Certification Policy of CERTUM's Qualified Certification Services

Version 3.6

Effective date: 1st of November , 2009

Status: previous

Unizeto Technologies S.A.
„CERTUM - Powszechne Centrum Certyfikacji"
ul. Bajeczna 13
71-838 Szczecin
http://www.certum.pl

Trademark and Copyright notices

Content

1. Introduction

Certification Policy of CERTUM's Qualified Certification Services describes general rules of certification practice of CERTUM (full name: CERTUM – General Certification Authority) used by part of CERTUM in the course of provision of certification services in accordance with the *Act on Electronic Signature of 18 September, 2001 - Dz.U. nr 130, poz. 1450, further referred to as the Act.*.

The Certification Policy is closely linked to the Certification Practice Statement of CERTUM's Qualified Certification Services. Certification Practice Statement of CERTUM's Qualified Certification Services is defined as a *declaration of the procedures used by the CA in the process of issuing a certificate* and for the provision of additional certification services.

Unizeto Technologies S.A. is a legal successor of Unizeto Sp. z o.o. According to Polish *Kodeks Spółek Handlowych* (commercial partnership regulation – Journal of Law No 94, item 1037 inc. later changes) universal succession was executed, resulting in Unizeto Technologies S.A. inherited all the rights and obligations of Unizeto Sp. z o.o.

1.1. Overview

Certification Policy of CERTUM's Qualified Certification Services is a description and basis for functioning of CERTUM (operating within Unizeto Technologies S.A. structure) and **certification authorities, registration authorities, subscribers** and **relying parties** associated with it. It also specifies rules of certification services such as the **issuance of qualified certificates** including: subscriber's registration, public key certification, rekey and certificates renewal, **certificates revocation** and **suspension,** and issuance of **timestamps tokens**, **certificate status tokens**, **data validation tokens**, **evidences of receipt and submission (including official evidence of receipt and submission[1])**, **deposit, registries and repositories tokens** (particularly regarding signed objects)**,** and the issuance of attribute certificates. CERTUM's qualified certification services are provided in accordance with the requirements of the **certification policy** described in *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*.

CERTUM obeys the law in force in the Republic of Poland and the requirements to be met by qualified certification service providers. These requirements are described in the *Act* and this **Certification Policy**. Unizeto Technologies S.A with its registered office in Szczecin, Królowej Korony Polskiej 21 street and with its service unit CERTUM providing qualified certification services, is a qualified certification service provider, in accordance with the *Act*, who has been entered under number 1in the register of qualified certification service providers.

The structure and contents of Certification Policy are in accordance with the recommendation of RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. In such a way it is possible to quickly compare the Certification Policy for similar documents issued by other certification authorities.

---

[1] Official Evidences of receipt and submission are issued in accordance with the Article *16 paragraph. 3 ustawy z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Dz. U. Nr 64, poz. 565)* and in accordance with the *Article 39 § 2 ustawy z dnia 14 czerwca 1960 r. Kodeks postępowania administracyjnego (Dz. U. z 2000 r. Nr 98, poz. 1071*. See also Glossary)

1.2. Document Name and its Identification

The following registered object identifier is connected with the Certification Policy document:

```
id-cck-pc-v1  OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
           organization(1) id-unizeto(113527) id-ccert(2) id-cck(4)
           id-cck-certum-certPolicy(1) id-certPolicy-doc(0) id-ccert-pc(1)
           version(3) 4}
```

in which the two last numeric values correspond to the current version and subversion of this document.

This document is available:

- As an electronic version at the repository at: http://www.certum.pl/repozytorium or on request sent to: info@certum.pl,
- As a paper copy - on request sent to the address of CERTUM (see Chapter 1.6).

Only certification policies identifiers belonging to the collection of certification policies incorporated by the present Certification Policy (described in Chapter Tab. 12 hereinafter) are included in certificates issued by CERTUM.

1.3. Certification Policy Parties and Applicability Range.

The following entities belong to CERTUM:

- Qualified certification authority **CERTUM QCA**,
- Qualified time – stamping authority **CERTUM QTSA**,
- Qualified online certificate status protocol authority **CERTUM QOCSP**,
- Qualified data validation and certification server authority **CERTUM QDVCS**,
- Qualified delivery authority **CERTUM QDA**,
- Qualified object deposits authority **CERTUM QODA**,
- Qualified registries and repositories authority **CERTUM QRRA**,
- Qualified attribute certificates authority **CERTUM QACA**,
- Primary Registration Authority (PRA),
- Registration Authorities (RA),
- notaries or persons confirming the identity,
- subscribers,
- relying parties.

1.3.1. Qualified Certification Authority CERTUM QCA

Certification authority **CERTUM QCA** belongs to CERTUM which provides qualified certification services and operates on the basis of the entry of the Unizeto Technologies S.A. in the register of qualified certification services providers. The Minister in charge of economy or

entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QCA** activity**.**

CERTUM QCA is the new authority which came into being after the actualization of the certificate evidence according to the Regulation of *Rozporządzenie Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Journal of Law No. 128 item 1101, of 2002).* The old certificate evidence will be used only to create and publish the lists of certificates revoked by the period till 16:16 2007 30 December 16:16:49 GMT.

The authority **CERTUM QCA** issues qualified certificates, certificates of infrastructure keys and certificates of certification authorities according to the *Act* and the Regulation: *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002)* and the Regulation: *Rozporządzenie Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Journal of Law No. 128 item 1101, of 2002).*

Tab. 1 Certification policy identifiers included in the certificate evidences issued by CERTUM QCA

Name of certificate	Certification policy identifier
Qualified certificates	1.2.616.1.113527.2.4.1.1
Certificate evidences	2.5.29.32.0
Certificates of infrastructure keys	1.2.616.1.113527.2.4.1.10

1.3.2. Qualified Time-Stamping Authority CERTUM QTSA

Certum's Qualified Time – Stamping Authority **CERTUM QTSA**, operating within **cckDomena** domain (Fig. 1) is a part of CERTUM infrastructure for qualified services. **CERTUM QTSA** operates on the basis of the entry of the Unizeto Technologies S.A. in the register of qualified certification services providers and based on the certificate evidence issued by the Minister in charge of economy. The minister or an entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QTSA** activity**.**

CERTUM QTSA is the new authority which came into being after the actualization of the certificate evidence in accordance with to the Regulation of *Rozporządzenie Ministra Gospodarki z dnia 9 sierpnia 2002 r. (Journal of Law No. 128 item 1101, of 2002).*

Tab. 2 **CERTUM Qualified Time-Stamping Authority** identifier**,** included in timestamp tokens issued by CERTUM QTSA

Nazwa tokena	Identyfikator polityki certyfikacji
Kwalifikowany token znacznika czasu wg. ETSI (TS 101 861)	1.2.616.1.113527.2.4.1.2

Qualified timestamp tokens, isued in accordance with the ETSI TS 101 861 recommendation and the policy described in Tab.2, are used primarily for securing long-term electronic signatures[2] and global transactions.

CERTUM Qualified Time-Stamping Authority applies solutions which guarantee synchronization with international time source (Coordinated Universal Time - UTC) within the accuracy more than 1 second.

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

1.3.3. Qualified online certificate status protocol authority CERTUM QOCSP

CERTUM beside standard certificate status verification based on Certificate Revocation List (CRL) offers online services – based on Online Certificate Status Protocol (OCSP). This service is provided by qualified online certificate status protocol authority **CERTUM QOCSP** (see Fig. 1) on the basis of the entry of the Unizeto Technologies S.A. in the register qualified certification services providers. Minister in charge of economy or entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QOCSP** activity**.**

Qualified online certificate status protocol authority CERTUM QOCSP should validates the status of qualified certificates only[3]. These confirmations are issued in accordance with the principles set out in this policy of certification.

1.3.4. Qualified data validation and certification server authority CERTUM QDVCS

Qualified data validation and certification server authority **CERTUM QDVCS** issues electronic confirmations (also called qualified data validation tokens) to validate qualified public key certificate, electronic signature, timestamp, certificate status token, delivery token and data validation token issued by **CERTUM QDVCS** or other qualified authorities. **CERTUM QDVC** also issues electronic confirmations of possession of data or claim of possession of data.

3 Also applies to certificates which are deemed to be qualified certificates in accordance with the *Article 3 of the Act on Electronic Signature of 18 September, 2001 (Journal of Law No. 130 item 1450, of 2001).*

Tab. 3 Certification policy identifiers accepted by CERTUM QDVCS and included in data validation tokens

Token name	Certification Policy Identifier
Qualified token of data possessing or declaration of data possessing	1.2.616.1.113527.2.4.1.3.1.616
Qualified validation token of qualified electronic signature[4]	1.2.616.1.113527.2.4.1.3.2.c[5]
Qualified validation token of qualified timestamp. [6]	1.2.616.1.113527.2.4.1.3.3.c
Qualified validation token of qualified certificate[7]	1.2.616.1.113527.2.4.1.3.4.c
Qualified validation token of certificate status (OCSP) token.	1.2.616.1.113527.2.4.1.3.5.c
Official qualified non-repudiation of receipt token	1.2.616.1.113527.2.4.1.3.6.616
Official qualified non-repudiation of submission token	1.2.616.1.113527.2.4.1.3.7.616
Qualified validation token of validation tokens[7]	1.2.616.1.113527.2.4.1.3.8.c
Qualified validation token of the certificate and certificate evidence.	1.2.616.1.113527.2.4.1.3.9.c
Qualified token of electronic signature validation	1.2.616.1.113527.2.4.1.3.10.c

CERTUM QDVCS operates on the basis of the entry the Unizeto Technologies S.A. in the register qualified certification services providers. Minister in charge of economy or entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QDVCS** activity.

Qualified data validation tokens are issued according to certification policies described in Tab. 4 and may be used primarily in the process of validation of qualified electronic signatures[8]. The last three digits of each of the ID policies contain a three-letter country code (according to ISO 3166). Putting this type of code in the data validation token (except qualified token of data possessing or declaration of data possessing) means that **CERTUM QDVCS** ensures that validated data (qualified electronic signature, qualified timestamp, qualified certificate, certificate status token) have been issued in accordance with formal requirements of the law of country whose code has been placed at the end of policy identifier.

Regardless of the type of issued data validation token, the **CERTUM QDVCS** authority ensures full compliance with all requirements set by the legal regulations in force in the Republic of Poland.

A request for the issuance of data validation token may include policy identifier. This allows the user to verify the validity of electronic signatures executed by the Polish citizen, not only in Poland but also in another country.

Qualified data validation authority **CERTUM QDVCS** certifies validity of public key certificates, digital signatures, timestamps, certificate status tokens, delivery status tokens and data

4 These are electronic signatures that is equivalent to personal signature by law of specified country.

5 Stamp 'c' means a three-letter country code according to ISO 3166, for example, Polish code is 616.

6 These are timestamps, certificate status tokens or data validation tokens which are issued by registered (i.e. qualified or accredited) certification authorities operated in accordance with the requirements defined in the act on electronic signature in force in the specified country.

7 These are certificates which are issued by registered (i.e. qualified or accredited) certification authorities operated in accordance with the requirements defined in the act on electronic signature in force in the specified country and used to verification of electronic signatures.

8 In this document the term of validation of electronic signature may be used alternatively to the term of verification of electronic signature (see Glossary)

validation tokens which are issued in accordance with the acts on electronic signature which are in force in the territory of the country indicated on the certification policy. These tokens are always issued at the time indicated in the request; in turn tokens of data possessing or declared data possessing shall be issued at the time of creating tokens.

Data validation tokens are issued by qualified data validation authority **CERTUM QDVCS** in accordance with the specific requirements of the *Act on electronic signature* for appropriate devices and software used to verify digital signatures.

1.3.5. Qualified delivery authority CERTUM QDA

Qualified delivery authority **CERTUM QDA** issues an **Official Evidence of Receipt** of electronic document, **official evidence of submission** of electronic document, **evidence of receipt** of electronic document and **evidence of submission** of electronic document. These evidences are issued on the basis of the *art. 16 par. 3 Act of 17 February 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne (Journal of Law No. 64 item 565)* and on the basis of *art.* 39^1 *§ 2 Act of 14 June 1960 Kodeks postępowania administracyjnego (Journal of Law No. 98 item 1071, of 2000 as amended).* CERTUM QDA provides this service to individuals who want to send digitally signed electronic document to any recipient, including a public entity.

Tab. 4 Certification policy identifiers included in tokens issued by CERTUM QDA

Evidence name	Certification Policy Identifier
Official Evidence of Receipt	1.2.616.1.113527.2.4.1.4.1
Evidence of Receipt	1.2.616.1.113527.2.4.1.4.2
xkOfficial Evidence of Submission	1.2.616.1.113527.2.4.1.4.3
Evidence of Submission	1.2.616.1.113527.2.4.1.4.4

CERTUM QDA operates on the basis of enter the Unizeto Technologies S.A. in the register of qualified certification services providers. Minister in charge of economy or entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QDA** activity.

Qualified Evidences of recipt and submission (including Official evidences of recipt and submission) are issued according to certification policies described in Tab.4.

CERTUM QDA issues evidence of receipts (including official evidences of receipt) which are proof for subscriber that **CERTUM QDA** has delivered an electronic document in such place from which it will be available for recipient and recipient received this document, was acquainted with the contents of an electronic document and confirms the correctness of its contents.

CERTUM QDA issues Evidences of Submission (including official evidences of submission) which are the proof for sender that **CERTUM QDA** has delivered an electronic document in such place from which it will be available for recipient. **CERTUM QDA** confirms that the document is deposited, but it does not mean confirmation of the correctness of its contents.

1.3.6. Qualified objects deposit authority CERTUM QODA

Qualified objects deposit authority **CERTUM QODA** provides services such a storage, issuance, download and preserving the authenticity of any electronic data objects, particularly objects digitally signed in accordance with the requirements of the *Act on Electronic Signature of 18 September, 2001 (Journal of Law No. 130 item 1450 as amended)*. **CERTUM QODA** treats storage data such as any bitstrings, which means that **CERTUM QODA** is not interested in their structure (syntax), or in their semantic.

In response to the request of the depositary for the inclusion of data object in the deposit, for the download the entry of an object from the deposit or release an object from the deposit **CERTUM QODA** shall issue the following deposit tokens:

- when an object is placed on the deposit – a token of an object deposit entry;
- when an object is released from deposit (release takes place on the basis of object entry) – a token of an object release from the deposit: objects and objects entries (on the basis of which objects have been released) are removed from deposit;
- after certified release an object from deposit – certified token of an object release from the deposit; objects and all validity confirmation data associated with them are removed from the deposit (including the entry on the basis of which object have been released)
- when an entry is downloaded from the deposit – a token of download an entry from the deposit: entries are not removed from the deposit;
- after certified download of entry from the deposit (including tokens of its validity) – certified token of download an entry from the deposit; the entry and the token of its validity are not removed from the deposit;
- when an object is downloaded from the deposit (download takes place on the basis of object entry) – a token of download an object from the deposit; objects are not removed from the deposit;
- after certified download an object from the deposit (download takes place on the basis of object entry) including all validity confirmation data associated with them – certified tokens of download an object from the deposit; objects and are not removed from the deposit;

Tab. 5 Certification Policy Identifiers, included in tokens issued by CERTUM QODA

Token name	Certification Policy Identifier
token of object deposit entry	1.2.616.1.113527.2.4.1.5.1
token of object release from the deposit	1.2.616.1.113527.2.4.1.5.2
certified token of object release from the deposit	1.2.616.1.113527.2.4.1.5.3
token of download an entry from the deposit	1.2.616.1.113527.2.4.1.5.4
certified token of download an entry from the deposit	1.2.616.1.113527.2.4.1.5.5
token of download an object from the deposit	1.2.616.1.113527.2.4.1.5.6
certified tokens of download an object from the deposit	1.2.616.1.113527.2.4.1.5.7

CERTUM QODA operates on the basis of the entry the Unizeto Technologies S.A. in the registry qualified certification services providers. Minister in charge of economy or entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QODA** activity.

Qualified tokens of objects deposit entry, tokens of objects release from the deposit, certified tokens of objects release from the deposit, tokens of download an entry from the deposit, certified tokens of download an entry from the deposit, tokens of download an object from the deposit and certified tokens of download an object from the deposit are issued in accordance with certification policies, described in Table 5.

1.3.7. Qualified registries and repositories authority CERTUM QRRA

Qualified registries and repositories authority **CERTUM QRRA** enables the recording of data objects and, optionally, placing them in the repository. CERTUM QRRA also enables the downloading of entries from the registry and objects from the repository, their modifying and maintaining their authenticity; these objects can be digitaly signed in accordance with the requirements of the *Act on Electronic Signature of 18 September, 2001* (*Journal of Law No. 130 item 1450, of 2001 as amended)*. When registered object is placed in the repository, CERTUM QRRA checks the correctness of its structure (syntaxes) and its semantic.

Registries and repositories managed by CERTUM QRRA may be divided thematically.

In response to register request i.e. to place an entry in the registry and optionally an object in the repository, to download an entry from the registry and an object from the repository, to modify an entry or data object, CERTUM QRRA issues the following registries and repositories tokens:

- when an entry is placed in the registry and optionally an object is placed in the repository – a token of a registry entry and a token of an object placement in the repository;
- when an entry is downloaded from registry – a token of download an entry from the registry; entries are not removed from the registry;

- after certified download an entry from the registry (including tokens of its authenticity) – certified token of download an entry from the registry; entries and their tokens of validity are not removed from the registry;
- when an object is downloaded from the repository (download takes place on the basis of object entry) – a token of download an object from the repository; downloaded objects are not removed from the repository
- after certified download of an object from the repository (including tokens of its authenticity) – certified token of download an object from the repository; the object and token of its validity are not removed from the repository;
- when an entry is modified – a token of a registry entry modification; modified entry is still stored in the registry;
- when an object is modified – a token of an object modification in the repository; modified object is still stored in the registry.

Tab. 6 Certification policy identifiers, included in tokens issued by CERTUM QRRA

Token name	Certification Policy Identifier
token of registry entry	1.2.616.1.113527.2.4.1.6.1
token of object placement in the repository	1.2.616.1.113527.2.4.1.6.2
token of download an entry from the registry	1.2.616.1.113527.2.4.1.6.3
certified token of download an entry from the registry	1.2.616.1.113527.2.4.1.6.4
token of download an object from the repository	1.2.616.1.113527.2.4.1.6.5
certified token of download an object from the repository	1.2.616.1.113527.2.4.1.6.6
token of registry entry modification	1.2.616.1.113527.2.4.1.6.7
token of object modification in the repository	1.2.616.1.113527.2.4.1.6.7

CERTUM QRRA operates on the basis of the entry the Unizeto Technologies S.A. in the register of qualified certification services providers. Minister in charge of economy or entity indicated by him (**National root NCCert**) supervise over the certification authority **CERTUM QRRA** activity.

Qualified tokens of the entry placement in the registry, token of object placement in the repository, tokens of download an entry from the registry, certified tokens of download an entry from the registry, tokens of download an object from the repository, certified token of download an object from the repository, tokens of entry modification in the registry and tokens of object modification in the repository are issued in accordance with certification policies, described in Table 6.

1.3.8. Qualified attribute certificates authority CERTUM QACA

Qualified attribute certificates authority **CERTUM QACA** issues attribute certificates to end users after reliable confirmation of the possibility of allocating a specific attribute to those users.

The end user who is the owner of an attribute certificate issued by CERTUM QACA is not allowed to issue any attribute certificates. This means that the rights (confirmed by CERTUM QACA) of the end user cannot be transferred to other individuals.

CERTUM QACA operates on the basis of entry the Unizeto Technologies S.A. in the register of qualified certification services providers. Minister in charge of economy or entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QACA** activity.

Qualified attribute certificates authority **CERTUM QACA** issues, provides and revokes certificates of attributes in accordance with defined attribute certificate policies. These policies determine the suitability and applicability of these certificates.

Tab. 7 Certification policy identifiers, included in tokens issued by CERTUM QACA

Name of attribute certification policy	Certification Policy Identifier
Standard attribute certification policy	1.2.616.1.113527.2.4.1.7.1
Attribute certification policy for authorization	1.2.616.1.113527.2.4.1.7.2
Dedicated attribute certification policies	1.2.616.1.113527.2.4.1.7.3.x

CERTUM QACA issues attribute certificates in accordance with three predefined groups of attribute certification policies (see Table 7). The first two policies have constant identifier. The third policy belongs to groups of policies which applicability depends on current needs. Their descriptions, applicability range and identifiers are placed in the repository of CERTUM. Identifiers of these policies are built on the basis of the pattern shown in Table 7, in which the character 'x' means the serial number of policy in a dedicated set of attribute certification policies.

1.3.9. Registration authorities, points of the identity and attributes verification

CERTUM QCA closely cooperates with Primary Registration Authority, the registration authorities and points of the identity and attributes verification. Registration authorities and points of identity and attributes verification operate on the basis of the authorization by an appropriate certification authorities CERTUM QCA and CERTUM QACA. The authorization concerns the registration, identification of the identity and attributes of a current or future subscriber.

CERTUM may authenticatesd the identity of the person requesting the certificate without his/her personal appearance at the point of registration, on the basis of a notary confirmation of identity. CERTUM may appoints the other persons who verifies the identity of the applicant on behalf of CERTUM and is authorized to make an agreement for offering the certification services.

Points of the identity and attributes verification, as opposed to registration authority, cannot tell the certificate authority to issue certificate. They also cannot make certificate applications notifications. Points of the identity and attributes verification only provide verification of a subscriber identity and check the correctness of a submitted application. Such a request is forwarded to the Primary Registration Authority. Additionally, points of the identity and attributes verification provide information about certification services.

The list of registration authorities and points of the identity and attributes verification currently accredited by Primary Registration Authority is available in the repository at::

http://www.certum.pl/repozytorium.

1.3.10. End Entities

1.3.10.1. Subscribers

Any private or legal entities and hardware devices they own could be the subscriber of CERTUM.

Organizations willing to receive certificates, tokens or other confirmations issued by CERTUM for their employees could do it by means of their authorized representatives, whereas individual subscribers always request a certificate, tokens or confirmations by themselves.

1.3.10.2. Relying Parties

A relying party, using CERTUM services can be any entity who accept the qualified electronic signature or other certified electronic confirmation (including attribute certificate), their authenticity or the authenticity of submitted objects (particularly electronic document) relying on:

- validity of the connection between subscriber's identity and his/her/its public key (confirmed by certification authorities **CERTUM QCA**), or
- connection between electronic signature and timestamp token issued by qualified time - stamping authority **CERTUM QTSA**, or
- confirmation of validity of certificate issued by qualified data validation and certification server authority **CERTUM QOCSP**, or
- data validation token issued by qualified data validation and certification server authority **CERTUM QDVCS**, or
- evidences of receipt and submission (including Official evidences of receipt and submission) issued by qualified delivery authority **CERTUM QDA**, or
- deposit token issued by qualified objects deposit authority CERTUM **QODA**, or
- registries and repositories token issued by qualified registries and repositories authority CERTUM **QRRA**
- validity of the connection between subscriber's identity and his/her/its attribute certificate issued by qualified attribute certificates authority **CERTUM QACA**

1.4. Certificate and Certificate Evidences Applicability Range

Qualified certificates issued by CERTUM QCA may be used only to verify secure electronic signatures which are proofs of act of will and proof of connection with the data of various trust levels to which it has been attached.

Certificate evidences are issued to the Minister in charge of economy or the entity providing qualified certification services under the authority and on behalf of the Minister in charge of economy. Certificate evidences are also issued for the keys of QCA exchange.

Certificates of infrastructure keys are issued to: personnel of CERTUM and to the hardware devices controlled by these persons. Subscribers and relying parties need to know about existing certificates only when using services provided by CERTUM.

Certificates of infrastructure cannot be used for verification of secure electronic signatures. (even if contain **digitalSignature** bit or **nonRepudiation** bit in the **keyUsage** extension.)

1.5. Timestamps Applicability Range

Time - stamping authority **CERTUM QTSA** issues time-stamping tokens which, in terms of the Civil Code (*Art.7, §2)*, produce legal consequences of a certified date. The primary use of time-stamps is to mark long-term electronic signature with reliable time. Time-stamps issued by the **CERTUM QTSA** may also be used in any other cases that require a comparable time-stamping service.

1.6. OCSP Response Tokens Applicability Range

Online certificate status protocol authority **CERTUM QOCSP** issues status tokens of qualified certificates and certificate evidences (issued by qualified certification authorities with accordance to the *Act*). These tokens are issued after checking certificate revocation list.

1.7. Data Validation Applicability Range

Data validation and certification server authority **CERTUM QDVCS** issues qualified data validation tokens only to validate qualified public key certificate, electronic signature, time-stamp, certificate status (OCSP) token and other data validation tokens. **CERTUM QDVCS** also issues electronic tokens of data possessing or declared data possessing.

Data validations tokens should be collected by entities in order to resolve any future disputes.

1.8. Delivery Services Applicability Range

Official evidence of receipt or **official evidence of submission** is the proof of sending an electronic document to a public entity which is acting in accordance with the *art. 16 par. 3 Act of 17 February 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne (Journal of Law No. 64 item 565)* and on the basis of *art.* 39[1] par. 2 *Act of 14 June 1960 Kodeks postępowania administracyjnego (Journal of Law No. 98 item 1071, of 2000)*.

Evidences of reciept and submission (including official evidences of receipt and submission) are used to verify the status of the message which is not addressed to public entity.

1.9. Deposit, Registries and Repositories tokens Applicability Range

The deposit token is a proof of any object storage in the deposit, registration of any object and download or release of any object (or its entry) from the deposit. Upon request, a deposit tokens may contain other evidences associated with the data object, which enable to download or release an object from the deposit in the state in which it was deposited. For example, if any signed document was deposited, after release of this object from the deposit its validity and validity of the electronic signature are the same as when they were deposited.

Deposits, Registries and Repositories tokens shall be issued every time when an entry is registered, downloaded or modified and when an object is deposited, downloaded and modified Registries tokens constitute a proof of operations performed in the registry such as entry and download or modify registry content. Repositories tokens constitute a proof of an object placement (upon request) in the repository, its download and modification and also constitute a syntax and semantics proof of compliance with the requirements specified for the repository. Authenticity of entries and the objects placed in the registers and repositories is maintained at a constant level from the time of their entry in the registry and repository.

Deposit, Registries and Repositories tokens may be reliable evidence used for the dispute resolving, including civil-law disputes or legal proceedings.

1.10. Attribute Certificates Applicability Range

Attribute certificates are issued by qualified attribute certificates authority CERTUM QACA and can be explicitly linked to qualified or non-qualified public key certificates being additional attributes of electronic signature or indicating the rights of signature owner. Regardless of whether they are explicitly linked to public key certificates or they don't, attribute certificates may be used to authorize the rights of certificate owner or to authorize the rights of entity requesting the performing of the task being under control e.g. the right to use the reserved name.

Attribute certificates applicability range depends on attribute type and may results from relevant legal regulations or is determined by the relying party, which may define the types of attributes required for dealing with the systems or applications providing through this party

1.11. Contact

All inquiries and comments concerning the contents of the mentioned documents should be directed to:

Unizeto Technologies S.A.

CERTUM – Powszechne Centrum Certyfikacji

PL 71-838 Szczecin, Bajeczna 13

Email: info@certum.pl

2. General Provisions

This Chapter describes obligations, guarantees and liability of CERTUM, registration authorities, subscribers and relying parties.

2.1. Obligations

2.1.1. CERTUM and registration authority obligations

CERTUM providing qualified certification services commits itself:

- to the subscribers' identity verification;
- to issue and revoke a qualified certificate on the basis of a valid request and to inform about this fact indicated requester;
- to revoke a certificate when any information within the certificate has changed or when a private key, associated with the certificate would be compromised;
- to made available a part of information about revocation or suspension of a qualified certificate to other entities (solely upon the subscriber's approval);
- to assure an appropriate length and structure of the certified public keys and to guarantee the uniqueness of the distinguished name (DN) assigned for subject of certificate;
- to assure respect for the rights of subscribers and relying parties arising from the provisions of law, regulations of CERTUM and agreements resolutions;
- to protection of personal data;
- to use parameters of cryptographic algorithms in accordance with requirements defined in the *appendix 3* (*Requirements for encryption algorithms*) of *Rozporządzenie RM z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002)*.

Registration authorities, persons who confirm subscribers' identity or points of identity verification are committed:

- to comply with CERTUM procedures, to validate of the identity of requesters, to issue or revoke a certificate and to issue a certification request tokens,
- to subordinate to CERTUM recommendations,
- to protect private keys of registration authority operators and private keys of operators of points of the identity verification
- to use private keys of the operators for purposes not other than those described herein.

2.1.2. Time - stamping authority obligations

Time – stamping authority CERTUMQTSA provides time - stamping services in accordance with requirements defined in *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002).* CERTUM QTSA ensures that:

CERTUM QTSA ensures that:

- it uses the technology, operational procedures and security management procedures, which prevent any possibility of manipulating the time,
- it uses parameters of cryptographic algorithms in accordance with appendix 3 of Requirements for encryption algorithms) of *Rozporządzenie RM z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002),*
- it defines at least one hash function which may be used to create hash of data marked with time,
- Coordinated Universal Time – UTC used in the timestamp tokens is provided with the accuracy of 1 second.

2.1.3. Certificate status authority and data validation authority obligations

Online certificate status protocol authority **CERTUM QOCSP** and data validation and certification server authority **CERTUM QDVCS** provide their services in accordance with the requirements defined in *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. (Dz.U. nr 128 poz. 1094)* and this Certification Policy. **CERTUM QOCSP** and **CERTUM QDVCS** ensure that they:

- use operational procedures and security management procedures, that prevent any possibility of manipulating the certificates, certificate evidences or data status,
- verify validity of qualified signatures used according to the requirements of *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002),*
- verify validity of qualified data validation tokens, timestamp tokens, certificate status tokens and evidences of receipt and submission (including official evidences of receipt and submission) issued by qualified certification service providers

2.1.4. Delivery authority obligations

Delivery authority **CERTUM QDA** provides services in accordance with the requirements defined in Regulations issued on the basis of *art. 16 par. 3 Act of 17 February 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne (Journal of Law No. 64 item 565, of 2005)* and *art.* 39^1 par. 2 *Act of 14 June 1960 Kodeks postępowania administracyjnego (Journal of Law No. 98 item 1071, of 2000 as amended)*.

W szczególności CERTUM QDA:

- it uses operational procedures and security management procedures that prevent any possibility of forgery of the receipt or submission status tokens (including official tokens),
- it uses parameters of cryptographic algorithms in accordance with requirements defined in the *appendix 3* (*Requirements for encryption algorithms*) of *Rozporządzenie RM z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002),*

- it issues evidences of receipt (including official evidences of receipt) only after verification of data authenticity of received electronic document, its formal correctness and only after CERTUM has delivered it in such place from which it will be available for recipient,
- it issues evidences of submission (including official evidences of submission) only after verification of data authenticity of received electronic document, its formal correctness and only after CERTUM has delivered it in the user's telecommunication system, this notification is not a confirmation of formal correctness of such document.

2.1.5. Object deposits authority and registries and repositories authority obligations

Objects deposit authority **CERTUM QODA** and registries and repositories authority **CERTUM QRRA** provide services in accordance with the requirements defined in Regulations issued in the basis of art. 5, par. 2a, 2b i 2c *Act of 14 July 1983 o narodowym zasobie archiwalnym i archiwach*, in *Rozporządzeniu Ministra Finansów of 14 July 2005 w sprawie wystawiania oraz przesyłania faktur w formie elektronicznej, a także przechowywania oraz udostępniania organowi podatkowemu lub organowi kontroli skarbowej tych faktur (Journal of Law No. 133 item 1119, of 2005)*, and also in accordance with requirements defined in the *Act of 17 February, 2005 o informatyzacji działalności podmiotów realizujących zadania publiczne (Journal of Law No. 64 item 565, of 2005)*.

CERTUM QODA and CERTUM QRRA ensure that::

- they use operational procedures and security management procedures, which preclude any possibility of forgery of the deposit, registries and repositories tokens,
- they use parameters of cryptographic algorithms in accordance with requirements defined in the appendix 3 (Requirements for encryption algorithms) of *Rozporządzenie RM z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002)*,
- only authorized persons are able to obtain access to the deposits, registries, and repositories,
- CERTUM QRRA stores in the repository only validated data objects according to the requirements for particular repository,
- authenticity of stored objects and entries are the same as when they were deposited or stored in the repository
- upon request from a depositary, CERTUM QODA will remove the object from the deposit.

2.1.6. Attribute Certificates Authority Obligations

Attribute certificate authority **CERTUM QACA** guarantees that it provides services in accordance with the requirements defined in *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. (Journal of Law No. 128 item 1094, of 2002)* and this Certification Policy[9], and also in accordance with requirements defined in ISO/TS 17090:2002 *Health informatics - Public key infrastructure* i ISO/TS 22600:2006 *Health informatics - Privilege management and access control* standards.

Additionally **CERTUM QACA** ensures that:

[9] This Certification Policy does not allow a possibility of actualization or modification of attribute certificates.

- it verifies that the attribute certificate requester is authorized and has rights to use the attribute or attributes. This also applies to the case when including the attribute in the certificate of attributes results in the transfer of rights,
- it accepts confirmation of rights to use the attribute or attributes issued by point of attributes verification or by notary,
- list of attributes that can be placed in attribute certificates is available to certification service users,
- list of dedicated certification policies which are adjusted to a particular purpose of relying party is available to certification service users.

2.2. End Users Obligations

2.2.1. Subscriber Obligations

Subscriber is committed:

- to use certificates and certificate evidences in accordance with the declared purpose
- to use certificates and certificate evidences only within the validity period of these certificates or certificate evidences,
- to keep confidential, and properly protect at all times the private key,
- to immediately inform CERTUM when a certificate must be revoked.

2.2.2. Relying Party Obligations

Relying party is committed to:

- thoroughly verify every electronic signature or confirmation made on a document or certificate, timestamp token, certificate status token, data validation and certification server token, delivery token, deposit, registries and repositories tokens and attribute certificate submitted to him/her/it.,
- consider an electronic signature to be invalid if by means of applied software and devices it is not possible to state if the electronic signature is valid or if the verification result is negative.

2.3. CERTUM liability

CERTUM acting within authorization of Unizeto Technologies S.A., bears liability for the consequences of the actions of certification authority **CERTUM QCA**, time – stamping authority **CERTUM QTSA,** online certificate status protocol authority **CERTUM QOCSP,** data validation and certificaton server authority **CERTUM QDVCS**, delivery authority **CERTUM QDA,** object deposits authority **CERTUM QODA**, registries and repositories authority **CERTUM QRRA**, attribute certificates authority **CERTUM QACA,** Primary Registration Authority and – if agreements state so – other certification authorities and registration authorities.

CERTUM certification authority bears liability for cases when direct or indirect damages incurred by a subscriber or a relying party result from mistakes made by CERTUM, particularly concerning the discrepancy between the process of identity verification and declared procedures,

inappropriate security of the private key of certification authorities or lack of access to rendered services (e.g. to CRLs),

CERTUM does not bear responsibility for the damages arising from the installation and usage of applications and devices used for generating and managing cryptographic keys, encryption, creating of an electronic signature that are included in the unauthorized applications list (applicable to relying parties) or are not included in the authorized applications list (applicable to subscribers),

CERTUM does not bear responsibility for the damages arising from inappropriate usage of issued certificates,

CERTUM does not bear responsibility for the storage of false data in CERTUM database and their publication in a public certificate key issued to the subscriber in case of subscriber's stating such false data.

2.4. Financial Responsibility

The financial warranty of Unizeto Technologies S.A. in relaton to individual event amounts equivalent of an 250.000 € but total financial warranties of Unizeto Technologies S.A. in relation to all such events cannot exceed the amount of 1.000.000 €. Financial liability applies to 12-month periods what is equivalent to the calendar year.

2.5. Governing Law and Dispute Resolution

2.5.1. Obowiązujące akty prawne

Operating of CERTUM is based on the general rules stated in the present Certification Policy, Certification Practice Statement and it is in accordance with the superior legal acts in force in the Republic of Poland.

2.5.2. Disputes Resolution

Disputes or complaints following the usage of certificates delivered by CERTUM will be resolved by mediation on the basis of written information.

If the complaint is not settled within the conciliatory process, the parties can hand over the dispute to appropriate court. The court, appropriate for case handling, will be the Public Court of the defendant.

2.6. Fees

CERTUM charges fees for its services. The extent of fees and categories of chargeable services are published in a price list available in the repository at:

http://www.certum.pl/repozytorium

2.7. Repository and Publication

2.7.1. Information Published by CERTUM

The whole information published by CERTUM is available in the repository at:

http://www.certum.pl/repozytorium

The information consists of:

- Certification Regulations of CERTUM's Qualified Certification Services,
- Certification Policy of CERTUM's Qualified Certification Services,
- Certification Practice Statement of CERTUM's Qualified Certification Services,
- templates of agreements with subscribers,
- unexpired and unrevoked certificate evidences,
- the list of recommended applications and devices approved by CERTUM,
- the lists of accredited notaries or persons confirming identity and attributes,
- Certificates Revocation Lists (CRLs);
- qualified public key certificates (with the consent of the owners) and attribute certificates,
- supplementary information, e.g. announcements and notifications.

2.7.2. Frequency of Publication

CERTUM publications below are issued with the following frequency:

- Certification Regulations of CERTUM's Qualified Certification Services, Certification Policy of CERTUM's Qualified Certification Services, Certification Practice Statement of CERTUM's Qualified Certification Services Statement – see Chapter 8,
- certificate evidences of all authorities functioning within CERTUM – upon every issuance of new certificates,
- lists of certificates revoked and suspended within 1 hour of request,
- supplementary information – upon every updating of it.

2.7.3. Access to Publications

The whole information published by CERTUM in its repository at http://www.certum.pl/repozytorium is accessible for the public.

2.8. Audit

CERTUM audit may be carried out by internal units of Unizeto Technologies S.A. (internal audit) and organizational units independent from Unizeto Technologies S.A. (external audit). External audit can be conducted at the request of the Minister in charge of economy under the *Act on electronic signature, Article 36.*

2.9. Confidentiality Policy

Unizeto Technologies S.A. ensures that the whole information it possesses is gathered, stored and processed in accordance with the law in force, particularly with *Personal Data Protection Law of 29th of August, 1997* including its later changes and execution acts.

Unizeto Technologies S.A. ensures that third parties are given the access only to the information that is publicly accessible in a certificate or certificate evidence and when a subscriber approves of the publication of that information.

2.10. Intellectual Property Rights

All trademarks, patents, brand marks, licenses, graphic marks, etc., used by Unizeto Technologies S.A. are intellectual property of their legal owners. CERTUM commits itself to place appropriate remarks (required by the owners) in this respect.

Every key pair associated with a public key certificate issued by CERTUM is the property of the subject of the certificate, described in the field **subject** of the certificate or is the property of the requester represented by the subscriber.

2.11. Time synchronization

All clocks operated within the system CERTUM providing qualified services and used to provide services are synchronized to the Coordinated Universal Time, with the accuracy of 1 second.

3. Identification and Authentication

This Chapter presents general rules of subscribers' identity verification applied by CERTUM to certificate issuance, revocation and suspension.

3.1. Registration of CERTUM QCA's subscriber

Subscriber's registration takes place when a subscriber applying for registration for the first time in **CERTUM.**

Every subscriber requesting public key infrastructure services and applying for certificate issuance should (prior to certificate issuance):

- remotely fill in a registration form on WWW pages of CERTUM or submit data required for certificate issue in the registration authority,
- indicates, in accordance with the provisions of *art. 20, par. 2* of the *Act on Electronic Signature,* at his/her/its role as a certificate user,
- enter, in the presence of the notary or other person confirming identity, into an agreement concerning services provided by CERTUM.

Applicant during registration process is informed, in a clear and generally understandable form, in writing or in the fom of an electronic document, about the detailed terms and conditions regarding the use of the certificate, including complaints and dispute settlement procedures and in particular about the essential terms and conditions thereof, including:

- the scope of application and limitations thereon,
- legal effects of the creation of electronic signatures verified by the certificate,
- the information about a voluntary accreditation scheme of the qualified entities and their significance

Registration of subscribers acting on behalf of another natural person, legal person or an organizational unit not endowed with legal personality is carried out analogically to registration of individual subscribers. In addition the registration is preceded by entering into a sponsor agreement concluded between Unizeto Technologies S.A. and requester.

3.1.1. Distinguished Names and categories of certificates

DN name may consist of the following fields:

- field C – international abbreviation of the country name (PL for Poland),
- field ST – the region/province where the subscriber lives or runs his/her business,
- field L – the city where the subscriber lives or has a seat,
- field S – the surname of subscriber,
- field G – the given name (names) of subscriber,

- field CN – the subscriber's common name or the name of the organization in which the subscriber works provided that fields O or OU (see below) appeared in DN; the name of a product or a device may also be provided in this field,
- field O – the name of the institution which the subscriber represents or additional distinguished name,
- field OU – the name of the organizational unit the subscriber represents or additional distinguished name,
- field SN – the serial number included NIP or PESEL
- field A – the subscriber's address
- field P – the subscriber's pseudonym (only in case of anonymous certificate)

Certificates are issued to various categories of entities:

- **category I** contains at least the following attributes: name of country, common name, serial number; this category applies to personal certificates only,
- **category II** contains at least the following attributes: name of country, surname, name (names), serial number; this category applies to professional certificates only,
- **category III** contains at least the following attributes: name of country, pseudonym; this category applies to anonymous certificates only,

CERTUM guarantees the uniqueness of the distinguished name (DN) assigned for subject of certificate.

3.1.2. Authentication of subscribers's identity

Verification of natural persons may be carried out in a registration authority, by notary or other person who confirm identity of subscriber.

The registration authority, notary or other person confirming identity should request suitable documents (ID card, passport) from the subscriber, which without any doubts confirm his/her/its identity. Additionally, in case of certificates category II and III submitted documents should prove:

- the right of the subscriber to act and to use the certificate on behalf of the institution or legal entity,
- recent extract from the National Court Register.

Documents confirming the identity of the subscriber and the other documents required to carry out the certification process will be copied and stored in CERTUM by appropriate period of time. Part of the data, in accordance with the requirements of GIODO is permanently removed from the copied documents.

In the case when the entity already possesses the certificates issued by CERTUM and has been already subjected to identity verification, further identity verification may be based on previous documents and data. This data may be electronically signed then verification of the identity of the subscriber requesting for certificate is carried out on the basis of electronically signed application for certification.

Authentication of the subscriber is validated by the registration inspector or other person who confirm identity of subscriber. Suitable statement should consist of a hand-written signature and PESEL number of those persons.

3.2. Subscriber's Identity Authentication in Rekey, Certificate Renewal or Certificate Modification

In the case of certification, rekey or certificate modification, subscriber is committed to submit suitable request. The request must be authenticated, i.e.:

- signed by the subscriber by using currently valid private key, associated with unexpired certificate, or
- confirmed by the registration inspector in the Primary Registration Authority or by the registration authority operator, a notary or other person who confirm subscriber's identity.

3.3. Subscriber's Identity Authentication in Certificate Revocation

Applications for revocation can be submitted by email directly to an appropriate certificate issuer or indirectly to a registration authority.

In all cases subscriber should submit the application to Primary Registration Authority. Registration inspector verifies the subscriber's knowledge of her/his/its secrets and compliance subscriber's personal data with his/her/its certificate. In the case of discrepancies, a certificate is suspended until explanation of reasons of the suspension.

Identification and authetication of subscriber in Primary Registration Authority is carried out analogically to initial registration.

3.4. Registration of subscribers of other CERTUM services

Registration of the subscriber of services rendered by the time – stamping authority CERTUM QTSA, online certificate status protocol authority CERTUM QOCSP, data validation authority CERTUM QDVCS, object deposits authority CERTUM QODA, registries and repositories authority CERTUM QRRA and attribute certificates authority CERTUM QACA is not obligatory and may be connected with the registration of the subscriber of CERTUM's QCA services.

Relying parties who are not registered users of the services of time – stamping authority CERTUM QTSA, online certificate status protocol authority CERTUM QOCSP, data validation authority CERTUM QDVCS, object deposits authority CERTUM QODA, registries and repositories authority CERTUM QRRA and attribute certificates authority CERTUM QACA may be required to authenticate each request sent to these authorities.

4. Operational Requirements

Certification procedures are presented below. Every procedure starts with a subscriber's submitting a suitable application to a registration authority, time – stamping authority, certificate status verification authority, data validation authority and delivery authority. On the basis of the application, the certification authority takes an appropriate decision about the delivery/rejection of the requested service.

4.1. Application Submission

Subscriber's applications are submitted indirectly by a registration authority or in electronic form. Applications submitted directly to Primary Registration Authority might concern only certificate revocation request.

4.1.1. Registration Application

An application for registration is submitted by an applicant personally to a registration authority or in an electronic form (in that case verification carried out by a notary or person who confirms subscribers' identity is necessary).

Upon authentication of the identity of the subscriber by a registration authority operator, a notary or other person who confirm subscriber's identity (see Chapter 3.1.2), an application is submitted to the Primary Registration Authority where a **certification request token** is prepared and submitted to certification authority

4.1.2. Certificate renewal, rekey, certification or modification application

An application for certification is submitted to a registration authority personally by a subscriber or in electronic form.

4.1.3. Certificate Revocation or Suspension Application

An application for certificate revocation is submitted to a Primary Registration Authority only by authorized persons (see Chapter **Błąd! Nie można odnaleźć źródła odwołania.**) personally, by phone call, by fax or by mail. Applications must be confirmed by registration inspector.

Application form is published in the CERTUM repository.

In the moment of certificate revocation, subscribers and requesters are notified about this fact.

4.1.4. Processing of applications in registration authority

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

In the case of electronic processing of rekey application the registration inspector or person who confirm subscriber's identity shall confirm, according to Act, the subscriber's identity by his/her own handwritten signature and

providing personal number PESEL in written statement.

4.2. Certificates Issuance

On receiving an appropriate certification request token and processing it, a certification authority **issues a certificate**. Date of issuance is recorded in the event journal.

In the moment of certificate issuance, subscribers and requesters are notified about this fact.

4.2.1. Certificate Issuance Awaiting

A certification authority should make efforts to ensure that on receiving application for registration and certification, and certification or renewal of keys or modification of certificate, the authority examines the application and issues a certificate as soon as possible. The issue time depends mainly on completeness of a submitted application and possible administration co-ordinations and explanations between CERTUM and the requester. Maximum awaiting period for certificate issuance is 7 days.

4.2.2. Denial of Certificate Issuance

The denial of certificate issuance can occur:

- when the subscriber cannot prove his/her rights to proposed **DN**,
- if there is suspicion or certainty that the subscriber falsified the data or stated false data,
- if the subscriber did not submit required documents,
- from other reasons not specified above, upon prior notice of **security inspector.**

Information concerning the decision about a denial of certificate issuance and its reasons is sent to the applicant. The requester can appeal against CERTUM's decision..

4.3. Certificate Acceptance

On receiving a certificate, a subscriber is committed to check its contents, particularly the correctness of the data and complementariness of a public key with the private key he/she/it possesses. If the certificate has any faults that cannot be accepted by the subscriber, the certificate should be immediately revoked (it is equal to lack of approval of the valid certificate expressed by the subscriber).

Certificate acceptance means occurrence of one of the following things within 7 days of the reception of a certificate:

- in the instance of approval of a certificate that was confirmed by a subscriber in a statement confirmed the handwritten signature or,
- lack of certificate revocation in above mentioned period.

Certificate acceptance is univocal to the subscriber's stating that prior to applying the public key or private key associated with it to any cryptographic operation, he/she/it thoroughly familiarized with agreement made with Unizeto Technologies S.A.

Lack of certificate acceptance for reasons other than resignation from services means a necessary to revoke the certificate and to issue a new certificate. Issuance of new certificate is possible only after receipt of notice of refusal to accept a certificate or on the basis of revocation request with the note added to the request that that the block of code PUK occurred during the first unlock the card.

If the reason for rejection was to block a Personal Unlocking Key (PUK), the certification authority might issue a new certificate on the basis of the same agreement with charging a fee for the new device. Such a decision must be taken only by the security inspector.

4.4. Recertification

Recertification of a certificate means replacement of a certificate being used (**currently valid**) with a new certificate without changing the public key or any other information in the certificate except a new key, certificate serial number and validity period.

Recertification (renewal) is performed only within the validity period of current certificate, on subscriber's or applicant representative demand and must be preceded by subscription of a suitable request form to the registration inspector or the other person who acts as a trusted role and verifies subscribers' identity and correctness of submitted certification application; authorizes certification request.

Recertification procedure can be also applicable for the certificate evidences. In such a case all customers of the certification authority should be informed about procedure execution.

CERTUM provides the services of recertification of the same pair of cryptographic keys upon subscriber's request (within the validity period of the certificate currently held by the subscriber and to itself. If the recertification procedure turns successful, the certificate and certificate evidence are not revoked or published on the Certificate Revocation List.

4.5. Certification and rekey (key update)

Certification and rekey (key update) occurs when a subscriber (already registered) generates a new key pair (or order a certification authority to generate such key pair) and requires issuance of a new certificate confirming possession of a newly created public key. Certification and rekey should be interpreted as follows:

- **key certification** is not associated with any valid certificate and is used by subscribers to obtain one or more (usually additional) certificate of any type, not necessarily within the same certification policy,
- **rekey** refers to a particular certificate, indicated in the request; due to above new certificate includes the same content; the only differences are: a new public key, a serial number, a validity period and a new certification authority signature; rekey may also be referred to as certificate renewal.

Certification and rekey is performed only on subscriber's demand and must be preceded by submission of a suitable electronic request to the registration inspector or the other person who acts as a trusted role and verifies subscribers' identity.

Modification of a certificate means replacement of a certificate being used (**currently valid**) with a new certificate in which – in contrast to the certificate being replaced – some of the data can be modified:

- public key affiliated with at least one of information presented below,

- the name of position at work or the name of performing role (authorization required),
- name of organizational unit or address of represented entity (appropriate documents required),
- subscriber's postal address, email address, fax and telephone number,
- other changes of certificate's extensions.

Modification request is available in an electronic form via CERTUM WWW site and must be confirmed by the registration inspector or other authorized person confirming identity.

4.6. Certificate revocation and suspension

Qualified certification service provider CERTUM provides a 24x7 capability to submit a revocation request.

Certificate revocation or suspension does not affect transactions made before revocation or suspension or obligations being result of following of present Certification Policy and Certification Practice Statement.

Certificate suspension is temporary (usually lasts until explanation of reasons of the suspension) and may be requested only by employee of CERTUM. **Possible unsuspension must be not later than within 7 calendar days of such suspension.**

4.6.1. Circumstances for certificate revocation

A basic reason for revoking a subscriber's certificate is loss of control (or even suspicion of such a loss) over a private key being owned by the subscriber of the certificate or material breach of obligation or requirements of Certification Policy or Certification Practice Statement by the subscriber. Revocation is performed also on subscriber's or requester's demand.

Certificate revocation request may be submitted to Primary Registration Authority directly or by fax or phone call.

4.6.2. Who can request certificate revocation

CERTUM complies with the general principle that only person who is the subject of a certificate, is indicated in the certificate or is a subscriber's requester may submit subscriber's certificate request revocation. However, there are situations when revocation request may be submitted by other interested parties. The list of such parties and the situations in which this can occur are presented in the Certification Practice Statement

4.6.3. Procedure for certificate revocation

Certificates are revoked or suspended after successful verification of the request.

If a revocation request was submitted and the identity of requester cannot be authenticated within 1 hour from reception of the requests such certificate is suspended.

Information about the revoked or suspended certificate is placed on **Certificate Revocation List**, issued by the certification authority.

A certification authority submits proof of the certificate revocation or decision about cancellation of the request, along with the reasons for the cancellation to the entity requesting certificate revocation.

4.6.4. Certificate revocation grace period

CERTUM guarantees that the maximum grace period for revocation request is 1 hour from reception of the request.

Information concerning certificate revocation is stored in CERTUM database. Revoked certificates are placed on Certificate Revocation List (CRL) according to disclosed CRL publishing periods.

4.6.5. Circumstances for certificate suspension

Suspension may be carried out solely in case of the data set in the revocation request could raise a reasonable suspicions, revocation request was submitted by phone call and the identity of requester cannot be authenticated within 1 hour from reception of the requests, if there is suspicion that the subscriber have not full capacity to enter into legal transactions, other circumstances that require explanations from subscriber, requester or applicant

Certificate suspension request contains similar information as in the case of a revocation request.

4.6.6. Who can request certificate suspension

Suspension request may be submitted only by the CERTUM personnel.

4.6.7. Procedure of certificate suspension and unsuspension

The suspension procedure is carried out analogically to revocation procedure. After the verification of application, certification authority changes a status of certificate for the suspended and places it on Certificate Revocation List (**certificateHold** as the reason of suspension.)

Certificate unsuspension requires a request of the security inspector. In the case of legitimate request the certification authority removes the certificate from the Certificate Revocation List.

The period of the suspension cannot be longer than 7 days. After this period a suspended certificate shall be revoked.

If during the period of suspension of the qualified certificate the certificate is revoked, then the date of the certificate revocation is the same as the suspension beginning date.

A certification authority submits proof of the certificate suspension or unsuspension or decision about cancellation of the request, along with the reasons for the cancellation to the requesting entity.

4.6.8. Limitation on suspension grace period

CERTUM guarantees the grace period in suspension request processing, as well as availability of certificate status verification to be the same as the in case of certificate revocation (see Chapter 4.6.4).

4.6.9. CRL issuance frequency

CERTUM QCA issues Certificate Revocation List.

Every Certificate Revocation List is updated at least once a day[10]. Notwithstanding, the new CRL is published in the repository after every certificate revocation. In the case of revocation of the certificate this certificate is immediately published on Certificate Revocation List (see Chapter. **Błąd! Nie można odnaleźć źródła odwołania.**).

4.6.10. Certificate Revocation List checking

A relying party, upon receiving an electronic document signed by a subscriber, is obligated to check whether a public key certificate, corresponding to the subscriber's private key used for creating digital signatures, is not placed on Certificate Revocation List. The relying party is obligated to retain a current CRL.

4.7. Time – stamping service

The primary objective of time-stamping service, provided by the time – stamping authority CERTUM QTSA is to mark an electronic documents, electronic signatures, electronic transactions, etc. with a reliable time. Timestamp is a proof that data object existed before the date placed in this timestamp.

Procedure of obtaining a time – stamp issued by time – stamping authority is carried out as follows

- applicant sends a request containing the value of the digest (associated with document, message etc.), the identifier of the hash function and the session identifier (*nonce*); the request shall contains OID policy used for the timestamp token issuance; the format of issuance is default in the case of lack of identifiers,
- time – stamping authority verifies completeness and correctness of application,
- time – stamping authority generates a timestamp,
- time – stamping authority submits a timestamp token to the requesting entity,
- requesting entity verifies the correctness of timestamp token:

4.8. On-line certificate status verification availability

CERTUM provides real-time certificate status verification service. This service is carried out on the basis of OCSP, laid down in RFC 2560[11]. Using OCSP, it is possible to acquire more frequent and up-to-date information (in comparison to sole CRL usage) about a certificate status.

OCSP operates on the basis of **request – response** model. As a response for each request, OCSP server, providing services for CERTUM, supplies the following information about the certificate status:

---

[10] Notification of the time of the next issuance may be also included in the contents of current CRL (see contents of the field **NextUpdate**, Chapter 7.2). Contents of this field describe not excessive date of the next CRL issuance. Publication of the succeeding CRL can be also made before this date. In the case of CERTUM, value of this field is set to one month (except **Certum CA**).

[11] RFC 2560 *Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP.*

- **good** – meaning a positive response to the request, which should be interpreted as confirmation of certificate validity,
- **revoked** – meaning the certificate has been revoked,
- **unknown** – meaning the certificate has not been issued by any of the affiliated certification authorities.

Certificate status is available in real-time

4.9. Data Validation Service

CERTUM QDVCS activity is based on DVCS protocol described in RFC 3029[12]. According to this protocol validation may applies to confirm validity of digitally signed document, timestamp tokens, data validation tokens and to confirm validity of public key certificates and the certificate of possession of data within a specified time and create on the request certificate (DVC) confirming this fact and to produce the certificate of claim of possession of data.

Procedure of obtaining data validation token is carried out as follows:

- an applicant submits the request containing information about types of validation and validated data,
- a data validation and certification authority server verifies format of the request, downloads type of validation and identifier of certification policy,
- a data validation and certification authority server creates token and sends it to applicant,
- an applicant checks the correctness of the token.

4.10. Delivery Authority Service

CERTUM QDA issues evidences of receipt and submission (including official evidences of receipt and submission). These evidences refer to documents submitted by subscribers to public entities with the system used **CERTUM QDA** authority or vice versa – to documents submitted by public entities to subscribers.

Procedure for official evidences of receipt is executed as follows:

- applicant (sender) sends an electronic document through dedicated system to **CERTUM QDA** with the request to forward this document to the indicated recipient (*public entity*),
- **CERTUM QDA** authority verifies format of the request, its completeness and correctness,
- **CERTUM QDA** authority submits the request to the recipient's tele-information system and issues official evidence of receipt,
- **CERTUM QDA** submits official evidence of receipt to the recipient and the sender,
- requesting entity checks completeness and correctness of evidence.

---

12 *RFC 3029 Internet X.509 Public Key Infrastructure: Data Validation and Certification Server Protocols*

Issuance of evidences of receipt is provided similarly as issuance of official evidences of receipt but in this case the sender of electronic document is a *public entity* and recipient is not a *public entity*.

Procedure of issuance of evidences of submission and official evidences of submission is carried out analogically to issuance of evidences of receipt and official evidences of receipt.

4.11. Deposits token issuance service

CERTUM QODA enables the users to deposit any object in the repository, multiple download and release them. Deposited objects are stored in a manner that enables the users to download or release them in the state they were at the time of deposit. Authorized user of CERTUM QODA services can also browse the entries relating to the deposited objects and make decisions to download or release an object from the deposit.

Deposits authority **CERTUM QODA** provides the following services:

- the issuance of token of object deposit entry,
- the issuance of token of object release from the deposit,
- the issuance of certified token of object release from the deposit,
- the issuance of token of download an entry from the deposit,
- the issuance of certified token of download an entry from the deposit,
- the issuance of token of download an object from the deposit,
- the issuance of certified tokens of download an object from the deposit.

The process of obtaining tokens, issued by the object deposits authority, is executed as follows:

- requester (sender) sends to **CERTUM QODA** authority a request for provision of any of the above services,
- **CERTUM QODA** authority verifies format of the request, its completeness and correctness,
- **CERTUM QODA** authority executes operations appropriate to the received request and on processing it, certification authority issues a relevant deposit token.
- **CERTUM QODA** authority submits deposits tokens to the requester (sender),
- requesting entity checks completeness and correctness of tokens.

CERTUM QODA records the fact of receipt of the request, although it is not obliged to their storage.

4.12. Registries and repositories tokens issuance service

CERTUM QRRA enables the users to place an entry into the registry or an entry with data objects associated with him. Entries and objects structure depends on registry class and is validated before placing them in the registry or/and repository. Entries and objects may be repeatedly downloaded, as well as modified. Recorded entries and objects are stored in a manner that allows downloading them in the state they were at the time of registration. Authorized user

of CERTUM QRRA services can also browse the entries and makes decision to download an entry and/or an object from the registry or the repository.

Registries and repositories authority **CERTUM QRRA** provides the following services:

- **token of registry entry,**
- **token of download an entry from the registry**,
- **token of download an object from the repository,**
- **certified token of download an entry from the registry**,
- **certified token of download an object from the repository,**
- **token of registry entry modification,**
- **token of object modification in the repository**

To obtain tokens, issued by the object registries and repositories authority the following process should be executed:

- requester (sender) sends a request for provision of any of the above services to **CERTUM QRRA** authority,
- **CERTUM QRRA** authority verifies format of the request, its completeness and correctness,
- **CERTUM QRRA** authority executes operations appropriate to the received request and as a result issues a relevant registries and repositories token.
- **CERTUM QRRA** authority submits registries an repositories token to the requester (sender),
- requesting entity checks completeness and correctness of tokens.

CERTUM QRRA records the fact of receipt of the request and is obliged to retain this requests for the period prescribed in an agreement between a subscriber and a CERTUM QRRA authority.

4.13. Attribute certificates issuance service

Attribute certificates authority **CERTUM QACA** provides the services of issuing, managing and revoking attribute certificates. Services are delivered only on the basis of the chain of registration authorities or points of the identity and attributes verification network. Contact addresses with them are listed in the repository of CERTUM

Certificates are issued on the basis of a request for issuance of an attribute certificate. An application might be submitted in electronic or paper form. An application is submitted to a registration authority or points of the identity and attributes verification.

An application should contain at least the following information:

- the name and surname of entity that has requested for certificate
- the attributes indication[13] that should be placed in the attribute certificate

[13] This indication is based on the list of the attributes published in repository by CERTUM QACA. The list can be updated by the attribute certificate authority.

- the data of an entity who hands over the rights to use the attributes listed in the preceding point,
- validity period of the certificate,
- information about revocation,
- information about publication of attribute certificates (optionally in the CERTUM repository).

If the usage of an attribute placed in certificate requires providing any evidence, an application must be submitted with appropriate declaration. Additional documents (i.e. declaration) are also required in the case of transfer of the rights for using an attribute/attributes to the person used the certificate (i.e. the user authorized in a relevant document).

Confirmation of the rights mentioned above might be carried out in a point of the identity and attributes verification or by the notary. This confirmation is carried out in accordance with procedure developed for each attribute supported by the CERTUM QACA.

The request is submitted by registration authority or points of identity and attributes verification to the Primary Registration Authority where a registration inspector prepares a token **of certification request** and later sends it to CERTUM QACA authority.

4.14. Events recording and audit procedures

In order to manage operation of CERTUM system and supervise CERTUM users and personnel efficiently, all events occurring in the system and having essential impact on CERTUM security are recorded.

4.14.1. Types of events recorded

CERTUM event logs store records of every activity generated by any software component within the system. Activities are recorded with the duties of the role of a qualified certification service provider. Description of the event is recorded in the Certification Practice Statement and other documents of CERTUM.

4.14.2. Frequency of event logs checking

In order to identify possible illegal activities, the system administrator and audit inspectors should analyze the information of event logs at least once a working day. Additionally, the security inspector is obligated to execute a review and assessment of the correctness and completeness of event logs in the security logs and to checks the consistency with CERTUM security procedures once a month. The result of internal audit should be response to the security requirements. The security inspector records these results in the security logs.

4.14.3. Event journals retention period

Records of registered events are stored in files on system disk for at least 6 months. In this time they are available *on-line*, on every authorized person's or process demand. After this period, the logs are stored in archives, and may be accessed only *off-line*.

Archived journals are retained for at least 20 years.

4.14.4. Protection of event logs

An event log may be reviewed solely by the authorized personnel or auditors. The records of events cannot be modified.

Archives should be electronically signed and marked with time.

4.14.5. Procedures for event logs backup

CERTUM security procedures require that the event logs should be subjected to copy in accordance with an established schedule. These backups are retained in main and alternate site of CERTUM. Backup copies are signed with a timestamp

4.15. Records archival

It is required that all data and files related to registration of information associated with the system security, requests submitted by subscribers, information about subscribers, issued certificates and CRLs, keys, used by certification and registration authorities, and whole correspondence within CERTUM and with the subscribers should be subjected to archive.

Archive might also contain the certificates issued 25 years (and more) in the past.

The archive also contains paper documents used to provide certification services. Archived paper documents are retained for at least 20 years.

Archived copies of electronic data are retained in main and alternate site of CERTUM.

It is recommended to encrypt and timestamp the archive. A key used for archive encryption is managed by the certification authority security inspector or system administrator.

4.16. Key changeover

Procedure for key changeover applies to the keys of certification authorities **CERTUM QCA** and other authorities providing certification services and it describes procedure for key update (rekey) for a certificate, CRL, timestamps, verified certificate status, validated data and receipt or submission tokens signing (including official tokens), which replaces a currently used key.

Rekey procedure is based on issuance of special certificates (certificate evidence) by the National root (NCCert).

Every key changeover is announced in advance by means of CERTUM repository.

4.17. Key security violation and disaster recovery

Security policy, executed by CERTUM, takes into consideration the physical corruption to the computer system of CERTUM, including network resources corruption, software and

application malfunction and loss of important network services, associated with CERTUM interests. It primary addresses power cuts and damages of the network connections.

CERTUM provides a capability to submit a revocation request, creating and publishing of CRLs also in the case of corruption restraining CERTUM activity through activate emergency facility allowing provision of CERTUM services in accordance with the requirements described in Chapter 4.6.9

In the case of CERTUM's private key compromise or suspicion of such compromise the National root NCCert is immediately informed about such fact and all certificate users are immediately informed about the compromise of the private key, by means of electronic mail. The certificate evidence corresponding to the compromised key and all certificates in the certification path of the compromised certificate are revoked. New certificates for subscribers are generated and submitted to them, without charging a fee for the operation; subscriber may refuse to accept an issued certificate.

4.18. Certification authority termination or service transition

CERTUM is obligated to notify about their intention to terminate services as the authorized certification authority (at least 90 days in advance) its subscribers who hold active (unexpired and unrevoked) certificates issued by this authority and the National root (NCCert) about decision to terminate its services.

All certificates which remain active in the declared moment of service termination have to be revoked and published in Certificate Revocation List. Certificates and private keys of certification authority **CERTUM QCA**, time – stamping authority **CERTUM QTSA**, online certificate status protocol authority **CERTUM QOCSP,** data validation and certification server authority **CERTUM QDVCS**, delivery authority **CERTUM QDA**, object deposits authority **CERTUM QODA**, registries and repositories authority **CERTUM QRRA** and attribute certificates authority **CERTUM QACA** have to be revoked and keys destroyed.

CERTUM pay compensations of issuance fees to the subscriber or his/her/its sponsor; compensations should be proportional to remaining validity period of the certificate.

Before a certification authority ceases its services, it is obligated to transmist the data, directly connected with certification services, to the minister in charge of the economy or to the entity designated by him.

To provide continuity of the certificate issuance services to subscribers, a terminating certification authority may sign up an agreement with another certification authority offering similar services, related to issuance of replacement certificates for certificates of the terminated certification authority remaining in usage.

5. Physical, organizational and personnel security controls

This Chapter describes general requirements concerning control, physical and organizational security, as well as personnel activity, used in CERTUM mainly in the time of key generation, entity authenticity verification, certificate issuance and publication, certificate revocation, audit and backup copy creation.

5.1. Physical security controls

5.1.1. CERTUM physical security controls

Network computer system, operator's terminals and information resources of CERTUM are located in the dedicated area, physically protected against unauthorized access, destruction or disruption to its operation. These locations are monitored.

CERTUM is located in the Unizeto Technologies S.A. seat, at the following address: ul. Bajeczna 13, Szczecin, Poland.

Physical access to the seat and CERTUM area is controlled and monitored by the integrated alarm system. Manned reception and outside security guards operate 24 hours a day. Fire and flood prevention system, intrusion detection system and emergency power system (securing against temporary and long-term power cuts) are employed.

Copies of passwords, PIN numbers and cryptographic cards are stored in safe-deposit box outside CERTUM seat. Offsite storage affects also archives, current copies of information processed by the system and full installation version of CERTUM applications..

Paper and electronic media containing information possibly significant for CERTUM security after expiration of the retention period (see Chapter 4.15) are destroyed in special shredding devices.

5.1.2. Registration authority security controls

Computers of Primary Registration Authority issuing certificates are located in specially designated area and operate in on-line mode (have to be connected to the network). Access to these computers is physically secured against unauthorized individuals. Computers may be operated solely by authorized individuals. Computers located in points of the identity and attributes verification are protected in accordance with the requirements applicable to the notary offices. Computers located in other registration authorities are protected in accordance with the agreement between CERTUM and administrator of registration authority

5.2. Organizational security controls

CERTUM provides organizational security controls by means of:

- trusted roles which should be manned with one or more individuals – in the certification authority and registration authority
- combine trusted roles,

- number of roles
- range of responsibilities and obligations associated with the acted role,
- identification and authentication of the personnel.

Extended description of the organizational security controls is published in the Certification Practice Statement and other CERTUM's documents.

5.3. Personnel controls

CERTUM has to be sure that the person performing his/her job responsibilities, arising from the acted role in a certification authority or a registration authority system:

- has graduated from at least the secondary school,
- has signed a work contract or other civil agreement describing his/her role in the system and corresponding responsibilities,
- has been subjected to required training on the range of obligations and tasks, associated with his/her position,
- has been trained in the field of personal data protection,
- has signed an agreement containing clause concerning sensitive (from the point of view of CERTUM security) information protection and confidentiality and privacy of subscriber's data,
- does not perform tasks which may lead to a conflict of interests between a certification authority and a registration authority acting on behalf of it.

5.3.1. Training requirements

Personnel performing roles and tasks arising from the employment in CERTUM or its registration authority have to complete following trainings: regulations of Certification Practice Statement of CERTUM's Qualified Certification Services, regulations of Certification Policy of CERTUM's Qualified Certification Services, regulations of procedures and documentation related with played role, procedures and security controls employed by a certification authority and a registration authority, system software of a certification authority and a registration authority, responsibilities arising from roles and tasks performed in the system, procedures executed upon system malfunction or disruption of certification authority operations.

5.3.2. Retraining Frequency and Requirements

Trainings described in Chapter have to be repeated or supplemented always in situation when significant modification to CERTUM or its registration authority operation is executed or when new version of CPS or CP is introduced.

6. Technical Security Controls

This Chapter describes procedures for the generation and management of a cryptographic key pair of a certification authority, a registration authority and a subscriber, including associated technical requirements.

6.1. Key Pair Generation

Procedures for the key management apply to secure storage and usage of the keys being held by their owner. Particular attention is required for generation and protection of private keys of CERTUM, influencing secure operation of the whole public key certification system.

CERTUM QCA certification authority owns at least one certificate that is used for signing of qualified certificates, public keys certificates, other certificates and CRL lists.

Key pairs owned by each certification authority should allow:

- certificate and CRL signing;
- signing messages, transmitted to subscribers,
- signing electronic confirmations (including cross-certificate)
- negotiation of keys used for confidential information exchange between the authority and its environment (the operational key).

An electronic signature is created by means of RSA algorithm in combination with SHA-1 cryptographic digest, while a key agreement employs Diffie-Hellman[14] algorithm.

6.1.1. Key pair generation

CERTUM certification authority keys are generated within CERTUM seat, in the presence of selected, trusted group of persons (comprising additionally security inspector and system administrator). The group is required only in the case of certificate and CRL signing key generation and timestamp tokens issuance. The operational keys may be generated in the presence of the security inspector and system administrator. Key pairs of certification authorities operating within CERTUM are generated on designated, authenticated workstation and connected to hardware security module, complying with the FIPS 140-2 Level 3 or superior requirements.

Registration authority operators possess only keys for signing (confirming) a subscriber's request and messages submitted to a certification authority. These keys are generated by the operator (in the presence of the security inspector) by means of authenticated software supplied by a certification authority and connected with certified hardware security module complying with FIPS 140-2 Level 2 requirements.

Subscriber's key pair shall be generated only by **CERTUM QCA.**

[14] **Diffie-Hellman protocol are not used to generate of secure signatures.**

6.1.2. Private Key Delivery to Entity

Subscriber's keys are generated by **CERTUM QCA** on cryptographic electronic card or in hardware security module and may be delivered to the subscriber personally or by means of registered mail. Data for the card activation (including PIN/PUK) or key decryption (password) are submitted separately from the media containing the key pair; the issued cards are personalized and registered by the certification authority.

6.1.3. Certification authority public key delivery to relying parties

Public keys of a certification authority issuing certificates to subscribers are distributed solely in a form of certificates complying with ITU-T X.509 v.3 recommendations. In the case of **CERTUM QCA** certification authority, certificates have a form of certificate issued by the National root NCCert

CERTUM certification authorities distribute their certificates in two different methods:

- placement in the publicly available web repository of CERTUM at http://www.certum.pl/repozytorium.
- distribution together with a dedicated software (e.g. web browsers, email clients, etc.), which allows usage of services offered by CERTUM.

6.1.4. Keys Sizes

Sizes of keys deployed in CERTUM by registration authority operators and subscribers are presented in Certification Practice Statement

6.2. Private Key Protection

Every subscriber, certification authority operator and registration authority operator store his/her/its private key employing a credible system preventing from private key loss, revelation, modification or unauthorized access.

Infrastructure keys used to ensure the confidentiality of communications and for purposes of data protection are retained in the individual key modules or in the other technical components.

6.2.1. Standards for Cryptographic Modules

Hardware security modules emploved by a certification authority, time – stamping authority, online certificate status protocol authority, data validation and certification server authority, delivery authority, registration authorities and subscribers comply with the requirements of FIPS 140-2 standard or ITSEC (*ITSEC v 1.2 issued by European Committee, Directories XIII/F, 1991*) requirements.

6.2.2. Private Key Multi-Person Control

Multi-person control of a private key applies to private keys of all certification authorities. The keys (symmetric or asymmetric) are distributed according to accepted threshold method (so called shadows) and transferred to authorized **shared secret holders**. Accepted number of a shared secret and required number of secrets allowing private key restoration are disclosed in Certification Practice Statement.

Shared secrets are stored on cryptographic cards, protected by a PIN number and transferred in an securely manner to their holders.

6.2.3. Private Key Escrow

Private keys of certification authorities or of subscribers requesting generation of a key by CERTUM authorities or which are available to the public are not subjected to escrow.

6.2.4. Private Key Backup

Certification authorities operating within CERTUM create a backup copy of their private key. The copies are used in the case of execution of standard or emergency (e.g. after disaster) key recovery procedure.

Shared secrets, copies of secret encryption key, as well as PIN numbers protecting the keys are retained in various, physically protected locations. None of these locations holds a set of cards and PIN number allowing restoration of certification authority key solely with the usage of this cards or PINs.

CERTUM does not retain copies of registration authority operator's and subscriber's private keys.

6.2.5. Private Key Archival

Private key of certification authority used for electronic signature creation are not archived and shall be destroyed immediately after the cessation of using it or after expiry of the public key certificate corresponding to private key after its expiration or revocation.

6.2.6. Private Key Entry into Cryptographic Module

Operation of entering of a private key into a cryptographic module is carried out in the following cases:

- in the case of creation of backup copies of private keys stored in a cryptographic module, it may be occasionally necessary (e.g. in the case of the module corruption or malfunction) to enter a key pair into a different security module,
- it is necessary to transfer a private key from the operational module used for standard operations by the entity to another module; the situation may occur in the case of the module defection or necessity of its destruction.

Entry of a private key into the security module is a critical operation, therefore measures and procedures, preventing key revelation, modification or forgery are implemented during execution of the operation.

6.2.7. Method of Activating Private Key

All private keys of certification authority **CERTUM QCA**, time – stamping authority **CERTUM QTSA**, online certificate status protocol authority **CERTUM QOCSP,** data validation and certification server authority **CERTUM QDVCS**, delivery authority **CERTUM QDA**, object deposits authority **CERTUM QODA**, registries and repositories authority **CERTUM QRRA** and attribute certificates authority **CERTUM QACA**, entered into the module after their generation, import in an encrypted form from another module or restoration from shared secrets by the authorized person, remain in the active state until their physical erasure from the module or removal from CERTUM services.

Signing private keys of registration authority operators, used for information signing, are activated after authentication of the operator (PIN number provision) and only for the time of a single cryptographic operation requiring usage of this key. Upon the completion of this operation the private key is automatically deactivated and has to be activated again before execution of another cryptographic operation.

Other private keys, e.g. used for authentication of registration authority applications or creation of encrypted network channel are automatically activated for a period of a single session, immediately after authentication of the operator. The completion of a session deactivates all previously activated private keys.

6.2.8. Method of Deactivating Private Key

In the case of CERTUM, deactivation of a private key is carried out by the security inspector only in the situation when the validity period of the private key has expired, the key has been revoked or there is immediate requirement to temporary suspend the activity of the system. Deactivation of a private key is carried out by resetting the memory of cryptographic module. Every private key deactivation is recorded in the event journal.

In the case of a subscriber or a registration authority operator, private signing key deactivation is carried out immediately after creation of an electronic signature.

6.2.9. Method of Destroying Private Key

Erasure of private keys of subscriber or registration authority operators involve respectively their erasure from the media (electronic card, hardware security module, etc), destruction of the media (electronic card) or at least taking over the control of the key in the case of the card preventing definite private key erasure from this card.

A Private key destruction of certification authority, time – stamping authority, online certificate status protocol authority, data validation and certification server authority, delivery authority, object deposits authority, registries and repositories authority and attribute certificates authority means physical destruction of the electronic cards and/or other media used for storage of copies or archives of shared secrets.

6.3. Other Aspects of Key Pair Management

6.3.1. Public Key Archive

The purpose of public key archive is to provide possibility of an electronic signature verification after removal of a certificate from the repository. It is extremely important in the case of providing of non-repudiation services, such as a timestamp service.

An archive of public keys involves storing the certificates containing these keys.

Within CERTUM, only the keys used for electronic signature verification are subjected to archival.

Public keys are retained in the public key archive for the period of 25 years.

6.3.2. Usage Periods of Public and Private Keys

Usage period of public keys is defined by the value of the field **validity** of every public key certificate. Validity period of a private key may be shorter than validity period of certificate (which results from the possibility to cease private key usage at any time).

Standard values of maximal usage period of certification authority, time – stamping authority, online certificate status protocol authority, data validation and certification server authority, delivery authority certificates are described in Table 8, while subscriber's certificates are presented in Table 9.

Starting date of the certificate validity period complies with the date of its issuance. It is not allowed to set this date in the future or in the past.

Tab. 8 Maximal usage periods of certification authority certificates and certificates of infrastructure keys.

Owner and key type		Main key usage		
		RSA for certificate and CRL signing	RSA for token signing	RSA key infrastructure
CERTUM QCA	certification authority certificate or certificates of infrastructure keys	5 years	–	3 years
	private key	3 years	–	3 years
CERTUM QTSA CERTUM QOCSP CERTUM QDVCS CERTUM QDA CERTUM QODA CERTUM QRRA	certification authority certificate	–	5 years	–
	private key	–	5 years	–
CERTUM QACA	certification authority certificate	5 years	–	–
	private key	3 years	–	–

Tab. 9 Maximal usage periods of the qualified certificate

Owner and key type		Main key usage
		RSA for secure electronic signatures
Private persons	Qualified certificate	2 years
	Private key	2 years

Tab. 10 Maximal usage periods of the attribute certificates

Owner and key type	Maximal validity period
Private persons	2 years

6.4. Computer Security Controls

Tasks of registration authorities and certification authorities operating within CERTUM are carried out by means of credible hardware and software, being a part of the system which complies with the requirements laid down in the document *Information Technology Security Evaluation Criteria*[15] (ITSEC), at least level E3.

6.5. Network Security Controls

Servers and trusted workstations of CERTUM system are connected by the designated and separated two-level internal LAN network. Access from the internet to any segment is protected by means of intelligent firewall of the E3 class (according to ITSEC) and by means of intrusion detection systems (IDS).

6.6. Time stamps as a security control

Request created within CMP and CRS protocol do not require signing with trusted time. In the case of any other messages exchanged between a certification authority, a registration authority and a subscriber, it is recommended to apply time stamps.

Time stamps for internal needs can be created within CERTUM system in accordance with the recommendation RFC 3161.

[15] Information System Security Controls Assesment Criteria

7. Certificate, CRL, timestamp token profile

Certificate profiles, qualified certificates profiles and Certificate Revocation List profile comply with the format described in ITU-T X.509 v.3 and profiles included in *Rozporządzeniu Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego*. The profile of OCSP token complies with the requirements of RFC 2560, while the profile of timestamp token complies with *ETSI Time stamping profile, TS 101 861 v1.2.1*. The profile of data validation tokens complies with the requirements of RFC 3029, while the profile of receipt or submission tokens (including official tokens) complies with *uniUPO* i *uniUPP* profiles prepared by Unizeto Technologies S.A. on the basis of requirements defined in polish standard PN-ISO/IEC 13888-3:1999 *Technika informatyczna. Techniki zabezpieczeń. Niezaprzeczalność. Mechanizmy wykorzystujące techniki asymetryczne.*.

7.1. Certificate Profile

Following the X.509 v.3 standard, a certificate is the sequence of the following fields: the first one contains the body of certificate (**tbsCertificate**), the second one– information about algorithm used for certificate signing (**signatureAlgorithm**), while the third one – an electronic signature created on the certificate by a certification authority (**signatureValue**).

7.1.1. Contents of the certificate

The contents of a certificate indude values of **basic fields** and **extensions** (standard, described by the norm, and private, defined by the certification authority).

7.1.1.1. Basic fields

CERTUM supports the following certificate basic fields described in Table 11:

Tab. 11 Profile of the basic fields of certificates

Field name	Value or value constraint	
Version	Version 3	
Serial Number	Unique value for all certificate issued by certification authorities within CERTUM	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (Distinguished Name)	Common Name (CN) =	CERTUM QCA
	Organization (O) =	Unizeto Technologies S.A.
	Country (C) =	PL
	Serial Number (SN) =	Entry number: 1
Not before (validity period beginning date)	Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard. CERTUM clock is	

Field name	Value or value constraint
	known as valid world Stratum I service
Not after (validity period ending date)	Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard. CERTUM clock is known as valid world Stratum I service
Subject (Distinguished Name)	Distinguished names comply with the requirements of: *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002 r. w sprawie określenia warunków technicznych i organizacyjnych dla kwalifikowanych podmiotów świadczących usługi certyfikacyjne, polityk certyfikacji dla kwalifikowanych certyfikatów wydawanych przez te podmioty oraz warunków technicznych dla bezpiecznych urządzeń służących do składania i weryfikacji podpisu elektronicznego.* DN profile depends on type of entity.
Subject Public Key Info)	Encoded in accordance with RFC 3280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key).
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 3280 and in *Rozporządzenie Rady Ministrów z dnia 7 sierpnia 2002.*

7.1.1.2. Extensions fields

CERTUM supports the following fields of extensions described in the Table 12:

Tab. 12 Standard extensions fields profile

Extension	Value or Value constraint	Extension status
AuthorityKeyIdentifier	SHA1 hash of the public key	Non-critical
KeyUsage (użycie klucza)	Allowed key usage. Non-repudiation, bit 1	Critical
ExtKeyUsage	Definition (constraint) of the key usage. This field should be interpreted as constraint of allowed key usage purpose defined in field **keyUsage**	Critical
CertificatePolicies	An information of the **PolicyInformation** type (identifier, electronic address) about a certification policy, applied by the issuing authority: • iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 1 – for qualified certificates • joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32) – for certificate evidences • iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 10 – for certificates of infrastructure keys	Critical
PolicyMapping	(Optional) This field contains one or more pairs of OID, defining equivalency of the issuer	Non-critical

Extension	Value or Value constraint	Extension status
	policy with the subject policy	
IssuerAlternativeName	(Optional) An alternative name of the certificate issuer	Non-critical
SubjectAlternativeName	An alternative name of the certificate subject	Non-critical
BasicContraints	The extension allows definition whether the subject of the certificate is a certification authority (**cA** field) and what is the maximum (assuming certification authorities are ordered hierarchically) number of certification authorities on the certification path from the considered authority to the subscriber (**pathLength** field)	Critical
CRLDistributionPoints	The extension defines network addresses hosting current CLR, issued by the certification authority (i.e. http://crl.certum.pl/qca.crl)	Non-critical
SubjectDirectoryAttributes	The extension contains additional attributes associated with the subscriber and supplementing information described in the field **subject** and **subjectAlternativeName**	Non-critical
AuthorityInfoAccessSyntax	(Optional) The field indicates the method of information and service provision by the issuer of the certificate (i.e. http://qocsp.certum.pl)	Non-critical
QCStatements	A statement that the certificate is a qualified certificate [16]. Transaction limit Indication of the authorization	Non-critical
BiometricSyntax	(Optional) An information about biometric parameters of the subject of the certificate: a hand-written signature and a photo.	Non-critical

7.1.2. Electronic signature algorithm identifier

The field of **signatureAlgorithm** contains a cryptographic algorithm identifier describing the algorithm applied for an electronic signature created by a certification authority on the certificate. In the case of CERTUM, RSA algorithm, in combination with SHA-1 cryptographic hash is used.

7.1.3. Electronic signature field

The value of the field **signatureValue** is a result of execution of cryptographic hash function algorithm for all fields of a certificate, described by the values of the certificate body (**tbsCertificate** fields) and encryption of the digest with a private key of the issuing authority.

16 This is the statement of Unizeto Technologies SA that qualified certificates are issued in accordance with the *Act on Electronic Signature*. Unizeto Technologies SA declares the consistency of the issued qualified certificates with the ETSI TS 101 861 specification [21], i.e. the statement always includes the following value of the object identifier: {itu-t (0) identified-organization (4) etsi (0) id-qc-profile (1862) 1 1}.

7.2. CRL profile

Certificate Revocation List (CRL) consists of three fields. The first field (**tbsCertList**) contains information about revoked certificates, the second and the third field - **signatureAlgorithm** and **signatureValue** contain information about respectively: the identifier of the algorithm used for list signing, and electronic signature created on the certificate by a certification authority. The meaning of the last two fields is the same as for the certificates.

The field of **tbsCertList** is the sequence of mandatory and optional fields described in the Table 13.

Tab. 13 CRL profile

	Field name	Critical	Value or Value constraint
	Version	n/d	CRL format version (3)
	Signature		The identifier of the algorithm used by a certification authority to sign CRL; CERTUM authorities sign **CRL** by means of **sha1WithRSAEncryption** algorithm
	Issuer		The name of the certification authority issuing CRL **(CERTUM QCA)**
	ThisUpdate		CRL publication date
	NextUpdate		Announcement of the date of the next CRL publication
	RevokedCertificates		The list of revoked certificates. The information consist of three sub-fields: • **userCertificate** - serial number of a revoked certificate • **revocationDate** - date of the certificate revocation • **crlEntryExtensions** - contains additional information about revoked certificates (optional)
	crlExtensions		An optional, extended information about Certificate Revocation List (i.e. fields **AuthorityKeyIdentifier** and **cRLNumber**)
	ReasonCode	No	The code of the reason for revocation: • **unspecified** – not specified; • **keyCompromise** – key revelation or compromise; • **cACompromise** – certification authority key revelation; • **affiliationChanged** – subscriber's data modification (affiliation); • **superseded** – certificate renewal; • **cessationOfOperation** – cessation of certificate usage • **certificateHold** – suspension of certificate; • **removeFromCRL** – certificate removal from CRL; • **privilegeWithdrawn** – certificate was revoked due to change of the certificate data concerning subjects role; • **aaCompromise** – applies to attributes certificates; meaning is the same as for withdrawal of privileges;
	HoldInstructionCode	No	Code of the operation on certificate suspension
	InvalidityDate	No	Date of revocation

Revoked certificates remain on Certificate Revocation Lists (issued by CERTUM) for the period of 25 years from the moment of their first appearance on the list.

The End Entity Attribute Revocation List (EARL) profile is identical to Certificate Revocation List. Because of effectiveness of the End Entity Attribute Revocation List management, these revoked attribute certificates are included in other lists than revoked public key certificates.

7.3. Timestamp token profile

Timestamp token, issued by Certum Time-Stamping Authority contains information on timestamp (**TSTinfo** structure), located in **SignedData** structure, signed by time - stamping authority and embedded in **ContentInfo** structure.

The extended description of timestamp token is published in the Certification Practice Statement.

7.4. OCSP response token, data validation token, Evidences of receipt and submission, deposits token, registries and repositories token and attribute certificates profiles

The profiles of on-line certificate status verification (OCSP) tokens, data validation tokens, Evidences of receipt and submission (including official evidences of receipt and submission), deposits tokens, registries and repositories tokens and attribute certificates issued by certification authority **CERTUM QCA**, time – stamping authority **CERTUM QTSA**, online certificate status protocol authority **CERTUM QOCSP,** data validation and certification server authority **CERTUM QDVCS**, delivery authority **CERTUM QDA**, object deposits authority **CERTUM QODA**, registries and repositories authority **CERTUM QRRA** and attribute certificates authority **CERTUM QACA** are described in the document of *Certificates, tokens and notifications profiles management.*

8. Certification Policy management

Every version of Certification Policy is in force (has a **current** status) up to the moment of publication and approval of its new version (see Chapter 8.3). A new version is developed by CERTUM personnel and with the status **requested for comment** supplied to approval questionnaire. Upon reception and inclusion of the remarks from the approval questionnaire, the new version of Certification Policy is supplied for approval. During CP approval process, new version of the document has the status **under approval**. After completion of the approval procedure, a new version of Certification Policy is marked with the status **valid**.

Subscribers are obligated to comply only with the currently valid Certification Policy.

8.1. Changes introduction procedure

Modification to Certification Policy may be a result of observed errors, CP update and suggestions from the affected parties.

Introduced modification may be generally divided into two categories: the one that does not require notification of subscribers, and the one that requires (usually in advance) notification of subscribers.

8.1.1. Items that can be changed without notification

The only items not requiring, according to Certification Policy, notification in advance apply to amendments resulting from implementation of editorial modifications, amendments to the contact information of the person responsible for CP management and changes not having a real impact on considerable group of individuals. Implemented changes do not require approval procedure execution, thus only build number of the document is changed.

8.1.2. Items that require notification

8.1.2.1. List of items

After notification in advance, each and every item of the Certification Policy may be subjected to amendment. Information about every significant modification is submitted to every affected party in the form of indication of a storage point of a new version of Certification Policy with the status **requested for comment**. Suggested modification may by published in the CERTUM repository and transmitted by the means of electronic mail.

8.1.2.2. Comment period

Comments on suggested modifications may be submitted by the affected parties within 10 working days of their announcement. If as a result of the submitted comments, the security inspector administered **significant modification** to the suggested changes, the changes have to be published once more and subjected to assessment. In other cases, a new version of Certification Policy receives the status **under approval** and is subjected to approval procedure

8.1.2.3. Changes requiring new identifier

In the case of amendments which may have influence on extensive group of certification service users, the security inspector may assign a new identifier (Object Identifier) for a modified document of Certification Policy. Identifiers of the certification polices applied by authorities issuing certificates may also be subjected to modification.

8.2. Publication

A copy of Certification Policy is available in an electronic form via:

- WWW site at the address: http://www.certum.pl/repozytorium
- email at the address: info@certum.pl

Three versions (if applicable) of Certification Policy are available (if possible) at the repository and via the email: the currently applicable version, the previous version and the version under approval.

8.3. CP Approval Procedures

If within 10 days of the publication of changes to Certification Policy incorporated on the basis of suggestions made on the stage of its acceptance questionnaire (method described in Chapter 8.2) the security inspector does not receive significant remarks concerning this changes, a new version of the document, with the status **under approval**, becomes a governing document of the certification policy, respected by all subscribers of CERTUM, and the status of the version is changed into **valid**.

Document History

Document modification history		
1.0	20th of August, 2002	Full version of the document. Document approved
1.1	23rd of October, 2002.	Editorial changes, incorporate the comments of the Ministry of Economy, new certification authority added: certificate status verification authority. Document approved.
2.0	1st February, 2005	Certification Policy reduced and adapted to the requirements of the auditors.
2.1	2nd of May, 2005	Change to the company legal form and name (Unizeto Sp. z o.o. changed to Unizeto Technologies S.A,)
2.2	20th of July, 2005	Change of service name from Unizeto CERTUM – Centrum Certyfikacji to CERTUM – Powszechne Centrum Certyfikacji.
2.3	1st of January, 2005	Information about generation of the new certificate evidences added. Highlighting the fact of subscriber's documents copying. Change the fax number.
3.0	15th of July, 2006	New certification services added: certificate status verification services, data validation services, delivery services.
3.1	05th of January, 2007	New certification service added: deposits services, registries and repositories services, and relocation of certification authority „CERTUM - Powszechne Centrum Certyfikacji".
3.2	17th of September, 2007	New certification service added: issuance of attribute certificates service.
3.3	1 st of March, 2008	Updating the profiles of certificates
3.4	14 th of July, 2008	Updating the information about QDVCS
3.5	24 th of July, 2009	Updating the information about recertification (renewal)
3.6	1st of November, 2009	Updating the profiles of certificates

1. Appendix 1: Abbreviations

CA Certification authority

CMP Certificate Management Protocol

CP Certification Policy

CPS Certification Practice Statement

CRL Certificate Revocation List, published usually by the very certificate issuer

DN Distinguished Name

KRIO Krajowy Rejestr Identyfikatorów Obiektów (National Object Identifiers Registry)

OCSP On-line Certificate Status Protocol

PKI Public Key Infrastructure

PRA Primary Registration Authority

PSE personal security environment

RA Registration Authority

RSA asymmetric cryptographic algorithm (name originates form first letters of its developers names: Rivest, Shamir and Adleman), in which single private transformation allows signing or decrypting a message, while single public transformation allows verification and encryption of the message

TSA Time Stamping Authority

TTP trusted third party; institution or its representative bearing other entities trust in the area of protection and authentication controls; bears the trust of both the entity being verified and/or verifying (after PN 2000)

2. Appendix 2: Glossary

Access – ability to use and employ any information system resource.

Access control – the process of granting access to information system resources only to authorized users, applications, processes and other systems.

Attribute certificate – electronic confirmation by which values of the attributes are assigned to a designated person in the certificate and associated with data identifying this person.

Audit – execution of an independent system review and assessment with the aim to test adequacy of implemented system management controls, to verify whether an operation of the system is performed in accordance with accepted Certification Policy and CPS and the resulting operational regulations, to discover possible security gaps, and to recommend suitable modification to control measures, the certification policy and procedures.

Audit data – chronological records of the system activities, allowing reconstruction and analysis of the event sequence and modification to the system, associated with the recorded event.

Authenticate – to confirm the declared identity of an entity.

Authentication – security controls aimed at providing reliability of transferred data, messages or their sender, or controls of authenticity verification of a person, prior to delivery of a classified type of information to the person.

Certificate and Certificate Revocation Lists publication – procedures of distribution of issued certificates and revoked certificates. Certificate distribution involves the submission of a certificate to the subscriber and may involve publication in the repository. Certificate revocation list distribution means publication of the list in the repository, submission to end entities or transferal to entities providing on-line certificate status verification service. In both cases the distribution should be performed with the usage of appropriate means (e.g. LDAP, FTP, etc.).

Certificate Revocation List (CRL) – list, signed electronically by a certification authority, containing serial numbers of revoked or suspended certificates and dates and reasons for their revocation or suspension, the name of the CRL issuer, date of publication and date of the next update. Above data are electronically signed by a certification authority.

Certificate Status Token – electronic data, containing information on current certificate status, certification path, which this certificate belongs to and other information useful for certificate verification, electronically signed by the certificate status verification authority

Certificate Status Verification Authority – trusted third party, providing relaying parties with the mechanisms for the certificate trustworthiness verification, as well as providing additional information on certificate attributes.

Certificate Suspension – special form of certificate (and corresponding key pair) revocation, which results in temporary lack of certificate acceptance in cryptographic operations (irrespective of the status of such operation); suspended certificate is listed on the Certificate Revocation List (CRL).

Certificate update – prior to the certificate validity period expiration the certification authority may refresh the certificate (update it), confirming validity of the same key pair for another, defined in certification policy, validity period.

Certificates revocation – procedures concerning revocation of a key pair (certificate revocation) in the case when an access to the key pair has to be restricted for the subscriber to prevent

possible usage in encryption or signature creation. A revoked certificate is placed on Certificate Revocation List (CRL).

Certification Authority – entity providing certification services, being a part of trusted third party is able to create, sign and create certificates and timestamp and certificate status tokens.

Certification path – ordered path of certificates, leading from a certificate being a **point of trust** chosen by a verifier up to a certificate subjected to verification. A certification path fulfils the following conditions:

- for all certificates Cert(x) included in the certification path {Cert(1), Cert(2), ..., Cert(n-1)} the subject of the certificate Cert(x) is the issuer of the certificate Cert(x+1),
- the certificate Cert(1) is issued by a certification authority (**point of trust**) trusted by the verifier,
- Cert(n) is a certificate being verified.

Every certification path may be bounded with one or more certification policies or such a policy may not exist. Policies ascribed to a certification path are the intersection of policies set whose identifiers are included in every certificate, incorporated in the certification path and defined in the extension **certificatePolicies**.

Certification Policy – document which specifies general rules applied by certification authority in public key certification process, defines parties, their obligations and responsibilities, types of the certificates, identity verification procedures and area of usage.

Certification Practice Statement – the document describing in details public key certification process, its parties and defining scopes of usage of issued certificates.

Certification request token – any data in electronic form, containing a certification request that was: (1) created by certification services provider and (2) authenticates the applicant and confirms the truthfulness of data provided in the application, and confirms the complementariness of a public key with the private key that are currently owned by the applicant, (3) signed with a timestamp issued by a certification authority with the accuracy of 1 second without the need for time synchronization and (4) signed with the electronic signature of the registration inspector.

CERTUM – Unizeto Technologies S.A.'s service unit, providing certification and qualified certification services (certification authority). Qualified certification services, time – stamping services, data validation services, certificate status verification services and delivery services are provided in accordance with *Act on Electronic Signature of 18 September, 2001 (Dz.U. nr 130, poz. 1450)*.

CERTUM Operational Team – personnel responsible for proper operation of CERTUM. This responsibility applies to financial support, dispute resolution, decision making and creation of Certum development policy. Personnel employed in Operational Team do not have access to workstation and the computer system of CERTUM.

Cross-certificate – public key certificate (1) issued to a certification authority, (2) containing different name of the issuer and the subject, (3) a public key of this certificate may be used solely for electronic signature verification, and (4) it is clearly indicated that the certificate belongs to the certification authority.

Cross-certification – procedure of issuance of a certificate by a certification authority to another authority, not directly or indirectly affiliated with the issuing authority. Usually a cross-certificate is issued to simplify the building and verification of certification paths containing certificates issued by various CA's. Issuance of a cross-certification may be (but not

necessarily) performed on the basis of a mutual agreement, i.e. two certification authorities issue cross-certification to each other.

Cryptographic module – (a) set comprising hardware, software, microcode or their combination, performing cryptographic operations, including encryption and decryption, executed within the area of this cryptographic module or (b) reliable implementation of cryptosystem, which securely performs operations of encryption and decryption

Data objects repository – IT solution used to manage and storage of data objects. Access to the objects registered in the data object repository is performed with reference to these objects stored in the registry. Repository provides controlled access to stored data objects, monitoring their version, cataloging, searching and update.

Certificate status token – data in electronic form containing the information on current certificate status, certificate evidence, certification path that the certificate or certificate evidence belongs to and other data useful for the verification, electronically confirmed by the certificate validation authority.

Digital signature – cryptographic transformation of data allowing the data recipient to verify the origin and the integrity of the data, as well as protection of the sender and recipient against forgery by the recipient; asymmetric electronic signatures may be generated by an entity by means of a private key and an asymmetric algorithm, e.g. RSA.

Distinguished name (DN) – set of attributes forming a distinguished name of a legal entity and distinguishing it from another entities of the same type, **e.g.** C=PL/OU=Unizeto Technologies S.A., etc.

Deposit – entrusting a storing party (established on the base of some agreement) with data objects keeping until their receipt by a submitter, guaranteeing that data objects taken back are in not worse state of validity than at the time of their entrusting. A storing party is obligated to give back the same data object received for a storage and (on request) all others related data providing its validity during a time period they are stored in a deposit. Entrusted data are made accessible to a depositor only (i.e. to a subject entrusting data objects to keep them in a deposit).

Download entry or object – obtaining copy of entry or copy of object from deposit, registry or repository without removing them from deposit, registry or repository.

Electronic evidence – electronic data, which are attached to or logically associated with other electronic data and which are used for identifying the certification services provider or the entity which created certificate evidence and complies with requirements described in *art. 3 par. 19 of the Act on Electronic Signature of 18 September, 2001.*

Electronic signature – electronic data, which are attached to or logically associated with other electronic data and which are used for identifying the person who created the signature.

End entity – authorized entity using the certificate as a subscriber or a relying party (not applicable to a certification authority).

End entity attribute revocation list (EARL) – A revocation list containing a list of attribute certificates issued to holders that are not attribute certification authorities that are no longer considered valid by the certificate issuer.

Entry or data object release – to obtain an original of an entry or an object together with their removal from the deposit. Objects and entries are not removed from the registry and the repositories.

Evidence – information used to establish the proof that action or fact happened (PN ISO/IEC 13888-1)

Evidence/proof of receipt – data in an electronic form that are attached to an electronic document delivered to an addressee (recipient) or associated with this document in such a manner that any subsequent change of the document is detectable; the evidence defines:

a) the full name of the recipient to whom the electronic document should be delivered;

b) the date and time of the electronic document delivery that indicates the date and time when this document is entered or moved to IT system storage area accessible to the recipient of this document; this is the date and time of the electronic document is received according to the recipient's claim;

c) the confirmation (the electronic signature) of the document's recipient;

d) the date and time of the evidence's creation, confirmed by the qualified time-stamp synchronized to signals of a national authority and Co-ordinated Universal Time UTC(PL).

If the qualified authority of receipt and submission issues the evidence, then the evidence of receipt is resent to the sender and to the recipient of the electronic document.

Evidence/proof of submission – data in an electronic form confirming that a qualified authority of evidences of receipt and submission has received an electronic document to send to a recipient, and associated with this document in such a manner that any subsequent change of the document is detectable; the evidence defines:

a) the full name of the document sender;

b) the full name of the recipient to whom the electronic document should be delivered;

c) the full name of the authority issuing the evidence;

d) the date and time of the electronic document submission that indicates the date and time when this document is entered or moved to IT system storage area accessible to the qualified authority of evidences of receipt and submission;

e) the confirmation (the electronic signature) of the qualified authority of evidences of receipt and submission;

f) the date and time of the creation of the evidence of receipt and submission, confirmed by the qualified time-stamp synchronized to signals of a national authority and Co-ordinated Universal Time UTC(PL);

The evidence of submission is resent to the sender and/or recipient of the electronic document.

Hardware Security Module – see **cryptographic module**.

Individual subscriber – private person who is the subject identified by the certificate issued to him/her/it, individual subscriber requests a certificate by himself/ herself/itself.

Individual subscriber agreement – the agreement between a subscribers and Unizeto Technologies S.A. for the issuance of certificates to act on their own behalf; subscriber is the user and the owner of a certificate.

Information system – entire infrastructure, organization, personnel and components used for assembly, processing, storage, transmission, publication, distribution and management of information.

Certificate of an infrastructure key – a certificate related to an infrastructure key

Infrastructure Keys – cryptographic keys that are used with an asymmetric cryptographic algorithm for purposes other than electronic signature creation or verification; these keys are particularly used: (a) in key agreement or distribution protocols, (b) to provide, during

transmission or storage, confidentiality and integrity of certification requests, subscriber's keys and event logs, (c) for verification of access to devices or applications.

Notice: the term Infrastructure Keys understood as the key used by entities (individual or legal) in the cases of key agreement, authentication of entities and subsystems, signing of event logs, encryption of transmitted or stored data.

National root NCCert – the minister in charge of the economy or an entity appointed by the minister according to the *Article 23 paragraph 4 or 5 of the Act on Electronic Signature of 18 September, 2001* to issuing certificates used for verifying electronic authentications of certification authorities.

Object – object with controlled access, e.g. a file, an application, the area of the main memory, assembled and retained personal data (PN-2000:2002).

Object Identifier (OID) – alphanumeric / numeric identifier registered in accordance with the ISO/IEC 9834 standard and uniquely describing a specified object or its class.

Original – each deposit or registry entry as well as each data object stored in a repository. An original entry is created at the moment of a request to store an object entry in a deposit or a registry, while an original object at the moment it is stored in a repository.

Personal Identification Number (PIN) – code securing cryptographic card against unauthorized usage

Personal Unlocking Key (PUK) – code used for cryptographic card unlocking and changing of the PIN

Point of trust – the most trusted certification authority, which a subscriber or a relying party trusts. A certificate of this authority is the first certificate in each certification path created by a subscriber or a relying party. The choice of point of trust is usually enforced by the certification policy governing the operation of the entity issuing a given certificate.

Primary Registration Authority (PRA) – registration authority whose additional duty is to approve the rest of the RA's and is allowed to generate – on behalf of a certification authority – key pairs, successively subjected to certification process.

Private key – one of asymmetric keys belonging to a subscriber, used only by this subscriber. In the case of asymmetric key system, a private key describes transformation of a signature. In the case of asymmetric encryption system, a private key describes decrypting transformation.

Notices: (1) In cryptography employing a public key – the key whose purpose is decryption or signature creation, for the sole usage of the owner. (2) In the cryptographic system with a public key – the one of the key from key pair which is known only to the owner.

Procedure for emergency situation operations – procedure being the alternative of a standard procedure path and executed upon the occurrence of emergency situation.

Proof of possession of private key (POP) – information submitted by a subscriber to a receiver in a manner allowing the recipient to verify validity of the binding between the sender and the private key, accessible by the sender; the method to prove possession of private key usually depends on the type of employed keys, e.g. in the case of signing keys it is enough to present signed text (successful verification of the signature is the proof of private key possession), while in the case of encrypting keys, the subscriber has to be able to decrypt information encrypted with a public key belonging to him/her/it. CERTUM carries out verification of associations between key pairs used for signing and encrypting only on the level of registration and certification authority.

Public entity – every entity complies with Article *2 Ustawa z dnia 17 lutego 2005 r. o informatyzacji działalności podmiotów realizujących zadania publiczne* (*Dz.U. nr 64, poz. 565*)

Public key – one of the keys from a subscriber's asymmetric key pair which may be accessible to the public. In the case of the asymmetric cryptography system, a public key defines verification transformation. In the case of asymmetric encryption, a public key defines encryption transformation.

Public key certificate – electronic confirmation containing at least the name or identifier of a certification authority, a subscriber's identifier, his/her/its public key, the validity period, serial number, and is signed by the certification authority.

Notice: a certificate may be in one of the three basic states (see Cryptographic key states): waiting for activation, active and inactive.

Public Key Infrastructure (PKI) – consists of elements of hardware and software infrastructure, databases, network resources, security procedures and legal obligation, bonded together, which collaborate to provide and implement certificate services, as well as other services e.g. time - stamping.

Qualified certification services – certification services provided by qualified certification services provider.

Qualified certificate – certificate that meets requirements of the '*Act on Electronic Signature*' and is issued by a qualified certification service provider.

Qualified certification service provider - certification service provider who has been entered in the register of qualified certification service providers,

Registration authority – authority providing services of identity verification and confirmation of the certificate requesters; they provide complex subscriber handling in the area of certification services

Relying party – the recipient who has received information containing a certificate or an associated electronic signature verified with a public key included in the certificate and who has to decide whether to accept or reject the signature on the basis of the trust for the certificate.

Repository – a set of publicly available electronic directories, containing issued certificates and documents related to operation of certification authority

Requester – subscriber in the period between submission of a request (application) to a certification authority and the completion of certificate issuance procedure.

Requester / payer – individual or institution which on behalf of the subscriber pays for certification services, provided by the authority issuing the certificate. The requester / payer is the owner of the certificate and has a right to request its revocation in cases described in Certification Practice Statement.

Revoked certificate – public key certificate placed on Certificate Revocation List, without cancellation of the reason for revocation (e.g. after unsuspension).

Secret key – key applied in symmetric cryptography techniques and used only by a group of authorized subscribers.

Notice: A secret key is intended for usage by very small group of persons for data encryption and decryption.

Self-signed certificate – any public key certificate, designed to verification of signature upon certificate, whose signature may be verified by public key included in the field

subjectKeyInfo, whose content of the fields **issuer** and **subject** are the same, and whose **cA** field of **BasicConstraints** extension is set to true.

Shared secret – part of a cryptographic secret, e.g. a key distributed among n trusted individuals (cryptographic tokens, e.g. electronic cards) in a manner, requiring m parts of the secret (where m<n) to restore the distributed key.

Shared secret holder – authorized holder of an electronic card, used for storing shared secret.

Signatory – natural person who holds a signature-creation device and acts either on his own behalf or on behalf of another natural person, legal person or an organizational unit not endowed with legal personality

Signature policy – detailed solutions, including technical and organizational solutions, defining the method, scope and requirements of confirmation and verification of an electronic signature, whose execution allows verification of signature validity.

States of cryptographic key – Cryptographic keys may have one of the three basic states (acc. to ISO/IEC 11770-1 standard)

waiting for activation (ready) – the key has already been generated but is not available for use,

active – the key may be used in cryptographic operations (e.g. creation of e-signature),

inactive – the key may be used for e-signature validation or decryption only (the subscriber cannot use the private key for creating a signature - key has expired or the public key to encrypt – public key has expired); Current date is later than expiration date and the key is not revoked.

Subscriber – entity (private person, legal entity, organizational unit not having a legal identity, hardware device owned by these entities or persons) that: (1) is the subject identified by the certificate issued to this entity, (2) posses a private key associated with the certificate issued to the entity and (3) does not issue certificates to other parties.

Subscriber's sponsor agreement – the agreement between a subscriber and Unizeto Technologies S.A.; a certificate is ordered by a sponsor but it is used by a subscriber to act on behalf of sponsor who is the owner of the certificate and has a right to request its revocation, a subscriber is the user of certificate.

Sponsor agreement – the agreement between a sponsor and Unizeto Technologies S.A; this agreement is a blanket agreement, authorizing Unizeto Technologies SA to enter into individual agreements with each of sponsor's subscriber (payer's subscriber), which are the subject of the sponsor agreement.

Sponsor's subscriber (payer's subscriber) – private person who is the subject identified by the certificate issued to him/her/it.

Timestamp token – electronic data, binding any action or fact with precise moment of time, creating a confirmation that action or fact happened preceding specific moment in time.

Timestamping – service basing on attaching time signature to electronic data, logically bounded with signed data or electronic signature; timestamp is certified by authority providing appropriate services.

Time-Stamping Authority (TSA) – entity issuing timestamp tokens.

Token – element of data used for exchange between parties and containing information transformed by means of cryptographic techniques. Token may be signed by a registration

authority operator and may be used for authentication of its holder in the contact with a certification authority.

Trusted path – connection allowing exchange of information associated with authentication of a user, an application or a device (e.g. an electronic cryptographic card) , protected in a manner preventing violation of the integrity of transmitted data by any malicious application.

Trusted Third Party (**TTP**) – institution or its representative trusted by an authenticated entity and/or entity performing verification and other entities in the area of operations associated with security and authentication.

Valid Certificate – public key certificate is valid only when (a) it has been issued by a certification authority, (b) has been accepted by the subscriber (subject of the certificate) and (c) it has not been revoked .

Validation of public key certificates –allowing validation whether the certificate is revoked. This problem may be solved by the interested entity on the basis of CRL or by the issuer of the certificate or an authorized representative on entity's request, directed to OCSP server.

Validation of Signature – aims at (1) verification of the signature being created by private key corresponding to public key, included in the certificate signed by certification authority, and (2) verification whether signed message (document) has not been modified since the time of signature creation.

Violation (e.g. data breach) – revelation of information to an unauthorized person, or interference that violate security system policy, resulting in unauthorized (intended or unintended) revelation, modification, destruction or compromise of any object.

X.500 – international norm, specifying Directory Access Protocol and Directory Service Protocol.