Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM

Wersja 4.3

Data: 23 grudzień 2016 r.

Status: archiwalny

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

Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM określa ogólne zasady stosowane przez wyodrębnioną część CERTUM (pełna nazwa: CERTUM - Powszechne Centrum Certyfikacji) w trakcie świadczenia usług certyfikacyjnych, polegających na:

- wydawaniu **kwalifikowanych certyfikatów klucza publicznego**[1], obejmującym rejestrację **subskrybentów**[2], certyfikację kluczy publicznych oraz aktualizację kluczy i certyfikatów,
- **unieważnianiu i zawieszaniu certyfikatów**,
- wystawianiu **tokenów znaczników czasu, tokenów statusu certyfikatów, tokenów walidacji danych** oraz **poświadczeń odbioru i przedłożenia** (w tym także **urzędowych poświadczeń odbioru i przedłożenia**[3]),
- wydawaniu **poświadczeń o przechowywaniu obiektów danych** (w szczególności obiektów podpisanych) **w depozycie**, **rejestrach i repozytoriach** oraz ich udostępnianiu, modyfikowaniu i usuwaniu.
- wydawaniu **certyfikatów atrybutów**, ich udostępnianiu oraz unieważnianiu.

Powyższe usługi są świadczone zgodnie z:

- wdrożonym przez Asseco Data Systems S.A. Zintegrowanym Systemem Zarządzania, który obejmuje zwłaszcza wymagania standardów PN-EN ISO:9001:2009 oraz PNISO/IEC 27001:2014,
- Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016, poz. 1579)
- standardem WebTrust[4] 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.
- 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, zwanym dalej w treści niniejszego dokumentu *Rozporządzeniem eIDAS*

---

[1] Określenia lub skróty i oznaczenia wprowadzane po raz pierwszy będą wyróżniane w tekście tłustym drukiem; ich znaczenie zdefiniowane jest w **Słowniku pojęć**, zamieszczonym na końcu dokumentu lub w rodz.1.7.

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

[3] 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) z późniejszymi zmianami. Patrz także: Słownik pojęć.

4 AICPA/CICA WebTrust Program for Certification Authorities

Niniejszy Kodeks Postępowania Certyfikacyjnego definiuje także uczestników tego procesu, ich obowiązki i odpowiedzialność, typy certyfikatów, procedury weryfikacji tożsamości używane przy ich wydawaniu oraz obszary zastosowań. Znajomość natury, celu oraz roli Kodeksu Postępowania Certyfikacyjnego, jak również Polityki Certyfikacji jest szczególnie istotna z punktu widzenia **Subskrybenta** oraz **strony ufającej**[5].

Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług precyzuje zasady, według których **CERTUM** wydaje użytkownikom końcowym kwalifikowane certyfikaty, znaczniki czasu, tokeny statusu certyfikatów, tokeny walidacji danych, poświadczenia odbioru i przedłożenia (w tym także urzędowe poświadczenia odbioru i przedłożenia), poświadczenia depozytowe, rejestrowe i repozytoryjne (o przechowywaniu podpisanych obiektów oraz ich udostępnianiu, modyfikowaniu i usuwaniu), certyfikaty atrybutów oraz zaświadczenia certyfikacyjne, zgodnie z wymaganiami wynikającymi z *Rozporządzenia Ministra Cyfryzacji z dnia 5 października 2016r. w sprawie krajowej infrastruktury zaufania*. Obszary zastosowań kwalifikowanych certyfikatów, tokenów statusu certyfikatów, tokenów walidacji danych, poświadczeń odbioru i przedłożenia (w tym także urzędowych poświadczeń odbioru i przedłożenia), poświadczeń depozytowych, rejestrowych i repozytoryjnych (o przechowywaniu podpisanych obiektów oraz ich udostępnianiu, modyfikowaniu i usuwaniu), certyfikatów atrybutów i zaświadczeń certyfikacyjnych wystawianych zgodnie z niniejszym dokumentem opisane są w rozdz.1.4, z kolei odpowiedzialność wynikająca ze stosowania ich przez CERTUM oraz użytkowników końcowych – w rozdz.2.2.

Struktura i merytoryczna zawartość Kodeksu Postępowania Certyfikacyjnego są zgodne z zaleceniem RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. Kodeks Postępowania Certyfikacyjnego został utworzony przy założeniu, że czytelnik jest ogólnie zaznajomiony z pojęciami dotyczącymi zaświadczeń certyfikacyjnych, certyfikatów, podpisów elektronicznych oraz Infrastruktury Klucza Publicznego (PKI).

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

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*).

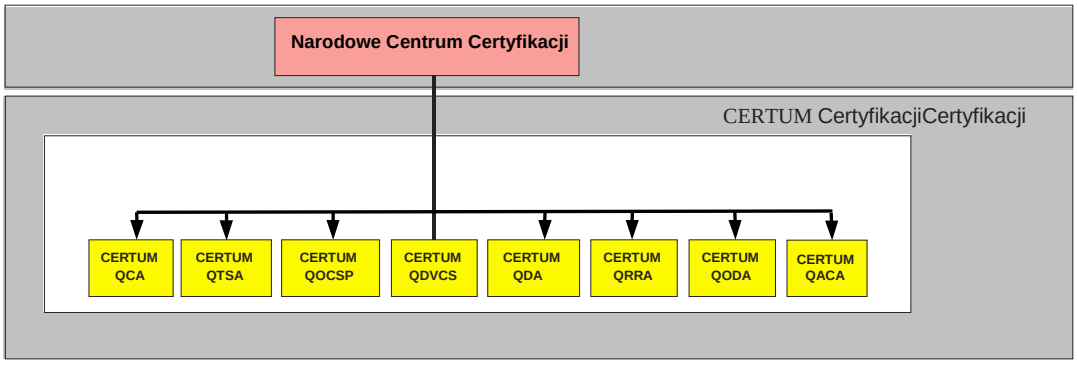
W związku z przeniesieniem całego majątki Spółki Unizeto Technologies S.A. na Spółkę Asseco Data Systems S.A. oświadczamy, że Spółka Asseco Data System S.A. zobowiązuje się do utrzymywania zaświadczenia certyfikacyjnego wydanego na Spółkę Unizeto Technologies S.A. do czasu wygaśnięcia ostatniego certyfikatu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

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

1.1. Wprowadzenie

Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM opisuje zakres działania **CERTUM** (działającego w ramach Asseco Data Systems S.A.) oraz związanych z nim **punktów rejestracji, subskrybentów**, jak również **stron ufających**. Określa także ogólne zasady świadczenia kwalifikowanych usług certyfikacyjnych, zgodnych z*) Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016r., poz. 1579), dalej w tekście zwanej Ustawą* tj. **wydawania kwalifikowanych certyfikatów** obejmującego rejestrację subskrybentów, certyfikację kluczy publicznych i aktualizację kluczy oraz certyfikatów, **unieważniania i zawieszania certyfikatów**, oraz wystawiania **tokenów znaczników czasu**, **tokenów weryfikacji statusu certyfikatów**, **tokenów walidacji danych, poświadczeń odbioru i przedłożenia** (w tym także **urzędowych poświadczeń odbioru i przedłożenia**), **poświadczeń depozytowych, rejestrowych i repozytoryjnych** (o przechowywaniu podpisanych obiektów oraz ich udostępnianiu, modyfikowaniu i usuwaniu) oraz certyfikatów atrybutów. Wydawanie certyfikatów, tokenów oraz poświadczeń odbywa się w oparciu o zaświadczenia certyfikacyjne wydane zgodnie z wymaganiami określonymi w *Ustawie*. Do zasad przedstawionych w tym dokumencie dostosowane powinny być działania tych podmiotów i dostawców usług, którzy korzystają z certyfikatów klucza publicznego i zaświadczeń certyfikacyjnych wystawionych przez CERTUM.

CERTUM świadczące kwalifikowane usługi tworzy oddzielną domenę certyfikacji z wydzielonym kwalifikowanym urzędem certyfikacji **CERTUM QCA**[6], kwalifikowanym urzędem znakowania czasem **CERTUM QTSA**[7], kwalifikowanym urzędem weryfikacji statusu certyfikatu **CERTUM QOCSP**[8], kwalifikowana usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS**[9], urzędem poświadczeń odbioru i przedłożenia **CERTUM QDA**[10], urzędem depozytów obiektów **CERTUM QODA**[11], urzędem rejestrów i repozytoriów **CERTUM QRRA**[12] oraz urzędem certyfikatów atrybutów **CERTUM QACA**[13]. Wymienione urzędy świadczą usługi w oparciu o zaświadczenia certyfikacyjne, wystawione przez ministra cyfryzacji lub upoważniony przez niego podmiot świadczący usługi certyfikacyjne w trybie Art.10.1 *Ustawy* (na rys.1 wystawca tych zaświadczeń certyfikacyjnych oznaczony jest jako **Narodowe Centrum Certyfikacji**).



[6] CA – *ang. Certification Authority*

[7] TSA – *ang. Time Stamping Authority*

[8] OCSP – *ang. On-line Certificate Status Protocol*

[9] DVCS – *ang. Data Validation and Certification Server*

[10] DA – *ang. Delivery Authority*

[11] ODA – *ang. Objects Deposits Authority*

[12] RRA – *ang. Registries and Repositories Authority*

[13] ACA – *ang. Attribute Certificate Authority*

Rys.1 Urzędy działające w ramach **kwalifikowanych usług CERTUM**.

Niniejszy Kodeks Postępowania Certyfikacji odnosi się do urzędu certyfikacji **CERTUM QCA** i związanych z nim punktów rejestracji, urzędu znakowania czasem **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, kwalifikowanej usługi walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS**, urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA**, urzędu rejestrów i repozytoriów **CERTUM QRRA**, urzędu certyfikatów atrybutów **CERTUM QACA**, a także konsumentów tych usług - subskrybentów kwalifikowanych certyfikatów, tokenów znacznika czasu, tokenów weryfikacji statusu certyfikatu, tokenów walidacji danych, poświadczeń odbioru i przedłożenia (w tym także urzędowych poświadczeń odbioru i przedłożenia), poświadczeń depozytowych, rejestrowych i repozytoryjnych, certyfikatów atrybutów oraz stron ufających, korzystających z usług lub wymieniających jakiekolwiek wiadomości z domeną **CERTUM**.

Certyfikaty i zaświadczenia wydawane przez CERTUM zawierają identyfikatory polityk certyfikacji[14], które umożliwiają stronom ufającym określenie, czy weryfikowane przez nie użycie certyfikatu jest zgodne z deklarowanym przeznaczeniem certyfikatu. Deklarowane przeznaczenie certyfikatu można określić na podstawie wpisów umieszczanych w strukturze **PolicyInformation** rozszerzenia **certificatePolicies** (patrz rozdz.7.1.1.2) każdego certyfikatu wydawanego przez CERTUM.

Identyfikatory polityk certyfikacji umieszczane są także w tokenach wystawianych przez kwalifikowany urząd znakowania czasem **CERTUM QTSA**, kwalifikowaną usługę walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS**, urząd poświadczania odbioru i przedłożenia **CERTUM QDA,** urząd depozytów obiektów **CERTUM QODA** urząd rejestrów i repozytoriów **CERTUM QRRA** oraz urząd certyfikatów atrybutów **CERTUM QACA**.

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

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

[14] Identyfikatory polityk certyfikacji dla kwalifikowanych usług Unizeto CERTUM budowane są w oparciu o identyfikator obiektu Unizeto Technologies S.A. zarejestrowany w Krajowym Rejestrze Identyfikatorów Obiektów (KRIO, http://www.krio.pl). Identyfikator ten ma wartość:

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

Tab. 1 Ważniejsze dokumenty towarzyszące Kodeksowi Postępowania Certyfikacyjnego

L.p.	Nazwa dokumentu	Status dokumentu	Sposób udostępniania
1.	Polityka Certyfikacji Kwalifikowanych Usług CERTUM	Jawny	http://www.certum.pl
2.	Dokumentacja zarządzania cyklem życia kluczy urzędów certyfikacji	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
3.	Dokumentacja personelu, zakres obowiązków i odpowiedzialności	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
4.	Dokumentacja punktu rejestracji	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
5.	Dokumentacja infrastruktury technicznej	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
6.	Dokumentacja zarządzania ciągłością działalności systemu	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
7.	Zarządzanie bezpieczeństwem CERTUM	Niejawny	lokalnie – tylko uprawnione osoby oraz audytorzy
8.	Informacja o infrastrukturze klucza publicznego CERTUM QCA	Jawny	http://www.certum.pl
9.	Polityka walidacji kwalifikowanej usługi CERTUM's Certum QDVCS walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych	Jawny	http://www.certum.pl

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

1.2. Nazwa dokumentu i jego identyfikacja

Niniejszemu dokumentowi Kodeksowi Postępowania Certyfikacyjnego przypisuje się nazwę własną o następującej postaci: **Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM** i jest on dostępny w postaci elektronicznej w serwisie internetowym urzędu certyfikacji dostępnym pod adresem http://www.certum.pl,

Z dokumentem Kodeksu Postępowania Certyfikacyjnego związany jest następujący zarejestrowany identyfikator obiektu (OID: 1.2.616.1.113527.2.4.1.0.1.4.3)[15]:

```
id-cck-kpc-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-kpc(1)
        version(4) 3}
```

[15] Identyfikatora dokumentu Kodeksu Postępowania Certyfikacyjnego nie należy mylić z identyfikatorem polityki certyfikacji (tzw. identyfikatorem OID), umieszczanym w treści wystawianego certyfikatu (patrz Tab.1.3); identyfikator dokumentu Kodeksu Postępowania Certyfikacyjnego jest tylko jeden, identyfikatorów polityki certyfikacji, według których wystawiane są certyfikaty może być więcej niż jeden.

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

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

1.3. Strony Kodeksu Postępowania Certyfikacyjnego

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

- kwalifikowanego urzędu certyfikacji **CERTUM QCA**,
- kwalifikowanego urzędu znacznika czasu **CERTUM QTSA**,
- kwalifikowanego urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**,
- kwalifikowanej usługi walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych **CERTUM QDVCS**,
- urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**,
- urzędu depozytów obiektów **CERTUM QODA**,
- urzędu rejestrów i repozytoriów **CERTUM QRRA**,
- urzędu certyfikatów atrybutów **CERTUM QACA**,
- Głównego Punktu Rejestracji (GPR),
- punktów rejestracji (PR),
- osób potwierdzających tożsamość,
- subskrybentów,
- stron ufających.

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

CERTUM świadczy kwalifikowane usługi certyfikacyjne w zakresie:

1. wydawania kwalifikowanych certyfikatów, w ramach których dokonuje następujących czynności:
    - rejestruje subskrybentów,
    - generuje klucze i kwalifikowane certyfikaty,

- dostarcza informacje o statusie certyfikatu w oparciu o listy certyfikatów unieważnionych,

2. unieważniania i zawieszania certyfikatów,
3. znakowania czasem,
4. weryfikowaniu statusu certyfikatów w trybie on-line,
5. walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych,
6. wystawiania poświadczeń odbioru i przedłożenia (w tym także urzędowych poświadczeń odbioru i przedłożenia),
7. wystawiania poświadczeń depozytowych o przechowywaniu, wydawaniu i pobieraniu obiektów w depozycie (w tym obiektów podpisanych),
8. wystawiania poświadczeń rejestrowych i repozytoryjnych o przechowywaniu, pobieraniu i modyfikowaniu wpisów w rejestrach oraz obiektów (w tym obiektów podpisanych) w repozytoriach,
9. wystawiania certyfikatów atrybutów oraz ich udostępniania i unieważniania.

1.3.1. Kwalifikowany urząd certyfikacji CERTUM QCA

W skład CERTUM świadczące usługi kwalifikowane wchodzi jeden urząd certyfikacji **CERTUM QCA** (rys.1), 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** wydaje kwalifikowane certyfikaty i zaświadczenia certyfikacyjne zgodne z politykami certyfikacji o identyfikatorach określonych w Tab.2 i w rozdz.7.1.1.2 oraz zgodnie z:

- *Rozporządzeniem eIDAS*
- *Ustawą o usługach zaufania oraz identyfikacji elektronicznej z dnia 5 września 2016 r. (Dz. U. 2016r., poz. 1579)Rozporządzeniem Ministra Cyfryzacji z dnia 5 października 2016r. (Dz.U. z 2016r. poz. 1632)*
- *standardem WebTrust Program for CAs 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.*

***Punktem zaufania** wszystkich subskrybentów i stron ufających dla kwalifikowanych usług **CERTUM** jest **Narodowe Centrum Certyfikacji** (rys.1). Oznacza to, że każda budowana przez nich ścieżka certyfikacji powinna prowadzić od certyfikatu krajowego urzędu certyfikacji dla **CERTUM QCA**.*

Urząd certyfikacji **CERTUM QCA** świadczy usługi certyfikacyjne dla:

- samego siebie (wystawia i zarządza zaświadczeniami certyfikacyjnymi),

- ministra cyfryzacji lub upoważnionego przez niego podmiotu świadczącego usługi certyfikacyjne;
- osób fizycznych, które dzięki kwalifikowanym certyfikatom chcą składać bezpieczne podpisy elektroniczne w rozumieniu *Rozporządzenia eIDAS*,
- operatorów systemu punktów rejestracji,
- personelu **CERTUM**.

Urząd certyfikacji **CERTUM QCA** świadczy usługi wydawania certyfikatów kwalifikowanych w strukturze eIDAS zgodnie *z rozporządzeniem UE 910/2014 z dniaz 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 oraz decyzjami wykonawczymi do niniejszego rozporządzenia.*

Tab. 2 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.)	1.2.616.1.113527.2.4.1.11
Certyfikaty kwalifikowane (struktura eIDAS) karta	1.2.616.1.113527.2.4.1.12.1
Certyfikaty kwalifikowane (struktura eIDAS) HSM	1.2.616.1.113527.2.4.1.12.2
Zaświadczenia certyfikacyjne	2.5.29.32.0

1.3.2. Kwalifikowany urząd znacznika czasu CERTUM QTSA

Elementem infrastruktury CERTUM dla kwalifikowanych usług, jest urząd znacznika czasu **CERTUM QTSA**. Działa on na podstawie wpisu Asseco Data Systems S.A. na listę kwalifikowanych podmiotów świadczących usługi certyfikacyjne i w oparciu o wydane mu przez ministra cyfryzacji zaświadczenie certyfikacyjne. Nadzór nad urzędem znacznika czasu **CERTUM QTSA** sprawuje minister cyfryzacji lub wyznaczony przez niego podmiot (**Narodowe Centrum Certyfikacji**).

Urząd znacznika czasu wydaje znaczniki czasu zgodnie z zaleceniami ETSI[16].Każdy token znacznika czasu zawiera identyfikator polityki certyfikacji, według której został wystawiony (jego wartość określona jest w Tab. 3 oraz w rozdz.7.3) oraz poświadczany jest wyłącznie przy pomocy klucza prywatnego wytworzonego specjalnie dla usługi znakowania czasem.

[16] ETSI EN 319 422 Time stamping protocol and time-stamp profiles March 2016

Tab. 3 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 Tab. 3, znajdują zastosowanie przede wszystkim do zabezpieczania długookresowych podpisów elektronicznych[17] 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** (patrz rys.1) 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 elektronicznej

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

Tab. 4 Identyfikatory polityki certyfikacji akceptowane przez CERTUM QDVCS i umieszczane w tokenach walidacji

Nazwa tokena walidacji	Identyfikator polityki usługi
Kwalifikowany token walidacji kwalifikowanego podpisu elektronicznego[18]	1.2.616.1.113527.2.4.1.3.2.c[19]
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[20]	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. 4 .

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[21]. 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.

---

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

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

[20] 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.

[21] Patrz: Słownik pojęć

Tab. 5 Identyfikatory 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. 5.

Urząd CERTUM QDA wydaje 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 wydaje 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**[22] obiektów **CERTUM QODA**, regulowany 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;

[22] Patrz: Słownik pojęć

- po uwierzytelnionym wydaniu obiektu (wraz z poświadczeniami potwierdzającymi jego ważność dowodową) - **uwierzytelnione poświadczenie wydania obiektu z 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. 6 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. 6.

1.3.7. Urząd rejestrów i repozytoriów CERTUM QRRA

Urząd **rejestrów** i **repozytoriów**[23] **CERTUM QRRA**, regulowany 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.

[23] Patrz: Słownik pojęć

Tab. 7 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. 7.

1.3.8. Urząd certyfikatów atrybutów CERTUM QACA

Urząd certyfikatów atrybutów **CERTUM QACA**, regulowany 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. 8 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. 8). 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. 8, 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 **CERTUM QCA** i **CERTUM QACA** w kontaktach z subskrybentami i działają w ramach oddelegowanych im przez te urzędy uprawnień w zakresie rejestracji subskrybenta, potwierdzania jego tożsamości oraz przypisywanych mu atrybutów.

Punkty rejestracji przyjmują, weryfikują i następnie aprobują lub odrzucają - otrzymywane od wnioskodawców - wnioski o zarejestrowanie i wydanie certyfikatu klucza publicznego lub certyfikatu atrybutów oraz inne wnioski związane z zarządzaniem certyfikatami (aktualizację, modyfikację, unieważnienie certyfikatu). Weryfikacja wniosków ma na celu uwierzytelnienie (na podstawie dokumentów dołączonych do wniosku) wnioskodawcy oraz danych, które zostały umieszczone we wniosku. Stopień dokładności potwierdzania tożsamości subskrybenta oraz przypisywanych mu atrybutów wynika z ogólnych wymagań określonych w **Polityce Certyfikacji Kwalifikowanych Usług CERTUM** (patrz rozdz.3). Szczegółowy zakres obowiązków punktów rejestracji, punktów potwierdzania tożsamości i atrybutów oraz ich operatorów określany jest przez niniejszy Kodeks Postępowania Certyfikacyjnego oraz procedury funkcjonowania punktu rejestracji..

Lista aktualnie akredytowanych punktów rejestracji, punktów potwierdzania tożsamości oraz punktów potwierdzania atrybutów dostępna jest w serwisie internetowym urzędu certyfikacji **CERTUM** dostępnym pod adresem:

http://www.certum.pl

Wyróżnia się dwa typy punktów rejestracji, którym urząd certyfikacji działający w ramach **CERTUM** może przekazać część swoich uprawnień:

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

Podstawowa różnica pomiędzy wymienionymi dwoma typami punktów rejestracji polega na tym, że punkty rejestracji nie mogą – w przeciwieństwie do Głównego Punktu Rejestracji – akredytować innych punktów rejestracji oraz punktów potwierdzania tożsamości i atrybutów. Dodatkowo punkty rejestracji nie posiadają uprawnień do poświadczania wszystkich żądań subskrybentów. Uprawnienia te mogą być ograniczone tylko do niektórych spośród wszystkich dostępnych typów certyfikatów lub zaświadczeń certyfikacyjnych. Stąd:

- **PR** rejestrują subskrybentów, którzy ubiegają się o kwalifikowane certyfikaty i certyfikaty atrybutów; oprócz tego udzielają wyczerpujących informacji o podpisie elektronicznym, w tym o skutkach jakie wywołuje, udostępniają informacje o typach potwierdzanych atrybutów, zawierają umowy na świadczenie usług certyfikacyjnych jego oraz mogą sprzedawać certyfikaty oraz zestawy do składania bezpiecznego podpisu,
- **GPR** rejestruje punkty rejestracji (PR) oraz punkty potwierdzania tożsamości i atrybutów aktualnych lub przyszłych subskrybentów; nie nakłada się żadnych ograniczeń (poza tymi, które wynikają z roli pełnionych w infrastrukturze klucza publicznego CERTUM) na typy certyfikatów wydawanych subskrybentom; dodatkowo GPR zatwierdza także nazwy wyróżnione aktualnych i tworzonych w przyszłości punktów rejestracji.

Główny Punkt Rejestracji CERTUM przygotowany jest do obsługi notarialnego potwierdzenia tożsamości lub atrybutów subskrybenta lub potwierdzenia wystawionego przez uprawnioną do tego osobę, bez konieczności osobistego stawienia się subskrybenta w punkcie rejestracji.

Notariusz sporządza własnoręcznie podpisane potwierdzenie zawierające dane tożsamości lub atrybuty, stawiającej się przed nim osoby oraz dane konieczne do wystawienia certyfikatu klucza publicznego lub certyfikatu atrybutów, o który ta osoba ubiega się. Potwierdzenie to wraz z podpisaną wcześniej umową stanowi zbiór dokumentów i danych identyfikujących podmiot, na podstawie którego w punkcie rejestracji inspektor ds. rejestracji poświadcza tożsamość i/lub atrybuty wnioskodawcy oraz tworzy zgłoszenie certyfikacyjne.

Osoba potwierdzająca w imieniu CERTUM tożsamość i/lub atrybuty wnioskodawcy jest uprawniona do przyjmowania wniosków oraz zawierania umów na świadczenie usług certyfikacyjnych. Przyjęcie wniosku i sporządzenie umowy musi być poświadczone przez tą osobę własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu o potwierdzeniu tożsamości lub/atrybutów wnioskodawcy.

1.3.10. Repozytorium urzędu certyfikacji

Repozytorium urzędu certyfikacji jest zbiorem publicznie dostępnych katalogów zawierających:

- zaświadczenia certyfikacyjne urzędu certyfikacji CERTUM**,**
- certyfikaty atrybutów,

- i inne (patrz rozdział 2.6.1)

Zawartość repozytorium urzędu certyfikacji dostępna jest w serwisie internetowym dostępnym pod adresem:

http://www.certum.pl

1.3.11. Użytkownicy końcowi

Pośród użytkowników końcowych wyróżnia się subskrybentów oraz strony ufające. Subskrybent jest tym podmiotem, którego identyfikator umieszczany jest w polu **podmiot** (*ang. subject*) certyfikatu i który sam dalej nie wydaje ani certyfikatów ani zaświadczeń certyfikacyjnych innym podmiotom, lub podmiotem, który korzysta z innych usług udostępnianych przez CERTUM. Strona ufająca jest z kolei podmiotem, który posługuje się kwalifikowanym certyfikatem i/lub certyfikatem atrybutów innego podmiotu w celu zweryfikowania jego podpisu elektronicznego, przypisanych mu atrybutów lub zapewnienia poufności przesyłanej informacji.

Tab. 9 Użytkownicy kwalifikowanych certyfikatów, zaświadczeń certyfikacyjnych, tokenów i poświadczeń wydawanych przez CERTUM

Nazwa certyfikatu /zaświadczenia certyfikacyjnego /tokenu	Użytkownicy
Kwalifikowane certyfikaty	Osoba składająca (subskrybent) i weryfikująca (strona ufająca) podpis elektroniczny w rozumieniu *Rozporządzenia e-IDAS*
Zaświadczenia certyfikacyjne	Strony ufające weryfikujące podpis elektroniczny w rozumieniu *Rozporządzenia e-IDAS*
Tokeny znacznika czasu	Strony ufające składające i weryfikujące podpis elektroniczny w rozumieniu *Rozporządzenia e-IDAS*
Token weryfikacji statusu certyfikatu w trybie *on-line*	Strony ufające weryfikujące status certyfikatu kwalifikowanego, w rozumieniu *Rozporządzenia e-IDAS*i wykorzystywane podczas weryfikowania ważności podpisów elektronicznych równoważnych podpisowi własnoręcznemu
Token walidacji	Strony ufające składające i weryfikujące podpis elektroniczny oraz pieczęć elektroniczną w rozumieniu *Rozporządzenia e-IDAS*
Poświadczenia odbioru i przedłożenia (w tym także urzędowych poświadczeń odbioru i przedłożenia)	Strony ufające składające i weryfikujące podpis elektroniczny składany pod dokumentami elektronicznymi wysyłanymi do podmiotów publicznych lub niepublicznych w trybie art. 16 ust. 3 ustawy z dnia 17 lutego 2005 r. o *informatyzacji działalności podmiotów realizujących zadania publiczne* (Dz. U. Nr 64, poz. 565).
Poświadczenie depozytowe	Strony ufające (osoby fizyczne, osoby prawne i instytucje nieposiadające osobowości prawnej), które chcą w sposób wiarygodny przechowywać dowolne obiekty danych (w tym w szczególności obiekty podpisane) i odebrać je w stanie ważności nie gorszym niż w momencie ich powierzenia.
Poświadczenie rejestrowe lub poświadczenie repozytoryjne	Strony ufające (osoby fizyczne, osoby prawne i instytucje nieposiadające osobowości prawnej), które chcą umieścić w rejestrze wpisy odnoszące się do określonej klasy podmiotów, obiektów, zdarzeń,

	działań, itp. oraz opcjonalnie powiązanych z tymi klasami obiektów danych w repozytorium; wpisy oraz obiekty mają dobrze sformułowaną składnię oraz semantykę.
Certyfikaty atrybutów	Strona składająca podpis i dołączająca do niego certyfikat atrybutu oraz strona ufająca weryfikująca podpis elektroniczny lub atrybuty w przypadkach, gdy niezbędne jest zawarcie lub uzyskanie dodatkowych informacji odnoszących się do pełnionej roli, zakresu pełnomocnictwa, upoważnień itp. przez stronę weryfikowaną

1.3.11.1. Subskrybenci

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

Organizacje pragnące uzyskać dla swoich pracowników certyfikaty, 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[24].

CERTUM *oferuje certyfikaty różnych typów. Subskrybent powinien zdecydować, jaki certyfikat jest najodpowiedniejszy do jego potrzeb (patrz rozdz.1.4).*

1.3.11.2. 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), ich ważności dowodowej lub ważności przedłożonego mu obiektu danych (w szczególności dokumentu elektronicznego), 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

[24] Niezależnie od tego czy subskrybent występuje o wydanie certyfikatu indywidualnie czy też robi to w jego imieniu upoważniony przedstawiciel (dotyczy to tzw. certyfikatów kwalifikowanych profesjonalnych (z dodatkowymi danymi)), to wydanie certyfikatu musi być poprzedzone zawarciem umowy pomiędzy subskrybentem a Asseco Data Systems S.A.

- poświadczenia rejestrowego lub poświadczenia repozytoryjnego wystawionego przez urząd **CERTUM QRRA**, lub
- ważności lub aktualności powiązania pomiędzy tożsamością subskrybenta a certyfikatem atrybutów wystawionym subskrybentowi i wydanym przez urząd certyfikatów atrybutów **CERTUM QACA**.

Strona ufająca jest odpowiedzialna za weryfikację aktualnego statusu certyfikatu subskrybenta, w tym w szczególności certyfikatów atrybutów oraz innych otrzymanych od niego tokenów i poświadczeń. Decyzję taką strona ufająca musi podjąć każdorazowo, gdy chce użyć certyfikatu. tokenów i poświadczeń do zweryfikowania podpisu elektronicznego, jego ważności dowodowej lub ważności dowodowej obiektów danych. Informacje zawarte w kwalifikowanym certyfikacie lub certyfikacie atrybutów (m.in. identyfikatory i kwalifikatory polityki certyfikacji) strona ufająca powinna wykorzystać do określenia czy certyfikat został użyty zgodnie z jego deklarowanym przeznaczeniem.

1.4. Zakres stosowania certyfikatów i zaświadczeń certyfikacyjnych

Zakres stosowania kwalifikowanych certyfikatów lub certyfikatów atrybutów i zaświadczeń certyfikacyjnych określa obszary tzw. dozwolonego użycia certyfikatu lub zaświadczenia certyfikacyjnego. Obszar ten określa naturę (charakter) zastosowania certyfikatu lub zaświadczenia certyfikacyjnego (np. uwierzytelnienie, niezaprzeczalność lub poufność).

Kwalifikowane certyfikaty wystawione przez kwalifikowany urząd certyfikacji **CERTUM QCA** mogą być stosowane tylko do weryfikowania kwalifikowanych podpisów, które są niezaprzeczalnym dowodem złożenia aktu woli i powiązania z podpisywaną informacją o różnym poziomie wrażliwości.

Poziom wrażliwości informacji oraz jej podatność na naruszenie powinny zostać oszacowane przez subskrybenta. Na podstawie tego oszacowania subskrybent powinien podjąć decyzję o pożądanym zakresie stosowania certyfikatu (patrz Tab.10[25]).

Wymagania określone przez stronę ufającą muszą być skonfrontowane przez subskrybenta z zakresami stosowania (Tab. 10) oraz typami certyfikatów (patrz odpowiednio Tab. 11, Tab. 12 i **Błąd! Nie można odnaleźć źródła odwołania.**), wydawanymi przez CERTUM QCA.

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

Tab. 10 Zakresy zastosowania certyfikatów i zaświadczeń certyfikacyjnych wydawanych przez CERTUM QCA

Nazwa polityki certyfikacji	Nazwa typu certyfikatu	Zakres stosowania
CERTUM QCA QC	Kwalifikowane certyfikaty	Bardzo wysoki poziom wiarygodności tożsamości podmiotu certyfikatu. Kwalifikowane certyfikaty wydawane są: (a) osobom prywatnym, (b) osobom fizycznym, będącymi pracownikami dowolnej instytucji lub reprezentującymi tą instytucję. Certyfikaty powinny być stosowane do składania bezpiecznych podpisów elektronicznych, zapewniających integralność (i autentyczność) podpisywanej informacji i nadających jej cechę niezaprzeczalności w środowisku, w którym występuje ryzyko naruszenia informacji oraz skutki tego naruszenia mogą być wysokie. Certyfikatów tego typu można używać w transakcjach finansowych lub transakcjach o znacznym poziomie ryzyka wystąpienia oszustw, a także w tych przypadkach, w których zwykle stosowany jest podpis własnoręczny. Certyfikaty kwalifikowane nie mogą być stosowane do szyfrowania danych lub kluczy kryptograficznych (ogólnie, w operacjach, których celem jest nadanie informacji cech poufności).
CERTUM QCA CertEvidences	Zaświadczenia certyfikacyjne	Bardzo wysoki poziom wiarygodności tożsamości podmiotu zaświadczenia certyfikacyjnego. Zaświadczenia certyfikacyjne wydawane są: (a) krajowemu urzędowi certyfikacji, działającego w imieniu i z upoważnienia ministra właściwego ds. gospodarki urzędom certyfikacji, (b) na potrzeby procesu wymiany kluczy urzędu certyfikacji **CERTUM QCA**.

1.4.1. Kwalifikowane certyfikaty

CERTUM wydaje **dwa podstawowe typy kwalifikowanych certyfikatów** (patrz Tab. 11). Kwalifikowane certyfikaty z tej listy wystawiane są subskrybentom (osobom fizycznym), którzy podpiszą umowę z Asseco Data Systems S.A. na świadczenie usług certyfikacyjnych i zaakceptują postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego.

Każdy kwalifikowany certyfikat wystawiany przez **CERTUM QCA** zawiera wskazanie, że jest kwalifikowanym certyfikatem. Stosowane są dwa wskaźniki. Pierwszy umieszczony jest w rozszerzeniu **CertificatePolicies** (patrz rozdz.7.1.2.1) i zawiera tekst wyraźnej deklaracji wystawcy, że jest to kwalifikowany certyfikat. Z kolei drugi ze wskaźników umieszczany jest w rozszerzeniu **QCStatements** (patrz rozdz.7.1.2.1), które zawiera identyfikator obiektu o wartości:

```
id-etsi-qcs   OBJECT IDENTIFIER ::= { itu-t(0) identified-organization(4)
                                          etsi(0) id-qc-profile(1862) 1 }
id-etsi-qcs-QcCompliance      OBJECT IDENTIFIER ::= { id-etsi-qcs 1 }
```

oznaczający, że certyfikat jest kwalifikowanym certyfikatem, wydanym przez kwalifikowany podmiot świadczący usługi certyfikacyjne. Wymienione wskaźniki mogą wystąpić w kwalifikowanym certyfikacie jednocześnie lub też tylko jeden z nich.

Tab. 11 Typy kwalifikowanych certyfikatów oraz ich zastosowania

Komercyjna nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań

CERTUM QCA QC	CERTUM QCA Osobisty – (uniwersalny)	Kwalifikowane podpisy elektroniczne dokumentów elektronicznych, składane przez osoby prywatne; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię (imiona) subskrybenta, numer seryjny.
	CERTUM QCA Profesjonalny – (z dodatkowymi danymi)	Kwalifikowany podpisy elektroniczne dokumentów elektronicznych, składane przez osoby fizyczne, będące pracownikami lub reprezentantami firm, organizacji, organów lub innych osób fizycznych; certyfikat zawiera przynajmniej: nazwę kraju, nazwisko i imię (imiona) subskrybenta, nazwę własną reprezentowanego podmiotu i numer seryjny.

1.4.2. Zaświadczenia certyfikacyjne

Zaświadczenia certyfikacyjne wystawiane są tylko:

- ministrowi cyfryzacji lub upoważnionemu przez niego kwalifikowanemu podmiotowi świadczącemu usługi certyfikacyjne,
- **CERTUM QCA** (w momencie zmiany kluczy do składania poświadczeń elektronicznych).

Tab. 12 Typy zaświadczeń certyfikacyjnych oraz ich zastosowania

Komercyjna nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
CERTUM QCA CertEvidences	CERTUM QCA Cross-Cert	Zaświadczenie certyfikacyjne wydane ministrowi cyfryzacji lub upoważnionemu przez niego podmiotowi świadczącemu usługi certyfikacyjne.
	CERTUM QCA Internal	Zaświadczenie certyfikacyjne wydawane na potrzeby procesu wymiany kluczy urzędu certyfikacji CERTUM QCA.

1.4.3. Rekomendowane urządzenia

Certyfikaty lub zaświadczenia certyfikacyjne wystawione dla kwalifikowanych usług zgodnie z jedną z polityk certyfikacji CERTUM mogą być stosowane z urządzeniami, które spełniają wymagania określone 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.”.

Lista bezpiecznych urządzeń opublikowana jest w serwisie internetowym CERTUM dostępnym pod adresem: http://www.certum.pl. .

Lista kwalifikowanych bezpiecznych urządzeń publikowana jest zgodnie z art. 31 *Rozporządzenia eIDAS*.

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§2pkt. 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. **CERTUM QTSA** wystawia tokeny znacznika czasu zgodnie z wymaganiami *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*, March 2016.

Usługa znacznika czasu jest publicznie dostępna. Urząd znacznika czasu **CERTUM QTSA** sprawdza jednak autentyczność każdego zgłoszenia żądania usługi i nie realizuje jej, gdy zgłoszenie nie odpowiada prawidłowemu formatowi.

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 e-IDAS*. 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. Np. jeśli do depozytu został złożony podpisany dokument, to po wydaniu tego obiektu z depozytu ważność zarówno obiektu, jak również podpisu elektronicznego będzie taka sama, jak w momencie ich składania do depozytu.

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.

Urząd certyfikatów atrybutów **CERTUM QACA** wydaje **trzy podstawowe typy certyfikatów atrybutów** (patrz Tab. 13). Certyfikaty atrybutów wystawiane są dowolnym subskrybentom (osobom fizycznym), którzy zaakceptują postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego. Certyfikaty atrybutów mogą być wydawane także: personelowi CERTUM, pracownikom punktów rejestracji, punktów potwierdzania tożsamości i atrybutów, które działają w imieniu CERTUM.

Tab. 13 Zakres zastosowania certyfikatów atrybutów wydawanych przez CERTUM QACA

Komercyjna nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań

Komercyjna nazwa polityki certyfikacji	Komercyjna nazwa typu certyfikatu	Opis i zalecane obszary zastosowań
CERTUM QACA Standard Policy	CERTUM QACA Standard	Certyfikaty wydawane na potrzeby procesu składania podpisu kwalifikowanego i jawnie powiązane są z certyfikatami kwalifikowanymi. Certyfikat atrybutów zawęża obszar zastosowań certyfikatu kwalifikowanego) i w związku z tym weryfikator, w zależności od kontekstu, powinien sprawdzić także jego autentyczność (dane identyfikacyjne tego certyfikatu są wpisane jawnie w certyfikacie atrybutów).
CERTUM QACA Authorization Policy	CERTUM QACA Authorization	Certyfikaty wykorzystywane w procesie autoryzacji uprawnień podmiotu certyfikatu atrybutu; zawierają atrybuty, które mogą być przydatne podczas potwierdzania uprawnień lub pełnomocnictw; certyfikaty atrybutów należące do tej grupy nie muszą być jawnie powiązane z certyfikatami klucza publicznego, w tym w szczególności z certyfikatami kwalifikowanymi.
CERTUM QACA Dedicated Policies	CERTUM QACA Dedicated	Certyfikaty wydawane na potrzeby konkretnych systemów lub aplikacji, w których wymagane jest uwierzytelnione potwierdzenie atrybutów przypisanych użytkownikom tych systemów i aplikacji. Dedykowane certyfikaty atrybutów wydawane są w ramach polityk certyfikacji atrybutów, których identyfikatory oraz zasady wydawania certyfikatów nie są publikowane w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego, ale tylko w dokumencie, dostępnym w repozytorium CERTUM.

Niezależnie od typu polityki certyfikacji atrybutów każdy certyfikat atrybutów jest wydawany przez urząd certyfikatów atrybutów CERTUM QACA dopiero po rzetelnym i wiarygodnym zweryfikowaniu powiązania tożsamości podmiotu certyfikatu z poświadczanym atrybutem lub atrybutami oraz zweryfikowaniu praw do posługiwania się przydzielonymi atrybutami.

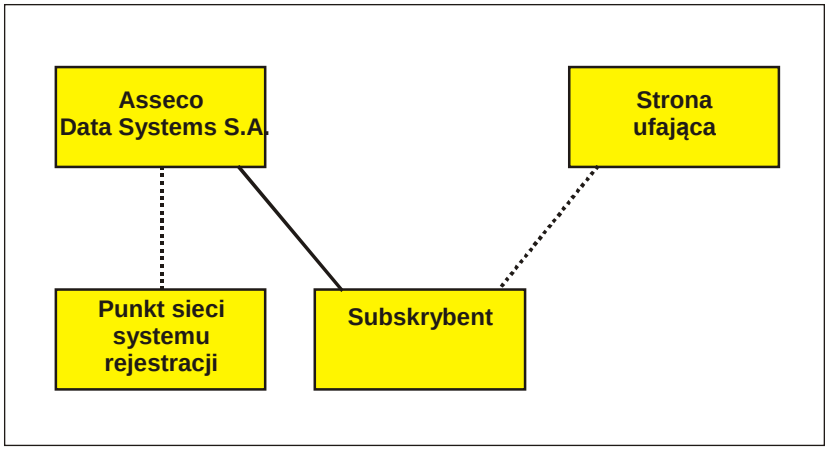
1.11. Kontakt

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

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 i odpowiedzialność CERTUM, punktów rejestracji (w tym punktów potwierdzania tożsamości i atrybutów), użytkowników certyfikatów (subskrybentów i stron ufających). Zobowiązania te oraz odpowiedzialność regulowane są przez wzajemne umowy zawierane pomiędzy wymienionymi stronami. Rys.2 przedstawia strony (podmioty) związane z usługami certyfikacji: dostawcę usług certyfikacyjnych CERTUM, punkt rejestracji, subskrybenta i stronę ufającą. Linie ciągłe łączące parami poszczególne podmioty oznaczają konieczność zawarcia umowy, regulującej ich wzajemne relacje. Umowy takie nie muszą być składane z kolei przez podmioty powiązane liniami przerywanymi. Subskrybent zawiera **umowy** bezpośrednio z Asseco Data Systems S.A. lub pośrednio przy udziale punktu rejestracji, działającego na rzecz CERTUM.



Rys.2 Umowy zawierane pomiędzy stronami

Przedmiotem umowy zawartej pomiędzy Asseco Data Systems S.A. i subskrybentami są kwalifikowane usługi udostępniane przez CERTUM, wzajemne zobowiązania oraz odpowiedzialności, w tym finansowe.

2.1. Zobowiązania

2.1.1. Zobowiązania CERTUM i punktów rejestracji

CERTUM świadcząc kwalifikowane usługi gwarantuje, że:

- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt zgodnie z 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,
- jego działalność oraz świadczone usługi są zgodne z prawem, a w szczególności nie naruszają postanowień *Rozporządzenia eIDAS, Ustawy* wraz z przepisami wykonawczymi

oraz praw autorskich i licencyjnych stron trzecich oraz nie naruszają praw autorskich i licencyjnych stron trzecich,

- świadczone usługi są zgodne z powszechnie akceptowanymi normami i standardami, m.in.:
    - usługi certyfikacyjne z zaleceniami ITU-T X.509 (odpowiada jej norma ISO/IEC 9594-8) i normą ISO/IEC 15945 (protokół CMP) oraz standardami *de facto* PKCS#10, PKCS#7, PKCS#12,
    - usługi certyfikacyjne ze standardem AICPA/CICA WebTrust Program for Certification Authorities Version 1.0,
    - usługi znakowania czasem z zaleceniami ETSI EN 319 422 *Time-stamping protocol and time-stamp profiles* oraz RFC 3161,
    - weryfikacja statusu certyfikatu (OCSP) - z zaleceniem RFC 2560,
    - usługi walidacji (DVCS) – zgodnie z polityką walidacji kwalifikowanej usługi walidacji dla kwalifikowanych podpisów i pieczęci elektronicznych
    - poświadczenia odbioru lub przedłożenia (w tym także urzędowego poświadczenia odbioru lub przedłożenia) - z normą PN-ISO/IEC 13888-3,
    - poświadczenia depozytowe, rejestrowe i repozytoryjne – ze specyfikacją OASIS Standard ebXML Registry Services and Protocols, Version 3.0, 2 May, 2005,
    - certyfikaty atrybutów – z zaleceniami RFC 3281 i RFC 4476.
- przestrzega i egzekwuje procedury certyfikacyjne opisane w niniejszym dokumencie,
- wystawiane certyfikaty zawierają dane zgodne z prawdą oraz że dane te były aktualne w momencie ich potwierdzania,
- wystawiane certyfikaty nie zawierają żadnych błędów, które powstały w wyniku zaniedbań lub naruszenia procedur przez osoby zatwierdzające wnioski o wystawienie certyfikatów lub wystawiające te certyfikaty,
- nazwy wyróżnione (DN) subskrybentów umieszczane w certyfikatach są unikalne,
- zapewnia ochronę danych osobowych subskrybenta zgodnie z *Ustawą z dnia 29 sierpnia 1997 r. o ochronie danych osobowych z późn. zm.* oraz dokumentami wykonawczymi do tej ustawy,
- nie kopiuje, ani nie przechowuje kluczy prywatnych swoich klientów, służących do składania podpisów elektronicznych,
- zatrudnia pracowników posiadających wiedzę, kwalifikacje i doświadczenie odpowiednie do pełnienia funkcji związanych z usługami certyfikacyjnymi, w tym w szczególności obejmujących dziedziny:
    - automatycznego przetwarzania danych w sieciach i systemach teleinformatycznych,
    - mechanizmów zabezpieczania sieci i systemów teleinformatycznych,
    - kryptografii, podpisów elektronicznych i infrastruktury klucza publicznego,
    - sprzętu i oprogramowania stosowanego do elektronicznego przetwarzania danych.

Ponadto *CERTUM* zobowiązuje się do:

- prowadzenia listy zarejestrowanych punktów sieci Systemu Rejestracji,
- udostępnienia odbiorcom usług certyfikacyjnych wykazu bezpiecznych urządzeń do składania i weryfikacji podpisów elektronicznych,
- zachowania w tajemnicy informacji związanych ze świadczeniem usług certyfikacyjnych, których nieuprawnione ujawnienie mogłoby narazić na szkodę Asseco Data Systems S.A. lub odbiorcę usług certyfikacyjnych przez okres 10 lat od ustania stosunków prawnych, o których mowa w art. 15 pkt.3 *Ustawy*, oraz do bezterminowego zachowania w tajemnicy danych służących do składania poświadczeń elektronicznych oraz do:
    a. przechowywania przez co najmniej 20 lat:
        - wydanych przez CERTUM kwalifikowanych certyfikatów,
        - wydanych przez CERTUM list CRL,
        - umów,
    b. przechowywania przez co najmniej 3 lata wszystkich stworzonych przez siebie rejestrów zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie.

W zakresie działania punktów Systemu Rejestracji, które funkcjonują w domenie **CERTUM** gwarantuje, że punkty Systemu Rejestracji:

- podporządkowane są w całości zaleceniom CERTUM,
- świadczą usług na zasadach jakie obowiązują w CERTUM, tj.: świadczą względem Subskrybentów usługi certyfikacyjne w zakresie weryfikacji tożsamości przy wydawaniu i unieważnianiu kwalifikowanych certyfikatów zgodnie z zasadami określonymi w niniejszym dokumencie i Polityce Certyfikacji, procedurach wewnętrznych oraz w obowiązujących przepisach prawa i zasadach współżycia społecznego ze szczególnym uwzględnieniem dochowania należytej staranności,
- przesyłają do CERTUM potwierdzone dane użytkowników,
- poddają się planowym audytom przeprowadzonym lub zleconym przez CERTUM.

2.1.1.1. Zobowiązania urzędu znacznika czasu

Urząd znacznika czasu **CERTUM QTSA** gwarantuje, że świadczy usługi znacznika czasu zgodnie z wymaganiami Rozporządzenia eIDAS i normy ETSI 319-421 Electronic Signatures and Infrastructures (ESI);.

W szczególności **CERTUM QTSA**:

- stosuje takie rozwiązania techniczne, procedury operacyjne oraz procedury zarządzania bezpieczeństwem, które wykluczają jakąkolwiek możliwość manipulowania czasem,
- stosuje co najmniej takie parametry algorytmów szyfrowych używanych do świadczenia usług certyfikacyjnych jak określono 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.

Ponadto **CERTUM QTSA** gwarantuje, że:

- zapewniony jest ciągły dostęp do serwisów świadczonych usług, w trybie 24/7/365 z wyłączeniem przerw technologicznych, związanych z konserwacją sprzętu i systemu,
- czas UTC, który zostaje umieszczony w tokenie znacznika czasu, podawany jest z dokładnością do 1 sekundy, co należy interpretować jako maksymalne dozwolone opóźnienie pomiędzy momentem otrzymania żądania, a pobraniem wiarygodnego czasu. Serwis zachowuje dokładność także przy wielu równocześnie podłączonych klientach,
- swoją działalność komercyjną realizuje w oparciu o wiarygodny sprzęt i oprogramowanie, tworzące system, który spełnia wymagania określone w *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time-Stamps*,
- jego działalność oraz świadczone usługi są zgodne z prawem, a w szczególności nie naruszają praw autorskich i licencyjnych osób trzecich,
- świadczone usługi są zgodne z z zaleceniem ETSI EN 319 422 *Time-stamping protocol and time-stamp profiles,*
- przechowywania przez co najmniej 3 lata wszystkich stworzonych przez siebie w trybie *Ustawy* rejestrów zdarzeń w sposób umożliwiający ich elektroniczne przeglądanie,
- wystawiane tokeny znacznika czasu nie zawierają błędów ani nieprawdziwych danych.

2.1.1.2. 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 niniejszym Kodeksie Postępowania Certyfikacyjnego 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,*
- urząd **CERTUM QOCSP** weryfikuje status certyfikatu (OCSP) zgodnie z zaleceniem RFC 2560 *Online Certificate Status Protocol (OCSP)*,
- usługa **CERTUM QDVCS** poświadcza wykonania walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.

2.1.1.3. 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.

Poświadczenia wystawiane przez urząd **CERTUM QDA** są zgodne z wymaganiami określonymi w polskiej normie PN-ISO/IEC 13888-3:1999 *Technika informatyczna. Techniki zabezpieczeń. Niezaprzeczalność. Mechanizmy wykorzystujące techniki asymetryczne.*

2.1.1.4. 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.

2.1.1.5. Zobowiązania urzędu certyfikatów atrybutów

Urząd certyfikatów atrybutów **CERTUM QACA** gwarantuje, że świadczy swoje usługi zgodnie z wymaganiami określonymi w Kodeksie Postępowania Certyfikacyjnego dla usług wydawania kwalifikowanych certyfikatów[26], 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.

2.1.1.6. Zobowiązania repozytorium urzędu certyfikacji

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

- terminowego publikowania i archiwizowania zaświadczeń certyfikacyjnych kwalifikowanego urzędu certyfikacji **CERTUM QCA**, kwalifikowanego urzędu znacznika czasu **CERTUM QTSA**, kwalifikowanego urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, kwalifikowanego urzędu walidacji **CERTUM QDVCS**, urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA** i urzędu rejestrów i repozytoriów **CERTUM QRRA**, urzędu certyfikatów atrybutów **CERTUM QACA**.
- publikowania i archiwizowania Polityki Certyfikacji, Kodeksu Postępowania Certyfikacyjnego (aktualnego i poprzednich), wzorów umów zawieranych z subskrybentami, list rekomendowanych aplikacji i urządzeń do składania i weryfikacji bezpiecznego podpisu elektronicznego oraz list podmiotów potwierdzających tożsamość,
- udostępniania na żądanie kwalifikowanych certyfikatów i certyfikatów atrybutów, po uzyskaniu zgody przez posiadaczy tych certyfikatów,
- udostępniania informacji o statusie certyfikatów poprzez publikowanie listy certyfikatów unieważnionych (CRL),
- zagwarantowania urzędom certyfikacji, punktom rejestracji, subskrybentom oraz stronom ufającym ciągłego dostępu do informacji zgromadzonej w repozytorium urzędu certyfikacji,
- szybkiego i zgodnego z okresami określonymi w Polityce Certyfikacji publikowania list CRL.

[26] Niniejszy Kodeks Postępowania Certyfikacyjnego nie dopuszcza jednak aktualizacji lub modyfikacji certyfikatów atrybutów.

2.1.2. Zobowiązania użytkowników końcowych

2.1.2.1. Zobowiązania subskrybenta

Poprzez własnoręczne podpisanie wniosku o wydanie certyfikatu oraz zawarcie umowy na świadczenie usług certyfikacyjnych subskrybent wyraża zgodę na przystąpienie do systemu certyfikacji na warunkach określonych w Umowie, Kodeksie Postępowania Certyfikacyjnego oraz Polityce Certyfikacji.

Subskrybent zobowiązany jest do:

- przestrzegania postanowień umowy podpisanej z Asseco Data Systems S.A.,
- dostarczenia obsługującemu go punktowi sieci Systemu Rejestracji prawdziwych i poprawnych informacji na każdym etapie współpracy,
- dostarczenia dokumentów potwierdzających prawdziwość danych zawartych we wniosku w celu wypełnienia określonych w Polityce Certyfikacji wymagań procesu rejestracji, unieważnienia i odnowienia certyfikatu,
- niezwłocznego poinformowania CERTUM o jakichkolwiek błędach lub wadach w jego certyfikacie lub o zmianach danych w nim zawartych,
- używania swojej pary kluczy i kluczy publicznych innych odbiorców usług certyfikacyjnych wyłącznie w sposób zgodny z Polityką Certyfikacji i zapewnienia bezpieczeństwa i integralności własnych kluczy prywatnych, włączając w to:
    - kontrolę i zabezpieczenie dostępu do urządzeń zawierających jego klucze prywatne,
    - niezwłoczne informowanie Głównego Punkt Rejestracji o wszelkich okolicznościach, w wyniku których jego klucz prywatny został ujawniony osobom trzecim lub w wyniku których subskrybent może podejrzewać, że klucz prywatny mógł ulec ujawnieniu osobom trzecim,
- nie składania podpisu elektronicznego przy pomocy należącego do niego klucza prywatnego, jeżeli certyfikat ten jest przeterminowany (minął jego okres ważności), jest unieważniony lub zawieszony,
- zabezpieczenia i ochrony dostępu do nośników na których przechowywane są hasła i klucze,
- nie przechowywania karty kryptograficznej zawierającej klucz prywatny razem z osobistym numerem identyfikacyjnym (PIN),
- traktowania utraty lub ujawnienia (przekazanie innej nieupoważnionej do tego osobie) hasła na równi z utratą lub ujawnieniem (przekazaniem innej nieupoważnionej do tego osobie) klucza prywatnego,
- nie udostępniania i nie przekazywania swoich kluczy prywatnych oraz używanych przez siebie haseł osobom trzecim,
- w przypadku naruszenia ochrony (lub podejrzenia naruszenia ochrony) swojego klucza prywatnego niezwłocznie przystępuje do procedury unieważnienia certyfikatu,
- wykorzystywania certyfikatu atrybutów oraz kwalifikowanego certyfikatu klucza publicznego i odpowiadającego mu klucza prywatnego tylko zgodnie z deklarowanym

w certyfikacie przeznaczeniem, celami i ograniczeniami określonymi w niniejszym dokumencie.

2.1.2.2. Zobowiązania stron ufających

W zależności od wzajemnych relacji pomiędzy stroną ufającą a CERTUM lub subskrybentem, a także od typów certyfikatów, tokenów i poświadczeń, które są przez stronę ufającą akceptowane, zobowiązania strony ufającej mogą być wyrażone w postaci umowy z Asseco Data Systems S.A. lub subskrybentem.

Niezależnie od postanowień umowy strona ufająca zobowiązana jest do:

- rzetelnej weryfikacji każdego podpisu lub poświadczenia elektronicznego[27] umieszczonego na dokumencie lub certyfikacie, tokenie znacznika czasu, w tokenie statusu certyfikatu, w tokenie walidacji, w poświadczeniu odbioru lub przedłożenia (w tym także w urzędowym poświadczeniu odbioru lub przedłożenia), w poświadczeniach depozytowych, rejestrowych i repozytoryjnych, w certyfikacie atrybutów, który do niej dotrze; w celu zweryfikowania podpisu lub poświadczenia strona ufająca powinna:
    - określić **ścieżkę certyfikacji**[28], zawierającą wszystkie zaświadczenia certyfikacyjne innych urzędów certyfikacji, które umożliwią wiarygodne przeprowadzenie weryfikacji poświadczenia elektronicznego zawartego w certyfikacie wystawcy podpisu,
    - upewnić się, że wybrana ścieżka certyfikacji jest najlepsza z punktu widzenia weryfikacji podpisu lub poświadczenia elektronicznego; istnieje bowiem możliwość, że od danego certyfikatu lub zaświadczenia certyfikacyjnego (przy pomocy którego zrealizowano podpis lub poświadczenie elektroniczne) do urzędu certyfikacji, któremu ufa weryfikujący podpis wiedzie więcej niż jedna ścieżka,
    - sprawdzić, czy certyfikaty i zaświadczenia certyfikacyjne tworzące ścieżkę certyfikacji nie występują na liście certyfikatów unieważnionych lub zawieszonych; unieważnienie lub zawieszenie któregokolwiek certyfikatu ze ścieżki certyfikacji ma wpływ na wcześniejsze zakończenie ważności okresu, w którym weryfikowany podpis mógł być utworzony,
    - sprawdzić, czy wszystkie zaświadczenia certyfikacyjne wchodzące w skład ścieżki certyfikacji należą do urzędów certyfikacji oraz czy nadano im prawo poświadczania innych zaświadczeń certyfikacyjnych,
    - opcjonalnie określić datę oraz czas złożenia podpisu na wiadomości lub dokumencie. Jest to możliwe tylko w przypadku, gdy wiadomość lub dokument zostały przed podpisaniem opatrzone znacznikiem czasu, uzyskanym z urzędu znacznika czasu lub też znacznik czasu został związany z podpisem elektronicznym już po jego umieszczeniu na dokumencie,

---

[27] Weryfikacja podpisu lub poświadczenia elektronicznego ma na celu określenie, czy (1) podpis lub poświadczenie elektroniczne został(-lo) zrealizowany(-ne) za pomocą klucza prywatnego odpowiadającego kluczowi publicznemu, zawartemu w certyfikacie kwalifikowanym subskrybenta lub urzędu certyfikacji, oraz (2) podpisana wiadomość (dokument) lub certyfikat nie został zmodyfikowana już po złożeniu na nim podpisu lub poświadczenia.

[28] Patrz **Słownik pojęć**

  - korzystając ze zdefiniowanej ścieżki certyfikacji zweryfikować prawdziwość poświadczenia w certyfikacie kwalifikowanym, a następnie oryginalność samego podpisu na wiadomości lub dokumencie,

- w przypadku weryfikacji poświadczenia umieszczonego w certyfikacie atrybutu podmiot weryfikujący musi sprawdzić, czy z danym certyfikatem atrybutów jest związana lista unieważnionych certyfikatów atrybutów użytkowników końcowych (EARL) i jeśli tak, to sprawdzić, czy certyfikat jest umieszczony na tej liście;
- właściwego i prawidłowego realizowania operacji kryptograficznych przy użyciu oprogramowania i sprzętu, których poziom bezpieczeństwa jest zgodny z poziomem wrażliwości przetwarzanej informacji i poziomem wiarygodności stosowanych certyfikatów,
- uznania podpisu elektronicznego lub poświadczenia za nieważny, jeśli przy użyciu posiadanego oprogramowania i sprzętu nie można rozstrzygnąć czy podpis elektroniczny lub poświadczenie są ważne lub uzyskany wynik weryfikacji jest negatywny,
- zaufania tylko tym kwalifikowanym certyfikatom lub certyfikatom atrybutów:
  - które używane są zgodnie z deklarowanym przeznaczeniem oraz są odpowiednie do zastosowań w obszarach, które wcześniej określiła strona ufająca,
  - których status został zweryfikowany w oparciu o aktualne listy certyfikatów unieważnionych.

W interesie strony ufającej jest dokonywanie rzetelnej weryfikacji każdego podpisu elektronicznego umieszczonego na dokumencie (w tym także poświadczeń elektronicznych w certyfikacie klucza publicznego lub certyfikacie atrybutów), który do niej dotrze.

Jeśli dokument lub podpis elektroniczny jest oznakowany czasem lub w jakikolwiek sposób powiązany z innymi tokenami, poświadczeniami lub certyfikatami atrybutów wystawianymi przez CERTUM, to w celu racjonalnego zbudowania zaufania do weryfikowanego tokena lub poświadczenia strona ufająca powinna dodatkowo:

- zweryfikować, czy token, poświadczenie lub certyfikat atrybutów zostały prawidłowo poświadczone elektronicznie oraz czy klucz prywatny użyty przez kwalifikowany urząd znacznika czasu **CERTUM QTSA**, kwalifikowany urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, kwalifikowaną usługę walidacji **CERTUM QDVCS**, urząd poświadczania odbioru i przedłożenia **CERTUM QDA**, urząd depozytów obiektów **CERTUM QODA**, urząd rejestrów i repozytoriów **CERTUM QODA** lub urząd certyfikatów atrybutów **CERTUM QACA** do wystawienia tokena/poświadczenia/certyfikatu atrybutów nie był ujawniony aż do momentu weryfikacji tokena, poświadczenia lub certyfikat atrybutów (chyba, że zawarty w nich czas spełnia wymagania daty pewnej); status klucza prywatnego można zweryfikować w oparciu o weryfikację komplementarnego z nim klucza publicznego,
- sprawdzić ograniczenia w stosowaniu tokenów znacznika czasu, tokenów weryfikacji statusu certyfikatów w trybie *on-line*, tokenów walidacji danych, poświadczeń odbioru i przedłożenia (w tym także urzędowych poświadczeń odbioru i przedłożenia), poświadczeń depozytowych, rejestrowych i repozytoryjnych, certyfikatów atrybutów określone w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz umowie zawartej z **CERTUM**.

2.2. Odpowiedzialność

CERTUM, działając w ramach umocowań Asseco Data Systems S.A., ponosi odpowiedzialność za skutki działań urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, usługi walidacji **CERTUM QDVCS**, urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA**, urzędu rejestrów i repozytoriów **CERTUM QODA** oraz urzędu certyfikatów atrybutów **CERTUM QACA**, Głównego Punktu Rejestracji i innych punktów systemu rejestracji oraz osób potwierdzających tożsamość w zakresie określonym w zawartych umowach.

Przedstawione poniżej zapisy o odpowiedzialności stron nie eliminują lub nie zastępują odpowiedzialności wynikającej z odrębnych przepisów prawa.

2.2.1. Odpowiedzialność CERTUM

2.2.1.1. Odpowiedzialność urzędu certyfikacji CERTUM QCA

Urząd certyfikacji **CERTUM QCA** ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego:

- są wynikiem udowodnionych błędów popełnionych przez 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,
- powstały wskutek naruszenia innych gwarancji CERTUM, określonych w rozdz.2.1.1.

Jedyną formą usług jaką zleca się podmiotom zewnętrznym są usługi świadczone w ramach prowadzenia tzw. Punktu Rejestracji. Mimo, że punkt rejestracji związany jest z Asseco Data Systems S.A. umową, to pełną odpowiedzialność za tę część jego pracy, która związana jest ze świadczeniem przez CERTUM usług certyfikacyjnych, ponosi CERTUM.

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

- za szkody powstałe na skutek działania siły wyższej lub innych, za których wystąpienie nie ponosi odpowiedzialności, tj.: pożaru, powodzi, wichury, wojny, aktów terroru, epidemii oraz innych klęsk naturalnych lub spowodowanych przez człowieka,
- za szkody powstałe na skutek instalacji, użytkowania oraz zarządzania aplikacjami innymi niż dostarczone przez CERTUM,
- za szkody powstałe na skutek niewłaściwego stosowania wydanych certyfikatów, przy czym przez słowo niewłaściwe należy rozumieć używanie certyfikatu przeterminowanego, unieważnionego lub zawieszonego oraz używanie niezgodnie z przeznaczeniem wynikającym z typu certyfikatu, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego, w tym w szczególności za szkody wynikające z przekroczenia najwyższej wartości granicznej transakcji, jeżeli wartość ta została zamieszczona w certyfikacie,

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

2.2.1.2. Odpowiedzialność urzędu znacznika czasu

Urząd znacznika czasu **CERTUM QTSA** ponosi odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez użytkownika:

- powstały pomimo przestrzegania przez nich zasad określonych w Regulaminie Kwalifikowanych Usług Certyfikacyjnych, Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez **CERTUM QTSA**, zwłaszcza w zakresie niewłaściwej ochrony klucza prywatnego, stosowanego do poświadczania tokenów znacznika czasu,
- powstały wskutek naruszenia innych gwarancji **CERTUM QTSA**, określonych w rozdz.2.1.1.1.

2.2.1.3. Odpowiedzialność urzędu weryfikacji statusu certyfikatów, urzędu walidacji danych, urzędu poświadczania odbioru i przedłożenia, urzędu depozytów obiektów, urzędu rejestrów i repozytoriów, urzędu certyfikatów atrybutów

Działające w ramach CERTUM urzędy weryfikacji statusu certyfikatu **CERTUM QOCSP**, walidacji **CERTUM QDVCS**, wystawiania elektronicznych poświadczeń przedłożenia i odbioru **CERTUM QDA**, depozytów obiektów **CERTUM QODA**, rejestrów i repozytoriów **CERTUM QODA** oraz certyfikatów atrybutów **CERTUM QACA** ponoszą odpowiedzialność w przypadkach, gdy bezpośrednie i pośrednie szkody poniesione przez subskrybenta lub stronę ufającą:

- powstały pomimo przestrzegania przez nich zasad określonych w Polityce Certyfikacji i Kodeksie Postępowania Certyfikacyjnego,
- są wynikiem udowodnionych błędów popełnionych przez **CERTUM QOCSP**, **CERTUM QDVCS**, **CERTUM QDA**, **CERTUM QODA**, **CERTUM QRRA** lub **CERTUM QACA**, zawłaszcza w zakresie niewłaściwej ochrony klucza prywatnego,
- powstały wskutek naruszenia innych gwarancji **CERTUM QOCSP**, **CERTUM QDVCS**, **CERTUM QDA**, **CERTUM QODA** lub **CERTUM QRRA** lub **CERTUM QACA**, określonych w rozdz.2.1.1.2, rozdz.2.1.1.3, rozdz.2.1.1.4 i rozdz.2.1.1.5.

2.2.1.4. Odpowiedzialność repozytorium urzędu certyfikacji

Pełną odpowiedzialność za funkcjonowanie repozytorium urzędu certyfikacji i treść opublikowanych w nim dokumentów oraz wynikłe z tego skutki ponosi CERTUM (patrz rozdz.2.1.1.6).

2.2.2. Odpowiedzialność użytkowników końcowych

2.2.2.1. Odpowiedzialność subskrybentów

Odpowiedzialność subskrybenta wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.2.1 niniejszego dokumentu.

2.2.2.2. Odpowiedzialność stron ufających

Odpowiedzialność strony ufającej wynika ze zobowiązań i gwarancji określonych w rozdz.2.1.2.2. Warunki tej odpowiedzialności może również regulować umowa zawarta z subskrybentem oraz z Asseco Data Systems S.A.

Umowy z subskrybentami i Asseco Data Systems S.A. wymagają, aby strony ufające potwierdziły, że dysponują wystarczającą ilością informacji umożliwiającą im podjęcie świadomej decyzji o akceptacji lub odrzuceniu podpisu/poświadczenia elektronicznego w momencie jego przedłożenia.

2.3. Odpowiedzialność finansowa

Asseco Data Systems S.A. posiada ubezpieczenie odpowiedzialności cywilnej zgodne z wymaganiami *Rozporządzenia Ministra Finansów z dnia 16 grudnia 2003r. 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.

2.4. Akty prawne i rozstrzyganie sporów

2.4.1. Obowiązujące akty prawne

Funkcjonowanie **CERTUM** oparte jest na zasadach zawartych w niniejszym Kodeksie Postępowania Certyfikacyjnego oraz obowiązujących przepisach prawa.

2.4.2. Postanowienia dodatkowe

2.4.2.1. Rozłączność postanowień

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

Rozłączność postanowień jest istotna zwłaszcza w przypadku umów podpisywanych z subskrybentem.

2.4.2.2. Ciągłość postanowień

Postanowienia niniejszego Kodeksu Postępowania Certyfikacyjnego obowiązują od daty zaakceptowania przez inspektora bezpieczeństwa i opublikowania, aż do momentu ich unieważnienia lub zastąpienia. Modyfikacja lub wprowadzenie nowych postanowień odbywa się zgodnie z procedurą przedstawioną w rozdz.8.

W przypadku, gdy umowy zawierają dodatkowe klauzule o poufności informacji lub postanowienia o ochronie praw autorskich i intelektualnych czas ich obowiązywania trwa także po ich ustaniu przez okres uzgodniony przez strony w zawartych umowach.

Praw wynikających z zawartych przez strony umów lub Kodeksu Postępowania Certyfikacyjnego nie wolno przenosić na osoby trzecie.

2.4.2.3. Powiadamianie

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

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

Niektóre komunikaty i informacje muszą być przekazywane stronom zgodnie z wcześniej uzgodnionym harmonogramem. Dotyczy to w szczególności publikowania list certyfikatów unieważnionych, informowania o naruszeniu klucza prywatnego urzędu certyfikacji oraz wszelkich zmianach dotyczących parametrów wydawanych przez CERTUM certyfikatów.

2.4.3. Rozstrzyganie sporów

Przedmiotem rozstrzygania sporów mogą być jedynie rozbieżności bądź konflikty powstałe pomiędzy stronami w zakresie wydawania i unieważniania kwalifikowanego certyfikatu w oparciu o regulacje Kodeksu Postępowania Certyfikacyjnego Kwalifikowanych Usług CERTUM oraz zawartych umów.

Spory bądź zażalenia powstałe na tle użytkowania certyfikatów, zaświadczeń certyfikacyjnych, tokenów znacznika czasu, tokenów weryfikacji statusu certyfikatów, tokenów walidacji danych oraz poświadczeń odbioru lub przedłożenia (w tym także urzędowych poświadczeń odbioru i przedłożenia), wystawianych przez CERTUM, będą rozstrzygane na podstawie pisemnych informacji w drodze mediacji. Postępowanie ze skargami jest zastrzeżone do wyłącznego działania Prezesa Zarządu. Podlegają one pisemnemu rozpatrzeniu w terminie do 10 dni.

Spory związane z kwalifikowanymi usługami certyfikacyjnymi świadczonymi przez CERTUM będą w pierwszej kolejności rozstrzygane na drodze postępowania pojednawczego.

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

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

2.5. Opłaty

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

http://www.certum.pl

CERTUM może stosować różne modele pobierania opłat za świadczone usługi, a w szczególności:

- **sprzedaż detaliczną** – opłaty pobierane są oddzielnie za każdą jednostkę usługową, np. za każdy pojedynczy certyfikat lub mały pakiet certyfikatów,
- **sprzedaż hurtową** – opłaty pobierane są za pakiet usług, np. dużą liczbę certyfikatów sprzedanych jednorazowo osobie prawnej,
- **sprzedaż abonamentową** – opłaty są pobierane najczęściej raz w miesiącu; wysokość opłaty abonamentowej uzależniona jest od rodzaju i liczby jednostek usługowych i jest stosowana w przypadku usługi znacznika czasu, usługi weryfikacji statusu certyfikatów, usługi walidacji danych, usługi poświadczania odbioru i przedłożenia, usługi poświadczania depozytów oraz usługi poświadczania rejestrów i repozytoriów,
- **sprzedaż pośrednią** – opłata jest pobierana za każdą jednostkę usługową od klienta, który świadczy usługi zbudowane na bazie infrastruktury **CERTUM**.

2.5.1. Opłaty za wydanie certyfikatu

CERTUM pobiera opłaty za wydanie certyfikatu.

2.5.2. Opłaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych

CERTUM nie pobiera opłaty za dostęp do certyfikatów i zaświadczeń certyfikacyjnych.

2.5.3. Opłaty za znaczniki czasu, inne tokeny i poświadczenia oraz certyfikaty atrybutów

CERTUM pobiera opłaty za wystawiane znaczniki czasu, tokeny weryfikacji statusu certyfikatu w trybie *on-line*, tokeny walidacji, poświadczenia odbioru lub przedłożenia (w tym za urzędowe poświadczenia odbioru lub przedłożenia), poświadczenia depozytowe, rejestrowe i repozytoryjne oraz certyfikaty atrybutów.

2.5.4. Opłaty za unieważnienie i informacje o statusie kwalifikowanego certyfikatu lub certyfikatu atrybutów

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

2.5.5. Inne opłaty

CERTUM może pobierać opłaty za inne usługi tj.:

- generowania kluczy na żądanie subskrybentom,
- testowania aplikacji i urządzeń oraz umieszczania jej na liście bezpiecznych urządzeń,
- sprzedaży licencji,
- realizacji prac projektowych, wdrożeniowych i instalacyjnych,
- sprzedaży Kodeksu Postępowania Certyfikacyjnego, Polityki Certyfikacji, podręczników, przewodników itp. wydanych w formie drukowanej,
- szkoleń.

2.5.6. Zwrot opłat

CERTUM dokłada wszelkich starań, aby świadczone usługi były na najwyższym poziomie. W każdym innym przypadku subskrybent może żądać zwrotu wniesionej opłaty, jeżeli usługa certyfikacyjna była wykonana niezgodnie z zasadami wynikającymi z umowy i postanowień niniejszego dokumentu.

Żądania o zwrot opłat należy kierować pod adres podany w rozdz.1.9.

2.6. Repozytorium urzędu certyfikacji i publikacje

2.6.1. Informacje publikowane przez CERTUM

Wszystkie dokumenty publikowane przez CERTUM dostępne są w repozytoriumserwisu internetowego urzędu certyfikacji dostępnym pod adresem:

http://www.certum.pl/

Są to następujące informacje:

- Polityka Certyfikacji Kwalifikowanych Usług,
- Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług,
- wzory umów,
- nieprzeterminowane i nieunieważnione zaświadczenia certyfikacyjne: urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, usługi walidacji **CERTUM QDVCS**, urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA**, urzędu rejestrów i repozytoriów **CERTUM QODA** oraz urzędu certyfikatów atrybutów **CERTUM QACA**,
- listy bezpiecznych urządzeń, rekomendowanych przez CERTUM,
- listy autoryzowanych punktów systemu rejestracji i innych osób potwierdzających tożsamość i atrybuty,
- listy certyfikatów unieważnionych (CRL); listy certyfikatów unieważnionych dostępne są w tzw. punktach dystrybucji CRL, których adresy umieszczane są w każdym certyfikacie lub zaświadczeniu certyfikacyjnym wydanym przez **CERTUM QCA**; podstawowym punktem dystrybucji list CRL jest: http://crl.certum.pl,
- informacje pomocnicze, np. ogłoszenia.

2.6.2. Częstotliwość publikacji

Wymienione poniżej publikacje CERTUM są ogłaszane z następującą częstotliwością:

- Polityka Certyfikacji Kwalifikowanych Usług oraz Kodeks Postępowania Certyfikacyjnego Kwalifikowanych Usług (patrz rozdz.8),
- zaświadczenia certyfikacyjne wszystkich urzędów świadczących usługi certyfikacyjne, funkcjonujących w ramach CERTUM – każdorazowo, gdy nastąpi emisja nowych zaświadczeń certyfikacyjnych,
- listy certyfikatów unieważnionych i zawieszonych (patrz rozdz.4.8.4 i 4.8.9),
- informacje pomocnicze – każdorazowo, gdy nastąpi ich uaktualnienie.

2.6.3. Dostęp do publikacji

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

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

2.7. Audyt

Celem audytu jest określenie stopnia zgodności postępowania jednostki usługowej CERTUM lub wskazanych przez nią elementów z wdrożonym przez Asseco Data Systems S.A. Zintegrowanym Systemem Zarządzania, który obejmuje zwłaszcza wymagania standardów PN-EN ISO:9001:2009 oraz PN ISO/IEC 27001:2014, oraz deklaracjami i procedurami właściwymi dla CERTUM (włączając w to Politykę Certyfikacji i Kodeks Postępowania Certyfikacyjnego).

Audyt CERTUM dotyczy przede wszystkim Głównego Punktu Rejestracji oraz procedur zarządzania kluczami. Przeglądom poddawane są także urzędy świadczące kwalifikowane usługi certyfikacyjne, punkty rejestracji oraz inne elementy infrastruktury klucza publicznego, m.in. repozytorium.

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 właściwego ds. gospodarki 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.

2.7.1. Częstotliwość audytu

Audyty sprawdzające prawidłowość i zgodność z uregulowaniami prawnymi i proceduralnymi (przede wszystkim zgodność z Kodeksem Postępowania Certyfikacyjnego i Polityką Certyfikacji) są wykonywane w zależności od potrzeb, na podstawie 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. Zgodnie postanowieniami rozdziału 7 normy ETSI EN 319 403 Audyt

zgodności dostawców usług zaufania – regulacje dla podmiotów potwierdzających zgodność dostawców usług zaufania, audyt certyfikujący dokonywany jest raz na dwa lata, natomiast zaleca się aby co najmniej jeden audyt utrzymaniowy był przeprowadzany pomiędzy dwoma audytami certyfikującymi.

2.7.2. Tożsamość/kwalifikacje audytora

Audyt zewnętrzny wykonywany jest przez upoważnioną do tego rodzaju działalności i niezależną od CERTUM instytucję krajową lub europejską posiadającą akredytację udzieloną przez Centrum Akredytacji w Polsce lub przez podmiot akredytujący jednostki oceniające zgodność na terenie Unii Europejskiej. System akredytacji i kompetencje audytora są określone przez rozporządzenie WE 765/2008 ustanawiające wymagania w zakresie akredytacji i nadzoru rynku odnoszące się do warunków wprowadzania produktów do obrotu i uchylające rozporządzenie EWG 339/93 oraz regulowane przez normę ISO 17065 Ocena zgodności -- Wymagania dla jednostek certyfikujących wyroby, procesy i usługi. Organ nadzoru może w dowolnym momencie przeprowadzić audyt – lub zwrócić się do jednostki oceniającej zgodność o przeprowadzenie oceny zgodności –Audyt wewnętrzny realizowany jest przez odpowiednią jednostkę organizacyjną, funkcjonującą w strukturze Asseco Data Systems S.A.

2.7.3. Zagadnienia obejmowane przez audyt

Audyt wewnętrzny i zewnętrzny powinien być prowadzony zgodnie z zasadami określonymi *Ustawie* oraz Rozporządzeniu 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, oraz normy *ETSI EN 319 403 Audyt zgodności dostawców usług zaufania – regulacje dla podmiotów potwierdzających zgodność dostawców usług zaufania.* Szczegółowy zakres kontroli określa upoważnienie, wydane kontrolerom przez ministra właściwego ds. gospodarki lub wynika z rodzaju świadczonych przez kwalifikowany podmiot świadczący usługi certyfikacyjne w związku z postanowieniami ww. rozporządzenia 910/2014 i wydanymi decyzjami wykonawczymi do niego. Audytem objęte są m.in. następujące zagadnienia:

- sprawdzenie wymagań organizacyjno-prawnych wynikających z *Ustawy* oraz, *Rozporządzenia eIDAS* i wydanymi decyzjami wykonawczymi do niego,
- zabezpieczenia fizyczne CERTUM,
- procedury weryfikacji tożsamości subskrybentów,
- usługi certyfikacyjne i procedury ich świadczenia,
- zabezpieczenia oprogramowania i dostępu do sieci,
- ochrona personelu CERTUM,
- rejestry zdarzeń i procedury monitorowania systemu,
- procedury sporządzania kopii zapasowych oraz ich odtwarzania,
- realizacja procedur archiwizacji,
- dokumentowanie zmian parametrów konfiguracyjnych CERTUM,
- dokumentowanie przeglądów i serwisu sprzętu oraz oprogramowania.

2.7.4. Podejmowane działania w celu usunięcia rozbieżności wykrytych podczas audytu

Raporty audytów wewnętrznych i zewnętrznych przekazywane są **Zespołowi Jakości Certum.** Zespół Jakości zobowiązany jest w terminie określonym w raporcie do przygotowania pisemnego stanowiska CERTUM wobec wszelkich uchybień wskazanych w raportach. Odpowiedź musi określić także sposoby i terminy usunięcia usterek. Informacja o usunięciu usterek przekazywana jest instytucji audytującej.

W przypadku audytu zleconego przez ministra cyfryzacji minister po zapoznaniu się z protokołem i zastrzeżeniami oraz wyjaśnieniami zgłoszonymi przez CERTUM powiadamia ten podmiot o wynikach kontroli i w razie stwierdzenia nieprawidłowości wyznacza termin ich usunięcia, nie krótszy niż 14 dni (Art.34 *Ustawy*).

2.7.5. Informowanie o wynikach audytu

Publikacji podlegają otrzymane certyfikaty zgodności usług z wymaganiami w serwisie internetowym dostępnym pod adresem www.certum.pl

2.8. Ochrona informacji

Asseco Data Systems S.A. gwarantuje, że wszystkie będące w jego posiadaniu informacje są gromadzone, przechowywane i przetwarzane zgodnie z obowiązującym w tym zakresie przepisami prawa, a w szczególności z *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 publicznie dostępne są w certyfikacie lub zaświadczeniu certyfikacyjnym. Pozostałe dane spośród tych, które dostarczane są we wnioskach kierowanych do CERTUM w żadnych okolicznościach nie zostaną ujawnione dobrowolnie lub świadomie innym podmiotom, z wyjątkami określonymi w *Ustawie, Art.15, ust.4,* tj. na żądanie:

- sądu lub prokuratora - w związku z toczącym się postępowaniem,
- ministra cyfryzacji - w związku ze sprawowaniem przez niego nadzoru nad działalnością podmiotów świadczących usługi certyfikacyjne,
- innych organów państwowych upoważnionych do tego na podstawie odrębnych ustaw - w związku z prowadzonymi przez nie postępowaniami w sprawach dotyczących działalności podmiotów świadczących usługi certyfikacyjne.

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

2.8.1. Informacje, które muszą być traktowane jako tajemnica

Asseco Data Systems S.A. i osoby w niej zatrudnione, bądź podmioty dokonujące czynności rejestracyjnych są obowiązane do zachowania w tajemnicy rozumianej jako tajemnica

przedsiębiorstwa[29], wszelkich informacji powziętych w trakcie zatrudnienia lub wykonywania czynności jak powyżej także po ustaniu okresu zatrudnienia bądź umocowania do ich wykonywania. Szczegółowy zakres tajemnicy przedsiębiorstwa określony jest w oddzielnych wewnętrznych zarządzeniach firmy. W szczególności dotyczy to:

- informacji otrzymywanej od subskrybentów, z wyjątkiem tej, bez której ujawnienia nie jest możliwe należyte wykonanie usług certyfikacyjnych; we wszystkich pozostałych przypadkach ujawnienie otrzymanej informacji wymaga uprzedniej pisemnej zgody jej właściciela lub wynika z wyjątków określonych w *Ustawie, Art.15, ust.4* (patrz także rozdz.2.8),
- informacji wpływającej od/do subskrybentów (m.in. treści umów z subskrybentami, rozliczeń, wniosków o zarejestrowanie, wydanie, odnowienie lub unieważnienie certyfikatów; część z powyższych informacji może być udostępniana wyłącznie za zgodą i w zakresie pisemnie określonym przez jej właściciela),
- zapisów transakcji systemowych (zarówno w całości, jak też w postaci **danych do przeglądu kontrolnego** transakcji, tzw. rejestrów transakcji systemowych),
- zapisów informacji o zdarzeniach związanych z usługami certyfikacyjnymi, zachowywanymi przez CERTUM oraz punkty systemu rejestracji,
- raportów kontroli wewnętrznej oraz zewnętrznej,
- planów działań awaryjnych,
- informacji o przedsięwziętych środkach zabezpieczających sprzęt oraz oprogramowanie, informacje o administrowaniu usługami certyfikacyjnymi oraz projektowanymi zasadami rejestrowania.

Asseco Data Systems S.A. obowiązuje zachowanie tajemnicy wobec strony umowy o świadczenie usług certyfikacyjnych. Osoby odpowiedzialne za zachowanie w tajemnicy zasad postępowania i ww. informacji ponoszą odpowiedzialność karną zgodnie z przepisami prawa. Obowiązek zachowania tajemnicy dla pracowników trwa przez okres 10 lat od ustania stosunków prawnych względem Asseco Data Systems S.A.

2.8.2. Informacje, które mogą być traktowane jako jawne

Wszystkie informacje, które niezbędne są w procesie prawidłowego funkcjonowania usług certyfikacyjnych uważane są za informacje jawne. W szczególności za informacje jawne uważa się te informacje, które umieszczane są w certyfikacie przez organy wydające certyfikaty zgodnie z opisem przedstawionym w rozdz.7. Subskrybent występując z wnioskiem o wydanie certyfikatu wyraża zgodę na upublicznienie informacji zawartej w certyfikacie.

Część informacji wpływających i przekazywanych od/do użytkowników może być udostępniana innym podmiotom wyłącznie za zgodą użytkownika, i w zakresie określonym w procesie rejestracji. Na równi z formą pisemną będą traktowane dokumenty elektroniczne zawierające podpis elektroniczny.

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

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

- Polityka Certyfikacji wraz z Kodeksem Postępowania Certyfikacyjnego,
- wzorce umów CERTUM z subskrybentami oraz stronami ufającymi,
- cennik usług,
- poradniki dla użytkowników,
- zaświadczenia certyfikacyjne urzędów certyfikacji,
- listy certyfikatów unieważnionych (CRL),
- informacje o szkoleniach.

2.8.3. Udostępnianie informacji o przyczynach unieważnienia certyfikatu

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

2.8.4. Udostępnianie informacji stanowiącej tajemnicę w trybie Art. 15 *Ustawy*

Informacja niejawna może zostać udostępniona na żądanie właściwych organów wymienionych w Art. 15 ust. 4 *Ustawy* tylko i wyłącznie po spełnieniu wszystkich wymagań stawianych przez obowiązujące na terenie Rzeczypospolitej Polskiej akty prawne.

2.8.5. Udostępnianie informacji stanowiącej tajemnicę w celach naukowych

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

2.8.6. Udostępnianie informacji stanowiącej tajemnicę na żądanie właściciela

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

2.8.7. Inne okoliczności udostępniania informacji stanowiącej tajemnicę

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

2.9. Prawo do własności intelektualnej

Wszystkie używane przez Asseco Data Systems S.A. znaki towarowe, handlowe, patenty, znaki graficzne, licencje i inne stanowią własność intelektualną ich prawnych właścicieli. CERTUM zobowiązuje się do umieszczania uwag właścicieli w tej dziedzinie.

Każda para kluczy, z którymi związany jest certyfikat klucza publicznego, wystawiony przez CERTUM jest – w przypadku subskrybenta certyfikatu kwalifikowanego osobistego – własnością

podmiotu tego certyfikatu, określonego w polu **subject** certyfikatu (patrz rozdz.7.1.1.1) lub - w przypadku subskrybenta certyfikatu kwalifikowanego profesjonalnego – własnością podmiotu reprezentowanego przez subskrybenta.

2.9.1. Znak towarowy

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

Rys.3 Logo **CERTUM**

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

Znak CERTUM jest dodatkowym elementem logo każdego punktu systemu rejestracji działającego z upoważnienia CERTUM.

2.10. Synchronizacja czasu

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

3. Identyfikacja i uwierzytelnienie

Poniżej przedstawiono ogólne zasady weryfikacji tożsamości subskrybentów, którymi kieruje się CERTUM podczas wydawania certyfikatów lub zaświadczeń certyfikacyjnych[30]. Zasady te dotyczą określonych typów informacji, które umieszczone w treści certyfikatu lub zaświadczenia certyfikacyjnego definiują środki, które należy przedsięwziąć w celu uzyskania pewności, iż informacje te są dokładne i wiarygodne w momencie wydawania certyfikatu.

Weryfikacja przeprowadzana jest obligatoryjnie podczas rejestracji subskrybenta oraz na żądanie CERTUM w przypadku każdej innej usługi certyfikacyjnej.

Każdy subskrybent składając wniosek o wydanie certyfikatu kwalifikowanego po raz pierwszy podlega procedurze rejestracji.

Certyfikacja i aktualizacja kluczy oraz modyfikacja certyfikatu jest możliwa tylko wówczas gdy subskrybent jest już zarejestrowany w systemie oraz gdy zweryfikowana została tożsamości subskrybenta na podstawie ważnego podpisu elektronicznego, złożonego pod wnioskiem o certyfikację i aktualizację kluczy oraz modyfikację certyfikatu.

Także wydanie kolejnego certyfikatu subskrybentowi jest możliwe tylko wówczas gdy subskrybent jest już zarejestrowany w systemie tj. posiadał już jakikolwiek inny certyfikat kwalifikowany wydany przez CERTUM – nawet, jeśli jest to certyfikat unieważniony lub przeterminowany oraz gdy zweryfikowana została tożsamości subskrybenta w sposób analogiczny jak w przypadku rejestracji początkowej.

CERTUM oraz podległe mu podmioty potwierdzają tożsamość i wszelkie specjalne atrybuty osoby fizycznej ubiegającej się o wydanie kwalifikowanego certyfikatu na podstawie ważnego dowodu osobistego lub paszportu, z zastrzeżeniem Art.24,[31] *Rozporządzenia eIDAS*.

3.1. Rejestracja początkowa

Rejestracja subskrybenta ma miejsce zawsze wtedy, gdy subskrybent składa wniosek o wydanie certyfikatu kwalifikowanego po raz pierwszy w urzędzie certyfikacji **CERTUM QCA**.

Rejestracja obejmuje szereg wewnętrznych procedur, które jeszcze przed wydaniem kwalifikowanego certyfikatu subskrybentowi mają na celu zgromadzenie przez punkt systemu rejestracji uwiarygodnionych danych o podmiocie, identyfikujących jego tożsamość oraz uprawnienia. Potwierdzenie tych danych wymaga osobistego kontaktu z punktem systemu rejestracji, notariuszem lub inną uprawnioną do tego osobą potwierdzającą tożsamość.

Subskrybent, obok podania danych będących treścią nazwy wyróżninej certyfikatu (patrz. rozdz. 3.1.3), jest zobowiązany udzielić w formularzu rejestracyjnym dodatkowych informacji pozwalających na jego identyfikację w tym:

- imiona rodziców,
- cechy dokumentu tożsamości,

---

30 Procedury rejestracji i uwierzytelniania podmiotów, które opisywane są w niniejszym rozdziale odnoszą się do żądań wydania lub unieważnienia certyfikatu. Jeśli procedura będzie odnosić się także do zaświadczenia certyfikacyjnego, to zostanie to wyraźnie zasygnalizowane.

31 *W przypadku gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu, a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone bezpiecznym podpisem elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat i certyfikat, którego dotyczy zgłoszenie certyfikacyjne, jest wydawany przez ten sam podmiot i w ramach tej samej polityki certyfikacji.*

- data urodzenia,
- dane kontaktowe.

Każdy subskrybent poddaje się procesowi rejestracji jednokrotnie. Po wypełnieniu elektronicznego wniosku, poprawnym zweryfikowaniu dostarczonych danych oraz po zawarciu umowy o świadczenie usług certyfikacyjnych w zakresie wydania i unieważnienia kwalifikowanego certyfikatu subskrybent zostaje wpisany na listę uprawnionych użytkowników usług CERTUM i zaopatrzony w żądany certyfikat klucza publicznego.

3.1.1. Rejestracja subskrybentów

Subskrybent certyfikatu, przed zawarciem umowy, jest zobowiązany zapoznać z warunkami świadczenia usług określonymi w niniejszym dokumencie.

Rejestracja może odbywać się tylko i wyłącznie na indywidualny wniosek subskrybenta. Wniosek moze zostać złożony za pośrednictwem strony internetowej lub w punkcie systemu rejestracji.

Każdy indywidualny wnioskodawca ubiegający się o wydanie certyfikatu lub zaświadczenia certyfikacyjnego musi wykonać następujące podstawowe czynności, poprzedzające wydanie certyfikatu:

- wypełnić elektroniczny wniosek o wydanie kwalifikowanego certyfikatu, stosowny do żądanego rodzaju certyfikatu (za pośrednictwem strony internetowej lub poprzez punkt systemu rejestracji),
- określićrodzaj kwalifikowanego certyfikatu,

Szczegółowy zakres uprawnień do występowania w cudzym imieniu powinno definiować pełnomocnictwo lub inny dokument upoważniający do występowania w cudzym imieniu.

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.

Składając wniosek przyszły subskrybent jest także zobowiązany do przedstawienia operatorowi punktu systemu rejestracji, notariuszowi lub innej osobie potwierdzającej tożsamość na podstawie ważnego dowodu osobistego lub paszportu:

- pełnomocnictw do składania podpisów w imieniu upoważniającego go podmiotu,
- innych dokumentów, które są niezbędne do potwierdzenia danych zawartych we wniosku, np. zaświadczenie o miejscu zatrudnienia.

Przy wypełnianiu wniosku przyszły subskrybent wyraża w formie oświadczenia zgodę na:

- stosowanie przez CERTUM danych służących do weryfikacji podpisu elektronicznego zawartych w żądanym certyfikacie,
- na przetwarzanie swoich danych osobowych przez Asseco Data Systems S.A. i punkt systemu rejestracji, dla potrzeb niezbędnych do realizacji procesu certyfikacji.

3.1.2. Typy nazw

Certyfikaty i zaświadczenia certyfikacyjne wydawane przez CERTUM są zgodne z normą X.509 v3. W szczególności oznacza to, że zarówno wydawca certyfikatu lub zaświadczenia certyfikacyjnego, jak też działający w jego imieniu punkt systemu rejestracji akceptują tylko takie nazwy subskrybentów, które są zgodne ze standardem X.509 (z powołaniem się na zalecenia serii X.501). Podstawowe nazwy subskrybentów oraz nazwy wystawców certyfikatów, umieszczane w certyfikatach lub zaświadczeniach certyfikacyjnych, wydawanych przez CERTUM są zgodne z nazwami wyróżnionymi DN (określanymi także mianem nazw katalogowych), budowanymi według rekomendacji X.501 i X.520. W ramach nazwy DN dopuszcza się także możliwość definiowania atrybutów systemu nazw domenowych (DNS, *ang. Domain Nameserver System*), określonych w RFC 2247 – dotyczy to jednakże jedynie zaświadczeń certyfikacyjnych. Powyższe rozwiązanie pozwala na posługiwanie się równolegle dwoma typami nazw: DN i DNS, co może być istotne zwłaszcza w przypadku wydawania certyfikatów serwerom.

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

Tab. 14 Wymagania nakładane na nazwę podmiotu certyfikatu lub zaświadczenia certyfikacyjnego

Certyfikaty /zaświadczenia certyfikacyjne	Wymagania
Kwalifikowany certyfikat	Nazwa DN podmiotu zgodna z X.500 i opcjonalnie alternatywna nazwa w przypadku, gdy jest zaznaczona jako niekrytyczna.

Zaświadczenie certyfikacyjne	Niepusta wartość pola **subject** zgodna z X.500 lub pusta w przypadku, gdy występuje pole alternatywnej nazwy podmiotu (**SubjectAltName**) i jest zaznaczone jako krytyczne[32].

Wszystkie przekazane przez subskrybenta we wniosku o rejestrację informacje, które zostaną umieszczone przez urząd certyfikacji w certyfikacie lub zaświadczeniu certyfikacyjnym są jawne. Szczegółowa lista danych umieszczanych w certyfikacie lub zaświadczeniu certyfikacyjnym jest zgodna z zaleceniem x.509 v.3 i podana jest w rozdz.7 (patrz także rozdz.3.1.3)

3.1.3. Konieczność używania nazw znaczących

Nazwy wchodzące w skład nazwy wyróżnionej DN pozwalają na jednoznaczne zidentyfikowanie podmiotu związanego z kluczem publicznym, umieszczonym w polu klucza publicznego wydanego certyfikatu lub zaświadczenia certyfikacyjnego i posiadają swoje znaczenie w języku polskim lub języku angielskim.

Struktura nazwy wyróżnionej (**DN**), akceptowana/przydzielana i weryfikowana w punkcie systemu rejestracji, uzależniona jest od typu subskrybenta oraz profilu certyfikatu lub zaświadczenia certyfikacyjnego.

Nazwa DN zawiera niektóre lub wszystkie atrybuty zawarte w następującym zbiorze atrybutów (opis atrybutu poprzedzano jego skróconą nazwą przyjętą za zaleceniem X.501; profil nazwy DN jest zgodny ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 - 5.

- **pole C** – międzynarodowy skrót nazwy kraju (w przypadku Polski – **PL**),
- **pole ST** – region/województwo, na którego terenie działa lub mieszka subskrybent,
- **pole L** – miasto, w którym ma siedzibę lub mieszka subskrybent,
- **pole S** – nazwisko subskrybenta (plus ewentualnie nazwisko rodowe lub nazwisko po mężu),
- **pole G** – imię (imiona) subskrybenta,
- **pole CN** – nazwa zwyczajowa subskrybenta lub nazwa organizacji, w której pracuje lub którą reprezentuje subskrybent, jeśli w nazwie DN wystąpiły pola O lub OU (patrz niżej),
- **pole O**[33] – nazwa instytucji, w której pracuje lub którą reprezentuje subskrybent,
- **pole OU** – nazwa jednostki organizacyjnej, zatrudniającej lub reprezentowanej przez subskrybenta,
- **pole SN** – numer seryjny, zawierający NIP lub PESEL subskrybenta,
- **pole A** – adres do korespondencji z subskrybentem,

Kwalifikowane certyfikaty są wydawane osobom fizycznym. Mogą być wydawane w różnych kategoriach:

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

[33] Argument ten umieszczany jest w nazwie DN tylko w przypadku, gdy osoba fizyczna jest pracownikiem firmy.

- **kategoria I** zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwisko, imię (imiona), numer seryjny; kategoria ta dotyczy certyfikatów osobistych,
- **kategoria II** zawiera przynajmniej następujące atrybuty: nazwa kraju, nazwa powszechna, numer seryjny; kategoria ta dotyczy certyfikatów profesjonalnych.

Jeśli nazwa organizacji zostanie włączona do nazwy podmiotu, to jednocześnie muszą być użyte atrybuty: ***nazwa województwa, nazwa miejscowości*** *i* ***adres****, które wtedy będą dotyczyły tej organizacji.*

3.1.4. Zasady interpretacji różnych form nazw

Interpretacja nazw pól umieszczanych przez CERTUM w wydawanych przez siebie certyfikatach lub zaświadczeniach certyfikacyjnych jest zgodna z profilem certyfikatów opisanym w ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 - 5.. Przy konstrukcji i interpretacji nazw wyróżnionych DN stosuje się zalecenia przedstawione w rozdz.

3.1.5. Unikalność nazw

Identyfikacja każdego podmiotu posiadającego certyfikat lub zaświadczenie certyfikacyjne wydawane przez CERTUM realizowana jest w oparciu o nazwę wyróżnioną DN.

CERTUM gwarantuje unikalność nazwy wyróżnionej (DN), przydzielonej podmiotowi certyfikatu lub zaświadczenia certyfikacyjnego.

Nazwa DN subskrybenta jest proponowana we wniosku przez samego subskrybenta. Jeśli nazwa ta jest zgodna z ogólnymi wymaganiami określonymi w rozdz.3.1.2 i 3.1.3, to operator punktu systemu rejestracji wstępnie akceptuje zgłoszoną propozycję. CERTUM zapewnia unikalność nadanych nazw **DN**, w domenie kwalifikowanych usług CERTUM.

Jeśli proponowana przez subskrybenta nazwa DN narusza prawa innych podmiotów do nazwy (patrz rozdz.3.1.4), to CERTUM może dodać dodatkowe atrybuty do nazwy DN i zagwarantować w ten sposób unikalność nazwy w swojej domenie. Subskrybent ma prawo w trybie przewidzianym w rozdz.4.3 odrzucić tak zaproponowaną nazwę DN.

Format globalnie unikalnej nazwy subskrybenta oparty jest o serialNumber, nazwę wystawcy i nazwę subskrybenta, gdzie serialNumber jest unikalną nazwą certyfikatu określonego subskrybenta.

Jeśli dowolny subskrybent zrezygnuje z kwalifikowanych usług świadczonych przez CERTUM, to żądanie rejestracji takiej samej nazwy DN przypisanej innemu subskrybentowi jest odrzucane.

CERTUM nie rejestruje subskrybenta pod nazwą DN używaną kiedyś przez innego subskrybenta, nawet na podstawie pisemnej zgody tego ostatniego.

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

3.1.6. Procedura rozwiązywania sporów wynikłych z reklamacji nazw

Zabrania się używania we wnioskach nazw, które nie są własnością subskrybenta lub podmiotu przez niego reprezentowanego. CERTUM nie odgrywa roli arbitra rozstrzygającego spory dotyczące praw własności do nazwy DN, nazwy handlowej lub znaku handlowego.

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

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

3.1.7. Dowód posiadania klucza prywatnego

Jeżeli certyfikowane klucze nie są generowane przez subskrybenta, nie nakłada się na subskrybenta obowiązku dostarczania dowodu posiadania klucza prywatnego. Jeżeli zaś subskrybent generuje klucze samodzielnie CERTUM może wymagać dowodu posiadania klucza prywatnego. Subskrybenci mają możliwość generowania nowych kluczy wyłącznie w przypadku posiadania ważnego certyfikatu kwalifikowanego wydanego przez CERTUM. Wówczas posiadanie ważnego certyfikatu kwalifikowanego uznaje się za dowód posiadania klucza prywatnego odpowiadającego kluczowi publicznemu certyfikowanemu przez CERTUM.

3.1.8. Weryfikacja tożsamości osób fizycznych

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

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.

Inspektorzy ds. rejestracji Głównego Punktu Rejestracji, operatorzy punktów systemu rejestracji, notariusze i inne osoby potwierdzające tożsamość zobligowane są do zweryfikowania poprawności oraz prawdziwości wszystkich danych zawartych we wniosku i dotyczących tożsamości wnioskodawcy oraz jego pełnomocnictw (patrz rozdz.4.1).

Procedura weryfikacji tożsamości osoby fizycznej przeprowadzana przez operatora punktu systemu rejestracji, inspektora ds. rejestracji Głównego Punktu Rejestracji lub inną osobę weryfikującą tożsamość polega na szczegółowej weryfikacji dokumentów i wniosku okazanych przez subskrybenta oraz opcjonalnie na zweryfikowaniu poprawności nazwy **DN**.

Po pozytywnym zakończeniu procedury weryfikacji operator punktu systemu rejestracji lub inna osoba weryfikująca tożsamość (poza notariuszem) podpisuje w imieniu Asseco Data Systems S.A. umowę z subskrybentem na świadczenie usług certyfikacyjnych. W przypadku weryfikacji wniosku przez notariusza, podmiot jednostronnie podpisuje umowę, która po przekazaniu do Asseco Data Systems S.A. jest podpisywana przez operatora systemu punktu rejestracji i odsyłana na adres wskazany przez wnioskodawcę.

Szczegółowy opis postępowania inspektora ds. rejestracji, operatora punktu systemu rejestracji, notariusza lub innej osoby potwierdzającej tożsamość przedstawiony jest w dokumentach dotyczących działania punktu rejestracji. Dokumenty mają status „niejawny" i udostępniane są tylko personelowi CERTUM, punktów systemu rejestracji, notariuszom, innym osobom potwierdzającym tożsamość oraz audytorom.

W szczególnym przypadku, gdy osoba ubiegająca się o wydanie kwalifikowanego certyfikatu posiada ważny kwalifikowany certyfikat, potwierdzenie jej tożsamości nie wymaga przedstawienia ważnego dowodu osobistego lub paszportu (oraz pozostałych dokumentów uwierzytelniających), a dane niezbędne do zgłoszenia certyfikacyjnego mogą być opatrzone kwalifikowanym podpisem elektronicznym tej osoby, o ile posiadany kwalifikowany certyfikat i żądany certyfikat, którego dotyczy zgłoszenie certyfikacyjne, jest wydawany przez CERTUM i w ramach tej samej polityki certyfikacji

3.1.9. Uwierzytelnienie pełnomocnictw i innych atrybutów

Inspektor ds. rejestracji Głównego Punktu Rejestracji oraz operator systemu punktu rejestracji jest zobowiązany zweryfikować posiadane przez subskrybenta pełnomocnictwo bądź upoważnienie zawsze wtedy, gdy subskrybent wnioskuje o wydanie certyfikatu kwalifikowanego, zawierającego wskazanie czy działa:

a) jako przedstawiciel innej osoby fizycznej, osoby prawnej albo jednostki organizacyjnej nieposiadającej osobowości prawnej,
b) w charakterze organu bądź członka organu osoby prawnej, albo jednostki organizacyjnej nieposiadającej osobowości prawnej,
c) organu władzy publicznej.

Uwierzytelnienie pełnomocnictw bądź uprawnień jest częścią procesu przetwarzania przez punkt systemu rejestracji i urząd certyfikacji wniosku o wydanie kwalifikowanego certyfikatu osobie fizycznej, reprezentującej interesy innej osoby (fizycznej lub prawnej). Wydany certyfikat jest w tym przypadku zaświadczeniem, że osoba fizyczna może posługiwać się kluczem prywatnym działając w imieniu innej osoby.

Proces uwierzytelniania pełnomocnictw stosowany w CERTUM oprócz weryfikacji samych pełnomocnictw obejmuje także uwierzytelnienie osoby fizycznej, która otrzymała pełnomocnictwo bądź upoważnienie.

Proces potwierdzania pełnomocnictw polega na weryfikacji dostarczonego pełnomocnictwa na podstawie:

- przedłożonych dokumentów upoważniających (np. notarialnie potwierdzonego dokumentu udzielenia pełnomocnictwa przez osobę fizyczną),
- sprawdzeniu czy dokument taki został podpisany przez osobę upoważnioną do reprezentacji,
- na sprawdzeniu zgodności danych podmiotu prawnego umieszczonych we wniosku z dostarczonymi dokumentami.

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

Uwierzytelnienie tożsamości lub pełnomocnictw subskrybentów, którzy złożyli wniosek o certyfikację, aktualizację kluczy lub modyfikację certyfikatu musi być realizowane przez inspektora ds. rejestracji Głównego Punktu Rejestracji, operatora systemu punktu rejestracji, notariusza lub inną osobę potwierdzająca tożsamość w następujących przypadkach:

- subskrybent reprezentuje inny podmiot (certyfikaty kategorii II), zaś uzyskiwany certyfikat przekracza okresem ważności uprzednio przedłożone pełnomocnictwo – dotyczy jedynie weryfikacji pełnomocnictwa,
- wniosek nie został podpisany lub poświadczony elektronicznie przy pomocy klucza prywatnego, komplementarnego z kluczem publicznym zawartym w certyfikacie lub zaświadczeniu wystawionym przez urząd certyfikacji **CERTUM QCA**,
- modyfikacji uległy dane zawarte w wystawionym certyfikacie (dotyczy wniosku o modyfikację certyfikatu),
- wniosek dotyczy certyfikacji kluczy, której wynikiem ma być kwalifikowany certyfikat wydany po raz pierwszy danemu subskrybentowi (dotyczy wniosku o certyfikację).

3.2.1. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy subskrybenta ma miejsce zawsze wtedy, gdy subskrybent występuje z wnioskiem o:

- dodatkowy certyfikat posiadanego lub nowego typu dla nowej pary kluczy, oraz
- aktualizację kluczy posiadanego certyfikatu.

W obu wymienionych przypadkach przedmiotem wniosków jest żądanie wygenerowania nowej pary kluczy i wydania certyfikatu. Wnioski muszą być uwierzytelnione, tzn.:

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

Aktualizacja kluczy może być realizowana przez subskrybenta okresowo, w oparciu o parametry wskazanego certyfikatu, będącego już w posiadaniu subskrybenta. W efekcie aktualizacji kluczy tworzony jest nowy certyfikat, którego parametry są takie same jak wskazanego we wniosku certyfikatu, poza zawartym w nim nowym kluczem publicznym, numerem seryjnym certyfikatu i innym okresem jego ważności (szczegóły patrz rozdz.4.6).

Weryfikacja tożsamości subskrybenta żądającego aktualizacji kluczy realizowana jest na podstawie podpisu elektronicznego, złożonego pod wnioskiem o aktualizację kluczy.

Certyfikacja kluczy – w przeciwieństwie do aktualizacji – nie jest związana z żadnym istniejącym certyfikatem i może dotyczyć wydania dowolnego, dopuszczalnego w systemie, typu certyfikatu (subskrybent musi jednakże być zarejestrowany w systemie, tj. posiadać jakikolwiek inny certyfikat kwalifikowany – nawet, jeśli jest to certyfikat unieważniony lub przeterminowany). Tożsamość wnioskodawcy, składającego wniosek dotyczący certyfikacji kluczy musi zostać zweryfikowana przez inspektora ds. rejestracji w Głównym Punkcie Rejestracji, operatora w punkcie systemu rejestracji, notariusza lub inną osobę weryfikującą tożsamość.

Procedura identyfikacji i uwierzytelnienia subskrybenta w przypadku certyfikacji lub aktualizacji (wtedy, gdy wynika to z umowy lub przyjętego maksymalnego dopuszczalnego okresu od ostatniej bezpośredniej weryfikacji tożsamości przez inspektora ds. rejestracji Głównego Punktu Rejestracji, operatora punktu systemu rejestracji, notariusza lub inną osobę weryfikującą tożsamość) przebiega identycznie jak w przypadku rejestracji (patrz rozdz.3.1).

3.2.2. Modyfikacja certyfikatu

Modyfikacja certyfikatu oznacza utworzenie nowego certyfikatu na podstawie certyfikatu, który jest aktualnie w posiadaniu subskrybenta, nie został unieważniony, zaś jego okres ważności nie minął. Nowy certyfikat posiada nowy klucz publiczny, nowy numer seryjny i różni się zawartością przynajmniej jednego z pozostałych pól certyfikatu. Modyfikacji nie może ulec identyfikator polityki certyfikacji, według której certyfikat został wystawiony.

Potrzeba modyfikacji może wystąpić np. w przypadku zmiany stanowiska w pracy lub zmiany adresu email pod warunkiem, że dane te zostały poprzednio umieszczone w certyfikacie lub powinny zostać dodane. Jeśli zmianie uległy dane, które zgodnie z procedurami uwierzytelniania subskrybenta są weryfikowane na podstawie odpowiednich dokumentów, np. zaświadczenia z pracy o zajmowanym stanowisku, to każdy taki wniosek musi być potwierdzony przez inspektora ds. rejestracji w Głównym Punkcie Rejestracji, operatora punktu systemu rejestracji, notariusza lub inną osobę potwierdzającą tożsamość (szczegóły patrz rozdz.4.7).

3.3. Uwierzytelnienie tożsamości subskrybentów w przypadku unieważniania certyfikatu

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

Z pośrednictwa punktu systemu rejestracji powinien skorzystać subskrybent, który jednocześnie zgubił (został mu skradziony, itp.) aktywny klucz prywatny lub – w przypadku zgłoszenia unieważnienia certyfikatu kwalifikowanego profesjonalnego – upoważniony przedstawiciel reprezentowanego podmiotu unieważniający certyfikat subskrybenta reprezentującego podmiot. Identyfikacja i uwierzytelnienie subskrybenta w punkcie systemu rejestracji przebiega identycznie jak w przypadku rejestracji początkowej (patrz rozdz. 3.1).

W przypadku realizacji unieważnienia za pośrednictwem poczty, telefonu lub faksu, subskrybent 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.

Dokładny opis procedury unieważniania certyfikatów jest opisany w rozdz.4.8.3.

3.4. Rejestracja odbiorców innych usług CERTUM

Rejestracja odbiorców usług 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 CERTUM QACA odbywa się na podstawie umowy zawartej pomiędzy subskrybentem a Asseco Data Systems S.A. Tożsamość subskrybenta zawierającego umowę jest weryfikowana:

- na podstawie podpisu elektronicznego złożonego pod umową (w postaci dokumentu elektronicznego) oraz zawartości kwalifikowanego certyfikatu; podpis elektroniczny może być złożony przez osobę fizyczną, która posiada nieprzeterminowany kwalifikowany certyfikat (niekonieczne wydany przez CERTUM),
- opcjonalnie przez inspektora ds. rejestracji, notariusza lub inna osobę potwierdzającą tożsamość zgodnie z zasadami opisanymi w rozdz.3.1, w przypadku subskrybenta, który nie posiada kwalifikowanego certyfikatu lub jest on przeterminowany lub unieważniony.

Rejestracja może być połączona z rejestracją subskrybenta urzędu certyfikacji CERTUM QCA. Rejestracja subskrybenta usług świadczonych przez urząd znacznika czasu CERTUM QTSA, urząd weryfikacji statusu certyfikatu CERTUM QOCSP, usługi walidacji CERTUM QDVCS nie jest wymogiem obowiązkowym.

W przypadku wydawania certyfikatów atrybutów stosowane są zasady i procedury opisane w rozdz.3.1 (poza podrozdz.3.1.8), w rozdz.3.2.1 (w zakresie certyfikacji) oraz w rozdz.3.3. Jeśli przytoczone zasady i procedury odnoszą się do kluczy kryptograficznych, to są one pomijane, chyba, że ma to związek z kluczami używanymi przez CERTUM QACA do wystawiania certyfikatów atrybutów i list unieważnionych certyfikatów atrybutów.

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. Składane wnioski powinny zawierać informacje, które są niezbędne do prawidłowego zidentyfikowania subskrybenta oraz danych zawartych w składanym wniosku.

CERTUM udostępnia następujące podstawowe kwalifikowane usługi certyfikacyjne:

- usługę wydawania kwalifikowanych certyfikatów obejmującą rejestrację i certyfikację, aktualizację kluczy, modyfikację certyfikatu, unieważnienie lub zawieszenie certyfikatu,
- usługę znakowania czasem,
- usługę weryfikacji statusu certyfikatu,
- usługę walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych,
- usługę urzędu poświadczania odbioru i przedłożenia,
- usługę urzędu depozytów obiektów,
- usługę urzędu rejestrów i repozytoriów,
- usługę urzędu certyfikatów atrybutów.

Usługi wydawania kwalifikowanych certyfikatów (nazywane dalej usługami wydawania certyfikatów) ich unieważniania i zawieszania/odwieszania oraz aktualizacji kluczy opisane są w rozdz.4.1-4.8, w rozdz.4.9 przedstawiono opis funkcjonalny usług znakowania czasem, w rozdz.4.8.11 - opis funkcjonalny usług weryfikacji statusu certyfikatu w trybie on-line, w rozdz.4.10 - opis funkcjonalny usług walidacji, z kolei w rozdz.4.11 - opis funkcjonalny usług wystawiania urzędowych poświadczeń odbioru lub przedłożenia.

CERTUM wydaje wzajemne zaświadczenia certyfikacyjne krajowemu urzędowi certyfikacji oraz zaświadczenia certyfikacyjne, wynikające z trybu zmiany kluczy (patrz rozdz.6.1). Zaświadczenia certyfikacyjne CERTUM wystawiane są w oparciu o procedury opisane w rozdz.6.1.1, zaś unieważniane są tak samo jak inne zaświadczenia urzędu certyfikacji CERTUM (patrz rozdz.4.8.15).

4.1. Składanie wniosków

Wnioski subskrybenta są składane przy udziale punktu systemu rejestracji. Bezpośrednio do Głównego Punktu Rejestracji mogą być składane jedynie wnioski o unieważnienie certyfikatu. 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.3.1.8 i 0) 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, recertyfikację, aktualizację kluczy lub modyfikację certyfikatu

Wniosek o certyfikację składany jest przez wnioskodawcę w punkcie systemu rejestracji osobiście lub poprzez elektroniczny formularz. Wniosek o recertyfikację, aktualizację kluczy lub modyfikację certyfikatu składany jest przez wnioskodawcę wyłącznie poprzez elektroniczny formularz.

4.1.3. Wniosek o unieważnienie

Wniosek o unieważnienie certyfikatu składany jest przez upoważnione do tego osoby (patrz rozdz.4.8.2 i 4.8.6) w Głównym Punkcie 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 wymaganiami niniejszego Kodeksu i wewnętrznymi regulacjami CERTUM potwierdzenie tożsamości wnioskodawcy własnoręcznym podpisem oraz podaniem swojego numeru PESEL w pisemnym oświadczeniu.

4.1.5. Przetwarzanie wniosków w urzędzie certyfikacji

Urząd certyfikacji pobiera tokeny zgłoszenia certyfikacyjnego ze skrzynki żądań, a następnie przetwarza go, a wszystkie czynności z tym związane odnotowywane są w bazie danych i rejestrach zdarzeń.

4.2. Wydanie certyfikatu lub zaświadczenia certyfikacyjnego

Urząd certyfikacji, po otrzymaniu tokena zgłoszenia certyfikacyjnego oraz jego pomyślnym przetworzeniu (patrz rozdz.4.1.5), **wydaje certyfikat**) lub zaświadczenie certyfikacyjne. Okresy ważności wydawanego certyfikatu lub zaświadczenia certyfikacyjnego zależą od typu certyfikatu lub zaświadczenia i są zgodne z okresami podanymi w Tab. 20 oraz 21.

Data wydania certyfikatu lub zaświadczenia certyfikacyjnego jest odnotowywana w bazie danych urzędu certyfikacji i nie jest nigdy późniejsza od daty początku okresu ważności certyfikatu lub zaświadczenia certyfikacyjnego, określonego w jego polu ***notBefore*** *(patrz rozdz.7.1).*

Każdy certyfikat wystawiany jest w trybie *off-line*[34].

O wydaniu certyfikatu informowany jest subskrybent oraz podmiot reprezentowany przez subskrybenta. Aby pobrać certyfikat subskrybent musi wpisać w specjalny formularz numer karty kryptograficznej, numer pesel (lub dane identyfikacyne z wniosku - w przypadku obcokrajowców) oraz specjalny kod, otrzymany od CERTUM, umożliwiający instalację certyfikatu na karcie kryptograficznej.

W tym samym kroku, jeszcze przed instalacją/pobraniem certyfikatu subskrybent musi pobrać kod PUK, który potrzebny będzie do nadania uwierzytelniającego kodu PIN.

Certyfikat można zainstalować na karcie automatycznie - za pomocą dedykowanej aplikacji JAVA lub pobrać do pliku i zainstalować przy pomocy oprogramowania autorskiego proCertum CardManager.

Opis działania mechanizmu automatycznego pobierania certyfikatu wygląda następująco:

- przeglądarka uruchamia VM Javy oraz applet,

- następnie uruchamiana jest dedykowana biblioteka, generującą klucze (próbuje ona połączyć się z mono.certum.pl, w tym momencie musi mieć bezpośredni dostęp do adresu, nie może zostać zablokowana przez żaden serwer Proxy).

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.

Czas ten zależy głównie od dokładności dostarczonego wniosku oraz ewentualnych administracyjnych uzgodnień i wyjaśnień pomiędzy CERTUM a wnioskodawcą. Jeśli przyczyny, ze względu na które mogą wystąpić ewentualne opóźnienia w wydaniu certyfikatu leżą tylko po

[34] Oznacza to, że zarówno tokeny zgłoszenia certyfikacyjnego jak i rejestracja użytkownika są przetwarzane w zamkniętej strefie wewnętrznej (na stacji operatora urzędu certyfikacji), do której nie ma dostępu z sieci globalnej, ze strefy przejściowej jak i z sieci wewnętrznej Asseco Data Systems S.A..

stronie 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 dowolnemu wnioskodawcy bez zaciągania jakichkolwiek zobowiązań lub narażania się na jakąkolwiek odpowiedzialność, które powstać mogą wskutek poniesionych przez wnioskodawcę (w wyniku odmowy) strat lub kosztów. CERTUM zwraca w takim przypadku wnioskodawcy wniesioną przez niego opłatę za wydanie certyfikatu (jeśli dokonał stosownej przedpłaty), chyba że wnioskodawca we wniosku o wydanie certyfikatu umieścił sfałszowane lub nieprawdziwe dane.

Odmowa wydania certyfikatu może nastąpić w następujących przypadkach:

- identyfikator subskrybenta (nazwa **DN**) ubiegającego się o wydanie certyfikatu pokrywa się z identyfikatorem innego subskrybenta,
- 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 krótkim uzasadnieniem przyczyny odmowy. Od odmownej decyzji wnioskodawca może odwołać się do CERTUM w terminie 14 dni od daty otrzymania decyzji.

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 przesłania go do CERTUM,
- braku w tym okresie pisemnej odmowy akceptacji certyfikatu.

Akceptacja certyfikatu jest także jednoznaczna z oświadczeniem subskrybenta, że zanim użył klucza publicznego zawartego w certyfikacie lub komplementarnego z nim klucza prywatnego w dowolnej operacji kryptograficznej, to dokładnie zapoznał się z treścią umowy z Asseco Data Systems S.A. zawartej w trakcie procedury rejestracji w punkcie systemu rejestracji.

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. Stosowanie kluczy oraz certyfikatów

Subskrybenci są zobowiązani do używania kluczy prywatnych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.7.1),
- zgodnie z treścią umowy zawartej pomiędzy subskrybentem a Asseco Data Systems S.A.,
- tylko w okresie ich ważności (nie dotyczy to certyfikatów do weryfikacji podpisów elektronicznych),
- tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu subskrybent nie może używać klucza prywatnego.

Z kolei strony ufające są zobowiązane do używania kluczy publicznych i certyfikatów:

- zgodnie z ich zastosowaniem, określonym w niniejszym Kodeksie Postępowania Certyfikacyjnego i zgodnym z treścią certyfikatu (pól **keyUsage** oraz **extendedKeyUsage**, patrz rozdz.7.1),
- tylko po zweryfikowaniu ich statusu oraz ważności poświadczenia elektronicznego urzędu certyfikacji, który wystawił certyfikat,
- w przypadku klucza publicznego do wymiany kluczy, szyfrowania danych lub uzgadniania kluczy tylko do momentu unieważnienia certyfikatu; w okresie zawieszenia certyfikatu strona ufająca także nie może używać tego typu kluczy publicznych.

4.5. 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 poprzedzone złożeniem odpowiedniego elektronicznego wniosku, weryfikowanego przez inspektora ds. rejestracji lub przez inną uprawnioną osobę potwierdzającą tożsamość.

Procedurze recertyfikacji mogą podlegać również zaświadczenia urzędów certyfikacji w trybie określonym w rozdz. 6.1.1. O zajściu tego zdarzenia informowani są wszyscy subskrybenci 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. Certyfikat i zaświadczenie certyfikacyjne, które było przedmiotem recertyfikacji nie jest unieważniane i umieszczane na liście CRL.

4.6. Certyfikacja i aktualizacja kluczy

Certyfikacja i aktualizacja kluczy ma miejsce zawsze wtedy, gdy subskrybent (już zarejestrowany) zażąda wygenerowania nowej pary kluczy i wystawienia nowego certyfikatu

potwierdzającego związek jego tożsamości z należącym do niego nowym kluczem publicznym. Certyfikację i aktualizację kluczy należy interpretować następująco:

- **certyfikacja kluczy** nie jest związana z żadnym ważnym certyfikatem i jest stosowana przez subskrybentów wtedy, gdy zachodzi potrzeba uzyskania jednego lub więcej certyfikatów dowolnego typu (jednakże subskrybent powinien być zarejestrowany w systemie, tzn. posiadać co najmniej jeden certyfikat – nawet jeśli ma on status unieważniony lub przeterminowany),
- **aktualizacja kluczy** dotyczy zawsze ściśle określonego, wskazanego we wniosku certyfikatu; z tego powodu nowy certyfikat posiada identyczną treść jak związany z nim certyfikat, zaś jedyne różnice to: nowy klucz publiczny, nowy numer seryjny i nowy okres ważności certyfikatu oraz nowe poświadczenie elektroniczne urzędu certyfikacji.

Elektroniczny wniosek o aktualizację kluczy złożony przez subskrybenta może dotyczyć tylko:

- ważnego certyfikatu,
- przypadku, gdy subskrybent posiada klucz prywatny powiązany z ww. certyfikatem do realizacji podpisów.

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

- nie posiada aktualnego i ważnego klucza prywatnego do realizacji podpisów,
- chce uzyskać dodatkowy certyfikat posiadanego lub innego typu, ale tylko w ramach polityki certyfikacji, zgodnie z którą został mu wydany przynajmniej jeden certyfikat (certyfikat ten nie musi być ważny).

Procedura przetwarzania wniosku o aktualizację i certyfikację kluczy jest zgodna z procedurą opisaną w rozdz.4.1.4 i 4.1.5:

Procedurze certyfikacji i aktualizacji klucza mogą podlegać także zaświadczenia certyfikacyjne urzędu certyfikacji CERTUM. O zajściu takiego zdarzenia informowani są wszyscy subskrybenci urzędu certyfikacji.

CERTUM informuje zawsze subskrybenta (co najmniej 14 dni wcześniej) o zbliżaniu się daty utraty ważności certyfikatu.

4.7. Modyfikacja certyfikatu

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

Modyfikacja certyfikatu:

- odbywa się tylko na żądanie subskrybenta i musi być poprzedzona złożeniem wniosku o modyfikację certyfikatu,
- może dotyczyć tylko certyfikatu, którego okres ważności nie minął i nie został wcześniej unieważniony.

Modyfikacji mogą podlegać:

- 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.

Uwaga:

(a) Modyfikacja może dotyczyć tylko wartości, atrybutów i rozszerzeń przewidzianych w ramach określonego typu certyfikatu lub zaświadczenia certyfikacyjnego. Np. jeśli modyfikacji podlega certyfikat kwalifikowany **CERTUM QCA Osobisty**, to jego zawartość można modyfikować tylko w ramach struktury zawartej w wydanym certyfikacie i określonej przez profil tego certyfikatu (patrz rozdz.7).

(b) Wniosek o modyfikację dotyczący certyfikatu kwalifikowanego weryfikującego podpisy lub poświadczenia elektroniczne zawiera żądanie wygenerowania kluczy w Głównym Punkcie Rejestracji.

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 potwierdzającą tożsamość.

Procedura przetwarzania wniosku o modyfikację certyfikatu jest zgodna z procedurą opisaną w rozdz.4.1.4 i 4.1.5. Dalej postępujemy jak w przypadku certyfikacji.

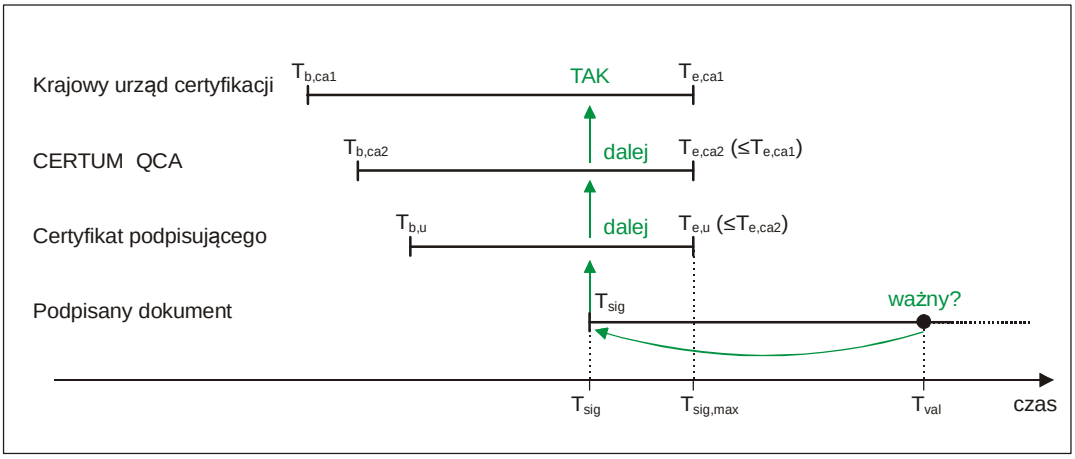
4.8. Unieważnienie i zawieszenie certyfikatu

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

Unieważnienie i zawieszanie certyfikatów oraz zaświadczeń certyfikacyjnych jest regulowane przez *Rozporządzenie eIDAS, Ustawę oraz Rozporządzenie do Ustawy z dnia 5 października 2016r. w sprawie krajowej infrastruktury zaufania.* W przypadku unieważnienia zaświadczenia certyfikacyjnego należącego do **Narodowego Centrum Certyfikacji** unieważnieniu nie ulegają automatycznie poświadczenia elektroniczne umieszczone przez ten urząd odpowiednio w zaświadczeniu certyfikacyjnym wydanym urzędom **CERTUM QCA**, **CERTUM QTSA**, **CERTUM QOCSP**, **CERTUM QDVCS**, **CERTUM QDA**, **CERTUM QODA**, **CERTUM QRRA**, **CERTUM QACA**, o ile tylko poświadczenia te zostały wystawione przed unieważnieniem zaświadczenia certyfikacyjnego krajowego urzędu certyfikacji.

Spełnienie przytoczonych powyżej wymogów jest szczególnie istotne w przypadku weryfikacji tzw. długookresowych podpisów elektronicznych, weryfikowanych po upływie okresu ważności kwalifikowanego certyfikatu, związanego z tym podpisem. Taka sytuacja zobrazowana jest na rys.4[35]. Co więcej powoduje, że wprowadzenie zakazu lub zaprzestanie działalności przez kwalifikowany podmiot świadczący usługi certyfikacyjne lub wykreślenie go przez ministra cyfryzacji z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne nie wpływa na ważność certyfikatów kwalifikowanych wydanych przez ten urząd.

[35] Przedstawiony scenariusz zaczerpnięto z *Common ISIS-MailTrust Specifications for Interoperable PKI Applications From T7 & Teletrust ISIS-MTT Specification Optional Profile, SigG-Profile, Version 1.0.2, July 19th 2002*.



Rys.4 Zakończona powodzeniem weryfikacja podpisu elektronicznego realizowana w oparciu o algorytm opisany w RFC 5280

Jeśli strona ufająca chce zweryfikować podpis elektroniczny w chwili T_{val} (jest to dowolny moment następujący po momencie T_{sig} podpisania dokumentu), to musi sprawdzić podpis elektroniczny złożony pod dokumentem, korzystając z klucza publicznego zawartego w certyfikacie podmiotu podpisującego, a następnie sprawdzić czy ten certyfikat i wszystkie zaświadczenia certyfikacyjne w ścieżce certyfikacji (prowadzącej do punktu zaufania) były ważne w chwili T_{sig}, w której został podpisany lub zweryfikowany (po raz pierwszy) dokumentW trakcie trwania zawieszenia lub natychmiast po unieważnieniu certyfikatu subskrybenta należy uznać, że certyfikat stracił ważność (jest w stanie unieważnienia). Podobnie w przypadku zaświadczeń certyfikacyjnych urzędów certyfikacji, anulowanie ważności tego rodzaju zaświadczenia oznacza cofnięcie jego posiadaczowi prawa do wydawania certyfikatów, ale nie wpływa na ważność certyfikatów wydanych przez ten urząd certyfikacji w okresie, gdy jego zaświadczenie certyfikacyjne było ważne.

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

Zawieszenie certyfikatu jest szczególną formą unieważnienia, dalej będziemy rozróżniać te dwa pojęcia dla podkreślenia istotnej różnicy pomiędzy nimi: zawieszenie certyfikatu można anulować, unieważnienie – nie. Raz unieważniony certyfikat nie może zostać przywrócony. (tam jednak gdzie wyraźnie nie zostanie to podkreślone, słowo unieważnienie obejmować będzie także zawieszenie certyfikatu).

Zawieszenie certyfikatu jest czasowe (zwykle do czasu wyjaśnienia wątpliwości, które były podstawą do zawieszenia) i może być jedynie wnioskowane przez pracownika CERTUM. **Ewentualne odwieszenie certyfikatu musi jednakże nastąpić nie później niż 7 dni od daty zawieszenia (w przeciwnym przypadku certyfikat zostaje unieważniony).**

Urząd certyfikacji unieważnia te zawieszone certyfikaty, których nie reaktywowano lub nie unieważniono w okresie 7 dni od daty zawieszenia.

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

4.8.1. Okoliczności unieważnienia certyfikatu

Podstawową przyczyną unieważnienia certyfikatu jest fakt utraty (lub samo podejrzenie takiej utraty) kontroli nad kluczem prywatnym, będącym w posiadaniu subskrybenta certyfikatu lub też rażące naruszenie przez subskrybenta zasad Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego oraz na każde żądanie subskrybenta lub – w przypadku zgłoszenia unieważnienia certyfikatu kwalifikowanego profesjonalnego – na żądanie upoważnionego przedstawiciela reprezentowanego podmiotu.

Unieważnienie certyfikatu ma miejsce w następujących okolicznościach:

- zawsze wtedy, gdy jakakolwiek informacja zawarta w certyfikacie zdezaktualizuje się,
- ilekroć klucz prywatny związany z kluczem publicznym zawartym w certyfikacie lub nośnik, na którym jest przechowywany lub istnieje uzasadnione podejrzenie, że może zostać ujawniony[36]; procedura unieważniania certyfikatu jest przeprowadzana na wniosek subskrybenta,
- subskrybent rezygnuje z umowy zawartej z Asseco Data Systems S.A. na świadczenie kwalifikowanych usług, jeśli subskrybent nie wystąpi z takim wnioskiem sam, prawo takie przysługuje urzędowi certyfikacji lub innej osobie upoważnionej do unieważnienia tego certyfikatu,
- na każde żądanie subskrybenta lub osoby trzeciej, wskazanej w certyfikacie,
- na zażądanie ministra cyfryzacji,
- w przypadku, gdy osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,
- przez wystawcę certyfikatu, tzn. przez CERTUM, np. wskutek nieprzestrzegania przez subskrybenta zaakceptowanej Polityki Certyfikacji,
- w przypadku zakończenia działalności przez urząd certyfikacji unieważnia się wszystkie certyfikaty wydane przez ten urząd przed upływem deklarowanego terminu zakończenia działalności, a także certyfikat samego urzędu certyfikacji,
- subskrybent lub podmiot reprezentowany przez subskrybenta zwleka lub ignoruje płatności za usługi świadczone przez urząd certyfikacji,
- klucz prywatny lub bezpieczeństwo systemu komputerowego urzędu certyfikacji zostały ujawnione w sposób, który bezpośrednio zagraża wiarygodności certyfikatów,
- subskrybent, będący pracownikiem organizacji, po rozwiązaniu z nim umowy o pracę nie oddał identyfikacyjnej karty elektronicznej, na której przechowywany był certyfikat i komplementarny z nim klucz prywatny,
- inne przyczyny opóźniające lub uniemożliwiające subskrybentowi wypełnianie postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego, powstałe wskutek klęsk żywiołowych, awarii systemu komputerowego lub sieci, zmian otoczenia prawnego, w którym działa subskrybent lub oficjalnych działań rządu lub jego agend.

Z wnioskiem o unieważnienie można występować (patrz rozdz.3.3) za pośrednictwem punktów systemu rejestracji. Wniosek o unieważnienie - po uprzednim zweryfikowaniu

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

tożsamości wnioskodawcy[37] - jest odsyłany jest do Głównego Punktu Rejestracji, który na jego podstawie unieważnia certyfikat.

4.8.2. Kto może żądać unieważnienia certyfikatu

Z żądaniem unieważnienia certyfikatu subskrybenta mogą występować następujące podmioty:

- subskrybent będący podmiotem unieważnianego certyfikatu,
- osoba trzecia, której dane występują w certyfikacie,
- autoryzowany przedstawiciel urzędu certyfikacji (w przypadku CERTUM rolę taką pełni inspektor bezpieczeństwa),
- upoważniony przedstawiciel reprezentowanego przez subskrybenta podmiotu,
- organ nadrzędny organizacji, w imieniu której występuje subskrybent,
- osoba fizyczna udzielająca pełnomocnictwa do reprezentowania jej interesów,
- minister cyfryzacji,
- operator punktu rejestracji, inspektor ds. rejestracji Głównego Punktu Rejestracji, którzy mogą wystąpić z takim wnioskiem w imieniu subskrybenta lub z własnej inicjatywy, jeśli są w posiadaniu informacji uzasadniającej unieważnienie certyfikatu.

Urzędy certyfikacji zachowują szczególną ostrożność przy rozpatrywaniu wniosków o unieważnienie certyfikatu, których autorem nie jest subskrybent i honorują tylko te, które obejmują przypadki wymienione w rozdz.4.8.1 oraz gdy ryzyko utraty zaufania do kwestionowanego certyfikatu przewyższa niedogodności i potencjalne straty subskrybenta, powstałe w wyniku unieważnienia.

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

- sprawdza, czy dany wnioskodawca może żądać unieważnienia certyfikatu,
- wysyła powiadomienie do subskrybenta o unieważnieniu lub zamiarze unieważnienia jego certyfikatu.

4.8.3. Procedura unieważniania certyfikatu

Unieważnienie certyfikatu można realizować na podstawie:

- pisemnego wniosku o unieważnienie, złożonego w Głównym Punkcie Rejestracji;
- telefonicznego lub faksowego wniosku o unieważnienie przekazanego do Głównego Punktu Rejestracji;

Po pozytywnej weryfikacji przez urząd certyfikacji żądania unieważnienia, certyfikat jest **unieważniany** lub tylko **zawieszany** (w przypadku, gdy mimo uzasadnionego podejrzenia, że istnieją przesłanki do unieważnienia kwalifikowanego certyfikatu, podmiot świadczący usługi certyfikacyjne nie jest w stanie w ciągu 1 godziny od momentu otrzymania żądania wyjaśnić

[37] Czynności tych dokonuje inspektor ds. rejestracji, lub inna osoba potwierdzająca tożsamość wnioskodawcy.

wszystkich wątpliwości). Informacja o unieważnionym lub zawieszonym certyfikacie umieszczana jest na liście **CRL** (patrz rozdz.7.2), 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.

Każdy wniosek o unieważnienie certyfikatu musi pozwolić na jednoznaczną identyfikację unieważnianego certyfikatu, zawierać przyczynę unieważnienia, odręczny podpis wnioskodawcy oraz musi być uwierzytelniony.

Wymaga się, aby wnioski o unieważnienie uwierzytelniane były przez inspektora ds. rejestracji Głównego Punktu Rejestracji.

Unieważniany certyfikat i komplementarny z nim klucz prywatny, przechowywane na identyfikacyjnej karcie elektronicznej, powinny być w sposób nieodwracalny usunięte z tego nośnika. Operacji tej dokonuje właściciel karty - osoba prywatna lub przedstawiciel działający z upoważnienia osoby prawnej.

4.8.4. Dopuszczalne okresy zwłoki w unieważnieniu certyfikatu

CERTUM gwarantuje, że maksymalne okresy zwłoki[38] 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 (patrz rozdz.4.8.9).

O unieważnieniu certyfikatu informowany jest subskrybent, zainteresowny wnioskodawca oraz podmiot w imieniu którego działa subskrybent.Informacja o aktualnym statusie certyfikatu jest dostępna za pośrednictwem opublikowanej listy CRL natychmiast po gwarantowanym czasie unieważnienia certyfikatu. Z żądaniem takiej usługi może wystąpić np. strona ufająca weryfikująca wiarygodność podpisu elektronicznego pod dokumentem otrzymanym od subskrybenta.

4.8.5. Okoliczności zawieszenia certyfikatu

Zawieszenie certyfikatu może mieć miejsce w następujących okolicznościach:

- dane zawarte w elektronicznym lub papierowym wniosku o unieważnienie budzą uzasadnione podejrzenia,
- wniosek o unieważnienie został przekazany telefonicznie i nie można w ciągu 1 godziny, liczonej od chwili otrzymania wniosku potwierdzić tożsamości wnioskodawcy, ale też zanegować słuszności złożonego wniosku,
- istnieje podejrzenie, że osoba składająca podpis elektroniczny utraciła pełną zdolność do czynności prawnych,

[38] Przez dopuszczalny okres zwłoki należy rozumieć maksymalny dozwolony czasu, jaki minie pomiędzy momentem otrzymania wniosku o unieważnienie a momentem zakończenia jego rozpatrywania, odnotowania w bazach urzędu certyfikacji i odesłania decyzji wnioskodawcy. Okresu tego nie należy mylić z okresem publikowania list CRL (patrz rozdz.4.8.9).

- urząd certyfikacji może niezwłocznie zawiesić certyfikat w przypadku uzasadnionego podejrzenia, że certyfikat wydano bez przestrzegania postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego; certyfikat może pozostać zawieszony do czasu aż urząd certyfikacji znajdzie podstawy do unieważnienia certyfikatu, nie dłużej jednak jak 7 dni,
- innych okoliczności wymagających wyjaśnień ze strony subskrybenta lub wnioskodawcy.

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

4.8.6. Kto może żądać zawieszenia certyfikatu

O zawieszenie certyfikatu mogą wnioskować jedynie pracownicy CERTUM.

Z wnioskiem o zawieszenie certyfikatu nie może występować subskrybent, będący podmiotem zawieszanego certyfikatu. Z tego powodu subskrybent musi być o fakcie zawieszenia niezwłocznie poinformowany.

4.8.7. Procedura zawieszenia i odwieszania certyfikatu

Procedura zawieszenia przebiega podobnie jak w przypadku unieważniania certyfikatu (patrz rozdz.4.8.3). Po poprawnej weryfikacji wniosku urząd certyfikacji zmienia status certyfikatu na zawieszony i umieszcza go na liście certyfikatów unieważnionych (z przyczyną unieważnienia **certificateHold**[39] (patrz rozdz.7.2.1).

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

- żądający odwieszenia certyfikatu subskrybent oraz urząd certyfikacji nawzajem potwierdzą swoją tożsamość,
- urząd certyfikacji stwierdzi, że ustąpiły lub nie potwierdziły się przyczyny z powodu których certyfikat zawieszono.

Odwieszenie certyfikatu odbywa się tylko i wyłącznie z inicjatywy inspektora bezpieczeństwa.

Jeśli wniosek o odwieszenie certyfikatu jest uzasadniony, to urząd certyfikacji usuwa certyfikat z listy CRL i staje się on pełnowartościowym certyfikatem, jakim był przed zawieszeniem. Jeśli przyczyny zawieszenia potwierdzą się lub certyfikat pozostaje w stanie zawieszenia dłużej niż 7 dni, to certyfikat jest unieważniany bez możliwości anulowania tej operacji.

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

[39] Certyfikat zawieszony.

4.8.8. Gwarantowany czas zawieszenia certyfikatu

Gwarantowany 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.4.8.4).

Okresy te nie obejmują czasu otrzymania potwierdzenia oraz umieszczenia zawieszonego certyfikatu na liście CRL (patrz rozdz.4.8.9).

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

4.8.9. 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[40] i automatycznie publikowane w repozytorium urzędu certyfikacji. W przypadku, gdy przyczyną unieważnienia certyfikatu jest ujawnienie klucza prywatnego, nowa lista CRL publikowana jest natychmiast po przetworzeniu wniosku o unieważnienie (patrz rozdz.4.8.4). Identycznym zasadom podlega unieważnienie dowolnego zaświadczenia certyfikacyjnego - jest ono natychmiast umieszczane na liście CRL.

4.8.10. Sprawdzanie list CRL

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

Weryfikację stanu certyfikatów strona ufająca może oprzeć na listach CRL.

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

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

W przypadkach, gdy certyfikat unieważniono, podając jako przyczynę:

```
affiliationChanged   - zamiana danych (afiliacji) subskrybenta
superseded           - zastąpienie (odnowienie) klucza
removeFromCRL[41]    - certyfikat wycofany z listy CRL (odwieszony)
```

ostateczna decyzja o zaufaniu (lub nie) weryfikowanemu certyfikatowi należy do strony ufającej. Przy podejmowaniu takiej decyzji należy wziąć pod uwagę, że z powodu wyżej wymienionych

---

[40] Zapowiedź terminu następnej publikacji może być także umieszczana w treści aktualnie wydanej listy CRL (patrz pole **NextUpdate**, rozdz.7.2). Wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy, co oznacza, że publikacja ta może nastąpić także przez upływem deklarowanego terminu.

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

przyczyn nie istnieje żadne uzasadnione podejrzenie lub pewność, że klucz prywatny subskrybenta został ujawniony.

4.8.11. Dostępność weryfikacji statusu certyfikatu w trybie on-line

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[42].

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 (tzn. natychmiast po unieważnieniu certyfikatu).

4.8.12. Obowiązek sprawdzania unieważnień w trybie on-line

Na stronę ufającą nie nakłada się obowiązku weryfikacji statusu certyfikatu w trybie *on-line*, realizowanej w oparciu o usługi i mechanizmy przedstawione w rozdz.4.8.11. Zaleca się jednak korzystanie z tej możliwości wtedy, gdy ryzyko zaakceptowania nieważnego lub sfałszowanego podpisu jest wysokie.

4.8.13. Inne dostępne formy ogłaszania unieważnień certyfikatów

W przypadku naruszenia ochrony (ujawnienia) klucza prywatnego urzędu certyfikacji funkcjonującego w ramach CERTUM informacja o tym jest umieszczana natychmiast na listach CRL oraz obligatoryjnie przesłana za pośrednictwem poczty elektronicznej do wszystkich subskrybentów urzędu certyfikacji. Informowani są wszyscy subskrybenci, których interesy mogą być w jakikolwiek sposób (bezpośredni lub pośredni) zagrożone.

4.8.14. Obowiązek sprawdzania innych form ogłaszania unieważnień certyfikatów

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

---

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

4.8.15. Unieważnienie lub zawieszenie zaświadczenia certyfikacyjnego urzędu certyfikacji

Zaświadczenie certyfikacyjne urzędu certyfikacji może zostać unieważnione lub zawieszone przez **Narodowe Centrum Certyfikacji**. Może to nastąpić w przypadku wystąpienia jednej z poniższych sytuacji:

- minister cyfryzacji działając w oparciu o zapisy Ustawy o usługach zaufania podejmie decyzję o wykreśleniu Asseco Data Systems S.A. z rejestru kwalifikowanych podmiotów świadczących usługi certyfikacyjne,
- **Narodowe Centrum Certyfikacji** jest przekonane, że dane zawarte w zaświadczeniu certyfikacyjnym urzędu, któremu wystawił to zaświadczenie są nieprawdziwe,
- klucz prywatny urzędu certyfikacji lub jego system komputerowy zostały ujawnione w sposób mający wpływ na pewność wydawanych przez niego zaświadczeń,
- urząd certyfikacji naruszył w sposób istotny zasady niniejszego Kodeksu Postępowania Certyfikacyjnego.

4.9. 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. Dzięki temu:

- urząd znacznika czasu potwierdza istnienie danych,
- urząd znacznika czasu stwarza możliwość zweryfikowania, że podpis elektroniczny został złożony pod danymi jeszcze przed unieważnieniem klucza użytego do podpisu.

*Urząd znacznika czasu **CERTUM QTSA** nie jest stroną w trakcie realizowania transakcji, które uzależnione są od czasu i oznaczane znacznikiem czasu.*

Proces uzyskania znacznika czasu, wystawianego przez urząd znacznika czasu przebiega w pięciu następujących etapach:

- 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 czasu (token znacznika czasu - TST), który zawiera m.in. numer seryjny, identyfikator protokołu, przy pomocy którego został utworzony znacznik czasu, zależny od czasu parametr (czas), pobrany z zaufanego źródła, dane (m.in. skrót), dostarczone w żądaniu, dane utworzone przez urząd znacznika czasu, które kryptograficznie wiążą wartość czasu z wartością skrótu, identyfikatorem funkcji skrótu oraz identyfikatorem sesji,
- 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.

Proces świadczenia usługi znacznika czasu przez **CERTUM QTSA** spełnia następujące wymagania bezpieczeństwa:

- zaufane źródło czasu **CERTUM QTSA** jest synchronizowane z międzynarodowym wzorcem czasu z dokładnością do 1 sekundy,
- numer seryjny umieszczony w tokenie znacznika czasu jest unikalny w domenie **CERTUM QTSA**; cecha ta jest zachowana także w przypadku wznowienia usługi po awarii,
- klucz prywatny urzędu znacznika czasu jest generowany i przechowywany w sprzętowym module kryptograficznym spełniającym wymagania FIPS 140 Level 3,
- urząd znacznika czasu **CERTUM QTSA** posiada własny klucz prywatny stosowany jedynie do poświadczania tokenów znacznika czasu.

4.10. Usługa walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych

Usługi **CERTUM QDVCS** przydatne są w trakcie realizacji procedur potwierdzania ważności podpisanych dokumentów, certyfikatów 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**, pracująca w oparciu o protokół DVCS, OASIS DSS, XKMS , może:

- weryfikować poprawność załączonego podpisu elektronicznego (ang. *validation of digitally signed document*, **vsd**), przy użyciu wszystkich odpowiednich informacji o statusie certyfikatów kluczy publicznych oraz na żądanie, stworzyć certyfikat (tzw. DVC), poświadczający ważność podpisu,
- weryfikować ważność załączonego certyfikatu (ang. *validation of public key certificates*, **vpkc**) i jego status nawet w przypadku, gdy minął jego okres ważności lub informacja o jego unieważnieniu nie jest już dostępna na liście CRL lub nie jest łatwo dostępna, i na żądanie stworzyć certyfikat DVC, poświadczający ważność certyfikatu i jego statusu,

Kwalifikowany urząd walidacji **CERTUM QDVCS** może walidować następujące typy tokenów i poświadczeń:

- kwalifikowany certyfikat klucza publicznego,
- kwalifikowany podpis elektroniczny, kwalifikowaną pieczęć elektroniczną,

Uzyskanie tokena walidacji przebiega następująco:

- wnioskodawca wysyła żądanie, zawierające informacje o typie pożądanej walidacji oraz walidowane dane,
- urząd walidacji danych weryfikuje poprawność formatu wniosku, pobiera żądany typ walidacji

- urząd walidacji danych 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 *Polityka walidacji kwalifikowanej usługi CERTUM walidacji kwalifikowanych podpisów elektronicznych i kwalifikowanych pieczęci elektronicznych.*

4.11. Usługa wystawiania urzędowych poświadczeń odbioru i przedłożenia

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. W pierwszym przypadku wystawiane są urzędowe poświadczenia odbioru lub przedłożenia, które stanowią dla klienta dowód, że przesyłany przez niego dokument elektroniczny został przesłany przez urząd **CERTUM QDA** i umieszczony w systemie teleinformatycznym adresata przesyłki. Z kolei w drugim przypadku wystawiane są poświadczenia odbioru lub przedłożenia stanowią dla *podmiotu realizującego zadania publiczne* dowód, że przesyłany przez niego dokument elektroniczny został przesłany poprzez urząd **CERTUM QDA** i umieszczony w systemie teleinformatycznym, który jest dostępny adresatowi (odbiorcy) przesyłki.

Usługa wystawiania urzędowego poświadczenia odbioru wykonywana jest następująco:

- wnioskodawca (nadawca) wysyła 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 formalna 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.

4.12. 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:

- umieszczenie obiektów w depozycie z możliwością poinformowania o tym fakcie wskazanych podmiotów lub subskrybentów depozytu; w wyniku zrealizowania usługi urząd wystawia **poświadczenie wpisu obiektu do depozytu**,
- wydanie obiektów z depozytu (wydanie odbywa się na podstawie przedłożonego wpisu); obiekty są usuwane z depozytu wraz z wpisem, na podstawie którego zostały wydane; w wyniku zrealizowania usługi urząd wystawia **poświadczenie wydania obiektu z depozytu**,
- uwierzytelnione wydanie obiektów (z poświadczeniami potwierdzającymi ich ważność dowodową); obiekty oraz wszystkie powiązane z nimi dane poświadczające ich ważność są usuwane z depozytu wraz z wpisem, na podstawie którego zostały wydane; w wyniku zrealizowania usługi urząd wystawia **uwierzytelnione poświadczenie wydania obiektu z depozytu**,
- pobranie wpisów z depozytu (wpisy nie są usuwane z depozytu); w wyniku zrealizowania usługi urząd wystawia **poświadczenie pobrania wpisu z depozytu**,
- uwierzytelnione pobranie wpisów z depozytu (wraz z poświadczeniami potwierdzającymi ich ważność dowodową); w wyniku zrealizowania usługi urząd wystawia **uwierzytelnione poświadczenie pobrania wpisu z depozytu**,
- pobranie obiektów umieszczonych w depozycie (w oparciu o przedstawione wpisy); w wyniku zrealizowania usługi urząd wystawia **poświadczenie pobrania obiektu z depozytu**,
- uwierzytelnione pobranie obiektu umieszczonego w depozycie (w oparciu o przedstawiony wpis) wraz ze wszystkimi powiązanymi z nimi danymi poświadczającymi ich ważność; w wyniku zrealizowania usługi urząd wystawia **uwierzytelnione poświadczenie pobrania obiektu z depozytu**.

Każde z wystawionych poświadczeń należy do grupy poświadczeń depozytowych, wystawianych przez urząd depozytów **CERTUM QODA**.

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.

4.13. 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:

- wpis do rejestru wraz z opcjonalnym umieszczeniem obiektów w repozytorium i opcjonalnym poinformowaniem o tym fakcie subskrybentów rejestru; w wyniku zrealizowania usługi urząd wystawia **poświadczenie umieszczenia wpisu w rejestrze** oraz opcjonalnie **poświadczenie umieszczenia obiektu w repozytorium**,
- pobranie wpisów znajdujących się w rejestrach; w wyniku zrealizowania usługi urząd wystawia **poświadczenie pobrania wpisu z rejestru**,
- pobranie obiektów umieszczonych w repozytorium (pobranie odbywa się na podstawie przedłożonych wpisów do rejestru); w wyniku zrealizowania usługi urząd wystawia **poświadczenie pobrania obiektu z repozytorium**,
- uwierzytelnione pobranie wpisu z rejestru z pozostawieniem go w rejestrze (wraz z poświadczeniami potwierdzającymi jego ważność dowodową); w wyniku zrealizowania usługi urząd wystawia **uwierzytelnione poświadczenie pobrania wpisu z rejestru**,
- uwierzytelnione pobranie obiektu z repozytorium z pozostawieniem go w repozytorium (wraz z poświadczeniami potwierdzającymi jego ważność dowodową); w wyniku zrealizowania usługi urząd wystawia **uwierzytelnione poświadczenie pobrania obiektu z repozytorium**,
- modyfikacja wpisu w rejestrze; w wyniku zrealizowania usługi urząd wystawia **poświadczenie modyfikacji wpisu w rejestrze**,
- modyfikacja obiektu w repozytorium; w wyniku zrealizowania usługi urząd wystawia **poświadczenie modyfikacji obiektu w repozytorium**.

Każde z wystawionych poświadczeń należy do grupy poświadczeń rejestrowych i repozytoryjnych, wystawianych przez urząd rejestrów i repozytoriów **CERTUM QRRA**.

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**.

4.14. 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.

Usługi urzędu certyfikatów atrybutów **CERTUM QACA** świadczone są tylko zarejestrowanym użytkownikom (subskrybentom) usług CERTUM. Jeśli użytkownik nie jest subskrybentem usług CETUM, to procedura jego rejestracji jest zgodna z postępowaniem opisanym w rozdz.4.1.1 i odbywa się na wniosek zainteresowanego użytkownika.

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[43], 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,

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

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**.

Wydanie certyfikatu atrybutów realizowane jest w trybie opisanym w rozdz.4.2, zaś jego akceptacja w trybie opisanym w rozdz.4.3.

Jeśli użytkownik składający wniosek o wydanie certyfikatu atrybutów jest subskrybentem usług CERTUM i posiada certyfikat kwalifikowany wydany przez dowolny podmiot świadczący usługi certyfikacyjne zgodne z Ustawą, to wniosek o wydanie certyfikatu może być opatrzony podpisem kwalifikowanym.

Certyfikat atrybutów może być unieważniany; nie można go jednak zawieszać i następnie odwieszać. W momencie unieważnienia certyfikatu atrybutów certyfikat ten jest umieszczany na liście unieważnionych certyfikatów atrybutów wraz z podaniem przyczyny.

W certyfikatach atrybutów może być umieszczane rozszerzenie *noRevAvail*, które jest deklaracją wystawcy certyfikatu, że certyfikat ten nie podlega procedurze unieważniania i w przypadku zażądania unieważnienia certyfikatu przez jego posiadacza lub inny upoważniony podmiot, informacja o unieważnieniu nie będzie umieszczana na **liście unieważnionych certyfikatów atrybutów użytkowników końcowych**.

Jeśli weryfikowany certyfikat znajduje się na liście unieważnionych certyfikatów atrybutów, to ufająca strona zobowiązana jest do odmowy wykonania czynności, do których uprawniałby atrybut lub atrybuty umieszczone w unieważnionym certyfikacie w przypadku, gdy certyfikat unieważniono z powodu:

privilegeWithdrawn - anulowanie uprawnień związanych z atrybutami

Procedura unieważniania certyfikatów atrybutów jest zgodna z zasadami opisanymi w rozdz.4.8. Jeśli zasady te odnoszą się do kluczy kryptograficznych, to są one pomijane, chyba, że ma to związek z kluczami używanymi przez CERTUM QACA do wystawiania certyfikatów atrybutów i list unieważnionych certyfikatów atrybutów.

Struktura unieważnionych certyfikatów atrybutów jest identyczna ze strukturą listy unieważnionych certyfikatów klucza publicznego (rozdz.7.2).

4.15. Rejestrowanie zdarzeń, zarządzanie incydentami bezpieczeństwa oraz audyty 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 maja istotny wpływ na bezpieczeństwo funkcjonowania CERTUM.

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

Wpisy do rejestru zdarzeń są realizowane automatycznie. Wszystkie wpisy do rejestrów i dzienników są przechowywane i udostępniane w czasie prowadzenia audytów.

Zespół Jakości CERTUM zobowiązany jest do regularnego przeprowadzania wewnętrznych audytów dotyczących zgodności wdrożonych mechanizmów z zasadami niniejszego Kodeksu Postępowania Certyfikacyjnego, a także do oceny efektywności istniejących procedur bezpieczeństwa.

4.15.1. Typy rejestrowanych zdarzeń

Wszystkie czynności krytyczne z punktu widzenia bezpieczeństwa CERTUM dokumentowane są w rejestrach zdarzeń oraz archiwizowane. Archiwa są poświadczane elektronicznie przez operatora systemu i zapisywane na nośnikach jednokrotnego zapisu.

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

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

Rejestrowanie zdarzeń ma charakter ciągły a przerwanie rejestracji może nastąpić wyłącznie z chwilą wyłączenia systemu, którego dotyczy rejestracja. Rejestry te są wspólne dla wszystkich komponentów zainstalowanych na danym serwerze lub stacji roboczej i mają z góry określoną pojemność. Po jej przekroczeniu automatycznie tworzona jest nowa wersja rejestru. Stary rejestr po zarchiwizowaniu jest usuwany z dysku.

Rekordy zdarzeń rejestrowane automatycznie lub ręcznie w rejestrach zdarzeń zawierają:

- typ zdarzenia,

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

Rejestrowane zdarzenia obejmują:

- alarmy generowane przez firewall i IDS,
- czynności związane z rejestracją, certyfikacją, aktualizacją, unieważnianiem i zawieszaniem certyfikatów, wystawianiem znacznika czasu, walidacją danych, weryfikacja statusu certyfikatu, wystawieniem poświadczenia odbioru lub przedłożenia (w tym także urzędowego poświadczenia odbioru lub przedłożenia) oraz innymi usługami świadczonymi przez CERTUM,
- wszelkie modyfikacje struktury sprzętowej i programowej,
- modyfikacje sieci i połączeń,
- fizyczne wejścia do obszarów zastrzeżonych oraz ich naruszenia,
- zmiany haseł, PIN-ów, uprawnień oraz ról personelu,
- udane i nieudane próby dostępu do oprogramowania serwerów CERTUM oraz jego baz danych,
- generowanie kluczy dla potrzeb urzędów CERTUM, jak również innych stron, np. subskrybentów i punktów rejestracji,
- każde zdarzenie związane z aktualizacją zaświadczeń certyfikacyjnych urzędu certyfikacji **CERTUM QCA** oraz pozostałych urzędów świadczących usługi certyfikacyjne,
- synchronizacje serwerów za pomocą protokołu NTP z zaufanym źródłem czasu,
- każdy fakt utraty synchronizacji zaufanego źródła czasu z międzynarodowym wzorcem czasu, w tym także przekroczenie przyjętej granicznej dokładności synchronizacji (1 sekunda),
- dowolne zdarzenie związane z użyciem klucza prywatnego, należącego do dowolnego kwalifikowanego urzędu CERTUM, świadczącego usługi certyfikacyjne,
- wszystkie otrzymywane wnioski oraz wydawane decyzje mające postać elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane w formie pliku lub poczty elektronicznej; obowiązek rejestrowania tego typu zdarzeń spoczywa nie tylko na urzędzie certyfikacji, ale także na punktach systemu rejestracji,
- historia tworzenia kopii bezpieczeństwa oraz archiwizowania rejestrów zdarzeń oraz baz danych.

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

Dostęp do zapisów rejestrowanych zdarzeń (logów) posiadają jedynie inspektor bezpieczeństwa, administrator systemu oraz inspektor ds. audytu (patrz rozdz.5.2.1.1).

4.15.2. Częstotliwość analizy zapisów rejestrowanych zdarzeń (logów)

W celu rozpoznania ewentualnych nieuprawnionych działań administrator systemu i inspektorzy ds. audytu powinni analizować informacje, o których mowa w rozdz.4.15.1, przynajmniej raz w każdym dniu roboczym.

Wszystkie zauważone istotne zdarzenia są wyjaśniane i opisane w rejestrze zdarzeń. Proces przeglądania rejestru zdarzeń obejmuje w pierwszym rzędzie sprawdzenie czy rejestr nie został sfałszowany, a następnie zweryfikowanie wszystkich występujących w rejestrze alarmów oraz anomalii. Wszystkie działania podjęte w wyniku zauważonych usterek muszą być odnotowane w rejestrze zdarzeń.

4.15.3. 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.

4.15.4. Ochrona zapisów rejestrowanych zdarzeń

Archiwa powinny być poświadczane elektronicznie i znakowane czasem.

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

- tylko osoby upoważnione, tj. audytorzy oraz osoby występujące w jednej z trzech wymienionych powyżej ról mają prawo czytania rekordów z rejestru zdarzeń,
- tylko inspektor bezpieczeństwa w obecności **administratora systemu** może archiwizować i usuwać, po zarchiwizowaniu, z systemu pliki zawierające zarejestrowane zdarzenia,
- możliwe jest wykrycie każdego naruszenia jego integralności; daje to możliwość upewnienia się, że rekordy nie zawierają luk lub sfałszowanych wpisów,
- żaden podmiot nie posiada prawa modyfikowania jego zawartości.

Dodatkowo procedury ochrony rejestrów zdarzeń są tak zaimplementowane, że nawet po ich zarchiwizowaniu niemożliwe jest ich usunięcie lub zniszczenie przed datą końca przewidywanego okresu przechowywania rejestrów (patrz rozdz.4.16.3).

4.15.5. Procedury tworzenia kopii zapisów rejestrowanych zdarzeń

Procedury bezpieczeństwa CERTUM wymagają, aby zapisy zdarzeń były kopiowane zgodnie z harmonogramem tworzenia kopii, nie rzadziej jednak niż 4 razy w roku. Kopie te przechowywane są w ośrodku głównym i zapasowym CERTUM. Kopie mogą być oznaczone znacznikiem czasu.

Czynności tworzenia kopii zapasowych wykonywane są przez operatora systemu w obecności inspektora bezpieczeństwa.

4.15.6. 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).*

W przypadku gdy w toku rozpoznawania zaistniałego incydentu zgodnie z procedurą zarządzania incydentami bezpieczeństwa stwierdzone zostanie, że zdarzenie to ma wpływ na usługi świadczone przez Pion Usług Bezpieczeństwa i Zaufania, CERTUM zawiadamia organ nadzoru nie później niż w ciągu 24 godzin od wystąpienia zdarzenia. Powiadomienie to wysyłane jest niezwłocznie faxem.

Organ nadzoru niezwłocznie po otrzymaniu zgłoszenia od CERTUM, powiadamia o zaistniałym naruszeniu bezpieczeństwa lub utracie integralności Generalnego Inspektora Danych Osobowych lub Krajowy Organ Bezpieczeństwa Informacji, o ile zdarzenie to ma znaczący wpływ na świadczoną przez CERTUM usługę zaufania lub przetwarzane w jej ramach dane osobowe.

Jeżeli w toku rozpoznawania zaistniałego incydentu bezpieczeństwa stwierdzone zostanie, że naruszenie bezpieczeństwa lub utrata integralności niekorzystnie wpłyną na osobę fizyczną lub prawną na rzecz, której świadczona była usługa zaufania, CERTUM niezwłocznie zawiadamia te podmioty, zgodnie z procedurą zarządzania incydentami bezpieczeństwa.

4.15.7. Powiadamianie podmiotów odpowiedzialnych za zaistniałe zdarzenie

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

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

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

4.15.8. Oszacowanie podatności na zagrożenia

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

mogą być także określone przez zewnętrzną instytucję, uprawnioną do przeprowadzania audytu w CERTUM.

Analiza ryzyka dla CERTUM prowadzona jest przynajmniej raz w roku lub przy wprowadzaniu nowych usług, dużych zmian w systemach certum lub w wyniku incydentu bezpieczeństwa. Za audyt wewnętrzny odpowiedzialny jest inspektor bezpieczeństwa, którego zadanie polega na kontroli zgodności zapisów w rejestrze bezpieczeństwa, poprawności przechowywania jego kopii, działań podejmowanych w sytuacjach zagrożeń oraz przestrzegania postanowień niniejszego Kodeksu Postępowania Certyfikacyjnego.

4.16. Archiwizowanie danych

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

Archiwum zawiera certyfikaty wydane maksymalnie do 25 lat wstecz.

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

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

Zaleca się poświadczanie elektroniczne oraz oznaczanie czasem archiwizowanych danych elektronicznych. Klucz, przy pomocy, którego poświadcza się archiwum, znajduje się pod kontrolą inspektora bezpieczeństwa.

4.16.1. Rodzaje archiwizowanych danych

Archiwizacji podlegają następujące dane:

- dane z przeglądu i oceny (z audytu) zabezpieczeń logicznych i fizycznych systemu komputerowego urzędu certyfikacji, punktu systemu rejestracji oraz repozytorium urzędu certyfikacji,
- otrzymywane wnioski oraz wydawane decyzje, mające postać papierową lub elektroniczną, które nadeszły od subskrybenta lub zostały mu przekazane,
- dokumenty wystawiane przez operatora systemu punktu rejestracji, notariusza lub inne osoby potwierdzające tożsamość wnioskodawcy w imieniu CERTUM,
- umowy o świadczenie usług certyfikacyjnych,
- baza danych subskrybentów, w tym wszystkie informacje zebrane w procesie rejestracji subskrybenta,
- baza danych certyfikatów,
- wydane listy CRL,
- historia kluczy urzędu certyfikacji, od ich wygenerowania do zniszczenia włącznie,

- wewnętrzna i zewnętrzna korespondencja (pisemna i elektroniczna) CERTUM z subskrybentami i innymi osobami uprawnionymi do wystąpienia z wnioskiem oraz ufającymi stronami przy operacjach zawieszania i odwieszania certyfikatów,
- pozostałe dokumenty papierowe, związane ze świadczeniem usług certyfikacyjnych.

4.16.2. Częstotliwość archiwizowania danych

Archiwizacja realizowana jest kilkupoziomowo w następujących odstępach czasowych:

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

4.16.3. Okres przechowywania archiwum

Archiwizowane dane (w formie elektronicznej i papierowej), wymienione w rozdz.4.16.1 przechowywane są przez minimalny okres 20 lat. Po upływie przyjętego okresu archiwizacji dane są niszczone. W przypadku niszczenia kluczy i certyfikatów proces niszczenia wykonywany zgodnie z wewnętrznymi procedurami.

4.16.4. Procedury tworzenia kopii zapasowych

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

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

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

4.16.5. Wymaganie znakowania archiwizowanych danych znacznikiem czasu

Zaleca się, aby archiwizowane dane elektroniczne oznaczane były znacznikiem czasu, tworzonym przez urząd znacznika czasu **CERTUM QTSA**, posiadający zaświadczenie wydane przez ministra cyfryzacji lub upoważniony przez niego podmiot świadczący usługi certyfikacyjne.

4.16.6. Procedury dostępu oraz weryfikacji zarchiwizowanej informacji

W celu sprawdzenia integralności zarchiwizowane dane są, co pewien okres testowane oraz porównywane z danymi oryginalnymi. Czynność ta może być przeprowadzona tylko przez inspektora bezpieczeństwa i jest odnotowywana w rejestrze zdarzeń.

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

4.17. 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.

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

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

Rozdział ten zawiera opis procedur postępowania, realizowanych przez CERTUM w wypadkach szczególnych (także klęsk żywiołowych) w celu przywrócenia gwarantowanego poziomu usług. Procedury te realizowane są według opracowanego planu podnoszenia systemu po katastrofie (*ang. disaster recovery plan*).

4.18.1. Uszkodzenie zasobów obliczeniowych, oprogramowania i/lub danych

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

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

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

- **Plan podnoszenia systemu po katastrofie.** Wszyscy subskrybenci oraz strony ufające są jak najszybciej i w sposób najbardziej odpowiedni do zaistniałej sytuacji powiadamiani o każdej poważnej awarii lub katastrofie, dotyczącej dowolnego komponentu systemu komputerowego i sieci. Plan podnoszenia systemu obejmuje szereg procedur, które są realizowane w momencie, gdy dowolna część systemu ulegnie skompromitowaniu (uszkodzeniu, ujawnieniu, itp.). Aby to było możliwe, wykonywane są następujące działania:
    - tworzone i konserwowane są kopie obrazu dysków każdego z serwerów oraz stacji roboczej systemu CERTUM; każda kopia przechowywana jest zarówno w siedzibie, jak i w bezpiecznym pomieszczeniu poza siedzibą CERTUM,
    - okresowo, zgodnie z procedurami opisanymi w rozdz.4.16.4 tworzone są kopie każdego z serwerów zawierające pełne kopie serwerów, wszystkie zgłoszone żądania ze strony subskrybentów, zapisy rejestrowanych zdarzeń (logi), wydane, aktualizowane i unieważnione certyfikaty; najbardziej aktualne kopie przechowywane są w bezpiecznym miejscu w siedzibie jak i poza siedzibą CERTUM,
    - klucze CERTUM, rozproszone zgodnie z zasadami sekretów współdzielonych, przechowywane są przez ich posiadaczy w miejscach tylko im znanych,

- wymiana komputera jest wykonywana tak, aby możliwe było odtworzenie obrazu dysku, w oparciu o najbardziej aktualne dane oraz klucze (dotyczy to serwera podpisującego),
- proces podnoszenia systemu po katastrofie jest okresowo testowany na każdym elemencie systemu i jest częścią procedur audytu wewnętrznego.

- **Kontrolowanie zmian.** W systemie docelowym instalacja uaktualnionych wersji oprogramowania możliwa jest tylko i wyłącznie po przeprowadzeniu na systemie modelowym testów, wykonywanych według ściśle opracowanych procedur. Wszystkie zmiany dokonywane w systemie wymagają akceptacji inspektora bezpieczeństwa CERTUM. Jeśli mimo stosowania się do tej procedury wdrożone nowe elementy spowodują awarię systemu docelowego, opracowane plany podnoszenia systemu po katastrofie pozwalają na powrót do stanu sprzed awarii.
- **System zapasowy.** W przypadku awarii uniemożliwiającej funkcjonowanie CERTUM w ciągu maksymalnie 1 godziny zostanie uruchomiona możliwość unieważniania certyfikatów w ośrodku zapasowym. Możliwość świadczenia wszystkich funkcji urzędów certyfikacji CERTUM, do czasu uruchomienia głównego ośrodka, zostanie zapewniona w ciągu maksymalnie 48 godzin. Z uwagi na regularne tworzenie kopii zapasowych, archiwizację, gromadzenie nieprzetworzonych przesyłek oraz redundancję sprzętowo-programową w przypadku awarii uniemożliwiającej funkcjonowanie CERTUM możliwe jest:
  - uruchomienie ośrodka zapasowego pozwalającego na uruchomienie CERTUM,
  - przetworzenie wszystkich zgromadzonych i nieprzetworzonych żądań,
  - do czasu regeneracji i ponownego uruchomienia ośrodka głównego - przetwarzanie na bieżąco przychodzących wiadomości od użytkowników.
- **System tworzenia kopii zapasowych.** System CERTUM korzysta z oprogramowania tworzącego kopie zapasowe z danych, które w każdej chwili umożliwiają ich odtworzenie oraz przeprowadzenie audytu systemu. Kopie zapasowe oraz archiwa tworzone są ze wszystkich danych, mających istotny wpływ na bezpieczeństwo i normalne funkcjonowanie CERTUM. Kopie są tworzone okresowo i zapisywane na taśmach, archiwa zaś na płytach CD-ROM. Kopie zapasowe mogą być chronione przy pomocy hasła, płyty CD-ROM są elektronicznie podpisywane i oznaczane czasem. Kopie danych i ich archiwa przechowywane są w siedzibie CERTUM, jak i poza miejscem lokalizacji głównego systemu przetwarzającego.
- **Usługi szczególne.** W celu zapobieżenia czasowemu zanikowi zasilania i zapewnienia ciągłości usług stosuje się zasilanie awaryjne (UPS-y i generator). System zasilania ciągłego sprawdzany jest co 6 miesięcy.

4.18.2. Ujawnienie lub podejrzenie ujawnienia kluczy prywatnych urzędu certyfikacji

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

- urząd certyfikacji generuje nową parę kluczy i występuje do krajowego urzędu certyfikacji z wnioskiem o wydanie nowego zaświadczenia certyfikacyjnego,

- w trybie natychmiastowym zostaną zawiadomieni o tym fakcie wszyscy użytkownicy certyfikatów za pośrednictwem komunikatu w środkach masowego przekazu oraz za pośrednictwem poczty elektronicznej,
- zaświadczenie certyfikacyjne, związane z ujawnionym kluczem prywatnym, znajdzie się na liście CRL z podaniem przyczyny unieważnienia,
- unieważnione i umieszczone na liście unieważnionych certyfikatów i zaświadczeń certyfikacyjnych wraz z podaniem odpowiedniej przyczyny unieważnienia zostaną także wszystkie certyfikaty subskrybentów oraz certyfikaty znajdujące się w ścieżce certyfikacji skompromitowanego zaświadczenia certyfikacyjnego,
- wygenerowane zostaną nowe certyfikaty użytkowników,
- nowe certyfikaty użytkowników zostaną przesłane do użytkowników bez obciążania ich kosztami za powyższą operację; użytkownik może odmówić akceptacji wystawionego certyfikatu.

4.18.3. Spójność zabezpieczeń po katastrofach

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

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

4.19. Zakończenie działalności lub przekazanie zadań przez urząd certyfikacji

Przedstawione poniżej obowiązki urzędu certyfikacji mają na uwadze redukcję wpływu skutków podjęcia przez ten urząd decyzji o zakończeniu swojej działalności i obejmują obowiązek odpowiednio wczesnego poinformowania o tym organu nadzoru, subskrybentów, kontrahentów, i Partnerów z którymi Centrum Certyfikacji jest związane umowami handlowym oraz przekazania dokumentów i danych związanych ze świadczeniem usług certyfikacyjnych organowi nadzoru. Szczegółowy sposób postępowania w przypadku zakończenia działalności przez Centrum Certyfikacji określa plan zakończenia działalności Centrum Certyfikacji, stanowiący wewnętrzną procedurę CERTUM.

4.19.1. Wymagania związane z przekazaniem obowiązków

Po podjęciu decyzji o zakończeniu działalności CERTUM zobowiązane jest do wykonania następujących czynności:

- powiadomienia krajowego urzędu certyfikacji o zamiarze zaprzestania działalności jako kwalifikowanego podmiotu świadczącego usługi certyfikacyjne; na co najmniej na 90 dni przed planowanym zakończeniem działalności,
- zawiadomienia (co najmniej na 90 dni wcześniej) wszystkich subskrybentów, którzy posiadają jeszcze ważny certyfikat, wydany przez likwidowany urząd, o zamiarze zakończenia działalności,
- powiadomienia Partnerów handlowych oraz Partnerów prowadzących Punkty Potwierdzenia Tożsamości oraz powiadomienia Punktów Rejestracji,
- unieważnienia wszystkich wydanych pełnomocnictw do potwierdzania tożsamości subskrybentów oraz podpisywania umów o świadczenie usług certyfikacyjnych w imieniu Asseco Data Systems S.A.
- powiadomienia innych podmiotów, z którymi CERTUM jest związane umowami handlowymi na świadczenie kwalifikowanych usług certyfikacyjnych,
- poinformowania wszystkich subskrybentów związanych z urzędem certyfikacji o zaprzestaniu działalności,
- dochowania najwyższej staranności, aby zaprzestanie działalności urzędu spowodowało jak najmniejsze szkody w działalności subskrybentów oraz osób prawnych, zaangażowanych w proces ciągłego weryfikowania podpisów elektronicznych (będących jeszcze w obiegu) przy pomocy kluczy publicznych, poświadczonych certyfikatami wydanymi przez likwidowany urząd certyfikacji,
- przekazania danych, bezpośrednio związanych z wykonywaniem usług certyfikacyjnych, organowi nadzoru lub wskazanemu przez niego podmiotowi,
- zwrotu subskrybentowi lub podmiotowi reprezentowanemu przez subskrybenta kosztów wydanego certyfikatu, proporcjonalnie do pozostałego okresu ważności wydanego certyfikatu.

4.19.2. Ponowne wydawanie certyfikatów przez następcę likwidowanego urzędu certyfikacji

Szczegółowy sposób postępowania w przypadku zakończenia działalności przez Centrum Certyfikacji określa plan zakończenia działalności Centrum Certyfikacji, stanowiący wewnętrzną procedurę CERTUM.”Wszystkie certyfikaty aktualnie ważne w dniu deklarowanego, definitywnego zaprzestania działalności muszą być unieważnione i umieszczone na liście CRL. Unieważnione muszą być także zaświadczenia certyfikacyjne 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**, urzędu 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.

5. Zabezpieczenia fizyczne, organizacyjne oraz personelu

W rozdziale opisano ogólne wymagania w zakresie nadzoru nad zabezpieczeniami fizycznymi, organizacyjnymi oraz działaniami personelu, stosowanymi w CERTUM m.in. podczas generowania kluczy, uwierzytelniania podmiotów, emisji certyfikatów, unieważniania certyfikatów i zaświadczeń certyfikacyjnych, audytu oraz wykonywania kopii zapasowych.

5.1. Zabezpieczenia fizyczne

5.1.1. Bezpieczeństwo fizyczne CERTUM

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

5.1.1.1. Miejsce lokalizacji oraz budynek

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

5.1.1.2. Dostęp fizyczny

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

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

Pomieszczenia CERTUM dzielą się na:

- pomieszczenie systemu komputerowego,
- pomieszczenie operatorsko - administracyjne.

Pomieszczenie systemu komputerowego, w tym także pomieszczenie, w którym znajduje się bezpieczny moduł kryptograficzny z pozostającymi w nim kluczami urzędu QCA, wyposażone jest w nadzorowany system zabezpieczeń, zbudowany w oparciu o czujniki ruchu, przeciwpożarowe oraz przeciwpowodziowe. Dostęp do pomieszczenia posiadają tylko osoby upoważnione, tzn. zaufany personel CERTUM oraz Asseco Data Systems S.A. Nadzorowanie praw dostępu realizowane jest w oparciu o posiadane przez nich karty identyfikacyjne oraz system kontroli dostępu, którego końcówki zamontowane są przy wejściu do pomieszczeń. Obecność innych osób (np. audytorów lub pracowników serwisu sprzętowego) wymaga obecności uprawnionego członka personelu oraz zgody Dyrektora Pionu Usług Bezpieczeństwa i Zaufania.

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

5.1.1.3. Zasilanie oraz klimatyzacja

W przypadku zaniku zasilania podstawowego system przechodzi na zasilanie awaryjne (generator prądu) poprzez UPS.

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

Wszystkie pomieszczenia są klimatyzowane.

5.1.1.4. Zagrożenie zalaniem

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

5.1.1.5. Ochrona przeciwpożarowa

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

5.1.1.6. Nośniki informacji

W zależności od stopnia wrażliwości informacji nośniki, na których przechowywane są archiwa oraz bieżące kopie danych składowane są w sejfach ognioodpornych zlokalizowanych w pomieszczeniach operatorsko-administracyjnych. Kopie stosownych dokumentów oraz kopie zapasowe i archiwalne są składowane również w ośrodku zapasowym, w sejfach ognioodpornych, trwale związanych z podłożem.

5.1.1.7. Niszczenie informacji

Papierowe oraz elektroniczne nośniki zawierające informacje mogące mieć wpływ na bezpieczeństwo CERTUM po upływie okresu przechowywania (patrz rozdz.4.16.3) niszczone są w specjalnych urządzeniach niszczących. W przypadku kluczy kryptograficznych oraz numerów PIN nośniki, na których informacje te były przechowywane są niszczone w urządzeniach klasy DIN-3 (dotyczy to tylko nośników, które nie zezwalają na definitywne usunięcie z nich informacji i ich ponowne użycie do tych samych lub innych celów).

5.1.1.8. Przechowywanie kopii bezpieczeństwa

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

5.1.2. Bezpieczeństwo punktów rejestracji

Komputery Głównego Punktu Rejestracji służące wydawaniu certyfikatów znajdują się w specjalnie przeznaczonym do tego celu pomieszczeniu oraz pracują w trybie *on-line* (muszą być włączone w sieć). Dostęp do nich jest fizycznie chroniony przed nieupoważnionymi osobami. Do ich obsługi dopuszczone są jedynie upoważnione do tego osoby. Komputery zlokalizowane w pozostałych punktach potwierdzania tożsamości podlegają ochronie, której zakres opisany jest w stosownych umowach pomiędzy CERTUM a administratorem danego punktu.

5.1.2.1. Miejsce lokalizacji oraz budynek

Punkty rejestracji CERTUM zlokalizowane są w następujących miejscach:

- Główny Punkt Rejestracji (GPR) - w pomieszczeniu operatorsko-administracyjnym CERTUM (patrz rozdz.5.1.1.1),
- lokalizacja innych punktów rejestracji dostępna jest w serwisie internetowym urzędu certyfikacji dostępnym pod adresem www.certum.pl i za pośrednictwem poczty elektronicznej: infolinia@certum.pl.

5.1.2.2. Dostęp fizyczny

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

5.1.2.3. Zasilanie oraz klimatyzacja

Pomieszczenie Głównego Punktu Rejestracji wyposażone jest w układ zasilania awaryjnego. Dodatkowo automatycznie uruchamiane są agregaty prądotwórcze podtrzymujące napięcie. Klimatyzacja nie jest wymagana. Na pozostałe punkty systemu rejestracji nie nakłada się wymagań odnośnie awaryjnych systemów zasilania oraz klimatyzacji.

5.1.2.4. Zagrożenie wodne

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

5.1.2.5. Ochrona przeciwpożarowa

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

5.1.2.6. Nośniki informacji

Nośniki informacji, na których przechowywane są archiwa, bieżące kopie danych oraz dokumenty papierowe składowane są w sejfach zlokalizowanych w pomieszczeniu Głównego Punktu Rejestracji i innych punktach systemu rejestracji, administrowanych przez CERTUM. Dodatkowo wymaga się, aby kopie dokumentów, które są potwierdzeniem realizacji procedur weryfikowania wniosków i tożsamości wnioskodawców, były archiwizowane także w Głównym Punkcie Rejestracji. Metody ochrony nośników i danych w punktach potwierdzania tożsamości, nie administrowanych przez CERTUM precyzowane są w umowach pomiędzy Asseco Data Systems S.A. a administratorem danego punktu.

5.1.2.7. Niszczenie informacji

Po upływie okresu przechowywania (patrz rozdz.4.16.3) papierowe oraz elektroniczne nośniki, zawierające informacje poufne lub sekretne są niszczone w specjalnych urządzeniach niszczących.

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

5.1.2.8. Przechowywanie kopii bezpieczeństwa

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

Zaleca się przechowywanie poza punktem systemu rejestracji archiwów oraz bieżących kopii informacji przetworzonej przez system komputerowy. W przypadku GPR kopie bezpieczeństwa przechowywane są w sejfach w ośrodku zapasowym.

5.1.3. Bezpieczeństwo subskrybenta

Subskrybent powinien chronić swoje hasło dostępu do systemu lub osobisty numer identyfikacyjny (PIN). Jeżeli używane hasło lub PIN są trudne do zapamiętania, mogą zostać zapisane jednak pod warunkiem przechowywania ich w sejfie, do którego dostęp mają tylko upoważnione osoby lub zaszyfrowaniu hasła (algorytmem znanym właścicielowi danego numeru PIN).

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

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

5.2. Zabezpieczenia organizacyjne

Poniżej przedstawiono listę ról, które mogą pełnić pracownicy zatrudnieni w CERTUM, jest ona zgodna z wymogami opisanymi ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers. Niniejszy dokument opisuje także odpowiedzialność związaną z każdą pełnioną rolą.

5.2.1. Zaufane role

5.2.1.1. Zaufane role w CERTUM

Osoby piastujące w CERTUM zaufane role podlegają szczególnej weryfikacji. CERTUM sprawdza informacje o ich kwalifikacjach, doświadczeniu zawodowym oraz niekaralności.

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

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

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

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

inspektora bezpieczeństwa, inspektora ds. rejestracji, administratora systemu czy operatora systemu.

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

5.2.1.2. Zaufane role w punkcie systemu rejestracji

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

- **osoba potwierdzająca tożsamość wnioskodawcyi atrybuty** – weryfikuje tożsamość subskrybenta, atrybuty wpisywane na jego żądanie do certyfikatu oraz poprawność złożonego przez niego wniosku, przygotowuje dane, zatwierdza przygotowane zgłoszenia certyfikacyjne i przekazuje je do urzędu certyfikacji, w imieniu Asseco Data Systems S.A. zawiera umowy ze subskrybentami na świadczenie usług,

Partner prowadzący autoryzowany punktu rejestracji – odpowiada za sprawne działanie punktu systemu rejestracji; jego rola polega na zapewnieniu finansowania pracowników, zarządzaniu pracą osób potwierdzających tożsamość wnioskodawców. Osoba potwierdzająca tożsamość wnioskodawców musi posiadać akredytację CERTUM. Po jej uzyskaniu (na swój wniosek lub Partnera autoryzowanego punktu rejestracji) może potwierdzać tożsamość wnioskodawców zarówno w siedzibie punktu systemu rejestracji jak też w miejscu pobytu wnioskodawcy.

5.2.1.3. Zaufane role u subskrybenta

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

5.2.2. Liczba osób wymaganych do realizacji zadania

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

- **inspektora bezpieczeństwa,**
- **administratora systemu (operatora modułu kryptograficznego),**
- **posiadaczy sekretów współdzielonych,**
- **obserwatorów – (opcjonalnie) np. przedstawiciele audytora**

Szczegółowa procedura generowania kluczy opisana jest w "Dokumentacji zarządzania cyklem życia kluczy urzędów certyfikacji" o statusie "niejawny".

5.2.3. Identyfikacja oraz uwierzytelnianie ról

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

- umieszczania na liście osób posiadających dostęp do pomieszczeń CERTUM,

- umieszczania na liście osób posiadających fizyczny dostęp do systemu i sieci CERTUM**,**
- wydawania poświadczenia upoważniającego do wykonywania przypisanej roli,
- przydzielania konta oraz hasła w systemie komputerowym CERTUM.

Każde z powyższych poświadczeń oraz przypisanych kont:

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

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

Konta oraz uprawnienia osób, które zakończyły pracę w CERTUM lub utraciły prawo do reprezentowania CERTUM, są natychmiast blokowane.

Zgodnie z Polityką Bezpieczeństwa Informacji oraz normą PN-ISO/IEC 27001:2014 Inspektorzy Bezpieczeństwa CERTUM prowadzą regularne - odbywające sie raz na kwartał - przeglądy kont i uprawnień w systemach CERTUM. Wszystkie nieużywane są blokowane.

5.3. Personel

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

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

personel CERTUM, zwłaszcza osoby piastujące tzw. zaufane role, zobowiązane są postępować zgodnie z przepisami Rozporządzenia e-IDAS UE 910/2014 i Ustawy z dnia 5 września o usługach zaufania oraz identyfikacji elektronicznej Zgodnie z Polityką Bezpieczeństwa Informacji, która jest elementem wdrożonego w Asseco Data Systems S.A. Zintegrowanego Systememu Zarządzania, realizowane są w CERTUM procedury gwarantujące zarządzanie uprawnieniami w sposób wymagany przez normę PN-ISO/IEC 27001:2014.

Oznacza to między innymi, że wobec informacji i zasobów sklasyfikowanych jako chronione obowiązuje zasada "wiedzy uzasadnionej", zgodnie z którą dostęp do tej kategorii informacji lub innego zasobu musi być uzasadniony realizacją powierzonych zadań.

5.3.1. Szkolenie

Personel wykonujący czynności w ramach obowiązków wynikających z zatrudnienia w urzędzie certyfikacji lub działających w jego imieniu punktach systemu rejestracji musi przejść cykl szkoleń dotyczących:

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

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

5.3.2. Częstotliwość powtarzania szkoleń oraz wymagania

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

5.3.3. Rotacja stanowisk

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

5.3.4. Sankcje z tytułu nieuprawnionych działań

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

5.3.5. Pracownicy kontraktowi

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

5.3.6. Dokumentacja przekazana personelowi

Kierownictwo CERTUM, jak również Partnerzy prowadzący punkt systemu rejestracji mają umożliwić swojemu personelowi dostęp do następujących dokumentów::

- Polityki Certyfikacji,

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

6. Procedury bezpieczeństwa technicznego

Rozdział ten opisuje procedury tworzenia oraz zarządzania parami kluczy kryptograficznych 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 kluczy prywatnych CERTUM, od których zależy bezpieczeństwo funkcjonowania całego systemu certyfikowania kluczy publicznych.

Urząd certyfikacji CERTUM QCA posiada przynajmniej jedno zaświadczenie certyfikacyjne, które stosowane jest w procesie elektronicznego poświadczania kwalifikowanych certyfikatów, zaświadczeń certyfikacyjnych i list CRL.

Klucze prywatne urzędu certyfikacji CERTUM QCA stosowane są do podpisywania certyfikatów oraz list CRL.

Dodatkowo klucze urzędu certyfikacji CERTUM QCA mogą być używane do podpisywania zaświadczeń certyfikacyjnych, w tym wzajemnych, w przypadkach określonych w rozdz.4.17.

Do realizacji podpisu elektronicznego stosowany jest algorytm RSA w kombinacji z funkcją skrótu SHA-1, zaś do uzgadniania kluczy – algorytm Diffie-Hellmana[44] lub RSA.

6.1.1. Generowanie klucza publicznego i prywatnego

Klucze wszystkich urzędów świadczących usługi certyfikacyjne generowane są w siedzibie CERTUM w obecności wybranej, przeszkolonej grupy zaufanych osób (w grupie tej muszą znajdować się także inspektor bezpieczeństwa, administrator systemu). Taka grupa osób konieczna jest tylko w przypadku generowania kluczy do elektronicznego poświadczania certyfikatów i list CRL, wystawiania tokenów znacznika czasu. Klucze urzędów świadczących usługi certyfikacyjne, funkcjonujących w ramach CERTUM, generowane są przy zastosowaniu wyodrębnionej, wiarygodnej stacji roboczej oraz sprzężonego z nią sprzętowego modułu kryptograficznego, spełniającego wymagania klasy FIPS 140-2 Level 3 lub wyżej.

Klucze urzędu certyfikacji, urzędu znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych oraz urzędu poświadczania odbioru i przedłożenia generowane są zgodnie z przyjętą w CERTUM procedurą generowania kluczy. Czynności wykonywane w trakcie generowania każdej pary kluczy są rejestrowane, datowane i podpisywane przez każdą uczestniczącą w procedurze osobę. Zapisy te są przechowywane dla potrzeb audytu oraz bieżących przeglądów systemu.

Klucze subskrybentów mogą być generowane w urzędzie certyfikacji **CERTUM QCA** lub samodzielnie przez subskrybenta z wykorzystaniem mechanizmów dostarczonych przez PCC CERTUM (patrz. 6.1.2).

[44] Algorytm Diffie– Hellmana nie jest wykorzystywany do tworzenia bezpiecznych podpisów i poświadczeń elektronicznych.

6.1.1.1. Procedury generowania początkowych kluczy urzędu certyfikacji

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

- bezpiecznym wygenerowaniu głównej pary kluczy do elektronicznego poświadczania certyfikatów i list CRL - główna para kluczy ma postać $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(1)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(1)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzeniu żądania wydania zaświadczenia certyfikacyjnego i przekazania go **krajowemu urzędowi certyfikacji**, żądanie zawiera, m.in. klucz publiczny **KGPK(1)** oraz dowód posiadania komplementarnego z nim klucza prywatnego.

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

Podobnie realizowana jest procedura generowania początkowych kluczy RSA do uzgadniania kluczy:

- wygenerowanie pary kluczy $\mathbf{KDH=\{K^{-1}_{KDH}, K_{KDH}\}}$ do uzgadniania kluczy, gdzie $\mathbf{K^{-1}_{KDH}}$ - klucz prywatny, zaś $\mathbf{K_{KDH}}$ - klucz publiczny,
- wydaniu certyfikatu kluczy infrastruktury $\mathbf{K_{KDH}}$, elektroniczne poświadczonego przy pomocy klucza prywatnego $\mathbf{K^{-1}_{GPK(1)}}$.

6.1.1.2. Procedury aktualizacji kluczy urzędu certyfikacji

Klucze **CERTUM QCA** mają skończony okres życia, po którego upływie muszą zostać uaktualnione.

Szczególna procedura stosowana jest podczas aktualizacji pary kluczy do elektronicznego poświadczania certyfikatów i list CRL. Polega ona na wydaniu przez **CERTUM QCA** specjalnych zaświadczeń certyfikacyjnych ułatwiających zarejestrowanym użytkownikom końcowym, posiadającym stare zaświadczenie certyfikacyjne **CERTUM QCA**, na bezpieczne przejście do pracy z nowym zaświadczeniem certyfikacyjnym, zaś nowym użytkownikom końcowym posiadającym nowe zaświadczenie certyfikacyjne na bezpieczne pozyskanie starego zaświadczenia certyfikacyjnego, umożliwiającego weryfikację istniejących danych (patrz RFC 2510).

Aby uzyskać wspomniany wyżej efekt **CERTUM QCA** musi stosować procedurę, która po wygenerowaniu nowej pary kluczy zabezpieczy (uwiarygodni) nowy klucz publiczny przy pomocy starego (poprzednio stosowanego) klucza prywatnego i odwrotnie, w tym samym czasie stary klucz publiczny zabezpieczony zostanie przy pomocy nowego klucza prywatnego. Oznacza to, że w momencie uaktualniania zaświadczenia certyfikacyjnego urzędu certyfikacji **CERTUM QCA**, oprócz nowego zaświadczenia certyfikacyjnego zostaną utworzone dwa dodatkowe zaświadczenia certyfikacyjne. Łącznie istnieją cztery zaświadczenia certyfikacyjne do elektronicznego poświadczania certyfikatów i list CRL: stare **zaświadczenie certyfikacyjne StaryStarym** (stary klucz publiczny podpisany starym kluczem prywatnym), nowe **zaświadczenie certyfikacyjne NowyNowym** (nowy klucz publiczny podpisany nowym kluczem prywatnym), **zaświadczenie certyfikacyjne StaryNowym** (stary klucz publiczny

podpisany nowym kluczem prywatnym) oraz **zaświadczenie certyfikacyjne NowyStarym** (nowy klucz publiczny podpisany starym kluczem prywatnym).

Procedura aktualizacji nowej pary kluczy **CERTUM QCA**, przeznaczonej do elektronicznego poświadczania certyfikatów i list CRL przebiega następująco:

- Generowanie nowej, kolejnej i-tej głównej pary kluczy $\mathbf{GPK_{(i)}=\{K^{-1}_{GPK(i)}, K_{GPK(i)}\}}$, gdzie $\mathbf{K^{-1}_{GPK(i)}}$ – klucz prywatny, zaś $\mathbf{K_{GPK(i)}}$ – klucz publiczny, rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową).
- Utworzenie żądania wydania zaświadczenia certyfikacyjnego i przekazania go **krajowemu urzędowi certyfikacji**, żądanie zawiera m.in. klucz publiczny $\mathbf{K_{GPK(I)}}$ oraz dowód posiadania komplementarnego z nim klucza prywatnego.
- **Narodowe Centrum Certyfikacji** tworzy zaświadczenie certyfikacyjne zawierające nowy klucz publiczny **CERTUM QCA**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ (**zaświadczenie certyfikacyjne NowyNowym**).
- **CERTUM QCA** tworzy zaświadczenie certyfikacyjne zawierające nowy klucz publiczny **CERTUM QCA**, podpisany przy pomocy starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ (**zaświadczenie certyfikacyjne NowyStarym**).
- Dezaktywacja starego klucza prywatnego $\mathbf{K^{-1}_{GPK(i-1)}}$ i aktywacja nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ - w sprzętowym module kryptograficznym znajduje się nowy klucz prywatny do podpisywania certyfikatów i list CRL.
- Utworzenie przez **CERTUM QCA** zaświadczenia certyfikacyjnego zawierającego stary klucz publiczny **CERTUM QCA**, podpisany przy pomocy nowego klucza prywatnego $\mathbf{K^{1}_{GPK(i)}}$ (**zaświadczenia certyfikacyjnego StaryNowym**).
- Opublikowanie utworzonych zaświadczeń certyfikacyjnych w repozytorium urzędu certyfikacji, rozesłanie informacji o nowych zaświadczeniach certyfikacyjnych.

Po wygenerowaniu i uaktywnieniu nowego klucza prywatnego (może to nastąpić w dowolnym momencie okresu ważności starego zaświadczenia certyfikacyjnego), urząd **CERTUM QCA** elektronicznie poświadcza certyfikaty subskrybentów tylko przy pomocy nowego klucza prywatnego.

Stary klucz publiczny (stare zaświadczenie certyfikacyjne) jest w użyciu aż do momentu, gdy wszyscy użytkownicy końcowi będą w posiadaniu nowego zaświadczenia certyfikacyjnego (nowego klucza publicznego) **CERTUM QCA** (powinno to nastąpić najpóźniej w momencie upływu okresu ważności starego zaświadczenia certyfikacyjnego).

Koniec okresu ważności **zaświadczenia certyfikacyjnego StaryNowym** pokrywa się z końcem okresu ważności starego zaświadczenia certyfikacyjnego.

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

Okres wykorzystywania **zaświadczenia certyfikacyjnego NowyNowym** dla użytkowników rozpoczyna się w chwili wygenerowania nowej pary kluczy, zaś kończy się przynajmniej 360 dni przed wygaśnięciem okresu jego ważności. Wymóg ten oznacza, że urząd certyfikacji **CERTUM QCA** zaprzestaje używać klucza prywatnego do elektronicznego poświadczania certyfikatów przynajmniej na 360 dni przed datą upłynięcia aktualności zaświadczenia certyfikacyjnego, z którym klucz prywatny jest związany.

Procedura aktualizacji kluczy **CERTUM QCA**, stosowanych przez urząd do podpisywania wiadomości i uzgadniania kluczy wygląda podobnie jak w przypadku aktualizacji kluczy użytkowników końcowych i przebiega następująco:

- generowanie przez **CERTUM QCA** nowej pary kluczy – klucz do podpisywania wiadomości RSA lub klucz do uzgadniania kluczy RSA oraz rozproszenie klucza prywatnego (zgodnie z przyjętą metodą progową),
- utworzenie zaświadczenia certyfikacyjnego dla wygenerowanego w poprzednim kroku nowego klucza publicznego **CERTUM QCA**, podpisany przy pomocy klucza prywatnego $\mathbf{K}^{-1}_{\mathbf{GPK(i)}}$,
- opublikowanie utworzonego zaświadczenia certyfikacyjnego w repozytorium urzędu certyfikacji i rozesłanie odpowiedniej informacji do użytkowników końcowych.

6.1.2. Przekazywanie klucza prywatnego użytkownikowi końcowemu

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.

Nowi subskrybenci kwalifikowanych usług CERTUM otrzymują personalizowane karty kryptograficzne. Personalizacja kart oznacza, że w zabezpieczonym pomieszczeniu – do którego dostęp posiadają wyłącznie wskazani pracownicy spośród osób pełniących zaufane role – na kartach generowane są klucze kryptograficzne subskrybentów i wraz z nimi zabezpieczające kody PUK oraz numery identyfikacyjne kart, które automatycznie zapisywane są do bazy danych. Proces personalizacji kart odbywa się na urządzeniach nie podłączonych do sieci.

Subskrybenci chcący odnowić posiadany na karcie kryptograficznej wydanej przez CERTUM ważny certyfikat kwalifikowany, mogą wygenerować zdalnie kolejną parę kluczy. Wówczas CERTUM udostępnia swoim subskrybentom dedykowaną aplikację, która tworzy klucze bezpośrednio na karcie kryptograficznej subskrybenta.

Dane do uaktywnienia karty (m.in. PUK/PIN) udostępniane są subskrybentom oddzielnie od wydawanych certyfikatów. Dane do uaktywnienia sprzętowego modułu kryptograficznego także przekazywane są oddzielnie, fakt wydania certyfikatu z wykorzystaniem sprzętowego modułu kryptograficznego rejestrowany jest przez urząd certyfikacji.

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

6.1.3. Przekazywanie klucza publicznego do urzędu certyfikacji

6.1.4. Nie dotyczy.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, przy czym w przypadku urzędu certyfikacji **CERTUM QCA** certyfikat ma postać zaświadczenia certyfikacyjnego, wydanego 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.
- dystrybuowane są za pomocą dedykowanego oprogramowania, które umożliwia korzystanie z usług CERTUM.

W przypadku aktualizacji kluczy urzędów certyfikacji CERTUM w repozytorium urzędu certyfikacji umieszczane są wszystkie dodatkowe zaświadczenia certyfikacyjne, powstałe w wyniku realizacji procedury opisanej w rozdz.6.1.1.2.

6.1.5. Długości kluczy

Wszystkie kwalifikowane urzędy certyfikacji działające w ramach CERTUM używają kluczy o długości 2048 bitów. Klucze nowych certyfikatów wydawanych użytkownikom końcowym także posiadają długość 2048 bitów.

Pozostaje jednak niewielka ilość subskrybentów usług kwalifikowanych, którzy posiadają karty kryptograficzne akceptujące wyłącznie klucze o długości 1024 bitów. Właściciele takich kart, którzy odnawiają certyfikat kwalifikowany, otrzymują certyfikaty zaopatrzone w klucze o długości 1024 bitów.

6.1.6. Parametry generowania klucza publicznego

Zarówno gdy klucze kryptograficzne generowane są przez CERTUM oraz w przypadku gdy samodzielnie tworzy je subskrybent korzystając z mechanizmów udostępnianych przez CERTUM (patrz. 6.1.2), parametry generowania klucza publicznego spełniają wymagania określone w normach ESTI EN 319 – 401 i 319 – 411-2

6.1.7. Weryfikacja jakości klucza

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

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

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

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

6.1.8. Sprzętowe i/lub programowe generowanie kluczy

W przypadku urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu 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** klucze generowane są za pomocą sprzętowych modułów kryptograficznych, zgodnych z wymaganiami opisanymi w rozdz.6.2.1.

Zgodne z wymaganiami określonymi w rozdz.6.2.1 powinny być generowane także wszystkie klucze stosowane do składania poświadczeń i podpisów elektronicznych, których część publiczna w postaci certyfikatu lub zaświadczenia certyfikacyjnego potwierdzana jest przez **CERTUM QCA**. Wymóg ten w szczególności dotyczy użytkowników końcowych, którzy występują do urzędu certyfikacji **CERTUM QCA** z żądaniem wydania certyfikatu kwalifikowanego.

Dopuszczalne sposoby generowania kluczy uzależnione są ich zastosowania przedstawione są Tab. 15.

Tab. 15 Sposób generowania kluczy

Certyfikaty /zaświadczenia certyfikacyjne/tokeny/poświadczenia	Sposób generowania kluczy
Kwalifikowany certyfikat klucza publicznego	Sprzętowy
Zaświadczenie certyfikacyjne	Sprzętowy
Tokeny	Sprzętowy
Poświadczenia	Sprzętowy
Certyfikat atrybutów	Sprzętowy

*) Tylko w przypadku kluczy, które nie są stosowane do składania podpisów lub poświadczeń elektronicznych

6.1.9. Zastosowania kluczy

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

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

a) digitalSignature: przeznaczenie certyfikatu do realizacji usługi uwierzytelnienia za pomocą podpisu cyfrowego w innych celach niż określone w pkt. b), f) i g);

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

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

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

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

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

g) **cRLSign**: klucz publiczny jest używany do weryfikacji poświadczeń elektronicznych w listach unieważnionych i zawieszonych certyfikatów oraz listach unieważnionych i zawieszonych zaświadczeń certyfikacyjnych wydanych przez kwalifikowany podmiot świadczący usługi certyfikacyjne;

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

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

Kwalifikowane certyfikaty wydawane subskrybentom mogą być używane jedynie do podpisywania. Ich tworzenie i zarządzanie podlega wymaganiom zdefiniowanym dla certyfikatów stosowanych jedynie dla zapewnienia usługi niezaprzeczalności (ustawiony bit **nonRepudiation**).

Urząd certyfikacji **CERTUM QCA** posiada klucze do elektronicznego poświadczania certyfikatów i list CRL (ustawione bity **keyCertSign** oraz **cRLSign**).Urząd znacznika czasu **CERTUM QTSA**, urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, urząd walidacji **CERTUM QDVCS**, urząd poświadczania odbioru i przedłożenia **CERTUM QDA**, urząd depozytów obiektów **CERTUM QODA** oraz urząd rejestrów i repozytoriów **CERTUM QRRA** posiadają klucze stosowane do elektronicznego poświadczania tokenów (ustawiony bit **digitalSignature** oraz bit **nonRepudiation**).

Urząd certyfikatów atrybutów **CERTUM QACA** posiada typ klucza stosowany do poświadczania certyfikatów atrybutów i list EARL (ustawione bity **keyCertSign** oraz **cRLSign**).

6.2. Ochrona klucza prywatnego

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

6.2.1. Standard modułu kryptograficznego

Sprzętowe moduły kryptograficzne używane przez urząd certyfikacji, urząd znacznika czasu, urząd weryfikacji statusu certyfikatu, urząd walidacji danych, urząd poświadczania odbioru

i przedłożenia, i subskrybentów są zgodne z wymaganiami normy FIPS 140 lub ITSEC (*ITSEC v 1.2 wydany przez Komisję Europejską, Dyrektoriat XIII/F, w 1991 r.*).

Tab. 16 Minimalne wymagania nakładane na moduł kryptograficzny

Typ podmiotu certyfikatu/zaświadczenia certyfikacyjnego	Wykorzystywany moduł kryptograficzny
Urząd certyfikacji CERTUM QCA	Sprzętowy FIPS 140-2 Level 3 i wyżej
Urząd znacznika czasu CERTUM QTSA	Sprzętowy FIPS 140-2 Level 3 i wyżej/EAL 4+
Urząd weryfikacji statusu certyfikatu czasu CERTUM QOCSP	Sprzętowy FIPS 140-2 Level 3 i wyżej/EAL 4+
Urząd walidacji CERTUM QDVCS	Sprzętowy FIPS 140-2 Level 3 i wyżej/EAL 4+
Urząd poświadczania odbioru i przedłożenia CERTUM QDA	Sprzętowy FIPS 140-2 Level 3 i wyżej
Urząd depozytów obiektów CERTUM QODA	Sprzętowy FIPS 140-2 Level 3 i wyżej
Urząd rejestrów i repozytoriów CERTUM QRRA	Sprzętowy FIPS 140-2 Level 3 i wyżej
Urząd certyfikatów atrybutów	Sprzętowy FIPS 140-2 Level 3 i wyżej
Osoba fizyczna lub urządzenie osoby fizycznej (subskrybenci)	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej
Punkt rejestracji	Sprzętowy FIPS 140 Level 2 i wyżej lub ITSEC E3 i wyżej

Klucze prywatne (a także publiczne) mogą znajdować się w jednym z trzech podstawowych stanów (zgodnie z normą ISO/IEC 11770-1):

- **w oczekiwaniu na aktywność (gotowy)** – klucz został już wygenerowany, ale nie jest jeszcze dostępny do użytku (aktualna data jest mniejsza od daty początku okresu ważności klucza),
- **aktywny** – klucz może być używany w operacjach kryptograficznych (np. do realizacji podpisów elektronicznych), zaś aktualna data zawiera się w okresie ważności klucza i klucz nie jest unieważniony,
- **uśpiony** – w tym stanie klucz może być stosowany tylko i wyłącznie w operacjach weryfikacji podpisu elektronicznego lub deszyfrowania (subskrybent nie może używać klucza prywatnego do realizacji podpisu elektronicznego - klucz jest przeterminowany lub też klucza publicznego do szyfrowania - klucz publiczny jest przeterminowany); aktualna data jest większa od daty końca okresu ważności klucza i klucz nie jest unieważniony.

6.2.2. Podział klucza prywatnego na części

Ochronie za pomocą podziału klucza na części podlegają klucze wszystkich urzędów świadczących usługi certyfikacyjne. W przypadku urzędu certyfikacji **CERTUM QCA** podziałowi podlegają: klucze do składania poświadczeń elektronicznych w certyfikatach, zaświadczeniach certyfikacyjnych i listach CRL.

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

W obu przypadkach klucze (odpowiednio asymetryczny lub symetryczny) dzielone są zgodnie z przyjętą metodą progową na **części** (tzw. cienie) i przekazywane autoryzowanym **posiadaczom sekretu współdzielonego**. Przyjęta liczba podziałów klucza na sekrety współdzielone oraz wartość progowa umożliwiająca odtworzenie tego klucza podane są w Tab. 17.

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

Tab. 17 Podział i dystrybucja sekretów współdzielonych

Nazwa podmiotu świadczącego usługi certyfikacyjne	Liczba sekretów współdzielonych wymagana do odtworzenia klucza prywatnego	Całkowita liczba dystrybuowanych sekretów
CERTUM QCA	3	5
CERTUM QTSA	3	5
CERTUM QOCSP	3	5
CERTUM QDVCS	3	5
CERTUM QDA	3	5
CERTUM QODA	3	5
CERTUM QRRA	3	5
CERTUM QACA	3	5

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

6.2.2.1. Akceptacja sekretu współdzielonego przez posiadacza sekretu

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

6.2.2.2. Zabezpieczenie sekretu współdzielonego

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

- nie ujawni, nie skopiuje, nie udostępni stronom trzecim, ani też nie użyje sekretu w sposób nieautoryzowany,

- nie wyjawi (bezpośrednio lub pośrednio), że jest posiadaczem sekretu współdzielonego,
- nie będzie przechowywał sekretu współdzielonego w miejscu, które uniemożliwi odzyskanie sekretu w przypadku, gdy posiadacz sekretu będzie poza miejscem normalnego pobytu lub będzie nieosiągalny.

6.2.2.3. Dostępność oraz usunięcie (przeniesienie) sekretu współdzielonego

Posiadacz sekretu współdzielonego powinien udostępniać współdzielony sekret autoryzowanym osobom prawnym (wyszczególnionym w formularzu, podpisanym przez posiadacza w momencie powierzania sekretu) tylko po uprzedniej autoryzacji czynności przekazania sekretu. Fakt ten powinien zostać odnotowany w systemie zabezpieczeń w postaci odpowiedniego wpisu do rejestru zdarzeń.

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

6.2.2.4. Odpowiedzialność posiadacza sekretu współdzielonego

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

6.2.3. Deponowanie klucza prywatnego

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

6.2.4. Kopie zapasowe klucza prywatnego

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

W zależności od zastosowanej metody podziału klucza na części (odpowiednio bezpośredniej lub pośredniej, patrz rozdz.6.2.2) kopie klucza prywatnego przechowywane są w częściach lub w całości (po zaszyfrowaniu kluczem symetrycznym). Skopiowane klucze przechowywane są wewnątrz sprzętowych modułów kryptograficznych. Moduł kryptograficzny stosowany do przechowywania kluczy prywatnych spełnia wymagania przedstawione w

rozdz.6.2.1. Kopia klucza prywatnego wprowadzana jest z kolei do modułu kryptograficznego zgodnie z procedurą opisaną w rozdz.6.2.6.

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

Urzędy CERTUM nie przechowują kopii kluczy prywatnych subskrybentów.

6.2.5. Archiwizowanie klucza prywatnego

Klucze prywatne urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu 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** stosowane do realizacji poświadczeń elektronicznych nie są archiwizowane i są niszczone natychmiast po zaprzestaniu wykonywania przy ich użyciu operacji poświadczania lub upływie okresu ważności komplementarnego z nimi zaświadczenia certyfikacyjnego lub jego unieważnieniu.

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

6.2.6. Wprowadzanie klucza prywatnego do modułu kryptograficznego

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

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

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

W CERTUM stosuje się dwie metody zapewnienia integralności ładowanemu kluczowi:

- po pierwsze, jeśli klucz występuje w całości, to nie jest on nigdy dostępny poza modułem w postaci jawnej; oznacza to, że w momencie wygenerowania klucza i konieczności załadowania go do innego modułu, klucz ten jest szyfrowany przy pomocy klucza tajnego; klucz tajny jest przechowywany w taki sam sposób aby nieupoważniona osoba nigdy nie otrzymała obu tych informacji jednocześnie,
- po drugie, jeśli klucz lub chroniące go hasło przechowywane są w częściach, to dzięki ładowaniu kolejnych fragmentów sam moduł jest w stanie zweryfikować potencjalne próby ataków lub oszustw.

Wprowadzenie klucza prywatnego do obszaru sprzętowego modułu kryptograficznego urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu walidacji **CERTUM QDVCS**, urzędu poświadczania odbioru i przedłożenia **CERTUM QDA**, urzędu depozytów obiektów **CERTUM QODA**, urzędu rejestrów i repozytoriów **CERTUM QRRA** lub urzędu certyfikatów atrybutów **CERTUM QACA** wymaga odtworzenia klucza z kart w obecności wymaganej w tym celu liczby posiadaczy sekretów współdzielonych lub kart administratorskich chroniących moduł z kluczami (patrz rozdz.6.2.2). Ponieważ każdy urząd certyfikacji może posiadać także zaszyfrowane kopie kluczy prywatnych (rozdz.6.2.4), stąd klucze te można w takiej postaci przenosić także pomiędzy modułami kryptograficznymi.

6.2.7. Metody aktywacji klucza prywatnego

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

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

Wszystkie klucze prywatne urzędu certyfikacji **CERTUM QCA**, urzędu znacznika czasu **CERTUM QTSA**, urzędu weryfikacji statusu certyfikatu **CERTUM QOCSP**, urzędu 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** 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

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

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

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.

6.2.9. Metody niszczenia klucza prywatnego

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

Niszczenie klucza prywatnego 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 lub ich bezpieczne wymazanie z nośnika (z karty elektronicznej, sprzętowego modułu kryptograficznego, itp.), na których są przechowywane kopie lub archiwizowane sekrety współdzielone.

6.3. Inne aspekty zarządzania kluczami

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

Z punktu widzenia technologii możliwe jest używanie tej samej pary kluczy zarówno do realizacji podpisu elektronicznego, jak też do szyfrowania informacji. Niniejszy Kodeks Postępowania Certyfikacyjnego nie zaleca jednak takiego postępowania, poza przypadkami opisanymi w rozdz.6.1.9. W przypadku kwalifikowanych certyfikatów postępowanie takie jest zabronione.

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 (patrz rozdz.2.6). Jest to szczególnie ważne w przypadku świadczenia usług niezaprzeczalności, takich jak np. usługa znacznika czasu.

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

Urząd certyfikacji przechowuje klucze publiczne tych subskrybentów, którym wydał je w postaci certyfikatów. Własne klucze publiczne urzędu certyfikacji, urzędu znacznika czasu, archiwizowane są w sposób przedstawiony w rozdz.6.2.5.

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

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

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

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

Klucze publiczne przechowywane są w archiwum kluczy publicznych przez okres 25 lat (patrz także rozdz.4.16.3).

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

6.3.2. Okresy stosowania klucza publicznego i prywatnego

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

Standardowe maksymalne okresy ważności kluczy prywatnych oraz związanych z nimi zaświadczeń certyfikacyjnych urzędu certyfikacji, urzędu znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych oraz urzędu poświadczania odbioru i przedłożenia podane są w Tab. 18, zaś maksymalne okresy ważności certyfikatów subskrybentów w Tab. 19.

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

W przypadku recertyfikacji okres ważności klucza prywatnego może byc dłuższy niż okres ważności certyfikatu z nim związanego.

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. 18 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 certyfikacyjne	5 lat	–	
	klucz prywatny	3 lata	–	
CERTUM QTSA	zaświadczenie	–	5 lat	
	klucz prywatny	–	5 lat	
CERTUM QOCSP	zaświadczenie	–	5 lat	
	klucz prywatny	–	5 lat	
CERTUM QDVCS	zaświadczenie	–	5 lat	

	klucz prywatny	–	5 lat	
CERTUM QDA	zaświadczenie	–	5 lat	
	klucz prywatny	–	5 lat	
CERTUM QODA	zaświadczenie	–	5 lat	
	klucz prywatny	–	5 lat	
CERTUM QRRA	zaświadczenie	–	5 lat	
	klucz prywatny	–	5 lat	
CERTUM QACA	zaświadczenie	5 lat	–	
	klucz prywatny	3 lata	–	

*Każdy z użytkowników, w tym przede wszystkim urząd certyfikacji **CERTUM QCA**, urząd znacznika czasu **CERTUM QTSA**, urząd weryfikacji statusu certyfikatu **CERTUM QOCSP**, urząd 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 **CERTUM QACA** może w dowolnym momencie zaprzestać stosowania klucza prywatnego do realizacji poświadczeń lub podpisów elektronicznych, mimo że zaświadczenie certyfikacyjne lub certyfikat są nadal aktualnie ważne. Urząd certyfikacji, urząd znacznika czasu, urząd weryfikacji statusu certyfikatu, urząd walidacji danych oraz elektroniczny urząd podawczy są jednak zobowiązane do poinformowania o tym fakcie (związanym ze zmianą kluczy) swoich subskrybentów.*

Tab. 19 Maksymalne okresy ważności kwalifikowanych certyfikatów klucza publicznego

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. 20 Maksymalne okresy ważności certyfikatów atrybutów

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

6.4. Dane aktywujące

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

6.4.1. Generowanie danych aktywujących i ich instalowanie

Dane aktywujące używane są w dwóch podstawowych przypadkach:

- jako element jedno- lub dwuczynnikowej procedury uwierzytelniania (tzw. frazy uwierzytelniania, np. hasła, numery PIN, itp.),

- jako część sekretu współdzielonego, który po zainstalowaniu w systemie umożliwia odtworzenie klucza lub kluczy kryptograficznych.

Operatorzy punktów rejestracji, urzędów certyfikacji oraz inne osoby pełniące role określone w rozdz.5.2.1 posługują się hasłami odpornymi na ataki brutalne (zwane także wyczerpującymi).

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

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

Sekrety współdzielone używane do ochrony kluczy prywatnych wszystkich urzędów świadczących usługi certyfikacyjne są generowane zgodnie z wymaganiami określonymi w rozdz.6.2 i zapisywane w tokenach kryptograficznych. Tokeny chronione są numerem PIN, którego procedura tworzenia jest zgodna z FIPS 112. Sekrety współdzielone stają się danymi aktywacyjnymi dopiero po ich uaktywnieniu, tj. prawidłowym podaniu numeru PIN chroniącego token.

6.4.2. Ochrona danych aktywujących

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

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

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

6.4.3. Inne problemy związane z danymi aktywującymi

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

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

Dane aktywujące nie są archiwizowane.

6.5. Zabezpieczenia systemu komputerowego

Zadania punktów rejestracji, urzędu certyfikacji, urzędu znacznika czasu, urzędu weryfikacji statusu certyfikatu, urzędu walidacji danych oraz urzędu poświadczania odbioru i przedłożenia,

funkcjonujących w ramach systemu CERTUM, realizowane są przy pomocy wiarygodnego sprzętu i oprogramowania, tworzących system, który spełnia wymagania określone w dokumencie *Information Technology Security Evaluation Criteria*[45] (ITSEC), przynajmniej na poziomie E3.

6.5.1. Wymagania techniczne dotyczące specyficznych zabezpieczeń systemów komputerowych

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

Komputery funkcjonujące CERTUM wyposażone są w następujące funkcje zabezpieczające:

- obligatoryjnie uwierzytelnione rejestrowanie się na poziomie systemu operacyjnego i aplikacji (w przypadkach gdy jest to istotne, np. z punktu widzenia pełnionej roli),
- uznaniową kontrolę dostępu,
- możliwość prowadzenia audytu zabezpieczeń,
- pracownik, który pełni zaufaną role jest zobowiązany do blokowania swojej stacji roboczej zawsze, jeśli pozostają one poza jego nadzorem,
- wymuszanie separacji obowiązków, wynikające z pełnionych zaufanych ról,
- wymuszanie wylogowania użytkownika po okresie bezczynności,
- identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- kryptograficzną ochronę sesji wymiany informacji oraz zabezpieczenia baz danych,
- archiwizowanie historii czynności wykonywanych na komputerze oraz danych dla potrzeb audytu,
- bezpieczną ścieżkę, pozwalającą na wiarygodną identyfikację i uwierzytelnienie ról oraz pełniących je osób,
- mechanizm odtwarzania kluczy (tylko w przypadku modułów kryptograficznych) oraz systemu operacyjnego i aplikacji,
- mechanizm monitorowania i alarmowania w przypadku wystąpienia zdarzeń nieautoryzowanego dostępu do zasobów komputera.

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

6.5.2. Ocena bezpieczeństwa systemów komputerowych

Systemy komputerowe CERTUM spełniają wymagania określone w *Information Technology Security Evaluation Cryteria* (ITSEC). Zostało to potwierdzone przez niezależnego audytora, oceniającego funkcjonowanie systemu CERTUM na podstawie kryteriów określonych w *Rozporządzeniu eIDAS* i *Ustawie*. Elementy systemu tworzą godną zaufania całość, która spełnia

[45] Kryteria Oceny Zabezpieczeń Systemów Informatycznych

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."

6.6. Kontrola techniczna

6.6.1. Kontrola zmian systemu

Aplikacje stosowane w systemie CERTUM są projektowane i implementowane przez Asseco Data Systems S.A.. Proces projektowania i implementowania oprogramowania, a także dokonywania zmian w oprogramowaniu jest zgodny z metodologią *Rational Unified Process (RUP)*.

W szczególności, w przypadku wymiany sprzętu:

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

6.6.2. Kontrola zarządzania bezpieczeństwem

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

Mimo, że prace administracyjne oraz zmiany w systemach CERTUM są rejestrowane, to każda z nich wymaga dodatkowo zweryfikowania i akceptacji przez przynajmniej dwóch administratorów CERTUM. System kontroli zmiany informuje uprawnionych pracowników o wystąpieniu modyfikacji w systemie CERTUM i wymaga jej weryfikacji przez osobę inną od tej, która wprowadzała daną zmianę.

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

6.6.3. Ocena cyklu życia zabezpieczeń

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

6.7. Zabezpieczenia sieci komputerowej

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

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

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

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

Wszelkie zmiany wprowadzane w urządzeniach sieciowych CERTUM wymagają wcześniejszej akceptacji Inspektora Bezpieczeństwa. Przeprowadzona zmiana zostaje zaimplementowana dopiero po zweryfikowaniu jej przez administratora, który nie brał bezpośredniego udziału w przygotowywaniu zmiany.

Szczegółowy opis konfiguracji sieci CERTUM oraz jej zabezpieczeń zawarty jest w dokumentacji infrastruktury technicznej systemu CERTUM. Dokument ma status „niejawny" i udostępniany jest tylko inspektorowi bezpieczeństwa, administratorowi systemu i audytorom.

6.8. Kontrola wytwarzania modułu kryptograficznego

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

Sprzętowe moduły kryptograficzne, dostarczane do CERTUM, są każdorazowo sprawdzane czy nie nastąpiło naruszenie przesyłki oraz czy moduł zachowuje integralność fizyczną oraz logiczną. Weryfikację, z której sporządzany jest raport, przeprowadza wyłącznie zaufany personel CERTUM. Sprzętowe moduły kryptograficzne, nie będące w użyciu, zabezpieczone są opakowaniem uniemożliwiającym otwarcie koperty bez pozostawienia śladów. Tak przygotowane moduły przechowywane są w sejfach zlokalizowanych w specjalnie strzeżonych pomieszczeniach, do których dostęp posiada wyłącznie wskazana grupa osób piastująca tzw. zaufane role w CERTUM.

6.9. Znaczniki czasu jako element bezpieczeństwa

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

Znaczniki czasu tworzone w ramach systemu CERTUM 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, list 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 Unizeto Technologies 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.

Przedstawione niżej informacje określają znaczenie poszczególnych pól certyfikatu lub zaświadczenia, list CRL, tokena znacznika czasu, stosowane rozszerzenia standardowe oraz prywatne, wprowadzone na użytek CERTUM.

7.1. Struktura certyfikatów i zaświadczeń

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 i zaświadczenia certyfikacyjnego

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

Rozszerzenia zdefiniowane w certyfikatach lub zaświadczeniach certyfikacyjnych zgodnych z rekomendacją X.509 v.3 umożliwiają przypisanie dodatkowych atrybutów subskrybentowi lub kluczowi publicznemu oraz ułatwiają zarządzanie hierarchiczną strukturą certyfikatów lub zaświadczeń certyfikacyjnych. Certyfikaty lub zaświadczenia certyfikacyjne zgodne z

rekomendacją X.509 v.3 pozwalają także na definiowanie własnych rozszerzeń, specyficznych dla zastosowań danego systemu.

7.1.1.1. Pola podstawowe

CERTUM obsługuje następujące pola podstawowe certyfikatu lub zaświadczenia certyfikacyjnego:

- **Version**: wersję trzecią (X.509 v.3) formatu certyfikatu lub zaświadczenia certyfikacyjnego;
- **SerialNumber**: numer seryjny certyfikatu lub zaświadczenia certyfikacyjnego, unikalny w ramach domeny urzędu certyfikacji;
- **Signature Algorithm**: identyfikator algorytmu stosowanego przez urząd certyfikacji do elektronicznego poświadczania certyfikatu lub zaświadczenia certyfikacyjnego;
- **Issuer**: nazwa wyróżniająca (DN) urzędu certyfikacji;
- **Validity**: data ważności certyfikatu określona przez początek (**notBefore**) oraz koniec (**notAfter**) ważności certyfikatu lub zaświadczenia certyfikacyjnego;
- **Subject**: nazwę wyróżniająca (DN) subskrybenta, otrzymującego certyfikat lub zaświadczenie certyfikacyjne;
- **SubjectPublicKeyInfo**: wartość klucza publicznego wraz z identyfikatorem algorytmu, z którym stowarzyszony jest klucz.

W certyfikatach lub zaświadczeniach certyfikacyjnych wydawanych przez CERTUM wartości tym polom nadawane są zgodnie z zasadami przedstawionymi w Tab. 21.

Tab. 21 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	Nazwa DN jest zgodna z wymaganiami określonymi w *ETSI EN*	

Nazwa pola	Wartość lub ograniczenie wartości	
DN)	*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)	Public Key Algorithm (algorytm klucza publicznego)	sha1WithRSAEncryption
	RSA Public Key (długość klucza)	2048 bits
	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 standardowych

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

CERTUM obsługuje następujące pola rozszerzeń podstawowych certyfikatu lub zaświadczenia certyfikacyjnego:

- **AuthorityKeyIdentifier**: identyfikator zaświadczenia certyfikacyjnego klucza publicznego urzędu certyfikacji komplementarnego z tym kluczem prywatnym, przy pomocy którego urząd certyfikacji poświadczał elektronicznie wydany certyfikat – **rozszerzenie nie jest krytyczne**;
- **KeyUsage:** dozwolone użycie klucza – **rozszerzenie jest krytyczne.** Rozszerzenie to określa sposób wykorzystania klucza, np. klucz do szyfrowania danych, klucz do podpisu elektronicznego, itp. (patrz niżej)

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

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

```
serverAuth      - uwierzytelnianie TLS Web serwera; bity pola keyUsage,
```

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

- **CertificatePolicies**: informacja typu **PolicyInformation** (identyfikator, adres elektroniczny) o polityce certyfikacji, realizowanej przez urząd certyfikacji – **rozszerzenie jest krytyczne**

Tab. 22 Identyfikatory polityk i ich opisy

Identyfikator polityki	Opis polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 1	Identyfikuje politykę certyfikacji, według której wydawane są certyfikaty kwalifikowane.
joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32)	Identyfikuje politykę certyfikacji, według której wydawane są zaświadczenia certyfikacyjne.

W certyfikatach lub zaświadczeniach certyfikacyjnych wydawanych przez urząd certyfikacji umieszczane są oba kwalifikatory polityki rekomendowane w RFC 5280.

- **PolicyMapping**: odwzorowanie polityki – **rozszerzenie nie jest krytyczne**; pole to zawiera jedną lub więcej par OID, które określają równoważność polityki wydawcy z polityką podmiotu;
- **IssuerAlternativeName**: alternatywna nazwa urzędu certyfikacji – **rozszerzenie nie jest krytyczne**;
- **SubjectAlternativeName**: alternatywna nazwa podmiotu – **rozszerzenie nie jest krytyczne**;
- **BasicContraints**: więzy podstawowe – **rozszerzenie jest krytyczne**. Rozszerzenie umożliwia określenie czy podmiot zaświadczenia certyfikacyjnego jest urzędem certyfikacji (pole **cA**) oraz ile maksymalnie (przy założeniu hierarchicznego uporządkowania urzędów certyfikacji) może być urzędów certyfikacji na ścieżce prowadzącej od rozpatrywanego urzędu certyfikacji do subskrybenta (pole **pathLength**);
- **CRLDistributionPoints**: punkty dystrybucji listy certyfikatów unieważnionych (CRL) – **rozszerzenie nie jest krytyczne**. Rozszerzenie określa adresy sieciowe, pod którymi można uzyskać aktualną listę CRL, wydaną przez **cRLIssuer**;

- **SubjectDirectoryAttributes**: atrybuty katalogu podmiotu - **rozszerzenie nie jest krytyczne**; pole zawiera dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**; w rozszerzeniu tym występują atrybuty, które nie należą do elementów wchodzących w skład nazwy DN podmiotu;
- **AuthorityInfoAccessSyntax**: dostęp do informacji urzędu certyfikacji - **rozszerzenie nie jest krytyczne**; pole wskazuje, w jaki sposób udostępniane są informacje i usługi przez wystawcę certyfikatu, w którego zaświadczeniu certyfikacyjnym to rozszerzenie występuje;
- **QCStatements**: deklaracje wystawcy certyfikatu kwalifikowanego – **rozszerzenie nie jest krytyczne**;
- **BiometricSyntax**: informacje o cechach biometrycznych podmiotu certyfikatu - **rozszerzenie nie jest krytyczne**; dostępne są dwa typy informacji biometrycznej: podpis odręczny oraz zdjęcie; w certyfikacie umieszczany jest jedynie skrót z cechy biometrycznej; wartość skrótu umieszczana jest w polu **biometricDataHash**, zaś identyfikator funkcji skrótu, przy pomocy której policzono tę wartość w polu **hashAlgorithm**; pełna informacja biometryczna o podmiocie (jego wzorzec biometryczny) przechowywana jest w bazie danych, której adres URI podany jest w polu **sourceDataUri**. Efektywne wykorzystanie informacji biometrycznej umieszczonej w certyfikacie (skrót) możliwe jest jedynie w przypadku, gdy nastąpi porównanie wzorca zawartego w bazie (informacja pełna) ze skrótem odczytanym z certyfikatu.

7.1.2. Rozszerzenia a typy wydawanych certyfikatów lub zaświadczeń certyfikacyjnych

Certyfikaty lub zaświadczenia certyfikacyjne wydawane przez urząd **CERTUM QCA** mogą zawierać różne kombinacje rozszerzeń wymienionych w rozdz.7.1.1.2. Ich dobór jest uzależniony głównie od zastosowania certyfikatu lub zaświadczenia certyfikacyjnego oraz tego, komu są wydawane.

7.1.2.1. Kwalifikowane certyfikaty

Kwalifikowane certyfikaty wydawane osobom fizycznym, spełniające wymagania *Rozporządzenia eIDAS* i *Ustawy* zawierają rozszerzenia wyspecyfikowane w Tab. 23.

Tab. 23 Rozszerzenia w kwalifikowanych certyfikatach osób fizycznych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier (identyfikator klucza wydawcy)	Skrót SHA-1 z wartości klucza publicznego.	Niekrytyczne
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage (użycie klucza)	Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
IssuerAlternativeName (alternatywna nazwa urzędu certyfikacji)	(opcjonalne) Alternatywna nazwa urzędu certyfikacji	Niekrytyczne
Subject Alternative Name (alternatywna nazwa podmiotu)	(opcjonalne) Email: customer@somewhere-in-world.com	Niekrytyczne
CRL Distribution Points (punkty dystrybucji listy CRL)	URI: http://crl.certum.pl/qca.crl	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	(opcjonalne) OCSP: http://qocsp.certum.pl	Niekrytyczne
Biometric Info (informacje biometryczne)	(opcjonalne) Zdjęcie podmiotu, DNA, wzór siatkówki oka, odcisk palca, bit 0 Wzór podpisu odręcznego podmiotu, bit 1 URI: lokalizacja danych biometrycznych	Niekrytyczne
QCStatements (deklaracje wydawcy certyfikatu kwalifikowanego)	(opcjonalne) Oświadczenie, że certyfikat jest kwalifikowanym certyfikatem[46]. Limit transakcji, którą jednorazowo można potwierdzić za pomocą certyfikatu. Wskazanie, w czyim imieniu działa podmiot składając podpis.	Niekrytyczne

[46] Jest to oświadczenie Asseco Data Systems S.A., że wydawane certyfikaty kwalifikowane są zgodne z wymaganiami Ustawy o usługach zaufania oraz Asseco Data Systems S.A. deklaruje dodatkowo w ten sposób zgodność wydawanych certyfikatów kwalifikowanych ze specyfikacją ETSI 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	Wartość lub ograniczenie wartości	Status rozszerzenia
Certificate Policies (polityka certyfikacji)	Polityki: 1.2.616.1.113527.2.4.1.1 (certyfikaty kwalifikowane przed 1 lipca 2016r), 1.2.616.1.113527.2.4.1.11 (certyfikaty kwalifikowane po 1 lipca 2016r), 1.2.616.1.113527.2.4.1.12.1 (certyfikat kwalifikowany (struktura eIDAS) karta), 1.2.616.1.113527.2.4.1.12.2 (certyfikat kwalifikowany (struktura eIDAS) HSM). KPC: http://www.certum.pl/repozytorium Numer wiadomości (notice number): zależy od typu certyfikatu. Organizacja: Asseco Data Systems S.A. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Krytyczne
Subject Directory Attributes (atrybuty katalogu podmiotu)	(opcjonalne) Dodatkowe atrybuty powiązane z podmiotem i dopełniające informacje zawarte w polu **subject** oraz **subjectAlternativeName**.	Niekrytyczne

7.1.2.2. Zaświadczenia certyfikacyjne

Zaświadczenia certyfikacyjne CERTUM mogą zawierać rozszerzenia określone w Tab. 24.

Tab. 24 Minimalne rozszerzenia w zaświadczeniach certyfikacyjnych urzędów certyfikacji

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji=brak - w przypadku urzędu **CERTUM QCA**.	Krytyczne
Key Usage (użycie klucza)	Klucz do podpisywania certyfikatów (keyCertSign), bit 5 Klucz do podpisywania list CRL (cRLSign), bit 6	Krytyczne

7.1.2.3. Wzajemne zaświadczenia certyfikacyjne

Wzajemne zaświadczenia certyfikacyjne mogą zawierać rozszerzenia wyspecyfikowane w Tab. 25.

Tab. 25 Rozszerzenia we wzajemnych zaświadczeniach certyfikacyjnych

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
Authority Key Identifier (identyfikator klucza wydawcy)	Skrót SHA-1 z wartości klucza publicznego.	Niekrytyczne
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=CA Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage (użycie klucza)	Poświadczanie zaświadczeń certyfikacyjnych (keyCertSign), bit 5	Krytyczne

Nazwa rozszerzenia	Wartość lub ograniczenie wartości	Status rozszerzenia
	Poświadczanie list CRL (cRLSign), bit 6	
Subject Alternative Name (alternatywna nazwa podmiotu)	(opcjonalne) URI: http://www. customer-service .pl Lokalizacja serwisu klienta.	Niekrytyczne
Authority Info Access (dostęp do informacji o urzędzie)	(opcjonalne) OCSP: http://qocsp.certum.pl	Niekrytyczne
Certificate Policies (polityka certyfikacji)	Polityki: 2.5.29.32.0 KPC: http://www.certum.pl/repozytorium Numer wiadomości (notice number): zależy od typu zaświadczenia. Organizacja: Asseco Data Systems S.A. Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	Krytyczne

7.1.3. Typy stosowanego algorytmu tworzenia 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.

7.1.4. 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. Profil 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 obowiązkowych i opcjonalnych. Pola obowiązkowe identyfikują wydawcę listy CRL, zaś opcjonalne zawierają unieważnione certyfikaty lub zaświadczenia certyfikacyjne oraz rozszerzenia listy CRL.

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

- **Version**: wersja formatu listy CRL;

- **Signature**: Pole to zawiera identyfikator algorytmu stosowanego przez urząd certyfikacji do poświadczenia elektronicznego listy **CRL**; urząd CERTUM poświadcza listę CRL przy użyciu algorytmu **sha1WithRSAEncryption**;
- **Issuer**: nazwa urzędu certyfikacji wydającego listę CRL (**CERTUM QCA**);
- **ThisUpdate**: data publikacji listy CRL;
- **NextUpdate**: zapowiedź daty następnej publikacji listy CRL; jeśli pole wystąpi, wartość tego pola określa nieprzekraczalną datę opublikowania kolejnej listy (publikacja może nastąpić wcześniej);
- **RevokedCertificates**: lista unieważnionych certyfikatów lub zaświadczeń certyfikacyjnych (pole puste w przypadku braku unieważnionych certyfikatów lub zaświadczeń certyfikacyjnych); informacja ta składa się z trzech podpól:

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

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

7.2.1. Obsługiwane rozszerzenia dostępu do listy CRL

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

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

```
unspecified          – nieokreślona (nieznana);
keyCompromise        – ujawnienie klucza;
cACompromise         – ujawnienie klucza urzędu certyfikacji;
affiliationChanged   – zamiana danych (afiliacji) subskrybenta;
superseded           – zastąpienie klucza publicznego certyfikatu lub
                       zaświadczenia certyfikacyjnego;
cessationOfOperation – zaprzestanie operacji z wykorzystaniem klucza;
certificateHold      – zawieszenie certyfikatu lub zaświadczenia
                       certyfikacyjnego;
removeFromCRL        – certyfikat (lub zaświadczenie certyfikacyjne)
                       wycofane z listy CRL;
privilegeWithdrawn   - certyfikat został unieważniony z powodu anulowania
                       uprawnień związanych z atrybutami i zawartych
                       w certyfikacie klucza publicznego lub
                       w certyfikacie atrybutów
aaCompromise         - dotyczy urzędu atrybutów i oznacza, że certyfikat
                       został unieważniony z powodu wycofania urzędowi
                       atrybutów prawa do potwierdzania atrybutu lub
                       atrybutów zawartych w certyfikacie atrybutów
```

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

7.2.2. Unieważnienie kwalifikowanego certyfikatu lub zaświadczenia certyfikacyjnego a listy CRL

Unieważnione certyfikaty i zaświadczenia certyfikacyjne umieszcza się na każdej liście zawieszonych i unieważnionych certyfikatów publikowanej przed dniem upływu okresu ważności certyfikatu oraz na pierwszej liście publikowanej po upływie tego okresu. Zasada ta dotyczy także unieważnionych zaświadczeń certyfikacyjnych urzędów certyfikacji: zaświadczenia certyfikacyjne muszą być umieszczane na kolejnych listach CRL publikowanych przez wydawcę unieważnionego zaświadczenia certyfikacyjnego (w przypadku zakończenia działalności przez wydawcę ostatnia opublikowana lista powinna być przekazana do repozytorium urzędu certyfikacji innego, np. nadrzędnego urzędu certyfikacji (patrz także rozdz.4.19).

7.2.3. Unieważnienie certyfikatu atrybutów a listy CRL

Profil listy unieważnionych certyfikatów atrybutów jest identyczny z opisem przedstawionym w rozdz.7.2. Ze względu na efektywność obsługi list unieważnionych certyfikatów atrybutów, unieważnione certyfikaty atrybutów umieszczane są na innych listach niż unieważnione certyfikaty klucza publicznego.

Unieważnione certyfikaty atrybutów pozostają na liście unieważnionych certyfikatów atrybutów przez okres ważności certyfikatu, zadeklarowany w jego treści. Po tym okresie unieważniony certyfikat atrybutów jest umieszczany jeszcze na kolejnej liście zaraz po upływie okresu jego ważności i następnie usuwany z listy.

7.3. Profil tokena znacznika czasu

Urząd znacznika czasu **CERTUM QTSA** poświadcza elektronicznie wystawiane przez siebie tokeny znaczników czasu przy pomocy jednego lub większej liczby kluczy prywatnych zarezerwowanych specjalnie do tego celu. Zgodnie z zaleceniem RFC 5280 komplementarne z nimi zaświadczenia certyfikacyjne kluczy publicznych zawierają pole precyzujące zawężenie dopuszczalnego zastosowania klucza (**ExtKeyUsageSyntax**) zaznaczone jako **krytyczne**.

Oznacza to, że zaświadczenie certyfikacyjne może być używane przez urząd znacznika czasu tylko do realizacji poświadczeń elektronicznych w wystawianych przez siebie znacznikach czasu.

Profil zaświadczenia certyfikacyjnego urzędu znacznika czasu **CERTUM QTSA** jest przedstawiony w Tab. 26.

Tab. 26 Profil zaświadczenia certyfikacyjnego urzędu TSA

Nazwa pola	Wartość lub ograniczenie wartości	
Version (wersja)	Version 3	
Serial Numer (numer seryjny)	Unikalne wartości we wszystkich zaświadczeniach certyfikacyjnych wydawanych przez **Narodowe Centrum Certyfikacji**	
Signature Algorithm (algorytm podpisu)	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (wystawca, nazwa DN)	Nazwa wyróżniająca DN krajowego urzędu certyfikacji, wystawcy zaświadczenia certyfikacyjnego dla CERTUM QTSA	
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)	Common Name (CN) =	CERTUM QTSA
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Serial Number (SN) =	Nr wpisu: 15
Subject Public Key Info (klucz publiczny podmiotu)	Pole kodowane jest zgodnie z wymaganiami określonymi w RFC 5280 zawiera informacje o kluczu publicznym RSA (identyfikatorze klucza, wartości klucza publicznego)	
Signature (podpis)	Podpis certyfikatu generowany i kodowany zgodnie z wymaganiami określonymi w RFC 5280	
Authority Key Identifier (identyfikator klucza wydawcy)	Skrót SHA-1 z wartości klucza publicznego.	Niekrytyczne
Basic Constraints (podstawowe ograniczenia)	Typ podmiotu=brak (użytkownik końcowy) Ograniczenie długości ścieżki certyfikacji=brak	Krytyczne
Key Usage (użycie klucza)	Podpisy cyfrowe (digital signature), bit 0 Niezaprzeczalność (non-repudiation), bit 1	Krytyczne
Extended Key Usage (rozszerzone użycie klucza)	Time Stamping Authority (TSA)	Krytyczne
Certificate Policies (polityka certyfikacji)	Polityka: 2.5.29.32.0 KPC:	Krytyczne

Nazwa pola	Wartość lub ograniczenie wartości	
	http://www.certum.pl/repozytorium Tekst jawny (explicit text): zależny od identyfikatora polityki (tekst jawny).	

Urząd znacznika czasu CERTUM QTSA akceptuje żądania wydania tokena znacznika czasu zgodne ze specyfikacją IETF RFC 3161 oraz wymaganiami ETSI EN 319 422 przy zastrzeżeniu, że:

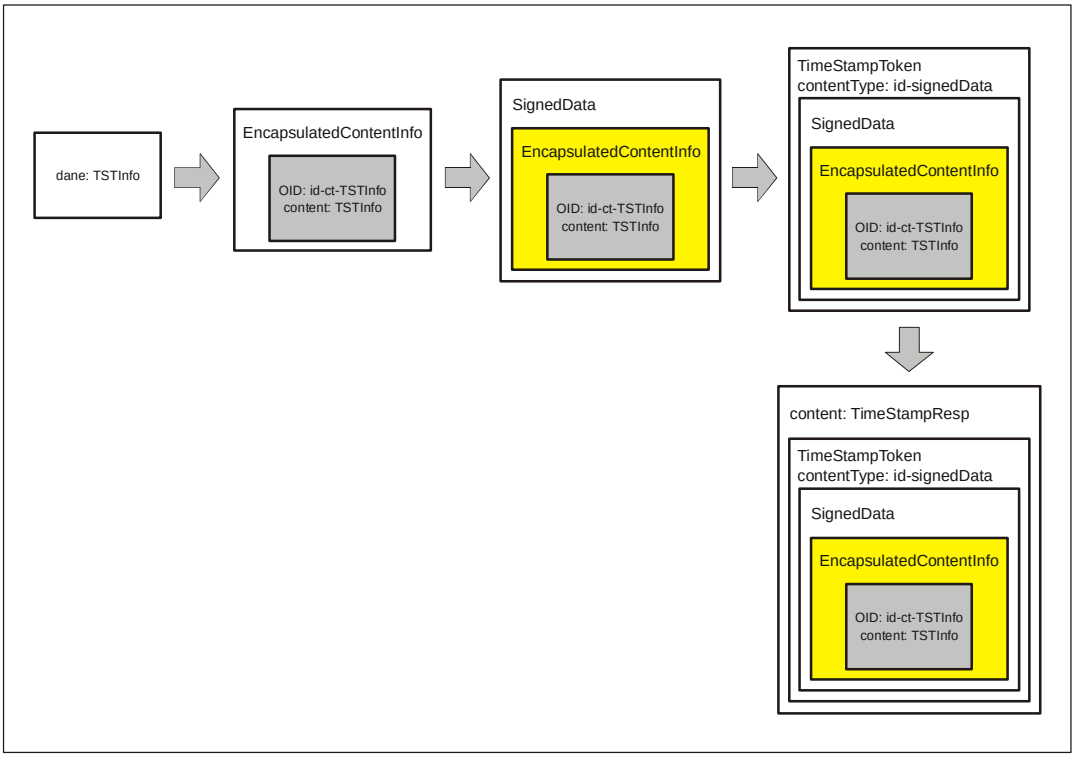
- żądanie wydania tokena znacznika czasu musi wskazywać algorytm funkcji skrótu SHA-1,
- żądanie wydania tokena znacznika czasu nie może wskazywać identyfikatora polityki za wyjątkiem identyfikatora urzędu znacznika czasu CERTUM QTSA (patrz rozdz. 1.3.2).

Token znacznika czasu wystawiony przez urząd znacznika czasu **CERTUM QTSA** zawiera (patrz rys.5) w sobie informację o znaczniku czasu (struktura **TSTInfo**), umieszczoną w strukturze **SignedData** (patrz RFC 2630), podpisanej przez urząd znacznika i zagnieżdżonej w strukturze **ContentInfo** (patrz RFC 2630).

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

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

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



Rys.5 Kapsułkowanie odpowiedzi żądania utworzenia znacznika czasu (patrz także Raport Techniczny [37]

Struktura PKIStatusInfo ma następującą postać:

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

Znaczenie pól:

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

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

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

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

```
    -- określający język, w którym zapisany jest tekst
```

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

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

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

```
TimeStampToken ::= ContentInfo
```

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

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

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

Zawartość informacyjna tokena znacznika czasu ma postać:

```
-- OBJECT IDENTIFIER (id-ct-TSTInfo)
TSTInfo ::= SEQUENCE  {
    version              INTEGER  { v1(1) },
    policy               TSAPolicyId,
    messageImprint       MessageImprint,
    serialNumber         INTEGER,
    genTime              GeneralizedTime,
    accuracy             Accuracy OPTIONAL,
    ordering             BOOLEAN DEFAULT FALSE,
    nonce                INTEGER OPTIONAL,
    tsa              [0] GeneralName OPTIONAL,
    extensions       [1] IMPLICIT Extensions OPTIONAL
}
```

Znaczenie ważniejszych pól **TSRInfo** jest następujące:

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

Identyfikator polityki	Nazwa polityki certyfikacji
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 2}	CERTUM QTSA Identyfikuje politykę certyfikacji, według której wydawane są tokeny znacznika czasu

- **messageImprint** zawiera informację przesłaną przez żądającego, która została oznaczona znacznikiem czasu;
- **serialNumber** określa numer seryjny tokena znacznika czasu wystawionego przez dany urząd znacznika czasu. Numer seryjny musi zawierać ściśle rosnące wartości całkowite;
- pole **genTime** oznacza datę oraz czas wystawienia przez urząd znacznika czasu z dokładnością do 1 sekundy;
- pole **accuracy** określa dokładność z jaką generowany jest czas przez urząd znacznika czasu (urząd **CERTUM QTSA** generuje czas z dokładnością 1 sekundy). W przypadku, gdy pole jest pominięte, domyślnie przyjmuje się dokładność jednej sekundy;
- jeśli pole **ordering** nie występuje lub jego wartość ustawiona została na FALSE, to pole **genTime** pokazuje jedynie czas utworzenia znacznika czasu przez urząd znacznika czasu. W tym przypadku uporządkowanie dwóch tokenów znacznika czasu wydanych przez ten sam lub różne urzędy znacznika czasu jest możliwe jedynie wtedy, gdy różnica pomiędzy **genTime** pierwszego tokena, a **genTime** drugiego tokena jest większa od sum pól określających dokładności każdego z tokenów; jeśli pole **ordering** występuje i jego wartość ustawiona została na TRUE, to każdy token znacznika czasu wydany przez ten sam urząd znacznika czasu może być tylko na podstawie znajomości pola **genTime**, niezależnie od dokładności pomiaru czasu. Urząd znacznika czasu CERTUM QTSA zawsze ustawia wartość tego pola na FALSE;
- **nonce** pole musi wystąpić, jeśli wystąpiło w żądaniu przesłanym przez subskrybenta i musi mieć taką sama wartość;
- pole **tsa** służy do identyfikacji nazwy urzędu znacznika czasu. Jeśli występuje, musi odpowiadać nazwie podmiotu zawartej w zaświadczeniu certyfikacyjnym wydanym urzędowi znacznika czasu przez **Narodowe Centrum Certyfikacji** i wykorzystywanym w procesie weryfikacji tokena.

Ze strukturą TimeStampToken związany jest zbiór atrybutów, które są podpisywane. W tokenie znacznika czasu występują przynajmniej następujące atrybuty:

1. Atrybut typu zawartości

```
Nazwa:      id-contentType
OID:        { iso(1) member-body(2)
                        us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
Składnia:   id-ct-TSTInfo
wartości:   wartość id-ct-TSTInfo jest ponowiona tylko raz
```

2. Atrybut skrótu wiadomości

```
Nazwa:      id-messageDigest
OID:        { iso(1) member-body(2)
                        us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
```

```
Składnia:   MessageDigest
wartości:   wartość typu MessageDigest jest ponowiona tylko raz

--skrót z pola eContent struktury EncapsulatedContentInfo
MessageDigest ::= Digest
Digest ::= OCTET STRING (SIZE(1..20))
```

3. Atrybut certyfikatu podpisującego

```
Nazwa:      id-aa-signingCertificate
OID:        { iso(1)
       member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
       smime(16) id-aa(2) 12 }
Składnia:   SigningCertificate
wartości:   wartość typu SigningCertificate jest ponowiona tylko raz

-- Podpisany atrybut certyfikatu
SigningCertificate ::= SEQUENCE {
    certs     SEQUENCE OF ESSCertID,
    policies  SEQUENCE OF PolicyInformation OPTIONAL
}
ESSCertID ::= SEQUENCE{
    CertHash       Hash,
    IsssuerSerial  IssuerSerial OPTIONAL
}
Hash ::= OCTET STRING –- SHA1 skrót z całego certyfikatu

IssuerSerial ::= SEQUENCE {
    Issuer         GeneralNames,
    SerialNumber   CertificateSerialNumber
}
GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

7.4. Profil tokena 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.

Dla każdego z dostępnych protokołów komunikacji token walidacji ma strukturę zgodna z wybranym protokołem:

- dla protokołu DVCS zgodnie z RFC 3029 (rozdział 9),
- dla protokołu XKMS zgodnie z protokołem XKMS 2.0,
- dla protokołu OASIS zgodnie z protokołem OASISS-DSS,

oraz na żądanie odbiorca usługi może otrzymać *Raport z walidacji* w postaci czytelnej dla człowieka jako dokument w formacie .pdf podpisany elektroniczne.

Szczegółowe opisy protokołów są dokumentami wewnętrznymi.

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, 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**, urząd rejestrów i repozytoriów **CERTUM QRRA** oraz urząd certyfikatów atrybutów **CERTUM QACA** opisane są w wewnętrznych dokumentach CERTUM.

8. Administrowanie Kodeksem Postępowania Certyfikacyjnego

Każda z wersji Kodeksu Postępowania Certyfikacyjnego jest obowiązująca (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 ankiety. Po otrzymaniu i uwzględnieniu uwag z ankiety, nowa wersja Kodeksu Postępowania Certyfikacyjnego przekazywana p, zostaje przekazana do zatwierdzenia przez osobę zarządzającą CERTUM i opublikowana. W czasie trwania procedury zatwierdzania nowa wersja dokumentu posiada status – **w zatwierdzeniu,** a po zakończeniu procedury osiąga status – **aktualny**.

Oprócz "wersji" istnieją także "wydania" Kodeksu Postępowania Certyfikacyjnego, które posiadają takie same statusy jak wersja.. Nowe wydanie Kodeksu Postępowania Certyfikacyjnego opatrzone jest zmiennym numerem umieszczanym po numerze wersji - oddzielonym znakiem kropki - aktualnego Kodeksu Postępowania Certyfikacyjnego.

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

Przedstawione poniżej dalsze zasady administrowania Kodeksem Postępowania Certyfikacyjnego obowiązują podczas wprowadzania zmian w Polityce Certyfikacji.

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

8.1. Procedura wprowadzania zmian

Niezależnie od prowadzonych w CERTUM audytów, raz w roku odbywa się przegląd obowiązujących wersji Kodeksu Postępowania Certyfikacyjnego oraz Polityki Certyfikacji. Wyznaczeni przez kierownictwo CERTUM pracownicy analizują treść dokumentów w kierunku ich zgodności z wdrożonymi procedurami oraz wymaganiami zewnętrznymi.

Zmiany w Kodeksie Postępowania Certyfikacyjnego mogą być wynikiem zauważonych błędów, uaktualnień oraz sugestii zainteresowanych stron. Propozycje zmian mogą być nadsyłane zwykłą pocztą lub elektroniczną na adresy kontaktowe CERTUM. Propozycje zmian powinny opisywać ich zakres, uzasadnienie oraz adres kontaktowy autora wprowadzenia zmian.

Podmioty mające prawo zgłaszać propozycję wprowadzania zmian do istniejącego Kodeksu Postępowania Certyfikacyjnego:

- minister cyfryzacji lub upoważniona przez niego osoba fizyczna lub prawna,
- instytucje audytujące,
- instytucje prawne, zwłaszcza wtedy, gdy zauważono iż Kodeks Postępowania Certyfikacyjnego jest sprzeczny z zasadami prawnymi obowiązującymi w Rzeczypospolitej Polskiej oraz może działać na niekorzyść subskrybenta,

- Zespół jakości, inspektorzy bezpieczeństwa, administrator systemu oraz inni pracownicy CERTUM,
- subskrybenci CERTUM,
- eksperci z zakresu zabezpieczeń systemów informatycznych.

Po wprowadzeniu każdej zmiany uaktualniana jest data opublikowania Polityki Certyfikacji lub Kodeksu Postępowania Certyfikacyjnego oraz modyfikowany jest identyfikator dokumentu, numer jego wersji lub wydania.

Wprowadzane zmiany można podzielić na dwie kategorie:

- zmiany nie wymagające informowania subskrybentów o modyfikacjach,
- zmiany wymagające informowania (zwykle odpowiednio wczesnego) subskrybentów o modyfikacjach.

8.1.1. Zmiany nie wymagające informowania

Jedynymi zmianami, które według Kodeksu Postępowania Certyfikacyjnego nie wymagają wcześniejszego informowania subskrybentów są zmiany wynikające z wprowadzenia korekt edycyjnych, zmian w sposobie kontaktowania się z osobą odpowiedzialną za zarządzanie dokumentem, zmiany nie mające rzeczywistego wpływu na znaczącą grupę użytkowników. Wprowadzone zmiany nie podlegają procedurze zatwierdzania i zmienia się jedynie wydanie Kodeksu Postępowania Certyfikacyjnego.

8.1.2. Zmiany wymagające informowania

8.1.2.1. Lista elementów

Po uprzednim poinformowaniu subskrybentów, zmianom mogą podlegać dowolne elementy Kodeksu Postępowania Certyfikacyjnego. Informacja o wszystkich istotnych, rozważanych zmianach w dokumencie jest przesyłana wszystkim zainteresowanym stronom w postaci informacji o miejscu dostępu nowej wersji Kodeksu Postępowania Certyfikacyjnego o statusie **w ankiecie**. Propozycje zmian mogą być otwarcie publikowane w repozytorium urzędu certyfikacji CERTUM lub rozsyłane pocztą elektroniczną. Do nowego Kodeksu Postępowania Certyfikacyjnego dołączona jest także informacja o wprowadzonych zmianach.

8.1.2.2. Okres oczekiwania na komentarze

Zainteresowane strony, w ciągu 10 dni roboczych od daty ich ogłoszenia mogą nadsyłać komentarze do 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 Kodeksu Postępowania Certyfikacyjnego przyjmuje status **w zatwierdzeniu** i poddana jest procedurze zatwierdzenia (rozdz.8.3).

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

8.1.2.3. Zmiany wymagające nowego identyfikatora

W przypadku zmian, które mogą mieć rzeczywisty wpływ na znaczącą grupę użytkowników usług certyfikacyjnych, inspektor bezpieczeństwa może przydzielić zmodyfikowanemu dokumentowi nowy identyfikator (OBJECT IDENTIFIER). Zmianie może ulec także identyfikator polityki certyfikacji, według której są świadczone usługi certyfikacyjne. Powyższy przypadek może mieć miejsce w szczególności po zmianach legislacyjnych dotyczących kwalifikowanych podmiotów świadczących usługi certyfikacyjne.

8.2. Publikacja

8.2.1. Elementy nie publikowane w Kodeksie Postępowania Certyfikacyjnego

Publicznie nie są dostępne zastosowane zabezpieczenia systemu komputerowego, procedury oraz mechanizmy uwierzytelniania, a także te elementy, których ujawnienie może osłabić zabezpieczenia oraz zasugerować ataki na nie. W szczególności nie ujawnia się:

- zastosowanych platform sprzętowo-programowych,
- szczegółów użytej konfiguracji sprzętowej,
- planu podnoszenia systemu po awariach i katastrofach,
- miejsc przechowywania kluczy CERTUM i chroniących je sekretów współdzielonych oraz numerów PIN do nich,
- listy osób posiadających sekrety współdzielone,
- przedsięwziętych sposobów ochrony personelu,
- zabezpieczeń sieci,
- procedur logowania się do systemu.

Nie publikowane elementy udostępniane są inspektorowi bezpieczeństwa, administratorowi systemu oraz instytucji audytującej. Z dokumentów, które opisują te elementy korzystać można tylko w siedzibie CERTUM w specjalnie przeznaczonym do tego celu pomieszczeniu.

8.2.2. Dystrybucja nowej wersji Kodeksu Postępowania Certyfikacyjnego

Kopia Kodeksu Postępowania Certyfikacyjnego dostępna jest w formie elektronicznej:

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

W repozytorium urzędu certyfikacji oraz za pośrednictwem strony WWW dostępne są zawsze trzy wersje (jeśli jest to możliwe) Kodeksu Postępowania Certyfikacyjnego: wersja aktualnie obowiązująca, wersja poprzednia oraz wersja podlegająca procedurze zatwierdzenia (patrz rozdz.8.3). W przypadku zmiany wydania Kodeksu Postępowania Certyfikacyjnego nie jest konieczne publikowanie poprzedniego wydania.

Za pośrednictwem tych samych adresów zaleca się udostępnienie także dokumentu, opisującego istotne różnice pomiędzy aktualnym (jeszcze obowiązującym) a Kodeksem Postępowania Certyfikacyjnego poddanym procedurze zatwierdzania.

8.3. Procedura zatwierdzania Kodeksu Postępowania Certyfikacyjnego

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

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	23 października 2002 r.	Pełna wersja dokumentu. **Dokument zatwierdzony**
2.0	01 lutego 2005 r.	Sprecyzowano zakres stosowania certyfikatów i zaświadczeń (rozdz.1.4), okoliczności i procedury modyfikacji certyfikatów i zaświadczeń (rozdz.3.2.2 i 4.7), ograniczono okres ważności certyfikatów i zaświadczeń tylko do okresu ważności zaświadczenia certyfikacyjnego (rozdz.4.2 i rozdz.6.3.2), dostosowano procedurze unieważniania certyfikatów do wymogu *Art.31 Ustawy z dnia 18 września o podpisie elektronicznym* (rozdz.4.8), skorygowano zawartości tabel w rozdz.7. Ujednolicono pisownię nazw własnych firmy. Poprawki edycyjne.
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; usunięcie zbędnych informacji na temat profili certyfikatów kluczy infrastruktury
3.3	01 marca 2008 r.	Aktualizacja profili certyfikatów.
3.4	14 lipca 2008 r.	Aktualizacja informacji na temat QDVCS.
3.5	24 lipca 2009r.	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, Aktualizacja zasady podziału sekretów współdzielonych
3.9	21 kwiecień 2015	Dostosowanie dokumentu do wymagań ETSI TS 101 456
4.0	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.
4.1	12 kwiecień 2016	Aktualizacja numeru wpisu kwalifikowanych podmiotów.
4.2	01 lipca 2016	Dostosowanie do wymogów Rozporządzenia UE 910/2014 eIDAS
4.3	23 grudzień 2016	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 subskrybenta 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 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 (kwalifikowany 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*, 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.

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* do wydawania zaświadczeń certyfikacyjnych, za pomocą którego dane służące do weryfikacji poświadczenia elektronicznego są przyporządkowane do ministra cyfryzacji lub tego podmiotu.

Naruszenie (np. danych) – ujawnienie informacji nieuprawnionym osobom lub taka ingerencja naruszająca politykę bezpieczeństwa systemu, w wyniku której wystąpi nieuprawnione (zamierzone lub niezamierzone) ujawnienie, modyfikacja, zniszczenie lub udostępnienie dowolnego obiektu.

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

Obiekt – jednostka do której dostęp jest kontrolowany, np. plik, program, obszar w pamięci głównej; gromadzone i utrzymywane dane osobowe (PN-2000:2002).

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).

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)

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.

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.

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*).