Polityka Certyfikacji Kwalifikowanych Usług CERTUM

Wersja 4.1

Data: 23 grudzień 2016 r.

Status: aktualny

Asseco Data Systems S.A.
ul. Żwirki i Wigury 15
81-387 Gdynia
„Certum - Powszechne Centrum Certyfikacji”
ul. Bajeczna 13
71-838 Szczecin
https://certum.pl

Klauzula: Prawa Autorskie

Spis treści

1. Wstęp

Polityka Certyfikacji Kwalifikowanych Usług CERTUM określa szczegółowe rozwiązania (w tym techniczne i organizacyjne) stosowane przez jednostkę organizacyjną **CERTUM (pełna nazwa: CERTUM - Powszechne Centrum Certyfikacji)** świadczącą kwalifikowane usługi certyfikacyjne wskazujące sposób, zakres, oraz warunki tworzenia i stosowania certyfikatów (*Ustawa z dnia 5 września 2016r. o usługach zaufania oraz identyfikacji elektronicznej* - Dz.U. 2016 poz. 1579*, dalej w tekście zwanej Ustawą*).

Z polityką certyfikacji ściśle związany jest kodeks postępowania certyfikacyjnego. Kodeks postępowania certyfikacyjnego definiowany jest jako *deklaracja procedur stosowanych przez urząd certyfikacji w procesie wydawania certyfikatów*[1] oraz świadczenia dodatkowych usług certyfikacyjnych.

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 majątku 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 majątki 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.

1.1. Wprowadzenie

Przedstawiona w niniejszym dokumencie Polityka Certyfikacji opisuje zakres działania **CERTUM** świadczącego kwalifikowane usługi certyfikacyjne (działającego w ramach Asseco Data Systems S.A.) oraz związanych z nim **punktów sieci systemu rejestracji**, **subskrybentów**, jak również **stron ufających**. Określa także zasady świadczenia kwalifikowanych usług certyfikacyjnych, polegających na **wydawaniu kwalifikowanych certyfikatów** obejmującym rejestrację subskrybentów, certyfikację kluczy publicznych i aktualizację kluczy oraz certyfikatów, **unieważnianiu i zawieszaniu certyfikatów**, **weryfikowaniu statusu certyfikatów w trybie *on-line***, **walidacji danych**, wystawianiu **tokenów znaczników czasu**, **poświadczeń odbioru i przedłożenia** (w tym także **urzędowych poświadczeń odbioru** i **przedłożenia)**[2], **poświadczeń depozytowych, rejestrowych i repozytoryjnych** (o przechowywaniu podpisanych obiektów oraz ich udostępnianiu, modyfikowaniu i usuwaniu) oraz certyfikatów atrybutów. Kwalifikowane usługi certyfikacyjne świadczone są przez CERTUM zgodnie z zasadami **polityki certyfikacji**, określonymi w Rozporządzeniu Ministra Cyfryzacji z dnia 5 października 2016 r. *w sprawie krajowej infrastruktury zaufania.*

CERTUM działa zgodnie z prawem obowiązującym na terytorium Rzeczypospolitej Polskiej, zasadami obowiązującymi kwalifikowane podmioty świadczące usługi certyfikacyjne,

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

[2] Są to urzędowe poświadczenia odbioru dokumentów wystawiane na podstawie art. 16 ust. 3 ustawy z dnia 17 lutego 2005 r. o *informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. Nr 64, poz. 565). Patrz także: Słownik pojęć.

określonymi w *Ustawie o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016 poz. 1579), standardzie WebTrust*[3] oraz normami, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznymoraz w zgodzie z niniejszą Polityką Certyfikacji. Asseco Data Systems S.A., z siedzibą w Gdyni, przy ulicy Żwirki i Wigury 15, którego jednostką organizacyjną jest CERTUM, świadczące kwalifikowane usługi certyfikacyjne, jest kwalifikowanym podmiotem świadczącym usługi certyfikacyjne, w myśl ww. *Ustawy*, wpisanym do rejestru kwalifikowanych podmiotów świadczących usług certyfikacyjne pod numerem 1.

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

Kwalifikowana usługa znakowania czasem oraz kwalifikowana usługa walidacji jest świadczona zgodnie z wymaganiami Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

1.2. Nazwa dokumentu i jego identyfikacja

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

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

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

Dokument ten jest dostępny w postaci elektronicznej w serwisie internetowym urzędu certyfikacji dostępnym pod adresie http://www.certum.pl.

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

1.3. Uczestnicy Polityki Certyfikacji oraz zakres jej stosowania

Elementami infrastruktury CERTUM, świadczącego kwalifikowane usługi certyfikacyjne są:

- kwalifikowany urząd certyfikacji CERTUM QCA,
- kwalifikowany urząd znacznika czasu CERTUM QTSA,
- kwalifikowany urząd weryfikacji statusu certyfikatu CERTUM QOCSP,
- kwalifikowanej usługi walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych CERTUM QDVCS,

3 AICPA/CICA WebTrust Program for Certification Authorities

- urząd poświadczania odbioru i przedłożenia CERTUM QDA,
- urząd depozytów obiektów CERTUM QODA,
- urząd rejestrów i repozytoriów CERTUM QRRA,
- urzędu certyfikatów atrybutów CERTUM QACA,
- Główny Punkt Rejestracji (GPR),
- punkty rejestracji (PR),
- osoby potwierdzające tożsamość,
- subskrybenci,
- strony ufające.

1.3.1. Kwalifikowany urząd certyfikacji CERTUM QCA

W skład CERTUM świadczącego usługi kwalifikowane wchodzi jeden urząd certyfikacji **CERTUM QCA**, działający na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem certyfikacji **CERTUM QCA** sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Urząd certyfikacji **CERTUM QCA** świadczy usługi zgodnie zgodnie z *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016 poz. 1579)*, *Rozporządzeniem Ministra Cyfryzacji z dnia 5 października 2016r. (Dz.U. z 2016r. poz. 1632)* oraz normami, o których mowa w *Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016 r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.*.

.

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

Nazwa certyfikatu /zaświadczenia certyfikacyjnego	Identyfikator polityki certyfikacji
Certyfikaty kwalifikowane (przed 1 lipca 2016r.)	1.2.616.1.113527.2.4.1.1
Certyfikaty kwalifikowane (po 1 lipca 2016r.)	1.2.616.1.113527.2.4.1.1.11
Certyfikaty kwalifikowane (struktura eIDAS) karta	1.2.616.1.113527.2.4.1.1.12.1
Certyfikaty kwalifikowane (struktura eIDAS) HSM	1.2.616.1.113527.2.4.1.1.12.2
Zaświadczenia certyfikacyjne	2.5.29.32.0

1.3.2. Kwalifikowany urząd znacznika czasu CERTUM QTSA

Kolejnym elementem CERTUM, świadczącego kwalifikowane usługi certyfikacyjne, jest urząd znacznika czasu **CERTUM QTSA**. Urząd znacznika czasu działa na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem znacznika czasu **CERTUM QTSA** sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

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

Nazwa tokena	Identyfikator polityki certyfikacji
Kwalifikowany token znacznika czasu	1.2.616.1.113527.2.4.1.2

Kwalifikowane znaczniki czasu, wydawane zgodnie z polityką określoną w **Błąd! Nie można odnaleźć źródła odwołania.**, znajdują zastosowanie przede wszystkim do zabezpieczania długookresowych podpisów elektronicznych[4] oraz transakcji zawieranych w sieci globalnej.

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

Kwalifikowana usługa znakowania czasem jest świadczona zgodnie z wymaganiami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym eIDAS*.

1.3.3. Kwalifikowany urząd weryfikacji statusu certyfikatu CERTUM QOCSP

CERTUM, oprócz standardowego sposobu weryfikacji statusu certyfikatu lub zaświadczenia certyfikacyjnego w oparciu o pobieranie listy certyfikatów unieważnionych (CRL) udostępnia także usługę weryfikacji statusu certyfikatu lub zaświadczenia certyfikacyjnego w trybie *on-line*. Usługa ta świadczona jest przez kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem weryfikacji statusu certyfikatu CERTUM QOCSP sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Urząd weryfikacji statusu certyfikatu CERTUM QOCSP poświadcza statusy tylko certyfikatów kwalifikowanych i jedynie na moment udzielania odpowiedzi. Poświadczenia te wystawiane są zgodnie z zasadami określonymi w niniejszej polityce certyfikacji.

1.3.4. Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych CERTUM QDVCS

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** wystawia elektroniczne poświadczenia (nazywane dalej kwalifikowanymi tokenami walidacji) o ważności kwalifikowanego certyfikatu klucza publicznego, kwalifikowanego podpisu elektronicznego, kwalifikowanej pieczęci elektroniczne.

Tab. 3 Identyfikatory polityki certyfikacji akceptowane przez CERTUM QDVCS i umieszczane w tokenach walidacji

Nazwa tokena walidacji	Identyfikator polityki usługi
Kwalifikowany token walidacji kwalifikowanego podpisu elektronicznego[5]	1.2.616.1.113527.2.4.1.3.2.c[6]
Kwalifikowany token walidacji kwalifikowanej pieczęci elektronicznej	od 1.2.616.1.113527.2.4.1.3.5.c do 1.2.616.1.113527.2.4.1.3.9.c, 1.2.616.1.113527.2.4.1.3.11.c
Kwalifikowany token walidacji certyfikatu kwalifikowanego[7]	1.2.616.1.113527.2.4.1.3.4.c

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych CERTUM QDVCS działa na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem walidacji CERTUM QDVCS sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Kwalifikowane tokeny walidacji wydawane są zgodnie z politykami certyfikacji określonymi w Tab.3.

Kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych jest świadczona zgodnie z wymaganiami *Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym eIDAS*.

1.3.5. Urząd poświadczania odbioru i przedłożenia CERTUM QDA

Urząd poświadczania odbioru i przedłożenia CERTUM QDA wystawia **urzędowe poświadczenia odbioru** dokumentu elektronicznego, **urzędowe poświadczenia przedłożenia** dokumentu elektronicznego, **poświadczenia odbioru** dokumentu elektronicznego oraz **poświadczenia przedłożenia** dokumentu elektronicznego[8]. Poświadczenie to jest wystawiane na podstawie art. 16 ust. 3 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565)*. Urząd CERTUM QDA świadczy tą usługę tym podmiotom fizycznym, którzy chcą przekazać dokument elektroniczny, opatrzony bezpiecznym podpisem, dowolnemu odbiorcy, w tym także podmiotowi realizującemu zadania publiczne.

---

[5] Są to te podpisy elektroniczne, które są uznawane na terytorium określonego kraju za podpisy równoważne podpisowi własnoręcznemu

[6] Znaczek ‘c’ oznacza trzycyfrowy kod kraju zgodny z ISO 3166, np. dla Polski jest on równy 616.

[7] Są to te certyfikaty, które wydawane są przez zarejestrowane (np. kwalifikowane) urzędy certyfikacyjne, działające zgodnie z wymaganiami zdefiniowanymi w ustawie o podpisie elektronicznym, obowiązującej na terytorium określonego kraju i wykorzystywane podczas weryfikowania ważności podpisów elektronicznych równoważnych podpisowi własnoręcznemu.

[8] Patrz: Słownik pojęć

Tab. 4 Identyfikator polityk certyfikacji umieszczane w poświadczeniach wydawanych przez CERTUM QDA

Nazwa poświadczenia	Identyfikator polityki certyfikacji
Urzędowe poświadczenie odbioru	1.2.616.1.113527.2.4.1.4.1
Poświadczenie odbioru	1.2.616.1.113527.2.4.1.4.2
Urzędowe poświadczenie przedłożenia	1.2.616.1.113527.2.4.1.4.3
Poświadczenie przedłożenia	1.2.616.1.113527.2.4.1.4.4

Urząd CERTUM QDA działa na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem poświadczania odbioru i przedłożenia CERTUM QDA sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Poświadczenia odbioru i przedłożenia (w tym także urzędowe poświadczenia odbioru i przedłożenia) wydawane są zgodnie z politykami certyfikacji, określonymi w Tab.4.

Urząd CERTUM QDA wstawia poświadczenia odbioru (w tym także urzędowe poświadczenie odbioru), które jest dla podmiotu wysyłającego dokument dowodem, że urząd CERTUM QDA dostarczył dokument w to miejsce systemu teleinformatycznego odbiorcy, z którego będzie on dla niego dostępny oraz, że odbiorca odebrał, zapoznał się z treścią dokumentu elektronicznego oraz potwierdza jego poprawność jego treści.

Urząd CERTUM QDA wstawia poświadczenia przedłożenia (w tym także urzędowe poświadczenie przedłożenia), które jest dla podmiotu wysyłającego dokument dowodem, że urząd CERTUM QDA dostarczył dokument w to miejsce systemu teleinformatycznego odbiorcy, z którego będzie on dla niego dostępny. Urząd CERTUM QDA potwierdza fakt zdeponowania dokumentu, ale nie oznacza to jednocześnie potwierdzenia poprawności jego treści.

1.3.6. Urząd depozytów obiektów CERTUM QODA

Urząd **depozytów**[9] obiektów CERTUM QODA, uregulowany na poziomie krajowym, udostępnia subskrybentom usługę przechowywania, wydawania, pobierania oraz utrzymywania ważności dowodowej dowolnych elektronicznych obiektów danych, w tym w szczególności obiektów podpisanych za pomocą podpisu elektronicznego. Urząd CERTUM QODA traktuje składowane dane jako dowolny ciąg bitów, co oznacza, że nie wnika ani w ich strukturę (składnię), ani też w ich semantyczne znaczenie.

W odpowiedzi na żądanie depozytariusza o umieszczenie obiektu danych w depozycie, pobrania wpisu obiektu z depozytu lub wydanie obiektu z depozytu urząd CERTUM QODA wystawia następujące poświadczenia depozytowe:

- po umieszczeniu obiektu w depozycie - **poświadczenie wpisu obiektu do depozytu** ,
- po wydaniu obiektu z depozytu (wydanie odbywa się na podstawie przedłożonego wpisu) - **poświadczenie wydania obiektu z depozytu**; obiekty są usuwane z depozytu wraz z wpisem, na podstawie którego zostały wydane;
- po uwierzytelnionym wydaniu obiektu (wraz z poświadczeniami potwierdzającymi jego ważność dowodową) - **uwierzytelnione poświadczenie wydania obiektu z**

[9] Patrz: Słownik pojęć

depozytu; obiekty oraz wszystkie powiązane z nimi dane poświadczające ich ważność są usuwane z depozytu wraz z wpisem, na podstawie którego zostały wydane;

- po pobraniu wpisu z depozytu - **poświadczenie pobrania wpisu z depozytu**; wpisy nie są usuwane z depozytu;
- po uwierzytelnionym pobraniu wpisu z depozytu (wraz z poświadczeniami potwierdzającymi jego ważność dowodową) - **uwierzytelnione poświadczenie pobrania wpisu z depozytu**; wpis oraz potwierdzenia jego ważności nie są usuwane z depozytu;
- po pobraniu obiektu umieszczonego w depozycie (w oparciu o przedstawione wpisy) - **poświadczenie pobrania obiektu z depozytu**; obiekty nie są usuwane z depozytu;
- po uwierzytelnionym pobraniu obiektu umieszczonego w depozycie (w oparciu o przedstawiony wpis) wraz ze wszystkimi powiązanymi z nim danymi poświadczającymi jego ważność - **uwierzytelnione poświadczenie pobrania obiektu z depozytu**; obiekt oraz potwierdzenia jego ważności nie są usuwane z depozytu.

Tab. 5 Identyfikatory polityk certyfikacji umieszczane w poświadczeniach wydawanych przez CERTUM QODA

Nazwa poświadczenia	Identyfikator polityki certyfikacji
Poświadczenie wpisu obiektu do depozytu	1.2.616.1.113527.2.4.1.5.1
Poświadczenie wydania obiektu z depozytu	1.2.616.1.113527.2.4.1.5.2
Uwierzytelnione poświadczenie wydania obiektu z depozytu	1.2.616.1.113527.2.4.1.5.3
Poświadczenie pobrania wpisu z depozytu	1.2.616.1.113527.2.4.1.5.4
Uwierzytelnione poświadczenie pobrania wpisu z depozytu	1.2.616.1.113527.2.4.1.5.5
Poświadczenie pobrania obiektu z depozytu	1.2.616.1.113527.2.4.1.5.6
Uwierzytelnione poświadczenie pobrania obiektu z depozytu	1.2.616.1.113527.2.4.1.5.7

Urząd CERTUM QODA działa na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem depozytów obiektów CERTUM QODA sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Poświadczenia wpisu obiektów do depozytu, poświadczenia wydania obiektów z depozytu, uwierzytelnione poświadczenia wydania obiektów z depozytu, poświadczenie pobrania wpisów z rejestru, uwierzytelnione poświadczenia pobrania wpisów z rejestru, poświadczenia pobrania obiektów z depozytu i uwierzytelnione poświadczenia pobrania obiektów z depozytu wydawane są zgodnie z politykami certyfikacji, określonymi w Tab.5.

1.3.7. Urząd rejestrów i repozytoriów CERTUM QRRA

Urząd **rejestrów** i **repozytoriów**[10] CERTUM QRRA, uregulowany na poziomie krajowym, umożliwia rejestrowanie obiektów danych z opcjonalną możliwością umieszczenia ich w repozytorium, pobieranie wpisów z rejestru i obiektów z repozytorium, ich modyfikowanie oraz utrzymywanie ich ważności dowodowej; obiekty te mogą być w szczególności opatrzone podpisem elektronicznym, spełniającym wymagania *Ustawy o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016r., poz. 1579)*. Jeśli z faktem zarejestrowania obiektu danych w rejestrze związane jest także umieszczenie obiektu w repozytorium, to urząd CERTUM QRRA przed umieszczeniem obiektu w repozytorium sprawdza także poprawność struktury obiektu oraz opcjonalnie (tam, gdzie jest to możliwe) jego semantykę (np. poprawność typów danych).

Rejestry i repozytoria zarządzane przez kwalifikowany urząd rejestrów i repozytoriów CERTUM QRRA mogą być podzielone tematycznie.

W odpowiedzi na żądanie umieszczenia wpisu w rejestrze i opcjonalnie obiektów w repozytorium, pobrania wpisu z rejestru lub obiektu z repozytorium, modyfikacji wpisu lub obiektu danych, urząd CERTUM QODA wystawia następujące poświadczenia rejestrowe lub repozytoryjne:

- po umieszczeniu wpisu w rejestrze oraz opcjonalnie obiektu w repozytorium – odpowiednio **poświadczenie umieszczenia wpisu w rejestrze** oraz **poświadczenie umieszczenia obiektu w repozytorium**;
- po pobraniu wpisów z rejestru - **poświadczenie pobrania wpisów z rejestru**; wpisy nie są usuwane z rejestru;
- po uwierzytelnionym pobraniu wpisu z rejestru (wraz z poświadczeniami potwierdzającymi jego ważność dowodową) - **uwierzytelnione poświadczenie pobrania wpisu z rejestru**; wpis oraz potwierdzenia jego ważności nie są usuwane z rejestru;
- po pobraniu obiektów umieszczonych w repozytorium (pobranie odbywa się na podstawie przedłożonych wpisów do rejestru) - **poświadczenie pobrania obiektu z repozytorium**; pobrane obiekty nie są usuwane z repozytorium;
- po uwierzytelnionym pobraniu obiektu z repozytorium (wraz z poświadczeniami potwierdzającymi jego ważność dowodową) - **uwierzytelnione poświadczenie pobrania obiektu z repozytorium**; obiekt oraz potwierdzenia jego ważności nie są usuwane z repozytorium;
- po zmodyfikowaniu wpisu w rejestrze - **poświadczenie modyfikacji wpisu w rejestrze**; modyfikowany wpis jest nadal przechowywany w rejestrze;
- po zmodyfikowaniu obiektu w repozytorium - **poświadczenie modyfikacji obiektu w repozytorium**; modyfikowany obiekt jest nadal przechowywany w rejestrze.

[10] Patrz: Słownik pojęć

Tab. 6 Identyfikatory polityk certyfikacji umieszczane w poświadczeniach wydawanych przez CERTUM QRRA

Nazwa poświadczenia rejestrowego lub repozytoryjnego	Identyfikator polityki certyfikacji
Poświadczenie umieszczenia wpisu w rejestrze	1.2.616.1.113527.2.4.1.6.1
Poświadczenie umieszczenia obiektu w repozytorium	1.2.616.1.113527.2.4.1.6.2
Poświadczenie pobrania wpisów z rejestru	1.2.616.1.113527.2.4.1.6.3
Uwierzytelnione poświadczenie pobrania wpisu z rejestru	1.2.616.1.113527.2.4.1.6.4
Poświadczenie pobrania obiektu z repozytorium	1.2.616.1.113527.2.4.1.6.5
Uwierzytelnione poświadczenie pobrania obiektu z repozytorium	1.2.616.1.113527.2.4.1.6.6
Poświadczenie modyfikacji wpisu w rejestrze	1.2.616.1.113527.2.4.1.6.7
Poświadczenie modyfikacji obiektu w repozytorium	1.2.616.1.113527.2.4.1.6.7

Urząd CERTUM QRRA działa na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad urzędem rejestrów i repozytoriów CERTUM QRRA sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Poświadczenia umieszczenia wpisów w rejestrze, poświadczenia umieszczenia obiektów w repozytorium, poświadczenia pobrania wpisów z rejestru, uwierzytelnione poświadczenia pobrania wpisów z rejestru, poświadczenia pobrania obiektów z repozytorium, uwierzytelnione poświadczenia pobrania obiektów z repozytorium, poświadczenia modyfikacji wpisów w rejestrze oraz poświadczenia modyfikacji obiektów w repozytorium wydawane są zgodnie z politykami certyfikacji, określonymi w Tab.6.

1.3.8. Urząd certyfikatów atrybutów CERTUM QACA

Urząd certyfikatów atrybutów **CERTUM QACA**, uregulowany na poziomie krajowym, wystawia certyfikaty atrybutów użytkownikom końcowym, po uprzednim wiarygodnym potwierdzeniu możliwości przypisania określonego atrybutu tym użytkownikom.

*Użytkownik końcowy, któremu urząd certyfikatów atrybutów **CERTUM QACA** wystawił certyfikat atrybutów, nie ma prawa wystawiania żadnych certyfikatów atrybutów. Oznacza to, że nie zezwala się na samodzielne przekazywanie przez użytkownika końcowego posiadanych przez siebie praw (i potwierdzonych przez urząd certyfikatów atrybutów **CERTUM QACA**) innym osobom.*

Urząd certyfikatów atrybutów **CERTUM QACA** działa na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne. Nadzór nad kwalifikowanym urzędem certyfikatów atrybutów **CERTUM QACA** sprawuje minister cyfryzacji lub wskazany przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Urząd certyfikatów atrybutów **CERTUM QACA** wydaje, udostępnia i unieważnia certyfikaty atrybutów zgodnie ze zdefiniowanymi politykami certyfikacji atrybutów. Polityki te są zbiorem zasad, które określają zakres przydatności certyfikatu atrybutów w różnych środowiskach i/lub do różnych klas zastosowań o takich samych wymaganiach bezpieczeństwa.

Tab. 7 Identyfikatory polityk certyfikacji umieszczane przez CERTUM QACA w certyfikatach atrybutów

Nazwa polityki certyfikacji atrybutów	Identyfikator polityki certyfikacji
Standardowa polityka certyfikacji atrybutów	1.2.616.1.113527.2.4.1.7.1
Polityka certyfikacji atrybutów na potrzeby autoryzacji	1.2.616.1.113527.2.4.1.7.2
Dedykowane polityki certyfikacji atrybutów	1.2.616.1.113527.2.4.1.7.3.x

Urząd CERTUM QACA wydaje certyfikaty atrybutów w oparciu o trzy predefiniowane grupy polityk certyfikacji atrybutów (Tab.7). Dwie pierwsze z polityk mają przypisany stały identyfikator. Ostatnia z polityk jest rodziną polityk, których zastosowania zależą od aktualnych potrzeb. Ich opisy, zakresy zastosowań oraz przypisane im identyfikatory są umieszczane w repozytorium urzędu certyfikacji CERTUM. Identyfikatory tych polityk budowane są w oparciu o wzorzec przedstawiony w Tab.7, w którym znak '*x*' oznacza kolejny numer polityki w ramach dedykowanego zbioru polityk certyfikacji atrybutów..

1.3.9. Punkty rejestracji oraz punkty potwierdzania tożsamości i atrybutów

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

Lista aktualnie autoryzowanych punktów rejestracji i punktów potwierdzania tożsamości dostępna jest w serwisie internetowym urzędu certyfikacji CERTUM dostępnym pod adresem:

http://www.certum.pl

1.3.10. Użytkownicy końcowi

1.3.10.1. Subskrybenci

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

Organizacje pragnące uzyskać dla swoich pracowników certyfikaty, tokeny lub poświadczenia wydane przez CERTUM mogą to uczynić poprzez swoich upoważnionych

przedstawicieli. Z kolei subskrybent indywidualny występuje o certyfikat, tokeny lub poświadczenia w swoim imieniu.

1.3.10.2. Strony ufające

Stroną ufającą, korzystającą z usług CERTUM jest dowolny podmiot, który podejmuje decyzję o akceptacji kwalifikowanego podpisu elektronicznego lub innego uwierzytelnionego poświadczenia elektronicznego (w tym certyfikatu atrybutów) i która może być w jakikolwiek sposób uzależniona od:

- ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a należącym do niego kluczem publicznym, potwierdzonym certyfikatem przez kwalifikowany urząd certyfikacji **CERTUM QCA**, lub
- powiązania podpisu elektronicznego z tokenem znacznika czasu, wydanym przez kwalifikowany urząd znacznika czasu CERTUM QTSA, lub
- potwierdzenia aktualnego statusu certyfikatu wystawionego przez kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, lub
- tokena walidacji wystawionego przez kwalifikowaną usługę **CERTUM QDVCS**, lub
- poświadczenia odbioru lub przedłożenia (w tym także urzędowego poświadczenia odbioru lub przedłożenia), wystawionego przez urząd **CERTUM QDA**, lub
- poświadczenia depozytowego, wystawionego przez urząd **CERTUM QODA**, lub
- poświadczenia rejestrowego lub poświadczenia repozytoryjnego, wystawionego przez urząd **CERTUM QRRA**, lub
- ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a certyfikatem atrybutów wystawionym subskrybentowi, wydanym przez urząd certyfikatów atrybutów **CERTUM QACA**.

1.4. Zakres stosowania certyfikatów i zaświadczeń certyfikacyjnych

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

Zaświadczenia certyfikacyjne wydawane są krajowemu urzędowi certyfikacji, działającemu w imieniu i z upoważnienia ministra cyfryzacji urzędom certyfikacji lub na potrzeby procesu wymiany kluczy urzędu certyfikacji.

1.5. Zakres stosowania znaczników czasu

Urząd znacznika czasu **CERTUM QTSA** wystawia tokeny znacznika czasu, które zgodnie z *Ustawą* wywołują w szczególności skutki prawne daty pewnej w rozumieniu przepisów *Kodeksu cywilnego (Art.81, §2 pkt. 3)*. Głównym zastosowaniem znaczników czasu jest znakowanie czasem bezpiecznych podpisów elektronicznych w przypadku ich długookresowej ważności. Znaczniki czasu wystawiane przez urząd znacznika czasu mogą być używane także w dowolnych innych przypadkach, wymagających porównywalnej jakości usługi znakowania czasem.

1.6. Zakres stosowania poświadczeń statusu certyfikatu

Urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** wystawia tokeny statusu kwalifikowanego certyfikatu klucza publicznego oraz zaświadczeń certyfikacyjnych wystawianych przez kwalifikowane urzędy certyfikacji zgodnie z *Rozporządzeniem eIDAS*. Tokeny te są wystawiane po uprzednim sprawdzeniu, czy certyfikat lub zaświadczenie certyfikacyjne jest umieszczone na liście unieważnionych certyfikatów lub zaświadczeń.

1.7. Zakres stosowania walidacji

Kwalifikowane tokeny walidacji są wystawiane przez urząd **CERTUM QDVCS** jedynie dla kwalifikowanych certyfikatów klucza publicznego, kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

Tokeny walidacji powinny być gromadzone przez podmioty w celu rozstrzygania ewentualnych sporów powstałych na tle rozbieżności w ocenie przez różne strony ważności kwalifikowanych podpisów lub innych dowodów elektronicznych.

1.8. Zakres stosowania poświadczeń odbioru i przedłożenia

Urzędowe poświadczenie odbioru lub przedłożenia dokumentu stanowi elektroniczny dowód przesłania przez nadawcę dokumentu elektronicznego podmiotowi realizującemu zadania publiczne, określone w *Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565)* oraz w *Ustawie z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz.U. 2016 poz. 23 z późn. zm.).*

Podobne zastosowanie mają poświadczenia odbioru lub przedłożenia dokumentu elektronicznego, których adresatem nie jest podmiot realizujący zadania publiczne.

1.9. Zakres stosowania poświadczeń depozytowych, rejestrowych i repozytoryjnych

Poświadczenia depozytowe stanowią elektroniczny dowód złożenia przez nadawcę dowolnego obiektu w depozycie, zarejestrowania tego obiektu, pobrania wpisu lub obiektu z depozytu, a także wydania obiektu z depozytu. Na żądanie, poświadczenie depozytowe może zawierać inne dowody powiązane z obiektem danych, które pozwalają na pobranie lub wydanie obiektu z depozytu w stanie, w jakim został złożony w depozycie.

Poświadczenia rejestrowe i repozytoryjne wydawane są odpowiednio po każdym umieszczeniu wpisu w rejestrze, pobraniu lub zmodyfikowaniu tego wpisu oraz po umieszczeniu obiektu w repozytorium i pobraniu lub zmodyfikowaniu tego obiektu. Poświadczenia rejestrowe stanowią dowód, że na rejestrze zostały wykonane operacje wpisu, pobrania lub zmodyfikowania ich zawartości. Z kolei poświadczenia repozytoryjne są dowodem na wykonanie (na żądanie nadawcy) operacji umieszczenia obiektu w repozytorium, jego pobrania lub zmodyfikowania, a także zgodności składni i semantyki obiektu z wymaganiami określonymi dla danego repozytorium. Moc dowodowa wpisów oraz obiektów umieszczanych w rejestrach i

repozytoriach jest utrzymywana na stałym poziomie od momentu ich umieszczenia w rejestrze i repozytorium.

Poświadczenia depozytowe, rejestrowe i repozytoryjne są wiarygodnymi dowodami, które można wykorzystywać w trakcie rozstrzygania sporów pomiędzy stronami, w tym także sporów cywilno-prawnych lub sądowych.

1.10. Zakres stosowania certyfikatów atrybutów

Certyfikaty atrybutów wydawane przez urząd certyfikatów atrybutów CERTUM QACA mogą być jawnie powiązane z kwalifikowanymi lub niekwalifikowanymi certyfikatami klucza publicznego, stanowiąc uwierzytelnione dodatkowe atrybuty podpisu elektronicznego lub uwierzytelnione prawa podmiotu podpisującego. Niezależnie od tego, czy certyfikat atrybutów jest lub nie jest jawnie powiązany z certyfikatami klucza publicznego (kwalifikowanymi lub niekwalifikowanymi), certyfikaty atrybutów mogą być stosowane w procesie autoryzacji praw podmiotu podpisującego lub podmiotu zlecającego wykonanie czynności podlegającej kontroli, np. prawa posługiwania się nazwą zastrzeżoną.

Zakres stosowania certyfikatów atrybutów zależy od typu atrybutu i może wynikać z odpowiednich przepisów prawa lub jest określony przez stronę ufającą, która może zdefiniować typy atrybutów niezbędnych w kontaktach z systemami lub aplikacjami udostępnianymi przez tą stronę.

1.11. Kontakt

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

Asseco Data Systems S.A.

Certum - Powszechne Centrum Certyfikacji
71-838 Szczecin, ul. Bajeczna 13
E-mail: info@certum.pl

2. Postanowienia ogólne

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

2.1. Zobowiązania

2.1.1. Zobowiązania CERTUM i punktów rejestracji

CERTUM, świadczące kwalifikowane usługi certyfikacyjne, zobowiązuje się do:

- przedsięwzięcia stosownych kroków, mających na celu weryfikację informacji identyfikującej tożsamość subskrybenta wniosków składanych przez strony;
- wydania, unieważnienia kwalifikowanego certyfikaty na podstawie prawidłowego wniosku oraz powiadomienia wnioskodawcy o realizacji lub odrzucenia wniosku;
- unieważnienie certyfikatu w przypadku gdy zawartość certyfikatu zdezaktualizowała się lub klucz prywatny związany z certyfikatem został skompromitowany (ujawniony, zgubiony, itp.);
- udostępnieniu informacji o wydaniu (gdy subskrybent wyrazi na to zgodę), unieważnieniu lub zawieszeniu kwalifikowanego certyfikatu;
- zapewnienia właściwej długości i struktury certyfikowanych kluczy oraz unikalności (w ramach swojej domeny) nazw wyróżnionych (DN) stosowanych w certyfikatach;
- respektowanie praw subskrybentów i stron ufających wynikających z przepisów prawa, uregulowań CERTUM i zawartych umów;
- zapewnienia należytej ochrony danych osobowych subskrybenta;
- stosowania co najmniej takich samych parametrów algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w dokumencie *ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites* .

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

- przestrzegania procedur potwierdzania tożsamości osób wnioskujących o wydanie/unieważnienie certyfikatu oraz wydawania koniecznych tokenów zgłoszenia certyfikacyjnego, upoważniających do skorzystania z określonej usługi CERTUM,
- podporządkowania się zaleceniom CERTUM,
- ochrony kluczy prywatnych operatorów punktu rejestracji i punktów potwierdzania tożsamości;
- nie używania kluczy prywatnych operatorów do innych celów niż tych, które określono w niniejszej Polityce Certyfikacji.

2.1.2. Zobowiązania urzędu znacznika czasu

Urząd znacznika czasu **CERTUM QTSA** gwarantuje, że świadczy usługi znacznika czasu zgodnie z wymaganiami *Rozporządzenia eIDAS, normy ETSI EN 319-421* oraz w niniejszej Polityce Certyfikacji.

W szczególności CERTUM QTSA:

- stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania czasem,
- stosuje co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w dokumencie *ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites*,
- określa przynajmniej jeden algorytm funkcji skrótu, który może być stosowany do obliczenia wartości skrótu z danych, które podlegają oznakowaniu czasem,
- gwarantuje, że czas UTC, który zostaje umieszczony w tokenie znacznika czasu, podawany jest z dokładnością do 1 sekundy.

2.1.3. Zobowiązania urzędu weryfikacji statusu certyfikatu i walidacji danych

Urzędy weryfikacji statusu certyfikatów **CERTUM QOCSP** oraz walidacji **CERTUM QDVCS** gwarantują, że świadczą swoje usługi zgodnie z wymaganiami określonymi w *Rozporządzeniu eIDAS* oraz w niniejszej Polityce Certyfikacji dla usług znacznika czasu oraz dodatkowo:

- stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania statusem certyfikatu, zaświadczenia certyfikacyjnego lub walidowanymi danymi,
- weryfikuje ważność podpisów kwalifikowanych złożonych zgodnie z wymaganiami określonymi w *Rozporządzeniu eIDAS*,
- usługa **CERTUM QDVCS** poświadcza wykonania walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

2.1.4. Zobowiązania urzędu poświadczania odbioru i przedłożenia

Urząd poświadczania odbioru i przedłożenia **CERTUM QDA** gwarantuję, że świadczy swoje usługi zgodnie z wymaganiami określonymi w Rozporządzeniach wydanych na podstawie art. 16 ust. 3 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).*

W szczególności CERTUM QDA:

- stosuje takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość fałszowania poświadczeń odbioru lub przedłożenia (w tym także urzędowych poświadczeń odbioru lub przedłożenia),
- stosuje co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites,

- wystawia poświadczenie odbioru (w tym także urzędowe poświadczenie odbioru) dopiero po poprawnym zweryfikowaniu danych uwierzytelniających otrzymany dokument elektroniczny, jego formalnej poprawności oraz po dostarczeniu go w to miejsce systemu teleinformatycznego, z którego jest on dostępny dla odbiorcy,
- wystawia poświadczenie przedłożenia (w tym także urzędowe poświadczenie przedłożenia) dopiero po poprawnym zweryfikowaniu danych uwierzytelniających otrzymany dokument elektroniczny oraz po dostarczeniu go do systemu teleinformatycznego odbiorcy; poświadczenie nie jest potwierdzeniem formalnej poprawności potwierdzanego dokumentu.

2.1.5. Zobowiązania urzędów depozytów, rejestrów i repozytoriów

Urzędy depozytów obiektów **CERTUM QODA** oraz rejestrów i repozytoriów **CERTUM QRRA** gwarantują, że świadczą swoje usługi zgodnie z wymaganiami określonymi m.in. w Rozporządzeniach wydanych na podstawie art.5, ust.2a, 2b i 2c *Ustawy z dnia 14 lipca 1983 r. o narodowym zasobie archiwalnym i archiwach*, w Ustawie o podatku od towarów i usług (art. 106 m i dalsze) Dz.U z 2016, poz. 710 także z wymaganiami nakładanymi na rejestry publiczne, określonymi w *Ustawie z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz.U. nr 64, poz. 565).*

W szczególności:

- urzędy CERTUM QODA i CERTUM QRRA stosują takie procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość fałszowania wystawianych poświadczeń depozytowych, rejestrowych i repozytoryjnych,
- urzędy CERTUM QODA i CERTUM QRRA stosują co najmniej takie same parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określone w „ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites",
- urzędy CERTUM QODA i CERTUM QRRA udostępniają odpowiednio depozyty i rejestry oraz repozytoria tylko upoważnionym do tego podmiotom,
- urząd CERTUM QRRA umieszcza w repozytoriach tylko te obiekty danych, które zostały pozytywnie zwalidowane na zgodność z wymaganiami określonego dla danego repozytorium,
- urzędy CERTUM QODA i CERTUM QRRA zapewniają przechowywanym wpisom i obiektom taką samą ważność dowodową, jak w momencie ich złożenia w depozycie lub repozytorium;
- urząd CERTUM QODA zapewnia pełne usunięcie obiektu z depozytu w momencie zażądania przez depozytariusza jego wydania.

2.1.6. Zobowiązania urzędu certyfikatów atrybutów

Urząd certyfikatów atrybutów **CERTUM QACA** gwarantuje, że świadczy swoje usługi zgodnie z wymaganiami określonymi w niniejszej Polityce Certyfikacji , a także z wymaganiami określonymi w RFC 3281 i RFC 4476.

Dodatkowo urząd certyfikatów atrybutów **CERTUM QACA**:

- weryfikuje prawo do posługiwania się atrybutem lub atrybutami przez wnioskującego o wydanie certyfikatu atrybutów; dotyczy to także przypadku, gdy wpisanie atrybutu do certyfikatu atrybutów wiąże się z przekazaniem uprawnień, które posiada podmiot uprawniający (np. podmiot, który przekazuje swoje pełnomocnictwa),
- akceptuje potwierdzenie prawa do posługiwania atrybutem lub atrybutami, o których mowa wyżej, wystawione w punkcie potwierdzania atrybutów lub w biurze notarialnym,
- udostępnienia odbiorcom usług certyfikacyjnych listy atrybutów, które mogą być umieszczane w uwierzytelnionych certyfikatach atrybutów,
- udostępnia listę dedykowanych polityk certyfikacji dostosowanych do potrzeb strony ufającej.

2.2. Zobowiązania użytkowników końcowych

2.2.1. Zobowiązania subskrybenta

Subskrybent zobowiązuje się do:

- używania certyfikatów i zaświadczeń tylko zgodnie z ich przeznaczeniem,
- używania certyfikatów i zaświadczeń tylko w ich okresie ważności,
- podjęcia wszelkie środki ostrożności w celu bezpiecznego przechowywania klucza prywatnego z certyfikowanej pary kluczy,
- w przypadku konieczności unieważnienia certyfikatu – do niezwłocznego zgłoszenia tego faktu w CERTUM.

2.2.2. Zobowiązania stron ufających

Strona ufająca zobowiązana jest do:

- rzetelnej weryfikacji każdego podpisu lub poświadczenia elektronicznego umieszczonego na dokumencie, w certyfikacie kwalifikowanym, w tokenie znacznika, w tokenie statusu certyfikatu, w tokenie walidacji, w poświadczeniu odbioru lub przedłożenia (w tym także w urzędowym poświadczeniu odbioru lub przedłożenia) lub certyfikacie atrybutów, który do niej dotrze,
- uznania podpisu lub poświadczenia elektronicznego za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis lub poświadczenie są ważne lub uzyskany wynik weryfikacji jest negatywny.

2.3. Odpowiedzialność CERTUM

CERTUM, świadczące kwalifikowane usługi certyfikacyjne, ponosi odpowiedzialność za skutki działań urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, usługi walidacji kwalifikowanej **CERTUM QDVCS**, urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA**, urzędu rejestrów i repozytoriów **CERTUM QRRA** oraz urzędu certyfikatów atrybutów **CERTUM QACA**, Głównego Punktu Rejestracji, punktów systemu rejestracji i innych osób potwierdzających tożsamość w zakresie określonym w zawartych umowach.

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

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

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

2.4. Odpowiedzialność finansowa

Asseco Data Systems S.A. posiada ubezpieczenie odpowiedzialności cywilnej zgodne z wymaganiami *Rozporządzenia Ministra Finansów z dnia 16 grudnia 2003 r. w sprawie obowiązkowego ubezpieczenia odpowiedzialności cywilnej kwalifikowanego podmiotu świadczącego usługi certyfikacyjne*.

Odpowiedzialność finansowa Asseco Data Systems S.A., w imieniu której CERTUM świadczy kwalifikowane usługi, w stosunku do jednego zdarzenia wynosi równowartość w złotych 250.000 Euro, ale nie więcej niż 1.000.000 Euro w odniesieniu do wszystkich takich zdarzeń. Odpowiedzialność finansowa dotyczy okresów 12-miesięcznych zgodnych z rokiem kalendarzowym.

2.5. Akty prawne i rozstrzyganie sporów

2.5.1. Obowiązujące akty prawne

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

2.5.2. Rozstrzyganie sporów

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

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

2.6. Opłaty

Za świadczone usługi CERTUM pobiera opłaty. Wysokości opłat, oraz rodzaje usług objętych opłatami są publikowane w cenniku, dostępnym w serwisie internetowym urzędu certyfikacji CERTUM dostępnym pod adresem:

http://www.certum.pl

2.7. Repozytorium urzędu certyfikacji i publikacje

2.7.1. Informacje publikowane przez CERTUM

Wszystkie dokumenty publikowane przez **CERTUM** dostępne są w repozytorium serwisu internetowego urzędu certyfikacji dostępnym pod adresem:

http://www.certum.pl

Są to następujące informacje:

- Polityka Certyfikacji,
- Kodeks Postępowania Certyfikacyjnego,
- wzory umów,
- nieprzeterminowane i nieunieważnione zaświadczenia certyfikacyjne**,**
- listy bezpiecznych urządzeń, rekomendowanych przez **CERTUM**,
- listy autoryzowanych punktów systemu rejestracji i innych osób potwierdzających tożsamość i atrybuty,
- listy certyfikatów unieważnionych (CRL),
- informacje pomocnicze, np. ogłoszenia.

2.7.2. Częstotliwość publikacji

Wymienione poniżej publikacje CERTUM są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji oraz Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług (patrz rozdz.8),
- zaświadczenia certyfikacyjne urzędów świadczących usługi certyfikacyjne – każdorazowo, gdy nastąpi emisja nowych zaświadczeń,
- listy certyfikatów unieważnionych i zawieszonych w ciągu 1 godz. od zgłoszenia,
- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.7.3. Dostęp do publikacji

Wszystkie dokumenty publikowane przez CERTUM są dostępne w repozytorium serwisu internetowego dostępnym pod adresem: http://www.certum.pl/repozytorium.

2.8. Audyt

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**). Audyt zewnętrzny może być przeprowadzony na wniosek ministra cyfryzacji w trybie *art. 31 Ustawy w związku z art. 20 pkt.1 i 17.4 Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (w skrócie Rozporządzeniem eIDAS) z dnia 23 czerwca 2014 roku, zastępującego Dyrektywę 1999/93/EC.*

2.9. Ochrona informacji

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 *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych.*

Asseco Data Systems S.A. gwarantuje, że stronom trzecim udostępniane są tylko te informacje, które są publicznie dostępne w certyfikacie i na których opublikowanie zgodę wyraził subskrybent certyfikatu.

2.10. 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.

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

2.11. Synchronizacja czasu

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

3. Identyfikacja i uwierzytelnianie

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

3.1. Rejestracja subskrybenta urzędu certyfikacji CERTUM QCA

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

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

- wypełnić elektroniczny wniosek o wydanie kwalifikowanego certyfikatu, stosowny do żądanego rodzaju certyfikatu (za pośrednictwem strony WWW lub poprzez punkt systemu rejestracji),
- określić rodzaj kwalifikowanego certyfikatu (w imieniu własnym, jako przedstawiciel innej osoby fizycznej, prawnej lub organu władzy publicznej),

Wnioskodawca w trakcie procesu rejestracji informowany jest na piśmie lub w formie dokumentu elektronicznego, w sposób jasny i powszechnie zrozumiały o:

- dokumentach regulujących świadczenie kwalifikowanych usług - Polityka Certyfikacji oraz niniejszy dokument,
- warunkach użytkowania usług kwalifikowanych,
- zobowiązaniach subskrybenta,
- informacjach dla stron ufających,
- informacjach o sposobie archiwizacji danych,
- zakresie i ograniczeniach odpowiedzialności Asseco Data Systems S.A.,
- zakresie i ograniczeniach świadczenia usług kwalifikowanych,
- zgodności świadczonych usług z Rozporządzeniem eIDAS i Ustawą
- sposobie rozpatrywania skarg i sporów,
- sposobie audytowania usług kwalifikowanych,
- informacjach kontaktowych do Certum,
- dostępności usług,
- o procedurze zgłaszania żądań unieważnienia kwalifikowanego certyfikatu,
- subskrybent jest zobowiązany potwierdzić zapoznanie się z powyższą informacją poprzez złożenie własnoręcznego podpisu pod treścią *Umowy z Subskrybentem o świadczenie usług certyfikacyjnych*. Podpisanie *Umowy* oznacza także, że:

- subskrybent wyraża zgodę na przetwarzanie przez Asseco Data Systems S.A. jego danych osobowych dla potrzeb niezbędnych dla procesu certyfikacji,
- subskrybent oświadcza, że informacje podane przez niego są zgodne z prawdą i zostały podane dobrowolnie,
- subskrybent, występując z wnioskiem o wydanie certyfikatu, jest świadom, jaka informacja umieszczana jest w certyfikacie i wyraża zgodę na jej upublicznienie.

Rejestracja subskrybentów występujących jako przedstawiciele innej osoby fizycznej, prawnej lub organu władzy publicznej przebiega podobnie jak w przypadku rejestracji subskrybentów indywidualnych.

3.1.1. Nazwy wyróżnione i kategorie certyfikatów

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

- **pole C**: międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**);
- **pole ST**: województwo, na którego terenie działa lub mieszka subskrybent;
- **pole L**: miasto, w którym ma siedzibę lub mieszka subskrybent;
- **pole S**: nazwisko subskrybenta,
- **pole G**: imię (imiona) subskrybenta,
- **pole CN**: nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje subskrybent,
- **pole O**: nazwa instytucji, w której pracuje subskrybent,
- **pole OU**: nazwa jednostki organizacyjnej, zatrudniającej subskrybenta,
- **pole SN**: numer seryjny, zawierający NIP lub PESEL subskrybenta,
- **pole A**: adres do korespondencji z subskrybentem**.**

Certyfikaty mogą być wydawane różnym kategoriom podmiotów:

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

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

3.1.2. Weryfikacja tożsamości subskrybentów

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

Potwierdzenie tożsamości subskrybenta - osoby fizycznej w punkcie systemu rejestracji, przy udziale notariusza lub innej osoby potwierdzającej tożsamość realizowane jest na podstawie ważnego dowodu osobistego lub paszportu oraz dodatkowo w przypadku, gdy subskrybent jest

osobą fizyczną dla której wydawany jest certyfikat kategorii II (pracownikiem organizacji lub jej reprezentantem):

- stosownego upoważnienia wystawionego przez daną organizację do reprezentowania jej interesów i umieszczenie danych organizacji w certyfikacie,
- aktualnego wypisu z Krajowego Rejestru Sądowego lub wypis z Centralnej Ewidencji i Informacji o Działalności Gospodarczej.

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

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

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

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

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

- podpisany przez subskrybenta przy użyciu ważnego klucza prywatnego, związanego z nie przeterminowanym certyfikatem, lub
- potwierdzony przez inspektora ds. rejestracji w Głównym Punkcie Rejestracji lub przez operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość.

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

Wnioski o unieważnienie certyfikatu lub zaświadczenia certyfikacyjnego mogą być składane telefonicznie, faksem lub pocztą poleconą.

We wszystkich przypadkach subskrybent (lub podmiot przez niego reprezentowany lub inny uprawniony podmiot) przekazuje wniosek o unieważnienie do Głównego Punktu Rejestracji. Inspektor ds. rejestracji dzwoniąc pod wskazany we wniosku telefon weryfikuje dane zawarte we wniosku. W przypadku niezgodności weryfikowanych danych certyfikat zostaje zawieszony do momentu wyjaśnienia powstałych niezgodności.

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

3.4. Rejestracja odbiorców innych usług certyfikacyjnych

Rejestracja odbiorców usług certyfikacyjnych świadczonych przez urząd znacznika czasu CERTUM QTSA, urząd weryfikacji statusu certyfikatu CERTUM QOCSP, usługi walidacji CERTUM QDVCS, urząd poświadczania odbioru i przedłożenia CERTUM QDA, urząd depozytów obiektów CERTUM QODA, urząd rejestrów i repozytoriów CERTUM QRRA oraz urząd certyfikatów atrybutów CERUM QACA nie jest obowiązkowa. Rejestracja użytkowników usług tych urzędów może być połączona z rejestracją subskrybenta urzędu certyfikacji CERTUM QCA. W momencie zawierania umowy z Asseco Data Systems S.A. subskrybent (lub podmiot przez niego reprezentowany) może zawrzeć także umowę na świadczenie usług wymienionych urzędów.

Od stron ufających, które nie są zarejestrowanymi użytkownikami usług urzędu CERTUM QTSA, urzędu CERTUM QOCSP, usługa CERTUM QDVCS oraz urzędu CERTUM QDA, urzędu depozytów obiektów CERTUM QODA, urzędu rejestrów i repozytoriów CERTUM QRRA oraz urzędu certyfikatów atrybutów CERTUM QACA może wymagać się uwierzytelnienia każdego żądania wysyłanego do tych urzędów.

4. Wymagania funkcjonalne

Poniżej przedstawiono sposób realizacji usług certyfikacji. Każdy etap rozpoczyna się od złożenia przez subskrybenta stosownego wniosku w punkcie systemu rejestracji, urzędzie znacznika czasu, urzędzie weryfikacji statusu certyfikatu, urzędzie walidacji danych oraz urzędzie poświadczania odbioru i przedłożenia. CERTUM podejmuje decyzję, co do dalszej realizacji wniosku, realizując żądaną usługę lub odmawiając jej realizacji.

4.1. Składanie wniosków

Wnioski subskrybenta są składane przy udziale punktu systemu rejestracji lub poprzez elektroniczny formularz. Bezpośrednio do Głównego Punktu Rejestracji mogą być składane jedynie wnioski o unieważnienie. Wnioski o unieważnienie certyfikatu przyjmowane są przez CERTUM przez całą dobę, siedem dni w tygodniu.

4.1.1. Wniosek o rejestrację i certyfikację

Wniosek o rejestrację i certyfikację składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście lub poprzez elektroniczny formularz (w tym przypadku konieczne jest potwierdzenie tożsamości za pośrednictwem notariusza lub innej osoby potwierdzającej tożsamość).

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

4.1.2. Wniosek o certyfikację, aktualizację kluczy lub modyfikację certyfikatu

Wniosek składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście lub poprzez elektroniczny formularz.

4.1.3. Wniosek o unieważnienie

Wniosek o unieważnienie certyfikatu składany jest przez upoważnione do tego osoby (patrz rozdz. 4.6.2) w Głównego Punktu Rejestracji lub przekazywany tam faksem, telefonicznie lub pocztą poleconą. Wniosek musi być potwierdzony przez inspektora ds. rejestracji.

Formularz wniosku opublikowany jest w repozytorium urzędu certyfikacji.

O unieważnieniu lub zawieszeniu certyfikatu są informowani subskrybenci, podmioty reprezentowane przez subskrybenta i wnioskodawcy (w przypadku wnioskowania przez inną osobę).

4.1.4. Przetwarzanie wniosków w punkcie systemu rejestracji

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

Inspektor ds. rejestracji lub osoba potwierdzająca tożsamość, w przypadku przetwarzania elektronicznego wniosku o aktualizację kluczy poświadcza, zgodnie z wymaganiami niniejszego dokumentu Polityki Certyfikacji i wewnętrznymi regulacjami CERTUM potwierdzenie tożsamości wnioskodawcy własnoręcznym podpisem wraz z podaniem swojego numeru PESEL w pisemnym oświadczeniu.

4.2. Wydanie certyfikatu lub zaświadczenia certyfikacyjnego

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

O wydaniu certyfikatu informowany jest subskrybent oraz podmiot reprezentowany przez subskrybenta..

4.2.1. Okres oczekiwania na wydanie certyfikatu

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

4.2.2. Odmowa wydania certyfikatu

CERTUM może odmówić wydania certyfikatu w następujących przypadkach:

- identyfikator subskrybenta (nazwa **DN**) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,
- uzasadnionego podejrzenia, że subskrybent sfałszował lub podał nieprawdziwe dane,
- nie dostarczenia przez wnioskodawcę kompletu wymaganych dokumentów,
- z innych ważnych nie wymienionych powyżej przyczyn, po uprzednim uzgodnieniu odmowy z **inspektorem bezpieczeństwa**.

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

4.3. Akceptacja certyfikatu

Po otrzymaniu certyfikatu subskrybent zobowiązany jest do sprawdzenia jego zawartości, w tym w szczególności poprawności zawartych w nim danych oraz komplementarności klucza publicznego z kluczem prywatnym. Jeśli wydany certyfikat zawiera jakiekolwiek wady, to powinien on zostać niezwłocznie unieważniony, a na jego miejsce wydany nowy pozbawiony błędów. W sytuacji takiej nie wymaga się podpisania umowy i/lub dostarczenia dodatkowych dokumentów.

Akceptacja certyfikatu oznacza wystąpienie w ciągu 7 dniu od daty otrzymania certyfikatu i danych niezbędnych do jego poprawnego użycia jednego z poniższych zdarzeń:

- złożenia przez subskrybenta oświadczenia o akceptacji oraz przesłanie go do CERTUM,
- braku w tym okresie pisemnej odmowy akceptacji certyfikatu.

Odmowa akceptacji certyfikatu z przyczyn innych niż rezygnacja z usług oznacza konieczność jego niezwłocznego unieważnienia oraz wydania nowego certyfikatu na podstawie nowej umowy. Wydanie nowego certyfikatu nastąpić może jedynie po otrzymaniu oświadczenia o odmowie akceptacji certyfikatu.

4.4. Recertyfikacja

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

Recertyfikacja odbywa się w okresie ważności obecnego certyfikatu na żądanie subskrybenta i musi być poprzedzona złożeniem odpowiedniego elektronicznego wniosku, weryfikowanego przez inspektora ds. rejestracji lub przez inną uprawnioną osobę potwierdzająca tożsamość.

Procedurze recertyfikacji mogą podlegać również zaświadczenia urzędów certyfikacji. O zajściu tego zdarzenia informowani są wszyscy subskrybenci i klienci urzędów certyfikacji.

CERTUM świadczy usługę recertyfikacji tej samej pary kluczy kryptograficznych na żądanie subskrybenta (posiadającego aktualnie ważny i nieprzeterminowany certyfikat) i na własne potrzeby. Certyfikaty i zaświadczenie certyfikacyjne, które było przedmiotem recertyfikacji nie jest unieważniane i umieszczane na liście CRL.

4.5. Certyfikacja i aktualizacja kluczy

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

- **certyfikacja kluczy** nie jest związana z żadnym innym ważnym certyfikatem (służy uzyskaniu nowego certyfikatu) - subskrybent jednakże powinien być zarejestrowany w CERTUM, tzn. posiadać co najmniej jeden certyfikat – nawet jeśli ma on status unieważniony lub przeterminowany,
- **aktualizacja kluczy** dotyczy określonego, wskazanego we wniosku ważnego certyfikatu (nowy certyfikat posiada identyczną treść jak związany z nim certyfikat; różnice to: nowy klucz publiczny, nowy numer seryjny certyfikatu, nowy okres ważności certyfikatu oraz nowy podpis urzędu certyfikacji).

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

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

- klucz publiczny w powiązaniu ze zmianą przynajmniej jednej z przedstawionych poniżej informacji,
- nazwa stanowiska pracy lub pełnionej roli (wymaga dostarczenia pełnomocnictwa),
- jednostki organizacyjnej lub adresu reprezentowanego podmiotu (wymaga dostarczania stosownych dokumentów),
- adres poczty elektronicznej, telefon, faks, miejsce zamieszkania, jeśli są umieszczone w certyfikacie,
- inne zmiany zawartości rozszerzeń certyfikatu.

Wniosek o modyfikację certyfikatu występuje tylko w formie elektronicznej poprzez dedykowany formularz na stronie WWW i musi być potwierdzony przez inspektora ds. rejestracji lub przez inną uprawnioną osobę potwierdzająca tożsamość.

4.6. Unieważnienie i zawieszenie certyfikatu

CERTUM zapewnia możliwość zgłoszenia wniosku o unieważnienie certyfikatu przez całą dobę.

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

Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia) i może być jedynie wnioskowane przez pracownika CERTUM. **Odwieszenie to musi jednak nastąpić nie później niż 7 dni od daty zawieszenia.**

4.6.1. Okoliczności unieważnienia certyfikatu

Unieważnienie certyfikatu jest wykonywane w przypadku utraty (lub zaistnienia podejrzenia takiej utraty) kontroli nad kluczem prywatnym, będącym w posiadaniu subskrybenta certyfikatu, rażącego naruszania przez subskrybenta zasad Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego lub na każde żądanie subskrybenta lub – w przypadku zgłoszenia unieważnienia certyfikatu kwalifikowanego profesjonalnego – na żądanie upoważnionego przedstawiciela reprezentowanego podmiotu lub innej upoważnionej osoby.

Wniosek o unieważnienie może być składany przy udziale Głównego Punktu Rejestracji, telefonicznie, faksem lub pocztą poleconą.

4.6.2. Kto może żądać unieważnienia certyfikatu

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

4.6.3. Procedura unieważniania certyfikatu

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

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

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

4.6.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

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

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

4.6.5. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu może mieć miejsce w przypadku, gdy dane zawarte w elektronicznym lub papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia, wniosek o unieważnienie nie został potwierdzony w wymaganym czasie, podejrzenie, że osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych lub innych okolicznościach wymagających wyjaśnień ze strony subskrybenta, lub wnioskodawcy.

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

4.6.6. Kto może żądać zawieszenia certyfikatu

O zawieszenie certyfikatu mogą wnioskować jedynie pracownicy CERTUM.

4.6.7. Procedura zawieszenia i odwieszania certyfikatu

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

Odwieszenie certyfikatu odbywa się tylko i wyłącznie z inicjatywy inspektora bezpieczeństwa. Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, urząd certyfikacji usuwa certyfikat z listy CRL.

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

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

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

4.6.8. Gwarantowany czas zawieszenia certyfikatu

Gwarantowane przez urząd certyfikacji czas na rozpatrzenie wniosków o zawieszenie certyfikatu, jak również dostępność statusu certyfikatu po jego zawieszeniu jest taki sam jak w przypadku unieważnienia certyfikatu (patrz rozdz. 4.6.4).

4.6.9. Częstotliwość publikowania list CRL

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

Wszystkie listy CRL uaktualniane są nie rzadziej, niż co 24 godziny i publikowane automatycznie w repozytorium urzędu certyfikacji. W przypadku unieważnienia certyfikatu nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie (patrz rozdz. 4.6.4).

4.6.10. Sprawdzanie list CRL

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

4.7. Usługa znakowania czasem

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

Uzyskanie znacznika czasu przebiega następująco:

- wnioskodawca wysyła żądanie, zawierające wartość skrótu (powiązana z dokumentem, wiadomością, itd.), identyfikator funkcji skrótu oraz identyfikator sesji (*ang. nonce*); żądanie powinno zawierać oid, wg. którego ma być wydany token znacznika czasu, w przypadku braku identyfikator token zostanie wydany zgodnie z domyślnym formatem,
- urząd znacznika czasu weryfikuje poprawność formatu wniosku oraz jego kompletność,
- urząd znacznika czasu tworzy znacznik,
- urząd znacznika czasu odsyła token znacznika czasu podmiotowi żądającemu,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena znacznika czasu, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

4.8. Usługa weryfikacji statusu certyfikatu

Kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP** udostępnia usługę weryfikacji certyfikatów kwalifikowanych w trybie on-line. Usługa tego typu realizowana jest w oparciu o protokół OCSP, przedstawiony w RFC 6960[11].

Protokół OCSP działa w oparciu o model **żądanie-odpowiedź**. W odpowiedzi na każde żądanie, urząd **CERTUM QOCSP** zwraca następujące standardowe, poświadczone przez niego informacje o statusie certyfikatu:

- **poprawny** (*ang. good*) – oznacza pozytywną odpowiedź na żądanie, którą należy jednoznacznie interpretować jako zaświadczenie, że certyfikat jest ważny,
- **unieważniony** (*ang. revoked*) – oznacza, że certyfikat został unieważniony,
- **nieznany** (*ang. unknown*) – oznacza, że weryfikowany certyfikat nie został wydany przez kwalifikowany urząd certyfikacji **CERTUM QCA**.

Status certyfikatu podawany jest w czasie rzeczywistym.

4.9. Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych

Usługi CERTUM QDVCS przydatne są w trakcie realizacji procedur potwierdzania ważności podpisanych dokumentów. Potwierdzenie wystawiane przez urząd CERTUM QDVCS przyjmuje postać certyfikatu potwierdzenia ważności danych i może być traktowane jako odpowiednik tokena notarialnego, zdefiniowanego w normie ISO/IEC 13888-3.

Usługa **CERTUM QDVCS**, pracuje w oparciu o protokół DVCS, OASIS DSS, XKMS.

Uzyskanie tokena walidacji przebiega następująco:

- wnioskodawca wysyła żądanie, zawierające informacje o typie pożądanej walidacji oraz walidowane dane,
- usługa walidacji weryfikuje poprawność formatu wniosku, pobiera żądany typ walidacji,
- usługa walidacji tworzy token i odsyła token walidacji danych podmiotowi żądającemu,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego tokena, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Opis polityki walidacji kwalifikowanej usługi walidacji znajduje się w dokumencie Polityk walidacji kwalifikowanej usługi walidacji CERTUM dla kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

4.10. Usługa wystawiania poświadczeń odbioru i przedłożenia

[11] RFC 6960 *Internet X.509 Public Key Infrastructure: On-line Certificate Status Protocol – OCSP*

Świadczona przez urząd **CERTUM QDA** usługa polega na wystawianiu poświadczeń odbioru lub przedłożenia (w tym także w urzędowych poświadczeń odbioru lub przedłożenia) dokumentów elektronicznych. Poświadczenia te dotyczą dokumentów przekazywanych przez klientów do *podmiotów realizujących zadania publiczne* za pośrednictwem systemu korzystającego z urzędu **CERTUM QDA** lub odwrotnie – przez *podmioty realizujące zadania publiczne* do klientów.

Usługa wystawiania urzędowego poświadczenia odbioru wykonywana jest następująco:

- wnioskodawca wysyła (nadawca) poprzez dedykowany system do urzędu **CERTUM QDA** dokument elektroniczny wraz z żądaniem przekazania go do wskazanego odbiorcy (*podmiotu realizującego zadania publiczne*),
- urząd **CERTUM QDA** weryfikuje poprawność formatu wniosku, jego kompletność oraz formalną poprawność,
- urząd **CERTUM QDA** przekazuje wniosek do systemu teleinformatycznego odbiorcy i wystawia urzędowe poświadczenie odbioru,
- urząd **CERTUM QDA** odsyła urzędowe poświadczenie odbioru nadawcy oraz odbiorcy,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego poświadczenia, i jeśli token nie budzi żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Usługa wystawiania poświadczenia odbioru przebiega podobnie jak wystawianie urzędowego poświadczenia odbioru z tym tylko, że nadawcą dokumentu elektronicznego jest *podmiot realizujący zadania publiczne*, zaś adresatem – dowolny podmiot nie będący *podmiotem realizującym zadania publiczne*.

Proces wystawiania poświadczenia przedłożenia a także urzędowego poświadczenia przedłożenia, przebiega podobnie, jak w przypadku wystawiania odpowiednio poświadczenia odbioru i urzędowego poświadczenia odbioru.

4.11. Usługa wystawiania poświadczeń depozytowych

Urząd depozytów obiektów **CERTUM QODA** świadczy usługi, które pozwalają ich użytkownikom na umieszczenie (zdeponowanie) dowolnego obiektu w depozycie, jego wielokrotne pobieranie, oraz wydanie. Zdeponowane obiekty przechowywane są w sposób, który pozwala na ich pobranie lub wydanie w stanie, w jakim były w momencie ich deponowania. Uprawniony użytkownik usług urzędu **CERTUM QODA** może także przeglądać wpisy związane ze zdeponowanymi obiektami i na tej podstawie podejmować decyzje o pobraniu lub wydaniu obiektu z depozytu.

Urząd depozytów **CERTUM QODA** świadczy następujące usługi:

- poświadczenie wpisu obiektu do depozytu,
- poświadczenie wydania obiektu z depozytu,
- uwierzytelnione poświadczenie wydania obiektu z depozytu,
- poświadczenie pobrania wpisu z depozytu,
- uwierzytelnione poświadczenie pobrania wpisu z depozytu,
- poświadczenie pobrania obiektu z depozytu,

- uwierzytelnione poświadczenie pobrania obiektu z depozytu.

Proces uzyskania poświadczeń, wystawianych przez urząd depozytów przebiega następująco:

- wnioskodawca (nadawca) wysyła do urzędu **CERTUM QODA** żądanie wykonania jednej z wymienionych powyżej usług,
- urząd **CERTUM QODA** weryfikuje poprawność formatu wniosku, jego kompletność oraz formalną poprawność,
- urząd **CERTUM QODA** wykonuje czynności właściwe dla otrzymanego żądania i po ich pomyślnym zakończeniu wystawia odpowiednie poświadczenie depozytowe,
- urząd **CERTUM QODA** odsyła poświadczenie depozytowe do nadawcy żądania,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego poświadczenia, i jeśli nie budzi ono żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Urząd depozytów **CERTUM QODA** rejestruje fakt otrzymania żądania i wystawienia poświadczenia depozytowego, chociaż nie jest zobligowany do ich przechowywania.

4.12. Usługa wystawiania poświadczeń rejestrowych i repozytoryjnych

Urząd rejestrów i repozytoriów **CERTUM QRRA** świadczy usługi, które pozwalają na umieszczenie w rejestrze tylko wpisu lub zarówno wpisu, jak i powiązanych z nim obiektów danych. Struktura wpisów i obiektów zależy od klasy rejestru i podlega walidacji przed każdym umieszczeniem w rejestrze i/lub w repozytorium. Wpisy i obiekty mogą być wielokrotnie pobierane, a także modyfikowane. Zarejestrowane wpisy i obiekty przechowywane są w sposób, który pozwala na ich pobranie w stanie, w jakim były w momencie ich rejestrowania. Uprawniony użytkownik usług urzędu **CERTUM QRRA** może także przeglądać wpisy i na tej podstawie podejmować decyzje o pobraniu wpisu i/lub obiektu odpowiednio z rejestru lub repozytorium.

Urząd rejestrów i repozytoriów **CERTUM QRRA** świadczy następujące usługi:

- poświadczenie umieszczenia wpisu w rejestrze,
- poświadczenie umieszczenia obiektu w repozytorium,
- poświadczenie pobrania wpisu z rejestru,
- poświadczenie pobrania obiektu z repozytorium,
- uwierzytelnione poświadczenie pobrania wpisu z rejestru,
- uwierzytelnione poświadczenie pobrania obiektu z repozytorium,
- poświadczenie modyfikacji wpisu w rejestrze,
- poświadczenie modyfikacji obiektu w repozytorium.

Proces uzyskania poświadczeń, wystawianych przez urząd rejestrów i repozytoriów przebiega następująco:

- wnioskodawca (nadawca) wysyła do urzędu **CERTUM QRRA** żądanie wykonania jednej z wymienionych powyżej usług,

- urząd **CERTUM QRRA** weryfikuje poprawność formatu wniosku, jego kompletność oraz formalną poprawność,
- urząd **CERTUM QRRA** wykonuje czynności właściwe dla otrzymanego żądania i po ich pomyślnym zakończeniu wystawia odpowiednie poświadczenie rejestrowe i repozytoryjne,
- urząd **CERTUM QRRA** odsyła poświadczenie rejestrowe i repozytoryjne do nadawcy żądania,
- podmiot żądający sprawdza kompletność i poprawność otrzymanego poświadczenia, i jeśli nie budzi ono żadnych zastrzeżeń, to zapamiętuje go łącznie z danymi, których dotyczy.

Urząd rejestrów i repozytoriów **CERTUM QRRA** rejestruje fakt otrzymania żądania i wystawienia poświadczenia rejestrowego lub repozytoryjnego i jest zobligowany do ich przechowywania przez okres wynikający z umowy pomiędzy subskrybentem usług a urzędem **CERTUM QRRA**.

4.13. Usługa wystawiania certyfikatów atrybutów

Urząd certyfikatów atrybutów **CERTUM QACA** świadczy usługi polegające na wydaniu, udostępnianiu i unieważnianiu certyfikatów atrybutów. Usługi te świadczone są w oparciu o sieć punktów rejestracji lub punktów potwierdzania tożsamości i atrybutów. Adresy tych punktów są publikowane w serwisie internetowym **CERTUM** dostępnym pod adresem www.certum.pl.

Certyfikaty wydawane są na podstawie wniosku o wydanie certyfikatu atrybutów. Wniosek ten może być składany w formie elektronicznej lub papierowej i przekazany na adres jednego z punktów rejestracji lub punktów potwierdzania tożsamości i atrybutów.

Wniosek powinien zawierać co najmniej:

- imię i nazwisko podmiotu, któremu ma być przypisany atrybut lub atrybuty,
- wskazanie atrybutów[12], które powinny zostać umieszczenia w certyfikacie atrybutów;
- dane podmiotu lub, które przekazały prawo posługiwania się atrybutami wymienionymi w punkcie poprzednim,
- dozwolony okres posługiwania się przypisanym atrybutem lub atrybutami,
- informacje, czy certyfikat atrybutów podlega procedurze unieważniania i umieszczania na liście unieważnionych certyfikatów atrybutów,
- wskazanie miejsca lub miejsc opublikowania certyfikatu atrybutów (w przypadku jego braku, certyfikat jest domyślnie publikowany w repozytorium **CERTUM**).

Jeśli posługiwanie się atrybutem umieszczonym w certyfikacie atrybutów wymaga przedłożenia dowodu, to do wniosku należy dołączyć odpowiednie zaświadczenie. Przedłożenie zaświadczenia jest wymagane także w przypadku, gdy wpisanie atrybutu wiąże się z przekazaniem uprawnień, które posiada podmiot uprawniający (np. podmiot, który przekazuje swoje pełnomocnictwa).

[12] Wskazanie to odbywa się na podstawie listy atrybutów opublikowanej przez CERTUM QACA w repozytorium. Lista może być aktualizowana przez urząd certyfikatów atrybutów

Potwierdzenie uprawnień, o których mowa wyżej, może odbywać się w punkcie potwierdzania tożsamości i atrybutów lub w biurze notarialnym. Potwierdzanie to odbywa się zgodnie z procedurą opracowana dla każdego atrybutu obsługiwanego przez CERTUM QACA.

Wniosek za pośrednictwem punktu rejestracji lub punktu potwierdzania tożsamości i atrybutów przekazywany jest do Głównego Punktu Rejestracji, gdzie inspektor ds. rejestracji przygotowuje **token zgłoszenia certyfikacyjnego** i przesyła go do urzędu **CERTUM QACA**.

4.14. Rejestrowanie zdarzeń, zarządzanie incydentami bezpieczeństwa

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

4.14.1. Typy rejestrowanych zdarzeń

Rejestry zdarzeń CERTUM przechowują zapisy o wszystkich zdarzeniach generowanych przez komponenty programowe, fizyczne i logiczne, wchodzące w skład systemu. Rejestrowane są działania związane z pełnieniem roli kwalifikowanego podmiotu świadczącego usługi certyfikacyjne. Opis rejestrowanych zdarzeń znajduje się w Kodeksie Postępowania Certyfikacyjnego i wewnętrznych dokumentach CERTUM.

4.14.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń

W celu rozpoznania ewentualnych nieuprawnionych działań administrator systemu i inspektorzy ds. audytu powinni analizować rejestry zdarzeń przynajmniej raz w każdym dniu roboczym.

4.14.3. Okres przechowywania zapisów rejestrowanych zdarzeń

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

Zarchiwizowane zdarzenia przechowywane są przez okres min. 20 lat.

4.14.4. Ochrona zapisów rejestrowanych zdarzeń

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

Archiwa rejestru zdarzeń są podpisywane i znakowane czasem.

4.14.5. Tworzenie kopii zapisów rejestrowanych zdarzeń

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

4.14.6. Zarządzanie incydentami bezpieczeństwa

CERTUM zarządza powstałymi incydentami bezpieczeństwa zgodnie z obowiązującą w Asseco Data Systems S.A. procedurą zarządzania incydentami bezpieczeństwa.

Procedura ta jest zgodna w wymaganiami art. 19.2 Rozporządzenia Parlamentu Europejskiego i Rady UE nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym (w skrócie *Rozporządzenie* eIDAS).

4.15. Archiwizowanie danych

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

Archiwum zawiera certyfikaty wydane maksymalnie do 20 lat wstecz. Archiwizowane są także wszystkie listy CRL wydane przez CERTUM.

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

Archiwalne kopie danych elektronicznych przechowywane są w siedzibie ośrodka głównego oraz w ośrodku zapasowym CERTUM.

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

4.16. Zmiana klucza

Procedura zmiany klucza odnosi się do kluczy urzędu certyfikacji **CERTUM QCA** oraz pozostałych urzędów świadczących usługi certyfikacyjne i dotyczy procesu aktualizacji kluczy, które zastąpią klucze używane dotychczas odpowiednio do podpisywania certyfikatów i list CRL oraz do podpisywania znaczników czasu, zweryfikowanych statusów certyfikatów, zwalidowanych danych, poświadczeń odbioru lub przedłożenia (w tym także urzędowych poświadczeń odbioru lub przedłożenia).

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

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

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

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

CERTUM zapewnia możliwość unieważnienia certyfikatów oraz tworzenia i publikowania list CRL również w przypadku awarii, w szczególności poprzez użycie zapasowego ośrodka przetwarzania danych, z zachowaniem obowiązku określonego w rozdz. 4.6.4 i 4.6.9.

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

4.18. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

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

Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważniony muszą być także certyfikaty urzędu certyfikacji, urzędu znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych oraz urzędu poświadczania odbioru i przedłożenia . Klucze prywatne urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, usługa walidacji **CERTUM QDVCS**, urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA**, urzędu rejestrów i repozytoriów **CERTUM QRRA** oraz urzędu certyfikatów atrybutów **CERTUM QACA** muszą być zniszczone.

CERTUM zwraca subskrybentowi koszty wydanego certyfikatu, proporcjonalnie do pozostałego okresu ważności wydanego certyfikatu.

Szczegółowy sposób postępowania w przypadku zakończenia działalności przez Centrum Certyfikacji określa plan zakończenia działalności Centrum Certyfikacji, stanowiący wewnętrzną procedurę CERTUM.

5. Zabezpieczenia fizyczne, organizacyjne oraz personelu

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

5.1. Zabezpieczenia fizyczne

5.1.1. Bezpieczeństwo fizyczne CERTUM

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

CERTUM mieści się w budynku Asseco Data Systems S.A., znajdującym się w Szczecinie przy ul. Bajeczna 13.

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

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

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

5.1.2. Bezpieczeństwo punktów systemu rejestracji

Komputery Głównego Punktu Rejestracji służące wydawaniu certyfikatów znajdują się w specjalnie przeznaczonym do tego celu pomieszczeniu. Dostęp do nich jest fizycznie i logicznie chroniony przed nieupoważnionymi osobami. Do ich obsługi dopuszczone są jedynie upoważnione osoby. Komputery zlokalizowane w notarialnych punktach potwierdzania tożsamości chronione są zgodnie z wymaganiami stosowanymi dla kancelarii notarialnych. Komputery zlokalizowane w pozostałych punktach potwierdzania tożsamości podlegają ochronie, której zakres opisany jest w stosownych umowach pomiędzy CERTUM a administratorem danego punktu.

5.2. Zabezpieczenia organizacyjne

CERTUM zapewnia realizację zabezpieczeń organizacyjnych poprzez określenie, między innymi:

- zaufanych ról, które mogą być pełnione przez jedną lub więcej osób – zarówno w urzędzie certyfikacji jak i w punktach systemu rejestracji,
- łączenia określonych ról,
- zakresu obowiązków i odpowiedzialności osób pełniących określone role,
- liczby osób koniecznych do realizacji poszczególnych zadań,
- identyfikacji oraz uwierzytelnianiu personelu.

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

5.3. Kontrola personelu

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

- posiadają minimum wykształcenie średnie,
- zawarły umowę o pracę lub inną umowę cywilno-prawną precyzującą rolę, którą mają pełnić i określającą wynikające z niej prawa i obowiązki,
- przeszły niezbędne przeszkolenie z zakresu obowiązków, które będą wykonywały,
- zostały przeszkolone w zakresie ochrony danych osobowych,
- podpisały klauzule o nieujawnianiu informacji wrażliwych z punktu widzenia bezpieczeństwa urzędu certyfikacji lub poufności danych subskrybenta,
- nie wykonują obowiązków, które mogą doprowadzić do konfliktu interesów pomiędzy urzędem certyfikacji a działającymi w jego imieniu punktami rejestracji.

5.3.1. Szkolenie

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

5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania

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

6. Procedury bezpieczeństwa technicznego

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

6.1. Generowanie par kluczy

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

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

- elektronicznego poświadczania certyfikatów i list CRL,
- elektronicznego poświadczania wiadomości, wymienianych z klientami,
- elektronicznego poświadczania zaświadczeń certyfikacyjnych,
- uzgadniania kluczy stosowanych do poufnej wymiany informacji pomiędzy urzędem a otoczeniem.

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

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze urzędu certyfikacji, używane do podpisywania certyfikatów i list CRL, wystawiania tokenów znacznika czasu, tokenów statusu certyfikatów, tokenów walidacji danych, poświadczeń odbioru i przedłożenia generowane są w siedzibie CERTUM w obecności wybranej, przeszkolonej grupy zaufanych osób. Wszystkie klucze urzędów generowane są zgodnie z wewnętrznymi procedurami CERTUM, przy użyciu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu generowania kluczy, spełniającego wymagania klasy FIPS 140-2 level 3 lub wyżej.

Klucze subskrybentów mogą być generowane w urzędzie certyfikacji **CERTUM QCA** lub samodzielnie przez subskrybenta z wykorzystaniem mechanizmów dostarczonych przez PCC CERTUM.

6.1.2. Przekazywanie klucza prywatnego subskrybentowi

Klucze subskrybentów generowane są przez urząd certyfikacji lub samodzielnie przez subskrybenta na kryptograficznej karcie elektronicznej lub w sprzętowym module kryptograficznym i mogą być przekazywane subskrybentowi osobiście lub pocztą kurierską. Dane do uaktywnienia karty (m.in. PUK/PIN) podane są oddzielnie; wydane karty są personalizowane i rejestrowane przez urząd certyfikacji. Dane do uaktywnienia sprzętowego modułu

kryptograficznego przekazywane są oddzielnie, fakt wydania certyfikatu z wykorzystaniem sprzętowego modułu kryptograficznego rejestrowany jest przez urząd certyfikacji.

6.1.3. Przekazywanie klucza publicznego urzędu certyfikacji stronom ufającym

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

Urząd certyfikacji CERTUM rozpowszechnia swoje zaświadczenia certyfikacyjne dwoma sposobami:

- umieszczają w ogólnie dostępnym repozytorium urzędu certyfikacji CERTUM w serwisie internetowym dostępnym pod adresem: http://www.certum.pl/repozytorium.
- za pomocą dedykowanego oprogramowania, które umożliwia korzystanie z usług CERTUM.

6.1.4. Długości kluczy

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

6.2. Ochrona klucza prywatnego

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

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urząd certyfikacji, urząd znacznika czas, urząd weryfikacji statusu certyfikatu, urząd walidacji danych i urząd poświadczania odbioru i przedłożenia, punkty rejestracji i subskrybentów są zgodne z wymaganiami normy FIPS 140-2 ITSEC (*ITSEC v 1.2 wydany przez Komisję Europejską, Dyrektoriat XIII/F, w 1991 r.*).

6.2.2. Podział klucza prywatnego na części

Ochronie za pomocą podziału klucza na części podlegają klucze wszystkich urzędów świadczących usługi certyfikacyjne. Klucze dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Kodeksie Postępowania Certyfikacyjnego.

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

6.2.3. Deponowanie klucza prywatnego

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

6.2.4. Kopie zapasowe klucza prywatnego

Wszystkie urzędy świadczące usługi certyfikacyjne tworzą kopie swoich kluczy prywatnych. Kopie te wykorzystywane są w przypadku potrzeby realizacji normalnej lub awaryjnej (np. po wystąpieniu klęski żywiołowej) procedury odzyskiwania kluczy.

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

Urzędy CERTUM nie przechowują kopii kluczy prywatnych operatorów punktów rejestracji i subskrybentów.

6.2.5. Archiwizowanie klucza prywatnego

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

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

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

- w przypadku tworzenia kopii zapasowych kluczy prywatnych, przechowywanych w module kryptograficznym może być czasami konieczne (np. w przypadku jego awarii) załadowanie kluczy do innego modułu kryptograficznego,
- konieczności przeniesienia klucza prywatnego z modułu operacyjnego, wykorzystywanego codziennie przez podmiot do innego modułu; sytuacja taka może wystąpić np. w przypadku defektu modułu lub konieczności jego zniszczenia.

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

6.2.7. Metody aktywacji klucza prywatnego

Wszystkie klucze prywatne urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu walidacji **CERTUM QDVCS** i urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA**, urzędu rejestrów i repozytoriów **CERTUM QRRA** oraz urzędu certyfikatów atrybutów **CERTUM QACA** 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 subskrybentów są uaktywniane dopiero po uwierzytelnieniu (podaniu numeru PIN) i tylko na czas wykonania pojedynczej operacji kryptograficznej z użyciem tego klucza. Po zakończeniu wykonywania operacji klucz prywatny jest automatycznie dezaktywowany i musi być ponownie uaktywniony przed wykonaniem kolejnej operacji niezależnie od tego czy klucze przechowywane są na karcie elektronicznej lub innym nośniku.

6.2.8. Metody dezaktywacji klucza prywatnego

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

W przypadku kluczy subskrybenta dezaktywowanie kluczy podpisujących następuje natychmiast po zrealizowaniu podpisu elektronicznego.

6.2.9. Metody niszczenia klucza prywatnego

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

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

6.3. Inne aspekty zarządzania kluczami

6.3.1. Archiwizacja kluczy publicznych

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

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

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

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

6.3.2. Okresy stosowania klucza publicznego i prywatnego

Okres życia klucza publicznego określony jest przez pole **validity** każdego certyfikatu lub zaświadczenia certyfikacyjnego. Okres ważności klucza prywatnego może być krótszy niż okres ważności certyfikatu lub zaświadczenia certyfikacyjnego (wynika to z możliwości zaprzestania używania klucza w dowolnym momencie lub wymagań stawianych urzędom certyfikacji, znacznika czasu, weryfikacji statusu certyfikatu, walidacji danych lub poświadczania odbioru i przedłożenia).

Standardowe maksymalne okresy ważności kluczy prywatnych oraz związanych z nimi zaświadczeń certyfikacyjnych urzędu certyfikacji, urzędu znacznika czasu, urzędu weryfikacji

statusu certyfikatu, urzędu walidacji danych i urzędu poświadczania odbioru i przedłożenia podane są w Tab.8, zaś certyfikatów subskrybentów w Tab.9.

Data początku ważności zaświadczenia certyfikacyjnego lub certyfikatu nie musi pokrywać się z datą jego wydania. Dopuszcza się, aby data ta ulokowana była w przyszłości, nigdy zaś w przeszłości.

Tab. 8 Maksymalne okresy ważności zaświadczeń certyfikacyjnych

Typ właściciela klucza i rodzaj klucza		Główny rodzaj zastosowania klucza	
		RSA do podpisu certyfikatów i list CRL	RSA do podpisu tokenów
CERTUM QCA	zaświadczenie	5 lat	–
	klucz prywatny	3 lata	–
CERTUM QTSA CERTUM QOCSP CERTUM QDVCS CERTUM QDA CERTUM QODA CERTUM QRRA	zaświadczenie	–	5 lat
	klucz prywatny	–	5 lat
CERTUM QACA	zaświadczenie	5 lat	–
	klucz prywatny	3 lata	–

Tab. 9 Maksymalne okresy ważności kwalifikowanych certyfikatów

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

Tab. 10 Maksymalne okresy ważności certyfikatów atrybutów

Typ właściciela kwalifikowanego certyfikatu atrybutów	Maksymalny okres ważności
Osoby fizyczne	2 lata

6.4. Zabezpieczenia systemu komputerowego

Zadania punktów rejestracji, urzędów certyfikacji i urzędów znakowania czasem funkcjonujących w ramach kwalifikowanego systemu CERTUM realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzącego system, który spełnia wymagania określone

w *Information Technology Security Evaluation Criteria* (ITSEC). Elementy systemu tworzą godną zaufania całość, która spełnia wymagania norm, o których mowa w Decyzji Wykonawczej Komisji (UE) 2016/650 z dnia 25 kwietnia 2016r. ustanawiające normy dotyczące oceny bezpieczeństwa kwalifikowanych urządzeń do składania podpisu i pieczęci na podstawie art. 30 ust. 3 i art. 39 ust. 2 rozporządzenia Parlamentu Europejskiego i Rady (UE) nr 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym.

6.5. Zabezpieczenia sieci komputerowej

Serwery oraz zaufane stacje robocze systemu komputerowego CERTUM połączone są przy pomocy wydzielonej dwusegmentowej sieci wewnętrznej LAN. Dostęp od strony Internetu do każdego z segmentów chroniony jest przy pomocy inteligentnych zapór sieciowych (firewall) o klasie E3 wg ITSEC oraz systemów wykrywania intruzów IDS.

6.6. Znaczniki czasu jako element bezpieczeństwa

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

Znaczniki czasu tworzone w ramach CERTUM w wyżej wymienionych celach są zgodne z zaleceniem RFC 3161. W przeciwieństwie do tych znaczników czasu, urząd znakowania czasem CERTUM QTSA wydaje tokeny znacznika czasu zgodnie z ETSI EN 319 422 (patrz. Rozdział 1.3.2).

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

Profile kwalifikowanych certyfikatów, zaświadczeń certyfikacyjnych oraz list certyfikatów unieważnionych są zgodne z formatami określonymi w normie ITU-T X.509 v3 oraz profilami zawartymi w *ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 - 5*. Z kolei profile tokena znacznika wystawiane są zgodnie z RFC 3161 oraz *ETSI* (*EN 319 422 Time-stamping protocol and time-stamp profiles*), tokeny statusu certyfikatu wg RFC 2560, tokeny walidacji danych wg RFC 3029, zaś poświadczenia odbioru i przedłożenia (w tym także urzędowe poświadczenia odbioru i przedłożenia) zgodnie z profilem *uniUPO* i *uniUPP*, opracowanym przez Asseco Data Systems S.A., w oparciu o wymagania określone w polskiej normie PN-ISO/IEC 13888-3:1999 *Technika informatyczna. Techniki zabezpieczeń. Niezaprzeczalność. Mechanizmy wykorzystujące techniki asymetryczne*.

Zgodnie z opinią wydaną przez Ministerstwo Rozwoju Departament Gospodarki Elektronicznej, w okresie przejściowym, który wskazany został w Art. 51, ust. 2 *ROZPORZĄDZENIA PARLAMENTU EUROPEJSKIEGO I RADY (UE) NR 910/2014 z dnia 23 lipca 2014 r. w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE*, CERTUM wykorzystuje w świadczonych przez siebie usługach kwalifikowanych algorytm SHA-1.

7.1. Struktura certyfikatów

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

7.1.1. Treść certyfikatu

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

7.1.1.1. Pola podstawowe

CERTUM obsługuje pola podstawowe certyfikatu opisane w Tab. 11:

Tab. 11 Profil podstawowych pól kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego

Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	Version 3	
Serial Number (numer seryjny)	Unikalne wartości we wszystkich certyfikatach wydawanych przez kwalifikowany urząd certyfikacji CERTUM.	
Signature Algorithm (algorytm podpisu)	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (wystawca, nazwa DN)	Common Name (CN) =	CERTUM QCA
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Serial Number (SN) =	Nr wpisu: 14
Not before (początek okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Not after (koniec okresu ważności)	Podstawowy czas wg UTC (Universal Coordinate Time). CERTUM posiada własny zegar satelitarny, taktowany atomowym wzorcem sekundy (PPS). Stosowany w CERTUM zegar jest znany jako ogólnoświatowe wiarygodne źródło czasu klasy Stratum I.	
Subject (podmiot, nazwa DN)	Nazwa DN jest zgodna z wymaganiami określonymi w *ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 - 5.* Struktura nazwy DN zależy od typu podmiotu, któremu wystawiany jest certyfikat.	
Subject Public Key Info (klucz publiczny podmiotu)	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 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.	

7.1.1.2. Pola rozszerzeń

CERTUM obsługuje pola rozszerzeń opisane w Tab. 12:

Tab. 12 Profil rozszerzeń standardowych certyfikatu lub zaświadczenia certyfikacyjnego

Nazwa rozszerzenia	Uwagi	Status rozszerzenia
AuthorityKeyIdentifier (identyfikator klucza wydawcy)	Skrót SHA-1 z wartości klucza publicznego zaświadczenia certyfikacyjnego urzędu	Niekrytyczne
KeyUsage (użycie klucza)	Dozwolone użycie klucza. W przypadku certyfikatów kwalifikowanych możliwa jedynie wartość **nonRepudiation**	Krytyczne
ExtKeyUsage (rozszerzone	Sprecyzowanie (ograniczenie) użycia klucza.	Krytyczne

Nazwa rozszerzenia	Uwagi	Status rozszerzenia
użycie klucza)	Pole to należy interpretować jako zawężenie dopuszczalnego obszaru zastosowania klucza, określonego w polu **keyUsage**	
CertificatePolicies (polityka certyfikacji)	Informacja o polityce certyfikacji, realizowanej przez urząd certyfikacji: • iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 1 – dla certyfikatów kwalifikowanych • joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32) – dla zaświadczeń certyfikacyjnych • iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 10 – dla kluczy infrastruktury	Krytyczne
PolicyMapping (równoważne polityki)	(opcjonalne) Pole to zawiera jedną lub więcej par OID, które określają równoważność polityki wydawcy z polityką podmiotu	Niekrytyczne
IssuerAlternativeName (alternatywna nazwa urzędu certyfikacji)	(opcjonalne) Alternatywna nazwa urzędu certyfikacji	Niekrytyczne
SubjectAlternativeName (alternatywna nazwa podmiotu)	Alternatywna nazwa podmiotu, np. adres email	Niekrytyczne
BasicContraints (podstawowe ograniczenia)	Umożliwia określenie czy podmiot jest urzędem certyfikacji (pole **cA**) oraz maksymalną długość ścieżki (pole **pathLength**)	Krytyczne
CRLDistributionPoints (punkty dystrybucji listy CRL)	Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL urzędu (np. http://crl.certum.pl/qca.crl)	Niekrytyczne
SubjectDirectoryAttributes (atrybuty katalogu podmiotu)	Atrybuty podmiotu dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**	Niekrytyczne
AuthorityInfoAccessSyntax	(opcjonalne) Dostęp do informacji urzędu certyfikacji, wskazuje, w jaki sposób wystawca certyfikatu udostępnia informacje i usługi (np. http://qocsp.certum.pl)	Niekrytyczne
QCStatements (deklaracje wydawcy certyfikatu kwalifikowanego)	Oświadczenie, że certyfikat jest kwalifikowanym certyfikatem[13]. Limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu. Wskazanie, w czyim imieniu działa podmiot składając podpis.	Niekrytyczne
BiometricSyntax (informacje	(opcjonalne) Informacje o cechach biometrycznych podmiotu certyfikatu: podpisie	Niekrytyczne

[13] Jest to oświadczenie Asseco Data Systems S.A., że wydawane certyfikaty kwalifikowane są zgodne z wymaganiami Ustawy o usługach zaufania. Asseco Data Systems S.A. deklaruje dodatkowo w ten sposób zgodność wydawanych certyfikatów kwalifikowanych ze specyfikacją EN 319-422, tj. oświadczenie zawsze zawiera identyfikator obiektu o wartości: {itu-t(0) identified-organization(4) etsi(0) id-qc-profile(1862) 1 1}.

Nazwa rozszerzenia	Uwagi	Status rozszerzenia
biometryczne)	odręcznym lub zdjęciu	

7.1.2. Typ stosowanego algorytmu poświadczenia elektronicznego

Pole **signatureAlgorithm** zawiera identyfikator algorytmu kryptograficznego, opisującego algorytm stosowany do realizacji poświadczenia elektronicznego, składanego przez urząd certyfikacji na certyfikacie lub zaświadczeniu certyfikacyjnym. W przypadku CERTUM stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1.

7.1.3. Pole poświadczenia elektronicznego

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

7.2. Struktura listy certyfikatów unieważnionych (CRL)

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

Pole informacyjne **tbsCertList** jest sekwencją pól opisanych w Tab. 13:

Tab. 13 Profil listy CRL

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

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

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

Profil listy unieważnionych certyfikatów atrybutów jest identyczny z opisem profilu listy unieważnionych kwalifikowanych certyfikatów. Ze względu na efektywność obsługi list unieważnionych certyfikatów atrybutów, unieważnione certyfikaty atrybutów umieszczane są na innych listach niż unieważnione certyfikaty klucza publicznego.

7.3. Profil tokena znacznika czasu

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

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

7.4. Profil tokena walidacji podpisów elektronicznych i pieczęci elektronicznych.

Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS** 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 3029 komplementarne z nimi zaświadczenia certyfikacyjne kluczy publicznych zawierają pole precyzujące zawężenie dopuszczalnego zastosowania klucza (**ExtKeyUsageSyntax**) zaznaczone jako **krytyczne**. Oznacza to, że zaświadczenie certyfikacyjne może być używane przez usługę walidacji tylko do realizacji poświadczeń elektronicznych w wystawianych przez siebie tokenach walidacji.

7.5. Profile tokenów weryfikacji statusu certyfikatów, poświadczeń odbioru i przedłożenia, depozytowych, rejestrowych i repozytoryjnych oraz certyfikatów atrybutów

Profile tokenów weryfikacji statusu certyfikatów, tokenów walidacji danych, poświadczeń odbioru lub przedłożenia (w tym także urzędowych poświadczeń odbioru i przedłożenia), poświadczeń depozytowych oraz poświadczeń rejestrowych i repozytoryjnych oraz certyfikatów atrybutów, wystawianych odpowiednio przez urząd weryfikacji statusu certyfikatu CERTUM QOCSP, urząd poświadczania odbioru i przedłożenia CERTUM QDA, urząd depozytów obiektów CERTUM QODA oraz urząd rejestrów i repozytoriów CERTUM QRRA oraz urząd certyfikatów atrybutów CERTUM QACA, opisane są w wewnętrznych dokumentach CERTUM.

8. Administrowanie Polityką Certyfikacji

Każda z wersji Polityki Certyfikacji obowiązuje (posiada status **aktualny**) do czasu zatwierdzenia i opublikowania nowej wersji (patrz rozdz. 8.3). Nowa wersja opracowywana jest przez pracowników CERTUM i ze statusem **w ankiecie** przekazana do rozpatrzenia. Po otrzymaniu i uwzględnieniu uwag z ankiety Polityka Certyfikacja przekazywana zostaje do zatwierdzenia przez osobę zarządzającą CERTUM i opublikowania. W czasie trwania procedury zatwierdzania nowa wersja dokumentu posiada status – **w zatwierdzeniu,** a po zakończeniu procedury osiąga status – **aktualny**.

Subskrybenci zobowiązani są stosować się jedynie do aktualnie obowiązującej Polityki.

8.1. Procedura wprowadzania zmian

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

Wprowadzane zmiany można ogólnie podzielić na dwie kategorie: takie, o których nie trzeba informować subskrybentów oraz takie, które wymagają (zwykle odpowiednio wczesnego) poinformowania.

8.1.1. Zmiany nie wymagające informowania

Jedynymi zmianami, które nie wymagają wcześniejszego informowania subskrybentów i innych użytkowników systemu, dotyczą zmian wynikających z wprowadzenia korekt edycyjnych lub zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie Polityką. Wprowadzone zmiany nie podlegają procedurze zatwierdzania.

8.1.2. Zmiany wymagające informowania

8.1.2.1. Lista elementów

Po uprzednim poinformowaniu, zmianom mogą podlegać dowolne elementy Polityki Certyfikacji. Informacja o wszystkich, rozważanych zmianach w Polityce jest przesyłana wszystkim zainteresowanym stronom w postaci nowej wersji Polityki Certyfikacji o statusie **w ankiecie**. Proponowane zmiany publikowane są na stronie internetowej **CERTUM** lub rozsyłane pocztą elektroniczną.

8.1.2.2. Okres oczekiwania na komentarze

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

8.1.2.3. Zmiany wymagające nowego identyfikatora

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

8.2. Publikacja

Kopia Polityki Certyfikacji dostępna jest w formie elektronicznej:

- na stronie WWW pod adresem: http://www.certum.pl/repozytorium
- via e-mail o adresie: info@certum.pl

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

8.3. Procedura zatwierdzania Polityki Certyfikacji

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

Decyzję o zatwierdzeniu nowej wersji Kodeksu Postępowania Certyfikacyjnego podejmuje osoba zarządzająca CERTUM. Wszystkie zmiany wprowadzane w dokumencie odnotowywane są w **Historii dokumentu**.

Historia dokumentu

Historia zmian dokumentu		
1.0	20 sierpnia 2002 r.	Pełna wersja dokumentu. Dokument zatwierdzony.
1.1	23 października 2002 r.	Poprawki edytorskie, uwzględnienie uwag Ministerstwa Gospodarki, dodanie urzędu weryfikacji statusu certyfikatu. Dokument zatwierdzony.
2.0	01 lutego 2005 r.	Skrócenie Polityki i aktualizacja informacji, zgodnie z zaleceniami uwag audytorskich.
2.1	02 maja 2005 r.	Zmiana formy prawnej spółki, przekształcenie Unizeto Sp. z o.o. w Unizeto Technologies S.A.
2.2	20 lipca 2005 r.	Zmiana nazwy urzędu certyfikacji z "Centrum Certyfikacji Unizeto CERTUM" na "CERTUM - Powszechne Centrum Certyfikacji".
2.3	01 stycznia 2006 r.	Dodanie informacji po generacji nowych zaświadczeń certyfikacyjnych. Podkreślenie faktu kopiowania dokumentów subskrybentów, wymaganych w realizacji procesu certyfikacji. Zmiana numeru faksu
3.0	15 lipca 2006 r.	Dodanie nowych usług certyfikacyjnych: usługi weryfikacji statusu certyfikatu, usługi walidacji danych i usługi urzędowego poświadczania odbioru i nadania, usprawnienie procesu wydawania certyfikatów.
3.1	05 stycznia 2007 r.	Dodanie nowych usług certyfikacyjnych: usługi poświadczania depozytowego, usług poświadczeń rejestrowych i repozytoryjnych, zmiana lokalizacji siedziby urzędu certyfikacji „CERTUM - Powszechne Centrum Certyfikacji”.
3.2	17 września 2007 r.	Dodanie nowej usługi certyfikacyjnej: usługi wydawania certyfikatów atrybutów.
3.3	01 marca 2008 r.	Aktualizacja profili certyfikatów.
3.4	14 lipca 2008 r.	Aktualizacja informacji na temat QDVCS.
3.5	24 lipiec 2009 r.	Aktualizacja informacji na temat recertyfikacji.
3.6	01 listopad 2009 r.	Aktualizacja profili certyfikatów.
3.7	15 kwietnia 2010 r.	Dodano informacje dotyczące zgodności działania CERTUM z wymaganiami standardów AICPA/CICA WebTrust Program for Certification Authorities Version 1.0 oraz Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements) [CWA 14167-1:2003]. Zaktualizowano słownik pojęć. Usunięto III kategorię certyfikatów kwalifikowanych. Dodano informację o możliwości generowania klucza prywatnego przez subskrybenta oraz wydawania certyfikatów z początkiem okresu ważności ulokowanym w przyszłości.
3.8	15 maj 2012	Aktualizacja logo CERTUM
3.9	01 kwiecień 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.
4.0	01 lipca 2016	Dostosowanie do wymogów Rozporządzenia UE 910/2014 eIDAS
4.1	23 grudzień	Dostosowanie do wymogów Ustawy o usługach zaufania oraz identyfikacji elektronicznej, aktualizacja norm.

Dodatek 1: Skróty i oznaczenia

CA urząd certyfikacji (*ang. certification authority*)

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

CRL lista certyfikatów unieważnionych, publikowana zwykle przez wydawcę tych certyfikatów

DN nazwa wyróżniona (*ang. Distinguished Name*)

GPR Główny Punkt Rejestracji

KPC Kodeks Postępowania Certyfikacyjnego

KRIO Krajowy Rejestr Identyfikatorów Obiektów

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

PC Polityka Certyfikacji

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

PR Punkt Rejestracji

PSE osobiste bezpieczne środowisko (*ang. personal security environment*)

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

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

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

Dodatek 2: Słownik pojęć

Aktualizacja certyfikatu (*ang. certificate update*) – przed upływem okresu ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności.

Audyt – dokonanie niezależnego przeglądu i oceny działania systemu w celu przetestowania adekwatności środków nadzoru systemu, upewnienia się czy system działa zgodnie z ustaloną Polityką Certyfikacji, Kodeksem Postępowania Certyfikacyjnego i wynikającymi z niej procedurami operacyjnymi oraz w celu wykrycia przekłamań zabezpieczeń i zalecenia wskazanych zmian w środkach nadzorowania, polityce certyfikacji oraz procedurach.

Autocertyfikat – dowolny certyfikat klucza publicznego przeznaczony do weryfikacji podpisu złożonego na certyfikacie, w którym podpis da się zweryfikować przy pomocy klucza publicznego zwartego w polu **subjectKeyInfo**, zawartości pól **issuer** oraz **subject** są takie same, zaś pole **cA** rozszerzenia **BasicConstrains** ustawione jest na **true**.

Bezpieczna ścieżka (*ang. trusted path*) – łącze zapewniające wymianę informacji związanych z uwierzytelnieniem użytkownika komputera, aplikacji lub innego urządzenia (np. identyfikacyjnej karty elektronicznej), zabezpieczone w sposób uniemożliwiający naruszenie integralności przesyłanych danych przez jakiekolwiek oprogramowanie.

CERTUM - Powszechne Centrum Certyfikacji (w skrócie: CERTUM) – jednostka usługowa Asseco Data Systems S.A., świadcząca niekwalifikowane i kwalifikowane usługi certyfikacyjne. Kwalifikowane usługi certyfikacyjne świadczy w zakresie wydawania kwalifikowanych certyfikatów klucza publicznego, znakowania czasem, weryfikowania statusu certyfikatów w trybie on-line, walidacji danych oraz poświadczania odbioru i przedłożenia, w szczególności zgodnie z *Ustawą z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016r. poz. 1579).*

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

UWAGA: Certyfikat może znajdować się w jednym z trzech podstawowych stanów (patrz Stany klucza kryptograficznego): w oczekiwaniu na aktywność, aktywny i uśpiony.

Certyfikat atrybutów (AC) – elektroniczne zaświadczenie za pomocą którego wartości atrybutów są przyporządkowane do wskazanej w zaświadczeniu osoby i powiązane z danymi identyfikacyjnymi tej osoby.

Certyfikat kwalifikowany osobisty (uniwersalny) – Certyfikat kwalifikowany osobisty może zawierać jedynie dane osobowe lub dane osobowe oraz dane reprezentowanego podmiotu i może być stosowany we wszystkich kontaktach z administracją publiczną, wszelkimi instytucjami (w tym z ZUS) oraz w relacjach biznesowych. Osoba posiadająca taki certyfikat i składająca podpis elektroniczny może działać zarówno we własnym imieniu, jak i w imieniu reprezentowanego podmiotu bez konieczności wpisania informacji o tym podmiocie do certyfikatu jeśli tylko zakres uprawnień danej osoby fizycznej wynika bezpośrednio z przepisów prawa. Subskrybent indywidualny zamawia certyfikat we własnym imieniu, do realizacji własnych potrzeb i jest jego właścicielem. Certyfikat kwalifikowany osobisty, zwierający dane subskrybenta, może zostać unieważniony tylko na jego wniosek.

Certyfikat kwalifikowany profesjonalny (z dodatkowymi danymi) – Certyfikat kwalifikowany profesjonalny oprócz danych osobowych zawiera informacje takie jak dane reprezentowanego podmiotu może być stosowany we wszystkich kontaktach z administracją

publiczną, wszelkimi instytucjami (w tym z ZUS) oraz w relacjach biznesowych. Osoba posiadająca taki certyfikat i składająca podpis elektroniczny może działać wyłącznie w zakresie uprawnień wynikających z reprezentowania podmiotu. Certyfikat kwalifikowany profesjonalny może zostać unieważniony zarówno przez subskrybenta jak i przez upoważnionego przedstawiciela reprezentowanego podmiotu.

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

Certyfikat ważny – certyfikat klucza publicznego jest ważny wtedy i tylko wtedy, gdy: (a) został wydany przez urząd certyfikacji, (b) został zaakceptowany przez podmiot wymieniony w tym certyfikacie oraz (c) nie jest unieważniony.

Dane do audytu – chronologiczne zapisy aktywności w systemie pozwalające na zrekonstruowanie i analizowanie sekwencji zdarzeń oraz zmian, z którymi związane jest zarejestrowane zdarzenie.

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

Dane walidacyjne – dodatkowe dane gromadzone przez osobę składająca i/lub weryfikaującą podpis niezbędne w procesie weryfikacji podpisu elektronicznego; dane te mogą dotyczyć: certyfikatów, informacji o statusie unieważnienia, znaczników czasu oraz innych **poświadczeń**.

Depozyt – powierzenie przechowawcy (na podstawie umowy) do przechowania obiektów danych aż do ich odebrania przez składającego, przy zagwarantowaniu, że odebrane obiekty danych są w stanie ważności nie gorszym niż w momencie ich powierzenia; przechowawca zobowiązany jest wydać ten sam obiekt danych, który otrzymał na przechowanie, a także na żądanie wszelkie inne dane związane z nim i zapewniające mu ważność w czasie przechowywania w depozycie. Powierzone dane udostępniane są tylko depozytariuszowi (podmiotowi, który powierzył dane do przechowania).

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. W CERTUM weryfikacja tego typu powiązań (pomiędzy parami kluczy stosowanych do podpisu i szyfrowania) realizowana jest tylko przez punkty rejestracji i urzędy certyfikacji, i jest zgodna z protokołem CMP.

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.

HSM (ang. Hardware Security Module) – sprzętowy moduł kryptograficzny; patrz **moduł kryptograficzny**.

Identyfikator obiektu (OID, *ang. Object Identifier*) – identyfikator alfanumeryczny/ numeryczny zarejestrowany zgodnie z normą ISO/IEC 9834 i wskazujący w sposób unikalny na określony obiekt lub klasę obiektów.

Infrastruktura klucza publicznego (PKI) – składa się z powiązanych z sobą elementów infrastruktury sprzętowej, programowej, baz danych, sieci, procedur bezpieczeństwa oraz zobowiązań prawnych, które dzięki współpracy realizują oraz udostępniają usługi

certyfikacyjne, jak również inne związane z tymi elementami usługi (np. usługi znacznika czasu).

Klucz prywatny – klucz pary kluczy asymetrycznych podmiotu, który jest stosowany jedynie przez ten podmiot. W przypadku systemu podpisu asymetrycznego klucz prywatny określa przekształcenie podpisu. W przypadku systemu szyfrowania asymetrycznego klucz prywatny określa przekształcenie deszyfrujące.

UWAGI: (1) W kryptografii z kluczem publicznym klucz, który jest przeznaczony do deszyfrowania lub podpisywania, do wyłącznego stosowania przez swego właściciela. (2) W systemie kryptograficznym z kluczem publicznym ten klucz z pary kluczy użytkownika, który jest znany jedynie temu użytkownika.

Klucz publiczny – klucz z pary kluczy asymetrycznych podmiotu, który może być uczyniony publicznym. W przypadku systemu podpisu asymetrycznego klucz publiczny określa przekształcenie weryfikujące. W przypadku systemu szyfrowania asymetrycznego klucz publiczny określa przekształcenie szyfrujące.

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.

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

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

Kopia – każdy wpis pobrany z depozytu lub rejestru, a także każdy obiekt danych pobrany z repozytorium.

Kwalifikowane usługi certyfikacyjne – usługi certyfikacyjne udostępniane przez kwalifikowany podmiot świadczący usługi certyfikacyjne.

Kwalifikowany certyfikat – certyfikat spełniający warunki określone w *Ustawie z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016r. poz. 1579)*, wydany przez kwalifikowany podmiot świadczący usługi certyfikacyjne.

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

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

Lista unieważnionych certyfikatów atrybutów użytkowników końcowych (EARL) – lista unieważnień zawierająca listę wskazań na certyfikaty atrybutów wydanych posiadaczom, którymi nie są urzędami atrybutów i które nie mogą być dalej uważane za ważne przez wydawców tych certyfikatów

Moduł kryptograficzny – (a) zestaw składający się ze sprzętu, oprogramowania, mikrokodu lub ich określona kombinacja, realizujące operacje lub procesy kryptograficzne, obejmujące szyfrowanie i deszyfrowanie wykonywane w obszarze kryptograficznym tego modułu, (b) wiarygodna implementacja kryptosystemu, który w bezpieczny sposób wykonuje operacje szyfrowania i deszyfrowania; operacje, o których mowa powyżej wykonywane sa w oparciu o **parametry bezpieczeństwa**, które są automatycznie usuwane, jeśli urządzenie zostanie otwarte.

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.

Narodowe Centrum Certyfikacji – minister cyfryzacji lub podmiot upoważniony przez niego w trybie art. 11 *Ustawy z dnia 5 września 2016 r. o usługach zaufania oraz identyfikacji elektronicznej (Dz.U. 2016r. poz. 1579)* do wydawania zaświadczeń certyfikacyjnych, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do ministra cyfryzacji lub tego podmiotu.

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).

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

Oryginał – każdy wpis znajdujący się w depozycie lub rejestrze, a także każdy obiekt umieszczony w repozytorium; oryginalny wpis jest utworzony w chwili żądania umieszczenia wpisu obiektu w depozycie lub rejestrze, zaś oryginalny obiekt w momencie zarejestrowania w repozytorium.

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

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

Parametry bezpieczeństwa - różnorodne, niejawne składniki nadzorujące procesy bezpieczeństwa systemów informatycznych, np. hasła, klucze szyfrowe, początkowe wartości szyfrów, "ziarna" generatorów liczb pseudolosowych, biometryczne parametry tożsamości (PN I-2000).

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

Pobranie wpisu lub obiektu danych – uzyskanie kopii wpisu lub kopii obiektu, lub z repozytorium obiektów danych bez ich usuwania odpowiednio z depozytu i rejestru oraz repozytorium.

Podmiot realizujący zadania publiczne (w skrócie podmiot publiczny) – każdy podmiot, do którego stosuje się Art.2 *Ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz.U. nr 64, poz. 565)

Podmiot reprezentowany przez subskrybenta – osoba lub instytucja, w imieniu której subskrybent posługuje się certyfikatem kwalifikowanym. Podmiot reprezentowany przez subskrybenta jest właścicielem certyfikatu i przysługuje mu prawo do zgłoszenia jego unieważnienia w przypadkach przewidzianych uregulowaniach Kodeksu Postępowania Certyfikacyjnego.

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

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

Polityka podpisu – szczegółowe rozwiązania, w tym techniczne i organizacyjne, wskazujące sposób, zakres oraz warunki potwierdzania oraz weryfikacji podpisu elektronicznego, których przestrzeganie umożliwia stwierdzenie ważności podpisu.

Posiadacz sekretu współdzielonego – autoryzowany posiadacz karty elektronicznej, na której przechowywany jest sekret współdzielony.

Poświadczenie - informacja, która samodzielnie lub użyta w powiązaniu z inną informacją wykorzystywana jest w celu ustanowienia dowodu wystąpienia lub niewystąpienia zdarzenia lub działania (PN ISO/IEC 13888-1).

Poświadczenie elektroniczne – dane w postaci elektronicznej, które wraz z innymi danymi, do których zostały dołączone lub logicznie z nimi powiązane, umożliwiają identyfikację podmiotu świadczącego usługi certyfikacyjne lub organu wydającego zaświadczenia certyfikacyjne.

Poświadczenie odbioru - dane elektroniczne dołączone do dokumentu elektronicznego doręczanego adresatowi (odbiorcy) lub połączone z tym dokumentem w taki sposób, że jakakolwiek późniejsza zmiana dokonana w tym dokumencie jest rozpoznawalna; poświadczenie to określa:

a) pełną nazwę adresata, któremu doręczono dokument elektroniczny,

b) datę i czas doręczenia dokumentu elektronicznego rozumiane jako data i czas wprowadzenia albo przeniesienia dokumentu elektronicznego do tego obszaru systemu teleinformatycznego, który jest dostępny dla adresata tego dokumentu; jest to data i czas otrzymania dokumentu elektronicznego według adresata,

c) potwierdzenie (podpis) adresata odebrania dokumentu,

d) datę i czas wytworzenia poświadczenia odbioru potwierdzone kwalifikowanym znacznikiem czasu synchronizowanym z sygnałem urzędowego i uniwersalnego czasu koordynowanego UTC(PL).

W przypadku, gdy poświadczenie jest wystawiane przez kwalifikowany urząd poświadczeń odbioru i przedłożenia, poświadczenie odbioru jest odsyłane do nadawcy dokumentu oraz do odbiorcy dokumentu.

Poświadczenie przedłożenia – dane elektroniczne potwierdzające, że kwalifikowany urząd poświadczeń odbioru i przedłożenia otrzymał dokument elektroniczny do przesłania

adresatowi i połączone z tym dokumentem w taki sposób, że jakakolwiek późniejsza zmiana dokonana w tym dokumencie jest rozpoznawalna; poświadczenie to określa:

a) pełną nazwę nadawcy dokumentu elektronicznego,
b) pełną nazwę adresata, do którego powinien zostać doręczony dokument elektroniczny,
c) pełną nazwę urzędu wydającego poświadczenie,
d) datę i czas przedłożenia dokumentu elektronicznego rozumiane jako data i czas wprowadzenia albo przeniesienia dokumentu elektronicznego do tego obszaru systemu teleinformatycznego, który jest dostępny dla urzędu poświadczeń odbioru i przedłożenia,
e) datę i czas wytworzenia poświadczenia przedłożenia potwierdzone kwalifikowanym znacznikiem czasu synchronizowanym z sygnałem urzędowego i uniwersalnego czasu koordynowanego UTC(PL).

Poświadczenie przedłożenia jest odsyłane do nadawcy dokumentu i/lub do odbiorcy dokumentu.

Procedura postępowania w sytuacji awaryjnej – procedura będąca alternatywą dla normalnej ścieżki realizacji procesu jeśli wystąpi sytuacja nadzwyczajna, lecz przewidywana.

Przejścia między stanami klucza – stan klucza kryptograficznego może ulec zmianie tylko w przypadku, gdy nastąpi jedno z przejść (zgodnie z normą ISO/IEC 11770-1):

generowanie – proces tworzenia klucza; generowanie klucza powinno być wykonywane zgodnie z ustalonymi zasadami generowania kluczy; proces może obejmować procedurę testową, służącą weryfikacji stosowania tych zasad,

aktywacja – powoduje, że klucz uzyskuje ważność i może być stosowany w operacjach kryptograficznych,

deaktywacja – ogranicza użycie klucza; sytuacja taka może zdarzyć się na skutek upływu terminu ważności klucza lub unieważnienia klucza,

reaktywacja – umożliwia ponowne użycie klucza znajdującego się w stanie ustania aktywności do operacji kryptograficznych,

zniszczenie – powoduje zakończenie cyklu życia klucza; pod tym pojęciem rozumie się logiczne zniszczenie klucza, ale może także oznaczać zniszczenie fizyczne.

Publikowanie certyfikatów i list certyfikatów unieważnionych (CRL) (*ang. certificate and certificate revocation lists publication*) – procedury dystrybucji utworzonych i unieważnionych certyfikatów. Dystrybucja certyfikatu obejmuje przesłanie go do subskrybenta oraz może obejmować jego publikację w repozytorium urzędu certyfikacji. Z kolei dystrybucja list certyfikatów unieważnionych oznacza umieszczenie ich w repozytorium urzędu certyfikacji, 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 Potwierdzania Tożsamości (PPT) – jego funkcją jest potwierdzanie tożsamości subskrybenta i zawarcie umowy o świadczenie kwalifikowanych usług certyfikacyjnych w procesie wydawania kwalifikowanych certyfikatów.

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

Punkt zaufania – najbardziej zaufany urząd certyfikacji, któremu ufa subskrybent lub strona ufająca. Certyfikat tego urzędu jest pierwszym certyfikatem w każdej ścieżce certyfikacji, zbudowanej przez subskrybenta lub stronę ufająca. Wybór punktu zaufania jest zwykle narzucany przez politykę certyfikacji, według której funkcjonuje podmiot świadczący usługi certyfikacyjne.

Recertyfikacja (*ang. certificate update*) – przed upływem okresu ważności certyfikatu urząd certyfikacji może odświeżyć go (zaktualizować), potwierdzając ważność tej samej pary kluczy na następny, zgodny z polityką certyfikacji, okres ważności.

Rejestr – uporządkowany w oparciu o jedno kryterium spis lub wykaz czegoś, np.: rejestr przedsiębiorstw państwowych, rejestr statków, rejestr stowarzyszeń, rejestr skazanych, rejestr spraw (ogólnie nazywanych rejestrami obiektami danych). Dalej pod tym pojęciem będziemy rozumieć wykaz, listę, spis lub inną formę ewidencji obiektów danych, służących do realizacji zadań wykonywanych przez administrację państwową, sądy, banki lub firmy prowadzące działalność gospodarczą. Rejestr zawiera wpisy związane z opisem zarejestrowanego obiektu (zarejestrowane obiekty mogą być dowolnymi elementami, które ich autor lub twórca chce udostępnić innym w taki sposób, aby mógł być łatwo odnaleziony i zastosowany przez klienta lub użytkownika). Wpisy w rejestrze mogą podlegać kontroli dostępu.

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

Repozytorium obiektów danych – rozwiązanie informatyczne przeznaczone do składowania i obsługi obiektów danych. Dostęp do obiektów zarejestrowanych w repozytorium obiektów danych odbywa się za pomocą referencji do tych obiektów, zapisanych w rejestrze. Repozytorium zapewnia kontrolowany dostęp do przechowywanych w nim obiektów danych, monitorowanie ich wersji, katalogowania, wyszukiwania oraz aktualizowania.

Rozporządzeniem e-IDAS - Rozporządzenia Parlamentu Europejskiego i Rady (UE) NR 910/2014 w sprawie identyfikacji elektronicznej i usług zaufania w odniesieniu do transakcji elektronicznych na rynku wewnętrznym oraz uchylające dyrektywę 1999/93/WE.

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**.

Stany klucza kryptograficznego (prywatnego, publicznego) – klucze kryptograficzne mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

w oczekiwaniu na aktywność (gotowy) – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku,

aktywny – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów elektronicznych),

uśpiony – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu elektronicznego lub deszyfrowania.

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

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

System informacyjny – całość infrastruktury, organizacja, personel oraz komponenty służące do gromadzenia, przetwarzania, przechowywania, przesyłania, prezentowania, rozgłaszania i zarządzania informacją.

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

Ścieżka certyfikacji (def.2) – uporządkowany ciąg zaświadczeń certyfikacyjnych lub zaświadczeń certyfikacyjnych i certyfikatu utworzony w ten sposób, że przy pomocy danych służących do weryfikacji poświadczenia elektronicznego i nazwy wydawcy pierwszego zaświadczenia certyfikacyjnego na ścieżce możliwe jest wykazanie, że dla każdych dwóch bezpośrednio po sobie występujących zaświadczeń certyfikacyjnych lub zaświadczenia certyfikacyjnego i certyfikatu poświadczenie elektroniczne zawarte w jednym z nich zostało sporządzone przy pomocy danych służących do składania poświadczenia elektronicznego związanych z drugim z nich; dane służące do weryfikacji pierwszego poświadczenia elektronicznego są dla weryfikującego „punktem zaufania".

Token - dane zawierające informacje, które zostały przekształcone z wykorzystaniem techniki kryptograficznej (PN I-2000)

Token statusu certyfikatu – dane w postaci elektronicznej, które zawierają informacje o aktualnym statusie certyfikatu, zaświadczenia certyfikacyjnego, ścieżki certyfikacji, do której należy określony certyfikat lub zaświadczenie certyfikacyjne oraz inne informacje przydatne podczas weryfikacji podpisu elektronicznego, poświadczone elektronicznie przez urząd weryfikacji statusu certyfikatu.

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

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

Umowa z subskrybentem – umowa zawierana jest pomiędzy Asseco Data Systems S.A. a subskrybentem zamawiającym certyfikat kwalifikowany osobisty do działania we własnym imieniu lub certyfikat kwalifikowany profesjonalny do wykonywania zadań w imieniu podmiotu reprezentowanego przez subskrybenta.

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

Urząd atrybutów (AA) – urząd, który wydając certyfikaty atrybutów poświadcza atrybuty przypisane posiadaczom tych certyfikatów.

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.

Urzędowe poświadczenie odbioru – poświadczenie odbioru dokumentu elektronicznego, którego adresatem jest podmiot publiczny.

Urzędowe poświadczenie przedłożenia – poświadczenie przedłożenia dokumentu elektronicznego, którego adresatem jest podmiot publiczny.

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.

Walidacja danych - proces stosowany w celu rozstrzygnięcia tego, czy dane są poprawne, kompletne lub czy spełniają wskazane kryteria. Walidacja danych może obejmować kontrole formatu, kontrole kompletności, testy klucza kryptograficznego, kontrole sensowności oraz kontrole wartości granicznych (PN I-2000).

Walidacja podpisu elektronicznego – patrz **weryfikacja podpisu elektronicznego**.

Ważny certyfikat – patrz **certyfikat ważny**.

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

Weryfikacja podpisu elektronicznego – walidacja danych, która ma na celu określenie przynajmniej, że 1) podpis elektroniczny został zrealizowany za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w podpisanym przez urząd certyfikacji certyfikacie subskrybenta, że 2) podpisana wiadomość (dokument) nie została zmodyfikowana już po złożeniu na nim podpisu oraz, że 3) format podpisu, certyfikatu i innych **danych walidacyjnych** związanych z podpisem jest zgodny z odpowiednimi wymaganiami (np. z przepisami prawa).

Weryfikacja statusu certyfikatów (*ang. validation of public key certificates*) – walidacja danych, która 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.

Wydanie wpisu lub obiektu danych – uzyskanie oryginału wpisu lub obiektu z jego jednoczesnym usunięciem z depozytu; z rejestrów lub repozytorium nie powinno się nic usuwać, ale można edytować wpisy i obiekty z zachowaniem oczywiście historii zmian.

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

Wzajemne zaświadczenie certyfikacyjne (ang. *cross-certificate*) – jest to takie zaświadczenie certyfikacyjne klucza publicznego wydane urzędowi certyfikacji, w którym nazwy wystawcy i podmiotu tego certyfikatu są różne, klucz publiczny zawarty w zaświadczeniu może być używany jedynie do weryfikacji poświadczeń elektronicznych oraz wyraźnie jest zaznaczone, że zaświadczenie certyfikacyjne należy do urzędu certyfikacji.

Zaświadczenie certyfikacyjne – elektroniczne zaświadczenie za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do podmiotu świadczącego usługi certyfikacyjne lub organu, które umożliwiają identyfikację tego podmiotu lub organu.

Zaufana Trzecia Strona (TTP) – instytucja lub jej przedstawiciel mający zaufanie podmiotu uwierzytelnionego i/lub podmiotu weryfikującego oraz innych podmiotów w zakresie działań związanych z zabezpieczeniem oraz z uwierzytelnianiem.

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

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

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

X.500 – norma międzynarodowa określająca protokół dostępu do katalogu DAP (*ang. Directory Access Protocol*), oraz protokół usług katalogowych DSP (*ang. Directory Service Protocol*).