należących do subskrybentów i stron ufających przedstawione są w kolejnych podrozdziałach niniejszego rozdziału.

CERTUM posiada wyłączne prawa do dowolnego produktu lub informacji projektowanej, implementowanej i wdrażanej na podstawie lub zgodnie z niniejszym Kodeksem Postępowania Certyfikacyjnego. Należące do CERTUM znaki towarowe, nazwy marek, symbole i emblematy firmowe nie mogą być wykorzystywane w jakikolwiek sposób bez uprzedniej pisemnej zgody CERTUM.

9.5.1. Prawa do własności w certyfikatach oraz informacji o unieważnieniach

Intelektualne prawa własności do certyfikatu subskrybenta, informacji o unieważnieniach oraz innych poświadczeń należą do CERTUM i działających w jego domenach podmiotów świadczących usługi certyfikacyjne (w tym podmiotów akredytowanych przy CERTUM). CERTUM przekazuje stronom trzecim prawa do kopiowania i dystrybucji certyfikatów bez żadnych zastrzeżeń oraz opłat za korzystanie. Korzystanie przez strony ufające z informacji o unieważnieniach oraz poświadczeniach może podlegać zastrzeżeniom i opłatom, o ile tak stanowią zawarte umowy lub ogólne zasady określone w niniejszym Kodeksie (patrz rozdz. 9.1.3).

9.5.2. Prawa własności do Kodeksu Postępowania Certyfikacyjnego

CERTUM posiada wyłączność do wszystkich intelektualnych praw własności odnoszących się lub powiązanych z niniejszym Kodeksem Postępowania Certyfikacyjnego.

9.5.3. Prawa własności do nazw

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

Rys.9.1. Logo CERTUM

Znak ten oraz napis tworzą łącznie logo CERTUM. Logo to jest zastrzeżonym znakiem towarowym Asseco Data Systems S.A. i nie może być używane przez żadną inną stronę bez uprzedniej pisemnej zgody Asseco Data Systems 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 Główny Punkt Rejestracji nowego Punktu Rejestracji.

Każdy subskrybent zachowuje wszystkie swoje prawa do znaków towarowych, znaków usługowych lub nazw handlowych zawartych we wniosku o wydanie certyfikatu oraz w nazwie wyróżnionej (DN) umieszczonej w certyfikacie wydanym subskrybentowi.

9.5.4. Prawa własności do kluczy

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) niezależnie od nośnika, w którym klucze są przechowywane i chronione.

Certyfikaty głównych urzędów certyfikacji CERTUM są własnością CERTUM. CERTUM udziela licencji każdemu zainteresowanemu wytwórcy oprogramowania lub sprzętu na utworzenie kopii certyfikatów urzędów głównych CERTUM i umieszczenie ich w wiarygodnym sprzęcie lub oprogramowaniu.

Własnością CERTUM są także cienie (udziały) kluczy prywatnych (patrz rozdz. 6.2) głównych urzędów certyfikacji, pośrednich urzędów certyfikacji podmiotów świadczących inne usługi niż tylko wydawanie certyfikatów, świadczone w domenach **certum** oraz **ctnDomena**.

9.6. Zobowiązania i gwarancje

W rozdziale tym przedstawione są zobowiązania/gwarancje i odpowiedzialność urzędów certyfikacji CERTUM, Głównego Punktu Rejestracji, Punktów Rejestracji, subskrybentów oraz stron ufających. Zobowiązania te oraz odpowiedzialność regulowane są przez wzajemne umowy zawierane pomiędzy wymienionymi stronami (patrz rys.9.2).

9.6.1. Zobowiązania i gwarancje urzędu certyfikacji

CERTUM świadcząc niekwalifikowane usługi certyfikacyjne gwarantuje, że:

- w chwili wydania subskrybentowi certyfikatu zweryfikowało, że subskrybent kontroluje nazwę domenową lub posiada prawo do posługiwania się nazwą domenową, która znajdzie się w certyfikacie,
- w chwili wydania subskrybentowi certyfikatu zweryfikowało, że subskrybent lub jego przedstawiciel są upoważnieni do złożenia wniosku certyfikacyjnego w imieniu podmiotu, który będzie właścicielem certyfikatu,
- w chwili wydania subskrybentowi certyfikatu zweryfikowało, że wszystkie informacje w certyfikacie (z wyjątkiem pola organizationalUnitName) są poprawne i zgodne ze stanem faktycznym,
- w chwili wydania subskrybentowi certyfikatu dopełniło starań aby zmniejszyć prawdopodobieństwo, że zawartość pola organizationalUnitName mogłaby wprowadzać w błąd użytkowników certyfikatu,
- w chwili wydania subskrybentowi certyfikatu (jeśli certyfikat zawiera dane identyfikujące subskrybenta) zweryfikowało tożsamość subskrybenta,
- unieważni każdy certyfikat, który spełnia warunki unieważnienia opisane w niniejszym Kodeksie.
- 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 Signa–ures - Part 1: System Security Requirements* oraz normie *FIPS PUB 140 Security Requirements for Cryptographic Modules*,
- swoją działalność realizuje zgodnie z wymaganiami:
  - *Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates,*
  - *Guidelines For The Issuance And Management Of Extended Validation Certificates,*
  - *Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates,*
  - *Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,*
- 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 lub specyfikacjami:
  - 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,

- przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym Kodeksie Postępowania Certyfikacyjnego, w szczególności w zakresie:
  - weryfikacji tożsamości subskrybenta, któremu wydawany jest certyfikat; 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 wydania lub unieważnienia certyfikatu,
  - publikowania list certyfikatów unieważnionych,
  - 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,
- 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 CERTUM,
- zlecania planowanych audytów CERTUM niezależnym audytorom, udostępniania im wszystkich niezbędnych informacji i dokumentów oraz stosowania się do ich zaleceń pokontrolnych.

9.6.2. Zobowiązania i gwarancje Punktów Rejestracji

Główny Punkt Rejestracji oraz każdy Punkt Rejestracji, który funkcjonuje w 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**[25], powiązanego z przedstawionym do certyfikacji kluczem publicznym,
  - procedur przyjmowania od klientów, rozpatrywania i potwierdzania lub odrzucania wniosków o wydanie certyfikatu, jego aktualizację i unieważnienie,,
  - procedur występowania do urzędu certyfikacji, na podstawie wcześniej zaakceptowanego wniosku subskrybenta, o wydanie certyfikatu, jego aktualizację i unieważnienie; 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,

25 Patrz **Słownik pojęć**

- 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[26] certyfikatów kluczy publicznych i list CRL urzędów certyfikacji CERTUM z wiarygodnych źródeł oraz ich rzetelnej weryfikacji.

9.6.3. Zobowiązania i gwarancje subskrybenta

Poprzez złożenie w Punkcie Rejestracji wniosku o rejestrację oraz zaakceptowanie certyfikatu (patrz rozdz. 4.3 i 4.4) 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 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 Głównego Punktu Rejestracji lub Punktu Rejestracji 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,

---

26 **Patrz Słownik pojęć**

- 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 w momencie składania podpisu,
- ogólnego zaznajomienia się z pojęciami dotyczącymi certyfikatów, podpisów cyfrowych oraz infrastruktury klucza publicznego (PKI).

Subskrybent 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 zaś w przypadku certyfikatów stosowanych do podpisywania kodu, generować i przechowywać klucz prywatny tylko i wyłącznie na zewnętrznym nośniku
- 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,
- zaakceptować fakt, że w przypadku gdy stosowany prze niego certyfikat służy lub służył do podpisywania szkodliwego oprogramowania/kodu oraz został na tej podstawie unieważniony, CERTUM zastrzega sobie prawo do rozpowszechnienia tej informacji wśród innych urzędów certyfikacji oraz producentów oprogramowania z członkami CA/Browser Forum włącznie.

9.6.4. Zobowiązania i gwarancje strony ufającej

Przedmiotem umowy pomiędzy stroną ufającą a:

- Asseco Data Systems 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**[27] każdego podpisu cyfrowego umieszczonego na dokumencie który do niej dotrze; w celu zweryfikowania podpisu strona ufająca powinna:
  - określić **ścieżkę certyfikacji**[28], 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; unieważnienie 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,

---

[27] 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.

[28] Patrz **Słownik pojęć**

- 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 jego jako skuteczny mechanizm weryfikacji tożsamości subskrybenta składającego podpis.

9.6.5. Zobowiązania i gwarancje innych użytkowników

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

9.7. Wyłączenie odpowiedzialności z tytułu gwarancji

Gwarancje CERTUM oparte są na ogólnych zasadach zawartych w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz są zgodne z obowiązującymi aktualnie na terenie Rzeczypospolitej Polskiej nadrzędnymi aktami prawnymi. Wyłączenia odpowiedzialności z tytułu gwarancji CERTUM umieszczane są w umowach zawieranych z klientami CERTUM.

CERTUM nie udziela żadnych gwarancji użytkownikom oprogramowania lub sprzętu, które wykorzystuje certyfikaty i poświadczenia wystawione przez CERTUM lub w których (na podstawie udzielonej licencji, patrz rozdz. 9.5.4) zostały umieszczone certyfikaty głównych urzędów certyfikacji. Zastrzeżenie to nie dotyczy przypadku, gdy CERTUM jest producentem tego typu oprogramowania lub sprzętu.

9.8. Ograniczenia odpowiedzialności

Jeśli szkody wystąpią z winy CERTUM lub z winy stron, z którymi Asseco Data Systems 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.9.1 polityk certyfikacji.

Tab.9.1 Maksymalne gwarancje finansowe

Typ wydawanych certyfikatów	Łączny limit gwarancji finansowej	Limit gwarancji finansowej dla pojedynczej szkody
Wszystkie w ramach polityk: Certum Level I CA oraz Certum Class 1 CA, Certum Class 1 CA SHA2	0 EUR	0 EUR
Certyfikaty osobiste z walidacją adresu email	6 000 EUR	600 EUR
Certyfikaty osobiste z walidacją danych DN[29]	60 000 EUR	6 000 EUR
Certyfikaty SSL z walidacją domeny (DV)	200 000 EUR	600 EUR
Certyfikaty SSL z walidacją organizacji (OV)	400 000 EUR	15 000 EUR
Certyfikaty SSL z rozszerzoną walidacją (EV)	1 000 000 EUR	15 000 EUR
Certyfikaty do podpisywania kodu	60 000 EUR	6 000 EUR
Certyfikaty do podpisywania kodu z rozszerzoną walidacją (EV)	1 000 000 EUR	15 000 EUR
Certyfikaty wydawane w ramach Certum Global Services CA	Określona w umowach	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 typu, ograniczona jest do kwot nieprzekraczających podanych w Tab.9.1.

9.9. Odszkodowania

9.9.1. Odszkodowanie z tytułu odpowiedzialności cywilnej subskrybenta

Odszkodowanie z tytułu odpowiedzialności cywilnej subskrybenta wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.3. Warunki tej odpowiedzialności reguluje umowa zawarta z Asseco Data Systems S.A.

9.9.2. Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej

Odszkodowanie z tytułu odpowiedzialności cywilnej strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz. 9.6.4. 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.

[29] Maksymalna wartość gwarancji możliwa do uzyskania dla dedykowanych umów

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. 9.6.4 niniejszego dokumentu.

9.10. Okres obowiązywania Kodeksu oraz jego ważności

9.10.1. Okres obowiązywania

Niniejszy Kodeks Postępowania Certyfikacyjnego obowiązuje od momentu nadania mu statusu **aktualny** i opublikowania go w repozytorium CERTUM. Załączniki do Kodeksu obowiązują od momentu ich opublikowania w repozytorium.

9.10.2. Wygaśnięcie ważności

Niniejszy Kodeks Postępowania Certyfikacyjnego obowiązuje do momentu zastąpienia go nową wersją i utraty statusu **aktualny**.

9.10.3. Skutki wygaśnięcia ważności Kodeksu I okres przejściowy

Po wygaśnięciu ważności niniejszego Kodeksu Postępowania Certyfikacyjnego użytkownicy certyfikatów CERTUM wydanych w okresie jego obowiązywania są dalej ograniczeni zapisami niniejszego Kodeksu aż do momentu utraty ważności certyfikatu.

9.11. Indywidualne powiadamianie i komunikowanie się z użytkownikami

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.

9.12. Poprawki Kodeksu

Niniejszy Kodeks jest aktualizowany przynajmniej raz w roku. Zmiany w Kodeksie Postępowania Certyfikacyjnego mogą być wynikiem zauważonych błędów, uaktualnień oraz sugestii zainteresowanych stron.

CERTUM aktualizuje na bieżąco Kodeks Postępowania Certyfikacyjnego przy okazji każdej zmiany, jak miała miejsce w następujących dokumentach, o ile zmiany te wpływają na działalność CERTUM:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,
- Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates and
- Guidelines For The Issuance And Management Of Extended Validation Certificates.

9.12.1. Procedura wnoszenia poprawek

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,
- 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.

Decyzję o zaakceptowaniu zmian w Kodeksie Postępowania Certyfikacyjnego dotyczących wersji lub wydania podejmuje osoba zarządzająca PCC CERTUM.

9.12.2. Mechanizm powiadamiania oraz okres oczekiwania na komentarze

Po uprzednim poinformowaniu subskrybentów, zmianom mogą podlegać dowolne elementy Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich istotnych, rozważanych przez CERTUM zmianach w dokumencie jest przesyłana wszystkim zainteresowanym stronom w postaci informacji o miejscu udostępnienia 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.

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.

9.12.2.1. Okres oczekiwania na komentarze

Zainteresowane strony, w ciągu 10 dni roboczych od daty ich ogłoszenia mogą nadsyłać komentarze do zmian proponowanych przez CERTUM. Jeśli w wyniku nadesłanych komentarzy dokonane zostaną istotne modyfikacje 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. 1.5.4).

CERTUM może w pełni akceptować zgłaszane uwagi, akceptować ze zmianami lub odrzucać je po upływie terminu nadsyłania odpowiedzi na rozesłaną i opublikowaną ankietę.

9.12.3. Okoliczności wymagające zdefiniowania nowego identyfikatora polityki

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników usług certyfikacyjnych, osoba zarządzająca PCC CERTUM 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,

9.13. Warunki rozstrzygania 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. Skargi należy kierować w formie pisemnej na adres:

Asseco Data Systems S.A.
ul. Podolska 21
81-321 Gdynia

Skargi rozpatrywane są przez Dział Prawny spółki. Podlegają one pisemnemu rozpatrzeniu w terminie 21 dni. W przypadku braku rozstrzygnięcia sporu w terminie 45 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 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.

9.14. Prawa właściwe

9.14.1. Ciągłość postanowień

Postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego obowiązują od daty zaakceptowania przez osobę zarządzającą PCC CERTUM aż do momentu ich unieważnienia lub zastąpienia innymi. Modyfikacja starych postanowień lub wprowadzenie nowych odbywa się zgodnie z procedurą przedstawioną w rozdz. 9.12. 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.

9.14.2. 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.

9.15. Zgodność z obowiązującym prawem

Wszystkie działania CETUM są zgodne z prawem obowiązującym na terytorium Polski.

9.16. Przepisy różne

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

9.16.1. Kompletność warunków umowy

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

9.16.2. Cesja praw

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

9.16.3. 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. 9.6. Nie umieszczenie w umowie klauzuli o rozłączności postanowień może uczynić całą umowę niezgodną z prawem nawet, jeśli nie jest to intencją stron.

9.16.4. Klauzula wykonalności

Jakiekolwiek wyraźne zrzeczenie się lub brak natychmiastowej realizacji jakiegokolwiek prawa wynikającego z niniejszego Kodeksu Postępowania Certyfikacyjnego nie oznacza trwałego zrzeczenia się takiego prawa ani nie upoważnia do oczekiwania odstąpienia od jego wykonania.

9.16.5. Siła wyższa

CERTUM jest stroną zwolnioną od odpowiedzialności w przypadku wystąpienia nieprzewidzianego zdarzenia poza jej kontrolą, które uniemożliwia jej wykonywanie jej zobowiązań wynikających z postanowień zawartych w niniejszym Kodeksie Postępowania Certyfikacyjnego (patrz rozdz. 9.6). Tego typu zastrzeżenie musi być umieszczone w umowach zawieranych z subskrybentami oraz stronami ufającymi.

9.17. Postanowienia dodatkowe

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

Załącznik 1: Skróty i oznaczenia

CA urząd certyfikacji (ang. certification authority)

CAA autoryzacja urzędu certyfikacji (*ang. Certification Authority Authorization*)

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)

Załącznik 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 EV SSL – Certyfikat przeznaczony do weryfikacji serwerów i zestawiania połączeń SSL/TLS w sieci WEB, zawierający informacje określone w specyfikacji *Guidelines for the issuance and Management of Extended Validation Certificates* oraz weryfikowany zgodnie z wymaganiami tej specyfikacji.

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.

Dokument Potwierdzający – dokument, na którego podstawie CERTUM potwierdza uprawnienia subskrybenta do posługiwania się określoną nazwą występującą w certyfikacie. W przypadku nazw osób prawnych będą to upoważnienia, pełnomocnictwa, zaświadczenia o zatrudnieniu. W przypadku nazw domenowych będą to opłacone faktury lub oświadczenia otrzymane od rejestratora danej nazwy domenowej.

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.

Kwalifikowane źródła informacji Regularnie aktualizowane i publicznie dostępne rejestry zarządzane przez agencje rządowe dostarczające aktualnej i wiarygodnej informacji niezbędnej podczas konfrontowania jej z informacją pochodzącą z innego źródła. Zgłaszanie i zapisywanie takiej informacji w tego typu rejestrach wymagane jest przez odpowiednie przepisy prawa. Rejestry komercyjne także mogą być kwalifikowanymi źródłami informacji, o ile **są** regularnie aktualizowane, publicznie dostępne i ogólnie rozpoznawane jako niezawodne źródło informacji oraz spełniają następujące warunki:

- ✓ Informacje w nich zawarte zostały zweryfikowane także przez inne niezależne źródła informacji;
- ✓ Baza danych wyraźnie odróżnia informacje pozyskane we własnym zakresie od informacji otrzymanych od innych niezależnych źródeł informacji;
- ✓ Dostawca, właściciel, zarządzający bazą informuje jak często ma miejsce aktualizacja danych;
- ✓ Zmiany zachodzące w danych znajdują odzwierciedlenie w bazie nie później niż w przeciągu 12 miesięcy;

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=Asseco Data Systems 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.

Strona ufająca będąca beneficjentem gwarancji – Subskrybent usług certyfikacyjnych CERTUM, 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), Cerm.in.), ..., 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 Asseco Data Systems 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. Zamawiający 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*).

Załącznik 3: Minimalne wymagania dla algorytmów kryptograficznych i długości kluczy

1. Certyfikaty głównych urzędów certyfikacji

L.p.	Nazwa algorytmu szyfrowego	Certyfikaty wydane przed 31 grudniem 2010 r.	Certyfikaty wydane po 31 grudnia 2010 r.
1.	Algorytm skrótu	MD5 (nie zalecany), SHA-1	SHA-1[30], SHA-256, SHA-384 lub SHA-512
2.	RSA	1024	2048
3.	ECC	NIST P-256	NIST P-256

2. Certyfikaty pośrednich urzędów certyfikacji

L.p.	Nazwa algorytmu szyfrowego	Certyfikaty wydane przed 31 grudniem 2010 r.	Certyfikaty wydane po 31 grudnia 2010 r.
1.	Algorytm skrótu	SHA-1	SHA-1[37], SHA-256, SHA-384 lub SHA-512
2.	RSA	1024	2048
3.	ECC	NIST P-256	NIST P-256

3. Certyfikaty subskrybentów

L. p.	Nazwa algorytmu szyfrowego	Certyfikaty wydane przed 31 grudniem 2010 r.	Certyfikaty wydane po 31 grudnia 2010 r.	Certyfikaty wydane po 1 stycznia 2015 r.
1.	Algorytm skrótu	SHA-1	SHA-1[37], SHA-256, SHA-384 lub SHA-512	SHA-256, SHA-384 lub SHA-512
2.	RSA	1024 lub 2048 (uwaga – certyfikaty subskrybentów z kluczem 1024 RSA MUSZĄ wygasnąć przed 31 grudniem 2010 r.)	2048	2048
3.	ECC	NIST P-256	NIST P-256	NIST P-256

[30] SHA-1 powinien być używany jedynie do czasu wsparcia SHA-256 przez większość stron ufających na świecie

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.
V 3.0	19 października 2009 r.	Dostosowanie struktury Kodeksu do wymagań RFC 3647 oraz procesu wydawania certyfikatów typu EV SSL. Dopisanie Dodatków 3-6.
V 3.1	12 sierpnia 2010 r.	Aktualizacja wymagań dot. weryfikacji subskrybenta. Aktualizacja Załącznika nr 3.
V 3.2	09 lutego 2011 r.	Aktualizacja informacji związanych z weryfikacją statusu certyfikatu, modyfikacja okresów ważności certyfikatów oraz inne mniejsze zmiany.
V 3.3	07 października 2011 r.	Aktualizacja informacji związanych z Certum Code Signing CA oraz inne mniejsze zmiany dotyczące oferty certyfikatów. Dodatnie informacji o nowym certyfikacie Root Certum Trusted Network CA 2
V 3.4	19 kwietnia 2012	Aktualizacja logo CERTUM
V 3.5	29 maja 2013	Zamieszczenie deklaracji stosowania wymagań *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*. Aktualizacja informacji związanych z procedurą zawieszania certyfikatów niekwalifikowanych.
V 3.6	13 września 2013	Dodanie odnośnika do *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*. Aktualizacja informacji związanych z częstotliwością publikowania list CRL.
V 3.7	31 października 2014	Dodanie nowych urzędów pośrednich, dodanie nowych algorytmów podpisu, dodanie informacji odnośnie automatyzacji aktualizacji kluczy i re certyfikacji. Usunięcie usługi zawieszania certyfikatów, usunięcie Załącznika nr 3.
V 3.8	14 kwietnia 2015	Dodanie informacji o przetwarzaniu rekordów DNS autoryzujących urzędu certyfikacji (CAA).
v 3.9	01 lipiec 2015	Aktualizacja do wymagań *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates*
v 4.0	03 Listopad 2015	Dodanie urzędu głównego Certum Trusted Network CA EC oraz urzędów pośrednich Certum Digital Identification CA SHA2 oraz Certum Extended Validation Code Signing CA SHA2.

V 4.1	01 kwietnia 2016	Przeniesienie własności z Unizeto Technologies S.A. na Asseco Data System S.A. Dodanie informacji o zobowiązaniu do utrzymywania zaświadczenia certyfikacyjnego wydanego dla Unizeto Technologies przez Asseco Data System S.A.
V 4.2	22 sierpień 2016	Aktualizacja informacji o nowym urzędzie znacznika czasu Certum EV TSA SHA2
V 4.3	22 listopad 2016	Dodanie nowych urzędów pośrednich
V 4.4	01 luty 2017	Aktualizacja informacji dot. certyfikatów Code Signing. Uzupełnienie informacji o obowiązujące akty normatywne CA/Browser Forum.
V 4.5	13 marzec 2017	Modyfikacja weryfikacji nazw domenowych (punkt 3.2.6) poprzez usunięcie metody weryfikacji domeny polegającej na „umieszczeniu określonych danych na stronie głównej domeny".
V 4.6	21 kwietnia 2017	Modyfikacja weryfikacji nazw domenowych (punkt 3.2.6): zmiana katalogu do umieszczenia pliku o określonej nazwie na /.well-known/pki-validation
V 4.7	01 sierpnia 2017	Zmiana adresu Asseco Data Systems S.A. Dodanie pośredniego urzędu certyfikacji: WoSign DV SSL CA. Dodanie Identyfikatorów polityki certyfikacji.
V 4.8	11 sierpnia 2017	Dodanie Identyfikatorów polityki certyfikacji.
V 4.9	08 wrzesień 2017	Wdrożenie obsługi rekordów CAA.
V 5.0	30 listopada 2017	Dodanie pośrednich urzędów certyfikacji: TrustAsia DV SSL CA - C3, TrustAsia OV SSL CA - C3, TrustAsia EV SSL CA - C3, TrustOcean Certificate Authority
V 5.1	07 Marca 2018	Dostosowanie do wymagań Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates w wersji 1.5.4