Certification Practice Statement of CERTUM's Qualified Certification Services

Version 4.1

Effective date: 12th of April, 2016

Status: previous

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

Trademark and Copyright notices

Content

1.Introduction

Certification Practice Statement of CERTUM's Qualified Certification Services describes general rules of certification practice of CERTUM (full name: CERTUM – General Certification Authority) used by distinguished part of CERTUM in the course of provision of certification services, apply to:

- the issuance of **public key qualified certificates**[1], including registration of **subscribers**[2], certification of public keys, rekey and certificates renewal
- the **revocation** and **suspension** of certificates
- the issuance of **timestamp tokens**, **certificate status tokens**, **data validation tokens,** and **evidences of receipt and submission (including Official evidences of receipt and submission**[3])
- the issuance of **deposit tokens** (particularly signed objects) and **registries and repositories tokens**
- the issuance, release and revocation of **attribute certificates.**

These services are provided in accordance with:

- the Integrated Management System, implemented by Asseco Data Systems S.A. ,which includes the requirements of the ISO: 9001: 2009 and PNISO/IEC 27001: 2007,
- the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450),*
- the current *WebTrust Program for CAs, and*
- the *CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.*

This Certification Practice Statement defines parties, their obligations and responsibilities, types of certificates, authentication procedures and applicability range. The knowledge of the nature, purpose and role of the Certification Practice Statement and the Certification Policy is particularly important for a **subscriber** and a **relying party**[4].

The Certification Policy and the Certification Practice Statement have been defined by CERTUM, which is a supplier of certification services rendered on the basis of the CP and the CPS. The procedure of defining and updating of the Certification Policy and the Certification Practice Statement is in accordance with the rules stated in chapter 8.

The Certification Practice Statement describes a set of rules applied by **CERTUM** to issue qualified certificates, timestamps tokens, certificate status tokens, data validation and certification server tokens, evidences of receipt and submission (including official evidences of receipt and

1 Terms introduced for the first time are marked in bold; they are defined in Glossary at the end of the document.

2 Entity that is a subject shown or identified in a certificate who is the originator of the message and signs it by using a private key that corresponds to public key, contained in the certificate.

3 Official Evidences of receipt and submission are issued in accordance with the *Art. 16, § 3* of the *Act of 17 February 2005 on Informatization of Operation of Entities Performing Public Tasks (Journal of Laws 2005 No. 64, item 565, as ammended)* and in accordance with the *Art. 39, § 2* of the *Code of Administrative Procedure (Journal of Laws 2000 No. 98, item 1071, as ammended)*. See also Glossary)

4 An individual or an organization that acts in reliance on a certificate and/or a digital signature.

submission), objects deposit tokens, registries and repositories tokens, attribute certificates, certificates of infrastructure keys used for CERTUM only, to the end-users, according to the requirements specified in the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094).*. The applicability ranges of the qualified certificates, timestamps tokens, certificate status tokens, data validation tokens, evidences of receipt and submission (including official evidences of receipt and submission), objects deposit tokens, registries and repositories tokens (particularly regarding signed objects), attribute certificates, certificates of infrastructure keys of CERTUM and certificated evidences issued in compliance with this CPS are described in Chapter 1.4. Responsibility of the certification authority and end-users is described in Chapter 2.2

The structure and contents of the Certification Practice Statement are in accordance with the recommendation of RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. The Certification Practice Statement was created assuming that the reader is generally familiar with the notions concerning certificates, certificate evidences, electronic signatures and a Public Key Infrastructure (PKI).

Applicable notions, terms and their meaning are defined in the ***Glossary*** *at the end of this document.*

The Asseco Data Systems S.A. company (Acquiring company) as part of the merger with Unizeto Technologies S.A. (Acquired company) that was carried out pursuant to art. 492 § 1 point 1 of the Act of 15 September 2000 Commercial Companies Code (Journal of Laws of 2013. Item. 1030, as amended. D., Referred to as "CCC"), has assumed all rights and obligations of the Unizeto Technologies S.A. company (General succession - Art. 494 § 1 of the CCC).

In connection with the transfer of the entire assets of the Unizeto Technologies S.A. company to the Asseco Data Systems S.A. company we declare that Asseco Data System S.A. undertakes to maintain the provider's certificate issued to Unizeto Technologies S.A. until the last certificate issued by the Unizeto Technologies S.A. company within its provider's certificate is expired.

1.1. Overview

The Certification Practice Statement of CERTUM's Qualified Certification Services is a description and basis for functioning of CERTUM (operating within Asseco Data Systems 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, a 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 evidences of receipt and submission)**, **objects deposit tokens, registries and repositories tokens** (particularly regarding signed objects)**,** and the issuance of attribute certificates according to the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* The issuance of certificates and tokens is based on the certificate evidence issued in accordance with the requirements of the *Act*. The principles set out in this document should be adjusted by the operation of those entities and the service providers who use certificates and public key certificates issued by CERTUM.

The CERTUM's qualified certification services are provided within the framework of the separate certification domain **cckDomena** (see Fig. 1.1) with the separate qualified certification authority **CERTUM QCA**[5]**,** the qualified time - stamping authority **CERTUM QTSA**[6]**,** the qualified Online Certificate Status Protocol authority **CERTUM QOCSP**[7]**,** the qualified Data Validation and Certification Server authority **CERTUM QDVCS**[8], the qualified delivery authority **CERTUM QDA**[9], the qualified object deposits authority **CERTUM QODA**[10], the qualified registries and repositories authority **CERTUM QRRA**[11], and the qualified attribute certificates authority **CERTUM QACA**[12]**.** These authorities provide services based on the certificate evidence issued by the Minister in charge of economy or an entity authorized by the Minister under the *Art.* 23, item 4 or 5 of the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450).*

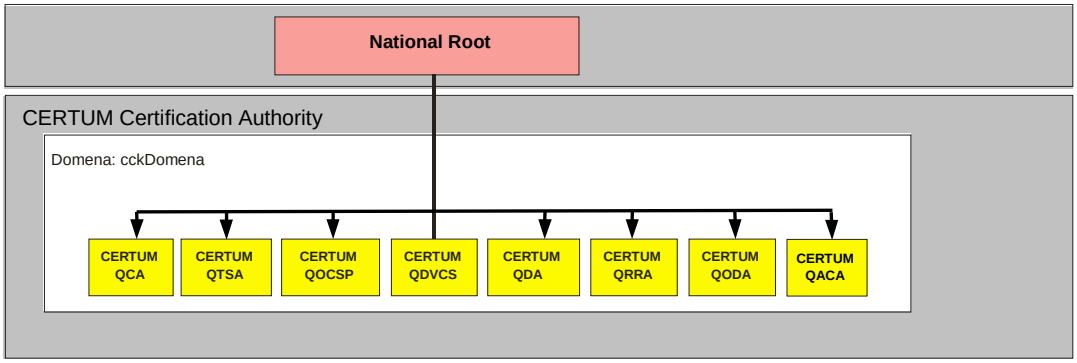

Fig.1.1 The authorities operating within CERTUM qualified services

CERTUM QCA *authority is independent from the other authorities (except the National root NCCert under the requirements of § 7 of the Regulation of the Minister of Economy of 9 August 2002 on determining the detailed procedure of creating and issuing the certificate of the certification associated with electronic signature (Journal of Laws 2002 No. 128, item 1101, as ammended) and is not bound by any cross-certification agreements.*

This Certification Practice Statement refers to the **CERTUM QCA** authority and registration authorities affiliated by the **CERTUM QCA,** the qualified time - stamping authority **CERTUM QTSA,** the qualified online certificate status protocol authority **CERTUM QOCSP,** the qualified data validation and certification server authority **CERTUM QDVCS**, the qualified delivery authority **CERTUM QDA**, the qualified object deposits authority **CERTUM QODA**, the qualified registries and repositories authority **CERTUM QRRA** and the qualified attribute certificates authority **CERTUM QACA,** and the service recipients – subscribers of qualified certificates, timestamps tokens, certificate status tokens, data validation tokens, evidences of receipt and submission (including official evidences of receipt and submission), deposit, registries and repositories tokens (particularly regarding signed objects), attribute certificates, and all relying parties that use the services or exchange any information with the **cckDomena** domain.

---

5 QCA – *Qualified Certification Authority*

6 QTSA – *Qualified Time Stamping Authority*

7 QOCSP – *Qualified On-line Certificate Status Protocol*

8 QDVCS – *Qualified Data Validation and Certification Server*

9 QDA – *Qualified Delivery Authority*

10 QODA – *Qualified Objects Deposits Authority*

11 QRRA – *Qualified Registries and Repositories Authority*

12 QACA – *Qualified Attribute Certificate Authority*

Certificates and tokens issued by CERTUM contain the identifiers[13] of certification policies enabling relying parties to state if the application of a certificate being verified by the party is in accordance with the declared purpose of the certificate. The declared purpose might be specified on the basis of values set in **PolicyInformation** structure of the extension **certificatePolicies** (see Chapter 7.1.1.2) of every certificate issued by CERTUM.

Identifiers of certification policies are also placed on tokens issued by the qualified time - stamping authority **CERTUM QTSA,** the qualified online certificate status protocol authority **CERTUM QOCSP,** the qualified data validation and certification server authority **CERTUM QDVCS**, the qualified delivery authority **CERTUM QDA**, the qualified object deposits authority **CERTUM QODA**, the qualified registries and repositories authority **CERTUM QRRA**, and the qualified attribute certificates authority **CERTUM QACA**.

CERTUM obeys the law in force in the Republic of Poland and the rules resulting from the compliance, interpretation and validity of the Certification Policy.

There are many additional documents connected with the Certification Practice Statement of CERTUM‘s Qualified Certification Services. They are used in CERTUM and regulate its functioning (see Table 1). These documents have a different status. They are usually not available for the public because of the importance of the information they contain and the system security.

Tab. 1 Important document connected with Certification Practice Statement

	Document name	Status	Availability
1.	Certification Policy of CERTUM’s Qualified Certification Services	Public	http://www.certum.eu
2.	Certification Regulations of CERTUM‘s Qualified Certification Services	Public	http://www.certum.eu
3.	Certification authorities keys life cycle management procedures	Non-public	Locally – only entitled persons and auditor
4.	Personnel book, range of duties and responsibilities	Non-public	Locally – only entitled persons and auditor
5.	Registration authority book	Non-public	Locally – only entitled persons and auditor
6.	Technical infrastructure book	Non-public	Locally – only entitled persons and auditor
7.	Business continuity plan	Non-public	Locally – only entitled persons and auditor
8.	CERTUM’s Security Management	Non-public	Locally – only entitled persons and auditor
9.	Certificate’s, token’s and notification’s profiles management	Public	On demand
10.	CERTUM QCA PKI Disclosure Statement	Public	http://www.certum.eu

Additional information and support are available by electronic mail at: info@certum.pl.

[13] Identifiers of CERTUM certification policies are constructed on the basis of the object identifier of Unizeto Sp. z o.o. registered in the National Register of Object Identifiers (Krajowy Rejestr Identyfiaktorów Obiektów), http://www.krio.pl. The identifier has the following value:

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

1.2. Document Name and its Identification

The present document of Certification Practice Statement is given a proper name of **Certification Policy of CERTUM's Qualified Certification Services**; this document is available as an electronic version at the repository at: http://www.certum.eu or on request sent to: info@certum.pl,

The following registered object identifier is connected with the certification practice statement document (OID: 1.2.616.1.113527.2.4.1.0.1.4.1)[14]:

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

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

The Certification Practice Statement Identifier is not included in the content of issued certificates. Only the certification policies identifiers belonging to the collection of certification policies incorporated by the present Certification Practice Statement (described in Chapter 7.1.1.2 hereinafter) and the identifier for qualified services used by CERTUM under the *§3 item 4 of the Regulation of the Minister of Economy of 9 August 2002 on determining the detailed procedure of creating and issuing the certificate of the certification associated with electronic signature (Journal of Laws 2002 No. 128, item 1101, as ammended)* are included in certificates issued by CERTUM.

1.3. Certification Practice Statement Parties

Certification Practice Statement regulates the most important relations between the entities belonging to CERTUM, its advisory teams (including auditors) and customers (users of supplied services). The regulations particularly apply to:

- 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.

[14] The Certification Practice Statement Identifier should not be confused with a certification policy identifier (OID) which is provided in a certificate (see Tab. 2) There is only one Certification Practice Statement Identifier while it could be more than one identifiers of a certification policy.

CERTUM provides certification services to all private and legal entities or entities not endowed with legal personality, accepting the regulations of the present Certification Practice Statement. The purpose of these practices (including key generation and certificate issuance rules as well as information system security) is to convince the users of CERTUM services that the declared trust levels of issued certificates are the reflection of certification authorities' practices.

CERTUM provides the qualified certification services in the range of:

1. the issuance of qualified certificates, including:
   - subscribers registration,
   - generating keys and qualified certificates,
   - distribution and publication of the information (e.g. information about the qualified certificates of the public key)
   - certificate and Certificate Revocation Lists publication,
2. revocation and suspension of certificates,
3. time – stamping,
4. online verification of certificate status,
5. data validation,
6. the issuance of evidences of receipt and submission (including official evidences of receipt and submission),
7. the issuance of object deposit confirmations (particularly signed object),
8. the issuance of registries and repositories confirmations,
9. the issuance, release and revocation of attribute certificates.

1.3.1. Qualified Certification Authority CERTUM QCA

CERTUM QCA belongs to CERTUM which provides qualified certification services and operates on the basis of the entry of the Asseco Data Systems S.A. in the register of qualified certification services providers. The Minister in charge of economy or the entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QCA** activity.

The authority **CERTUM QCA** issues qualified certificates, certificates of infrastructure keys and certificates of certification authorities according to certification policies (identifiers values are described in Tab. 2 and chapter 7.1.1.2) and according to the following requirements:

- the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450),*
- the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)*,
- the current *WebTrust Program for CAs,* and
- the *CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*

National root NCCert (see Fig. 1) is a ***point of trust***[8] *for all subscribers and relying parties of CERTUM's qualified services. What follows is that every certification path must start with a certificate of National root NCCert for certification authority* ***CERTUM QCA****.*

CERTUM QCA provides certification services to:

- itself (issues and renews self-certificates),
- Minister in charge of economy or an entity authorized by the Minister which provides certification services in accordance with the ∫ *7* of the *Regulation of the Minister of Economy of 9 August 2002 on determining the detailed procedure of creating and issuing the certificate of the certification associated with electronic signature (Journal of Laws 2002 No. 128, item 1101, as ammended),*
- natural persons who wish to execute a secure electronic signature using the qualified certificates within the meaning of the *Act*,
- registration authority operators,
- notaries confirming the identity of any certificate applicant,
- employees of CERTUM.

Tab. 2 The Certification policy identifiers included in the certificates 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

The Certum's Qualified Time – Stamping Authority **CERTUM QTSA**, operating within the **cckDomena** domain (Fig. 1) is a part of CERTUM infrastructure for qualified services. **CERTUM QTSA** operates on the basis of the entry of the Asseco Data Systems 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 the 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 the *Regulation of the Minister of Economy of 9 August 2002 on determining the detailed procedure of creating and issuing the certificate of the certification associated with electronic signature (Journal of Laws 2002 No. 128, item 1101, as ammended).*

The Certum's Qualified Time – stamping authority **CERTUM QTSA** issues timestamp tokens in accordance with ETSI[15] recommendation. Each timestamp token contains identifier of the policy, under which the token has been issued (identifier value is described in Table 3 and Chapter 7.2.3). Timestamp tokens are signed with a private key issued solely for time - stamping service.

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

Tab. 3 The identifier for the **CERTUM Qualified Time-Stamping Authority** policy included in timestamp tokens issued by **CERTUM QTSA**

Token name	Certification Policy Identifier
Qualified timestamp token	1.2.616.1.113527.2.4.1.2

The qualified timestamp tokens, issued in accordance with policy described in Tab.3, are used primarily for securing long-term electronic signatures[16] and global transactions.

The 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.

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 the qualified online certificate status protocol authority **CERTUM QOCSP** (see Fig. 1) on the basis of the entry of the Asseco Data Systems S.A. in the register qualified certification services providers. Minister in charge of economy or the entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QOCSP** activity.

The qualified online certificate status protocol authority **CERTUM QOCSP** should validates the status of qualified certificates only[17]. 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

The qualified data validation and certification server authority **CERTUM QDVCS** issues electronic confirmations (also called qualified data validation tokens) to validate a qualified public key certificate, an electronic signature, a timestamp, certificate status token, a delivery token and a 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.

---

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

17 *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. 4 The 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[18]	1.2.616.1.113527.2.4.1.3.2.c[19]
Qualified validation token of qualified timestamp. [20]	1.2.616.1.113527.2.4.1.3.3.c
Qualified validation token of qualified certificate[21]	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 Asseco Data Systems S.A. in the register qualified certification services providers. Minister in charge of economy or the entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QDVCS** activity.

Qualified data validation tokens are issued according to the certification policies described in Tab. 4 and may be used primarily in the process of validation of qualified electronic signatures[22]. 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 a 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.

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

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

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

20 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.

21 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.

22 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 the 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

The 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 § 3* of the *Act of 17 February 2005 on Informatization of Operation of Entities Performing Public Tasks (Journal of Laws No. 64, item 565, as ammended)* and on the basis of *art.* 39^1 § 2 of the *the Code of Administrative Procedure (Journal of Laws 2000 No. 98, item 1071, as ammended).* **CERTUM QDA** provides this service to individuals who want to send digitally signed electronic document to any recipient, including a public entity.

Tab. 5 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
Official 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 Asseco Data Systems 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 receipt and submission (including official evidences of receipt and submission) are issued according to certification policies described in Table 5.

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

The 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 2001 No. 130, item 1450). **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. 6 The 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 Asseco Data Systems S.A. in the registry qualified certification services providers. Minister in charge of economy or the 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 6.

1.3.7. Qualified registries and repositories authority CERTUM QRRA

The qualified registries and repositories authority **CERTUM QRRA** enables the recording of data objects and, optionally, placing them in the repository. **CERTUM QRRA** also enables downloading of entries from the registry and objects from the repository, their modifying and maintaining their authenticity; these objects can be digitally 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 QODA** 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) – a **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) – a **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. 7 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 Asseco Data Systems S.A. in the register of qualified certification services providers. Minister in charge of economy or the 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 7.

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 Asseco Data Systems 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. 8 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 the three predefined groups of attribute certification policies (see Table 8). 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. The identifiers of these policies are built on the basis of the pattern shown in Table 8, 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, 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 the appropriate certification authorities CERTUM QCA and CERTUM QACA. The authorization concerns the registration, identification of the identity and attributes of the current or future subscriber.

Registration authorities receive, verify and approve or reject applications for registration and issuance of a public key certificate or an attribute certificate and other applications related to the management of certificates (rekey, modification or revocation of a certificate). Verification of applications intends to authenticate (on the basis of the documents enclosed to the applications) the requester, as well as the data included in the application. The level of accuracy of subscriber's identity and attributes identification results from the general requirements described in the Certification Practice Statement of CERTUM's Qualified Certification Services (see Chapter 3). The scope of duties of registration authorities and points of the identity and attributes verification are defined in this Certification Practice Statement, procedures for registration authorities and the Certification Policy of CERTUM's Qualified Certification Services.

Any individual or institution (legal entity) might operate as a registration authority and point of the identity and attributes verification accredited by CERTUM QCA and CERTUM QACA, provided that this individual or institution submit an appropriate application to Primary Registration Authority and fulfill other conditions stated in Certification Practice Statement.

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.eu

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 Primary Registration Authority. Additionally, points of the identity and attributes verification provide information about certification services.

The certification authorities operating within CERTUM can delegate a part of their authority to two types of registration authorities:

- registration authorities (RA),
- Primary Registration Authority (PRA).

The main difference between these types is that registration authorities, unlike Primary Registration Authority, cannot accredit other registration authorities and register new certification authorities. Moreover, the registration authorities do not have the rights to confirm all requests of a subscriber. The rights might be limited only to some of all available types[23] of certificates. Therefore,

- **RAs** register subscribers that request for qualified certificates and attribute certificates, in addition, they provide comprehensive information on digital signatures, including the effects of using it, provide information on the types of attributes, enter into a certification services agreement and may sell the certificates and secure devices,
- **PRA** registers registration authorities (RA), notaries and points of the identity and attributes verification of the current or the future subscriber; there are no restrictions (apart from the ones that result from the role played in public key infrastructure of CERTUM) imposed on the types of certificates issued to the subscribers registered in PRA; additionally, PRA approves distinguished names (DNs) of the current and the future registration authorities.

Primary Registration Authority is located at the seat of CERTUM. Contact addresses with PRA are listed in Chapter 1.9.

Primary Registration Authority CERTUM is prepared to handle notary's confirmation of the identity or attributes of a subscriber or confirmation issued by a qualified person, without the need for a subscriber to appear at the registration authority.

Notary notarizes the identity document or the document containing the individual's attributes and data necessary for the issuance of a public key certificate or an attribute certificate. Notarized documents with signed agreement are the set of documents and data identifying entity on the basis of which a registry inspector verifies the identity and/or attributes of a subscriber and she/he make a certificate application notification.

Person who verifies the identity and/or attributes of the applicant on behalf of CERTUM should be authorized to make an agreement for offering the certification services. The acceptance of the application and execution of an agreement must be authenticated by his/her own signature and the person must present his/her own national identification number (PESEL) on the written confirmation of the identity and/or attributes of the applicant.

1.3.10. Repository

Repository is a collection of publicly available directories containing:

- certificate evidences
- certificates of infrastructure keys,
- attribute certificates,
- other (see Chapter 2.6.1)

[23] Types of certificates are described in Charter 1.4

*In the **cckDomena** domain there is only one repository, common for all certification authorities operating within or related to the domain.*

The contents of the repository are available at: http://www.certum.eu

1.3.11. End Entities

End entities include subscribers and relying parties. A subscriber is an entity whose identifier is placed in the field **subject** of a certificate and who does not issue certificates and certificates of certification authorities to others. A relying party is an entity who uses other subject's qualified certificate and/or attribute certificate in order to verify other party's electronic signature or to secure the confidentiality of information that is being sent.

Tab. 9 Users of the CERTUM qualified certificates, CERTUM certificates of certification authorities and tokens issued by CERTUM.

Certificate/ /token name	Users
Qualified certificates	A person who signs (a subscriber) and verifies (a relying party) an electronic signature under the *Act* or in accordance with an act on electronic signature in force in territory of another country.
Certificate evidences	Relying parties who verify an electronic signature under the *Act*..
Certificates of infrastructure keys	Subscribers and relying parties (e.g. employees and customers of CERTUM and registration authority operators), of which CERTUM pursues key-agreement protocol and other cryptographic protocols. Devices such as servers are considered to be subscribers and relying parties.
Timestamp tokens	Relying parties signing and verifying an electronic signature under the Act or in accordance with an act on electronic signature in force in territory of another country.
QOCSP tokens	Relying parties verifying status of qualified certificate issued under the *Act* or in accordance with an act on electronic signature in force in territory of another country.
Data validation tokens	Relying parties signing and verifying an electronic signature or requesting other certification services under the *the Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* or in accordance with an act on electronic signature in force in territory of another country.
Evidences of receipt and submission (including Official evidences of receipt and submission)	Relying parties signing and verifying an electronic signature for documents submitted to public or non-public entities under the *Art. 16 of the Act of 17 February 2005 on Informatization of Operation of Entities Performing Public Tasks (Journal of Laws No. 64, item 565, as ammended)* and *the Art. 39[1], § 2 of the Code of Administrative Procedure (Journal of Laws 2000 No. 98, item 1071, as ammended).*
Deposit tokens	Relying parties (individuals, entities and legal persons

	and entities), who wish to storage any data objects in reliable way (particularly signed objects)
Registries and repositories tokens	Relying parties (individuals, entities and legal persons and entities), who wish to make an entries into a register which corresponds to the appropriate classes of entities, objects, events etc. and to the data objects associated with these classes.
Attribute certificates	The user of electronic signatures to which an attribute certificate can be attached. and the relying party that verifies an electronic signature under the *Ac* t or verify attributes if required.

1.3.11.1. 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.

CERTUM offers certificates of different types and of different trust levels. Subscribers should decide what type of certificate is the most suitable for their needs (see Chapter 1.4).

1.3.11.2. 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

A relying party is responsible for verification of the current status of a subscriber's certificate (including attribute certificates, tokens or other confirmations). Such a decision must be taken any time when a relying party wishes to use a certificates or tokens to verify an electronic signature, its authenticity and authenticity of data objects. A relying party should use the information in qualified certificate and attribute certificate (e.g. identifiers and qualifiers of certification policy) to state whether a given certificate was used in accordance with its declared purpose.

1.4. Certificate Applicability Range

Qualified certificate, attribute certificates and certification authorities certificates applicability range states the scope of permitted certificate or certification authorities certificates usage. This scope defines the character of certificate or certification authorities certificate applicability (e.g. authentication, non-repudiation or confidentiality).

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.

Information sensitivity level and information vulnerability to **breach**[24] should be evaluated by a subscriber.

A relying party bears responsibility for stating the trust level of a certificate that is applied to a given purpose. On considering various important risk factors, this party should state which of the certificates issued by CERTUM meet the formulated requirements. Subscribers should be familiar with the requirements of a relying party (e.g. the requirements can be published as ***signature policy*** *or the policy of information system security) and then apply to CERTUM for issuance of an appropriate certificate that meets these requirements.*

The requirements set out by the relying party must be confronted by the subscriber with applicability range (Table 10) and types of certificates (Table 11, Table 12, Table 13) issued by CERTUM QCA.

Tab. 10 The applicability ranges of certificates and certificate evidences of certification authorities issued by CERTUM QCA

Certification policy	Commercial name of certificate type	Description and recommended applicability
CERTUM QCA QC	Qualified certificates	Very high trust level of the identity of a certificate subject. Qualified certificates are issued to (a) individuals, (b) natural persons who are employees or representatives of any organizations or institutions. Certificates should be use for signing and verifying secure electronic signatures. These certificates can be used to authenticate and control the integrity of the information that was signed giving them a characteristic of non-repudiation They can be used if the risk of unauthorized access to secured information is high and consequences of breach are serious. These certificates can be applied to financial transactions or transactions of a high level of fraud occurrence risk. Qualified certificates cannot be used to data or keys encrypted

24 See **Glossary**

CERTUM QCA CKI	Certificates of infrastructure keys	Very high trust level of the identity of a certificate entity. Certificates of infrastructure keys are issued to: (a) CERTUM personnel, (b) CERTUM network devices and servers, (c) CERTUM system software, (d) for the purpose of certification and encryption of CERTUM operational data. These certificates can be used to authenticate and control the integrity and to secure confidentiality of information. Certificates cannot be used for verification of secure electronic signatures. (even if contain **digitalSignature** bit or **nonRepudiation** bit in the **keyUsage** extension.)
CERTUM QCA CertEvidences	certificate evidence	Very high trust level of the identity of a certificate entity. Certificate evidences are issued to: (a) The National root NCCert acting under the authority and on behalf of the Minister in charge of economy, (b) for **CERTUM's QCA** keys exchange

1.4.1. Qualified certificates

CERTUM issues **two basic types of certificates** (see Table 11). Qualified certificates from this list are issued to any subscribers who entered into an agreement with Asseco Data Systems S.A. and accepted the rules of this Certification Practice Statement.

Every qualified certificate issued by the CERTUM QCA provides of indication that it is a qualified certificate. There are two indicators included in every qualified certificate. The first is contained in **CertificatePolicies** extension and the second is contained in **QCStatements** extension. This extension has the following value of the object identifier:

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

This means that a certificate is the qualified certificate, issued by accredited entity providing qualified certification services. These indicators may occur simultaneously or separately.

Tab. 11 Types of qualified certificates and their applicability

Certification policy	Commercial name of certificate type	Description and recommended applicability
CERTUM QCA QC	CERTUM QCA Personal	Electronic mail security, electronic signatures of electronic data; certificate contains at least: name of country, name of subscriber and serial number of certificate
	CERTUM QCA Professional	Electronic mail security, electronic signatures of electronic data. These certificates are used by individuals who are an employees or representatives of any organizations, institutions, enterprises or by the representatives of other individuals; certificate contains at least:: name of country, name of subscriber, name of entity and serial number of certificate.

1.4.2. Certificate evidence

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
- **CERTUM QCA** (applicable to keys exchange)

Tab. 12 Types of certificate evidences and their applicability

Certification policy	Commercial name of certificate evidences	Description and recommended applicability
CERTUM QCA CertEvidences	CERTUM QCA Cross-Cert	Certificate evidences are issued to the Minister in charge of economy or to the entity providing certification services under the authority, and on behalf of the Minister in charge of economy
	CERTUM QCA Internal	Certificate evidences are issued for the purposes of keys of CERTUM QCA exchanging

1.4.3. Certificates of infrastructure keys

Certificates of infrastructure keys are issued to: personnel of CERTUM, registration authority operators acting on behalf 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. (this requirement applies only to the verification of the messages transmitted to CERTUM)

Tab. 13 Types of certificates of infrastructure keys

Certification policy	Commercial name of certificate type	Description and recommended applicability
CERTUM QCA CKI	CERTUM QCA Personnel	Certificates necessary to support certification authorities within CERTUM.
	CERTUM QCA CMP Message	Certificates used to authenticate CMP messages by CERTUM QCA
	CERTUM QCA Keys encryption	Certificates used for confidential transport of keys between certification authority and subscriber or between certification authority and registration authority
	CERTUM QCA Data encryption	Data encryption, crypto file systems

1.4.4. Recommended Applications

The certificates or certificate evidences of certification authorities issued in accordance with one of the certification policies can be used with applications and devices that meet the requirements described in the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094).*

The list of recommended and approved (by CERTUM) applications is published in the repository at: http://www.certum.eu

Applications are included in the list of recommended applications on the basis of written statements of producers to comply with PN-EN ISO/IEC 17050-1:2005 and/or on the basis of tests carried out by CERTUM. Devices recommended by CERTUM must have certificates of the compliance with the requirements for technical components, as defined in *the Art.5* of the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)* and the *CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.*

1.5. Timestamps Applicability Range

Time - stamping authority **CERTUM QTSA** issues time-stamping tokens which, in terms of the Civil Code, 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. Time - stamping authority **CERTUM QTSA** issues time-stamping tokens in accordance with the *CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements.*

Time-stamping service is available to public, however time - stamping authority **CERTUM QTSA** verifies authenticity of the each request and rejects it when the format of the request is not correct or the request comes from someone who is not entitled to receive this service, or whose identity cannot be confirmed.

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 proof of sending an electronic document to a public entity which is acting in accordance with the *Art. 16 § 3* of the *Act of 17 February 2005 on Informatization of Operation of Entities Performing Public Tasks (Journal of Laws No. 64, item 565, as ammended)* and on the basis of the *Art.* 39^1 *§* 2 of the *Code of Administrative Procedure (Journal of Laws 2000 No. 98, item 1071, as ammended).*

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.

Qualified attribute certificates authority CERTUM QACA issues **three basic types of qualified attribute certificates** (see Table 14). Qualified attribute certificate are issued to any subscribers who accepted the regulations of the present Certification Practice Statement. Attribute certificates may also be issued to CERTUM personnel, registration authority employees and points of identity and attributes verification employees acting on behalf of CERTUM.

Tab. 14 Types of qualified attribute certificates issued by CERTUM QACA and their applicability

Certification policy	Commercial name of certificate type	Description and recommended applicability
CERTUM QACA Standard Policy	CERTUM QACA Standard	Certificates are issued for purposes of qualified electronic signature generation and are explicitly linked to qualified certificates. Attribute certificates narrows the area of qualified certificates usage.

Certification policy	Commercial name of certificate type	Description and recommended applicability
CERTUM QACA Authorization Policy	CERTUM QACA Authorization	Certificates are used to authorize the rights of a subject of a attribute certificate. Certificates contain attributes that may be useful during the entity's rights validation; attribute certificates belonging to this group needn't to be explicitly linked to public key certificates, particularly to qualified certificates
CERTUM QACA Dedicated Policies	CERTUM QACA Dedicated	Certificates are intended for use in specific systems or applications when certified confirmations of attributes of systems or applications are required. Dedicated attribute certificates are issued in accordance with attributes certification policy; identifiers of certification policy and certification policies are not published in the Certification Policy and the Certification Practice Statement CERTUM.

Regardless of type of attribute certification policy each of attribute certificates is issued by qualified attribute certificates authority CERTUM QACA only after reliable verification of connection between subscriber identity and confirmed attribute or attributes and verification of subscriber's rights to use these attributes.

1.11. Contact

PKI Services Development Team directly administers the present Certification Practice Statement, Certification Policy and other documents concerning PKI services delivered by CERTUM. The PKI Services Development Team comprises at least two board members, the director of CERTUM and managers who supervise a vital areas of Asseco Data Systems S.A.Above mentioned Team also test the compliance of Certification Practice Statement and Certification Policy. All inquiries and comments concerning the contents of the mentioned documents should be directed to:

Asseco Data Systems 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 (including points of the identity and attributes verification), subscribers and relying parties. The obligations and liability are governed by mutual agreements made by the parties mentioned above (see Fig. 2.1). Figure 2 presents the parties (entities) associated with certification services: CERTUM certification services provider, registration authority, subscriber and relying party. Continuous lines connecting various pairs of entities mean a need to enter into a contractual relationship. Dotted lines mean that an agreement is unnecessary. Subscriber signs **agreements** directly with Asseco Data Systems S.A. or indirectly with registration authority operating within CERTUM.

Contracts for the provision of certification services should be concluded in writing under pain of invalidity, subject to the provisions of *Art. 16, § 3 of the the Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450).*

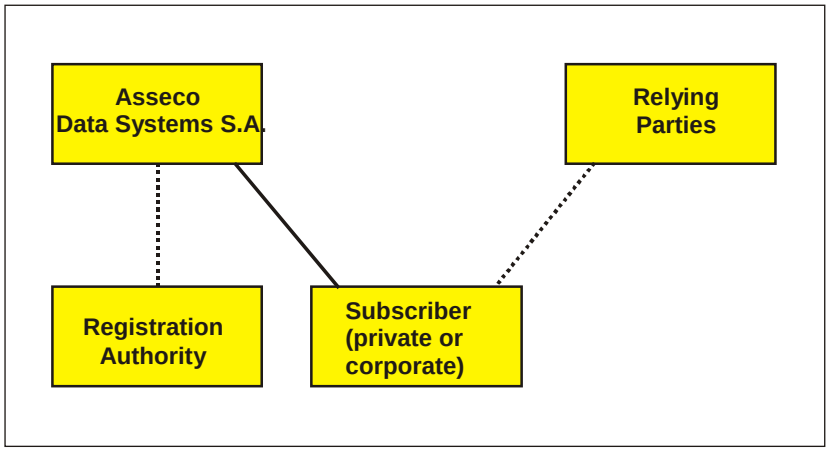

Fig. 2 Agreements between parties

Asseco Data Systems S.A. agreements with subscribers describe types of qualified certification services provided by CERTUM, mutual obligations and liabilities (including financial ones).

2.1. Obligations

2.1.1. CERTUM and registration authority obligations

CERTUM providing qualified certification services ensures that:

- its commercial activity is based on reliable devices and software creating a system that fulfils requirements stated in the *CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements* and FIPS PUB 140 norm *Security Requirements for Cryptographic Modules*,
- its activity and services are in accordance with the law; in particular they do not violate the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)*, included copyrights and licensed third parties rights,
- its services are in accordance with widely accepted standards or specifications:

  - certification services - with *ITU-T X.509 (ISO/IEC 9594-8), ISO/IEC 15945* (CMP protocol) and PKCS#10, PKCS#7, PKCS#12 standards,
  - certification services – withe the *AICPA/CICA WebTrust Program for Certification Authorities*,
  - timestamp services – with ETSI TS 101 861 *Time stamping profile* and RFC 3161 recommendations,
  - certificate status verification (OSCP) – with *RFC 2560* recommendation,
  - notary services (DVCS) – with *RFC 3029* recommendation,
  - Evidences of receipt and submission (including official evidences of receipt and submission) – with *PN-ISO/IEC 13888-3* standard,
  - deposit, registries and repositories tokens – with OASIS Standard ebXML Registry Services and Protocols, Version 3.0, 2 May, 2005
  - attribute certificates – with *RFC 3281* and *RFC 4476* recommendations.
- it complies with and exacts the procedures described in the present Certification Practice Statement,
- issued certificates contain accurate data that were actually at the time of their confirmation,
- issued certificates do not contain any mistakes resulting from negligence or procedure violence by the people confirming applications for certificate issuance or issuing certificates,
- subscribers' Distinguished Names (DN) listed in certificates are unique within **cckDomena** domain,
- it secures personal data protection in accordance with the *Act of August 29, 1997 on the Protection of Personal Data* including its later changes and accomplishing regulations,
- it does not copy or store private keys of its customers,
- it hires employees who possess a knowledge, a qualifications and an experience appropriate to providing qualified services, particularly in the area of:
  - automatic data processing in telecommunication networks and systems,
  - network and systems security mechanisms,
  - cryptography of electronic signatures and public key infrastructure,
  - devices and applications used for electronic data processing,
- if a key pair is generated with the subscriber's authorization, the key pair is confidentially delivered to the subscriber.

Additionally, CERTUM commits itself to:

- manage a list of registered registration authorities,
- manage a list of recommended software and devices,
- carry out scheduled audits in certification authorities and registration authorities belonging to or connected with **certum** domain and **ctnDomena** domain.

- keep information secret relating to CERTUM's certification services and, to secure these information from unauthorized disclosure for a period of 10 years from the moment of termination of legal relationship in accordance with art. 12 pkt.2 of the *Act,* and to protect of data used in confirmation processes for an indefinite period, and to:
    a. retain for at least 20 years:
        - qualified certificates issued by CERTUM,
        - Certificate Revocation Lists issued by CERTUM
        - agreements,
    b. retain of every event logs for at least 3 years in a manner allowing authorized parties to access appropriate and required information.

Regarding registration authorities operating within **cckDomena,** CERTUM ensures that registration authority:

- is subordinated to CERTUM recommendations,
- provides services such as verification of the identity are delivered on the basis of procedures which are adjusted to the recommendations of the present Certification Practice Statement; Certification Policy, internal procedures and legal regulations in force in Republic of Poland, with particular consideration of due diligence requirements,
- sends confirmed data of users to CERTUM certification authority
- is subjected to scheduled external and internal audits carried out by CERTUM service unit or to the ones commissioned by this unit.

2.1.1.1. Time - stamping authority obligations

Time – stamping authority CERTUM QTSA provides time - stamping services in accordance with requirements defined in the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)..* 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 the Appendix 3 (Requirements for encryption algorithms) of the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094).,*
- 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.

Additionally, CERTUM QTSA commits itself to:

- provide continuous 24/7/365 access to supporting services except for technical breaks,,
- use in the timestamp tokens the Coordinated Universal Time – UTC that is provided with the accuracy of 1 second what needs to be interpreted as the maximum permitted delay between the moment of receipt of request, and downloading reliable time. Accessibility and accuracy are ensured even if a number of clients are simultaneously connected,
- base its commercial activity on reliable devices and software in accordance with the requirements defined in: *CAW 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements and ETSI TS 102 023 Policy requirements for time-stamping authorities,*
- conduct its activity and services in accordance with the law; in particular they do not violate copyrights and licensed third parties rights,
- issue timestamp tokens in accordance with *ETSI TS 101 861 Time stamping profile*,
- retain, under the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)*, the every recorded event logs for at least three years,
- issue timestamp tokens that do not contain errors or inaccurate information.

2.1.1.2. 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 the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)* and this Certification Practice Statement.

CERTUM QOCSP and **CERTUM QDVCS** ensure that they:

- use operational procedures and security management procedures, which preclude any possibility of manipulating the certificates or data status,
- verify validity of qualified signatures used according to the requirements of the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094),*
- **CERTUM QOCSP** verify certificate status in accordance with *RFC 2560 Online Certificate Status Protocol (OCSP)* recommendation,
- **CERTUM QDVCS** certify the fact of possession of data or claim of possession of data, 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); tokens are issued according to the requirements defined in *RFC 3029 Data Validation and Certification Server Protocols (DVCS)* recommendation.

2.1.1.3. Delivery authority obligations

Delivery authority **CERTUM QDA** provides services in accordance with the requirements defined in the regulations issued on the basis of the *Art. 16, § 3* of the *Act of 17 February 2005 on Informatization of Operation of Entities Performing Public Tasks (Journal of Laws No. 64, item 565, as ammended)* and the *Art.* 39[1], §. 2 of the *the Code of Administrative Procedure (Journal of Laws 2000 No. 98, item 1071, as ammended).*

CERTUM QDA ensures that:

- 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 the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094),*
- 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.

Evidences issued by **CERTUM QDA** comply with the requirements of *PN-ISO/IEC 13888-3:1999 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques.*

2.1.1.4. 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 the regulations issued on the basis of the Art. 5, § 2a, 2b i 2c of the *Act of 14 July 1983 on National Archival Resources and Archives*, in the *Regulation of the Minister of Finance of 14 July 2005 on electronic invoicing and on sending invoices by electronic interchange, as well as on storage of these invoices and making them available to tax authorities or fiscal control authorities (Journal of Laws No 133, item 1119),* and also in accordance with requirements defined in the *Act of 17 February 2005 on Informatization of Operation of Entities Performing Public Tasks (Journal of Laws No. 64, item 565, as ammended).*

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 the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these*

entities and the technical conditions for secure devices for the creation and verification of electronic signatures (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.

Tokens issued by **CERTUM QODA** and **CERTUM QRRA** comply with the requirements of *OASIS Standard ebXML Registry Services and Protocols, Version 3.0, 2 May, 2005* specification.

2.1.1.5. Attribute Certificates Obligations

Attribute certificate authority CERTUM QACA guarantees that it provides services in accordance with the requirements defined in *the Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)* and this Certification Practice Statement[25], and also in accordance with requirements defined in *ISO/TS 17090:2002 Health informatics - Public key infrastructure* and *ISO/TS 22600:2006 Health informatics - Privilege management and access control* standards.

Additionally CERTUM QACA ensures that:

- 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.

Certificates issued by **CERTUM QACA** comply with the requirements of *RFC 3281* and *RFC 4476* standards.

2.1.1.6. Repository Obligations

The repository is managed and controlled by CERTUM. Therefore, CERTUM is obliged to:

- publish and archive certificate evidences of qualified certification authority **CERTUM QCA**, qualified time – stamping authority **CERTUM QTSA,** qualified

[25] This Certification Practice Statement does not allow a possibility of actualization or modification of attribute certificates.

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.**

- publish and archive Certification Policy of CERTUM's Qualified Certification Services, Certification Practice Statement of CERTUM's Qualified Certification Services, Certification Regulations of CERTUM's Qualified Certification Services, templates of subscriber agreements, lists of recommended applications and devices and list of notaries or entity that perform subscriber's identification and authentication accredited by CERTUM,
- give access to the qualified certificates and attribute certificates, but only in the case when they are publicly available with the subscriber's consent,
- give access to the information concerning certificates status by publishing of CRL's,
- secure constant access to information in the repository for certification authorities, registration authorities, subscribers and relying parties,
- publish CRL's swiftly and in accordance with the deadlines specified in the Certification Policy,

2.1.2. End Users Obligations

2.1.2.1. Subscriber Obligations

By applying for the certificate issuance (request should consist of a hand-written signature) and entering into an agreement with Asseco Data Systems S.A., a subscriber agrees to enter the certification system on the conditions stated in Agreement, Certification Regulations of CERTUM's Qualified Certification Services and Certification Policy of CERTUM's Qualified Certification Services.

Depending on relations between CERTUM and a subscriber and on trust level of the certificate that a subscriber applies for, the obligations can be formulated as an official agreement or an informal agreement between a subscriber and CERTUM.

Subscriber is committed to:

- comply with the rules of the agreement made with Asseco Data Systems S.A.,
- state true data in applications submitted to a registration authority,
- submit or present copies of required documents confirming the information included in a submitted application according to the requirements of the Certification Policy,
- immediately inform CERTUM about any errors, defects or changes in the certificate,
- apply his/her/its own key pair and the public keys of other certification services users only for the purposes stated in the Certification Practice Statement and to take all reasonable measures to keep confidential, and properly protect at all times the private key, including:
    - control of the access to devices containing his/her/its private key,
    - immediately inform Primary Registration Authority when a private key, has been, or there is a reason to strongly suspect it would be compromised,

- create no any electronic signature with its private key if the validity period of certificate has expired and certificate has been revoked or suspended,
- control the access to this software, media, and devices on which the keys or passwords are stored,
- store no any personal identification number password (PIN) in the same place as the cryptographic card containing a subscriber's private key,
- regard the loss or revelation of the password (revealing it to an unauthorized person) as the loss or revelation of the private key (revealing it to an unauthorized person),
- make his/her/its private keys inaccessible to other persons,
- start a procedure of revocation in the case of security violation (or security violation suspicion) of their private keys,
- apply attribute certificate and qualified certificate and the corresponding private keys only for the purpose stated in the certificate and in accordance with the aims and restrictions stated in Certification Practice Statement

In the case when subscriber uses the services of 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 i**t is recommended that each time the subscriber receives (upon request) a token it should check its authenticity and time accuracy, i.e. whether the time difference between local time of token's receiving and time included in token is not greater than accepted (by the user) threshold.

2.1.2.2. Relying Party Obligations

Depending on relations between a relying party and CERTUM or a subscriber and on the types of the certificates, tokens and confirmations approved by a relying party, relying party obligations might be formulated as an agreement between CERTUM and a subscriber.

Disregarding of the character of an agreement, a relying party is committed to:

- thoroughly verify[26] 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. In order to verify the signature a relying party should:
  - specify a **certification path**[27] containing all certificates belonging to other certification authorities that make it possible to verify the signature on the certificate of a signature issuer,
  - make sure that the certification path chosen is the best in terms of verifying the electronic signature or certification, because it is possible that there is more

[26] Electronic signature verification aims at stating whether: (1) an electronic signature was created by means of a private key corresponding to a public key set in a subscriber's certificate issued by CERTUM, and (2) a signed message (document) was not modified after signing it.

[27] See **Glossary**

than one certification path leading from certificate or confirmation to trusted certification authority,

- check whether neither of certificates creating a certification path are placed on the list of revoked or suspended certificates; revocation or suspension of any certificate from certification path influences the earlier expiry of the validity date up to which the verified signature could have been created,
- check if all certificates belonging to a certification path belong to certification authorities and if they are authorized to sign other certificates,
- (optionally) specify the date and time of signing a document or a message. It is possible only when the document or message were signed (prior to signing them) with a timestamp issued by a timestamp authority, or a timestamp was associated with an electronic signature just after the creation of the electronic signature on the document,
- using a defined certification path, verify trustworthiness of the certificate of a signature issuer on a message or a document, and the signature validity on the document or the message,

- in the case of certification made on an attribute certificate, an relying party has to check whether neither of certificates are placed on the End Entity Attribute Revocation List (EARL),
- carry out cryptographic operations accurately and correctly, using the software and devices whose security level complies with the sensitivity level of a certificate being processed and the trust level of applied certificates,
- 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,
- trust only these public certificate keys that:
  - are used in accordance with the declared purpose and are appropriate for applicability ranges that were specified by a relying party,
  - status was verified on the basis of the valid Certificate Revocation Lists or OCSP service, available at CERTUM.

It is in relying party's interest to thoroughly verify each of electronic signature placed on the document (including electronic confirmations in public key certificate or attribute certificate) submitted to him/her/it.

If an electronic document is marked with time or associated with other tokens, confirmations or attribute certificates issued by CERTUM, in order to build a reasonable assurance to the verified tokens or confirmations, a relying party should additionally:

- verify whether the tokens or attribute certificate was correctly electronically certified and verifies whether the private key used by 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** to issuance of token and attribute certificate was not disclosed until the token or attribute certificate verification (unless the time included in comply with the requirement of the

certain time); status of private key may be verified on the basis of verified corresponding public key.

- check the restrictions for using timestamp tokens, certificate status token, data validation and certification server token, delivery token, deposit, registries and repositories tokens and attribute certificate described in this Certificate Practice Statement and stated in agreement with CERTUM.

2.2. Liability

CERTUM acting within authorization of Asseco Data Systems 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 certification 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.

The record of parties' liability stated below does not eliminates nor substitutes for the liability stated in agreements between parties or resulting from separate law regulations.

2.2.1. CERTUM liability

2.2.1.1. Certification authority CERTUM QCA liability

CERTUM QCA 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),
- occurred as a result of the violation of other CERTUM warranties, specified in Chapters 2.1.1

The only services which are outsourced to external entities are the services provided within the framework of registration authority. Despite the fact that the registration authority is linked to a contract with Asseco Data Systems S.A., CERTUM takes full responsibility for this part of the registration authority's work that is related to the provision certification services on behalf of CERTUM.

Nevertheless, CERTUM does not take any responsibility for the actions of third parties, subscribers and other parties not associated with CERTUM. In particular, CERTUM does not bear responsibility for:

- the damages arising from forces of nature: fire, flood, gale, other situations such as war, terrorist attack, epidemic, and other natural disasters or disasters caused by people,
- 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),

- the damages arising from inappropriate usage of issued certificates (term inappropriate understood as the use of a revoked, invalidated or suspended certificate, and not in accordance with the declared purpose of a certificate type, stated in the present Certification Practice Statement),
- 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.

2.2.1.2. Time – stamping authority liability

Time – stamping authority CERTUM QTSA bears liability for cases when direct or indirect damages incurred by a subscriber or a relying party:

- arising despite they have complied with the principles described in Certification Regulations of CERTUM's Qualified Certification Services, Certification Policy of CERTUM's Qualified Certification Services and Certification Practice Statement of CERTUM's Qualified Certification Services,
- result from mistakes made by **CERTUM QTSA**, particularly concerning inappropriate security of the private key used to confirm validity of the timestamp tokens,
- occurred as a result of the violation of other **CERTUM QTSA** warranties, specified in Chapters 2.1.1.1

2.2.1.3. Online certificate status protocol authority, data validation and certification server authority, delivery authority, object deposits authority, registries and repositories authority and attribute certificates authority liability

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** operating within CERTUM bear liability for cases when direct or indirect damages incurred by a subscriber or a relying party:

- arising despite they have complied with the principles described in Certification Policy of CERTUM's Qualified Certification Services and Certification Practice Statement of CERTUM's Qualified Certification Services,
- result from mistakes made by **CERTUM QOCSP**, **CERTUM QDVCS**, **CERTUM QDA**, **CERTUM QODA**, **CERTUM QRRA** or **CERTUM QACA**, particularly concerning inappropriate security of the private key,
- occurred as a result of the violation of **CERTUM QOCSP**, **CERTUM QDVCS**, **CERTUM QDA**, **CERTUM QODA**, **CERTUM QRRA** or **CERTUM QACA**, warranties, specified in Chapters 2.1.1.2, 2.1.1.3, 2.1.1.4 and 2.1.1.5.

2.2.1.1. Repository liability

The liability for functioning of the repository and results of its functioning is taken by CERTUM (See chapter 2.1.1.6).

2.2.2. End user liability

2.2.2.1. Subscribers liability

Subscriber liability results from the obligations and warranties stated in Chapter 2.1.2.1.

2.2.2.2. Relying parties liability

Relying party liability results from the obligations and warranties stated in Chapter 2.1.2.2. The liability conditions may be governed by an agreement with Asseco Data Systems S.A. and a subscriber.

Agreements with subscribers and CERTUM require that relying parties have a sufficient amount of information to make a decision about the approval or rejection of an electronic signature or confirmation while verifying it.

2.3. Financial Responsibility

The financial warranty of Asseco Data Systems S.A. in relation to individual event amounts equivalent of an 250.000 € but total financial warranties of Asseco Data Systems 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.

2.4. Governing Law and Dispute Resolution

2.4.1. Governing Law

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

2.4.2. Supplementary Resolutions

2.4.2.1. Resolution Severability

If particular parts of the present document or the agreements made on the grounds of it are regarded as violating the law in force or against the law, then a court can order to respect the remaining (i.e. in accordance with the law) part of Certification Practice Statement or agreements already made, unless questioned parts are not significant from the point of view of exchange (e.g. commercial transaction) that the parties agreed on.

Resolution severability is particularly crucial in the subscriber agreements.

2.4.2.2. Resolution Survival

The resolutions of the present Certification Practice Statement are valid of the date of the approval by security inspector and publication in the repository up to the invalidation or substitution of the resolutions. Modifications of the resolutions or introduction of new resolutions are carried out in accordance with the procedures presented in Chapter 8.

If the agreement made on the grounds of the present Certification Practice Statement contains contents confidentiality clause or a clause concerning the confidentiality of the

information that the parties possessed when the agreement was in force, copyrights clause or intellectual rights clause, these clauses are assumed in force also after the validity period expires, for a period that should be agreed by the parties in the agreements.

Agreements resolutions or Certification Practice Statement resolutions cannot be transferred to third parties.

2.4.2.3. Resolution Notice

The parties mentioned in the present Certification Practice Statement can state, by means of agreements, the methods of notifying one another. If they did not, the present document allows for information exchange by means of regular mail, electronic mail, fax, telephone, and network protocols (e.g. TCP/IP, HTTP), etc.

The choice of the means can be extorted by the type of information. For instance, most services delivered by CERTUM require the application of one or more permitted network protocols.

Some information and announcements must be supplied to parties in accordance with an established schedule or deviation from this schedule. This applies, in particular, to the publication of certificate revocation list (CRLs), information on the breach of the CA's private key, and to any changes to parameters of certificates issued by CERTUM..

2.4.3. Disputes Resolution

The subject of disputes resolution can only be discrepancies or conflicts between the parties in respect to issuance and revocation of qualified certificate based on the present Certification Practice Statement and concluded agreements.

Disputes or complaints following the usage of certificates, certificate evidences, timestamp tokens, certificate status tokens, data validation tokens and Evidences of receipt and submission (including Official evidences of receipt and submission) delivered by CERTUM will be resolved by mediation on the basis of written information. Complaint handling is reserved for Chairman of Asseco Data Systems S.A. Board. Complaints are proceeded within 10 days of their delivery.

Disputes related to CERTUM's qualified services will be first settled through conciliation.

If the complaint is not settled within 30 days of the commencement of 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.

In the instance of the occurrence of arguments or complaints following the usage of an issued certificate or services delivered by CERTUM, subscribers commit themselves to notify CERTUM of the reason for the argument or complaint.

2.5. Fees

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

http://www.certum.eu

CERTUM may apply different models of charging for its services:

- **retail sale** – fees are charged separately for every service unit, e.g. every single certificate or a small package of certificates,

- **wholesale** – fees are charged for a package of certificates, a number of certificates sold once,
- **subscription sale** – fees are charged once a month; the extent of this charge depends on a type and number of service units and is particularly used in timestamp services and certificate status verification by means of OCSP protocol,
- **indirect sale** – fees are charged for every service unit from a customer who renders services established on the basis of CERTUM infrastructure.

2.5.1. Certificate issuance fees

CERTUM charges a fee for issuance of a certificate.

2.5.2. Certificates and certificate evidences access fees

CERTUM does not charge a fee for access to certificates and certificate evidences.

2.5.3. Timestamps, tokens and attribute certificates fees

CERTUM charges a fee for issued timestamps, certificate status tokens (OCSP response tokens), data validation tokens, status delivery tokens (including official tokens), deposit, registries and repositories tokens, and attribute certificates.

2.5.4. Qualified certificate or attribute certificate revocation and status information access fees

CERTUM does not charge a fee for qualified certificates or attribute certificates revocation, publishing certificates in CRLs and making CRLs published in the repository (or elsewhere) accessible to relying parties.

2.5.5. Other Fees

CERTUM can charge fees for other services. The services might concern:

- generating keys to subscribers,
- testing of applications and devices and including them in the recommended applications list,
- sale of license,
- execution of design, implementation and installation tasks,
- sale of Certification Practice Statement, Certification Policy, handbooks, guides, etc, published in print,
- trainings.

2.5.6. Fees Refund

CERTUM makes efforts to secure the highest level of its services. If a subscriber or a relying party is not satisfied with the services, they may request certificate revocation and fee refund only if CERTUM does not fulfill its obligations and duties specified in the present Certification Practice Statement.

Fees refund claims should be submitted to the addresses stated in Chapter 1.9.

2.6. Repository and Publication

2.6.1. Information Published by CERTUM

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

http://www.certum.eu

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,
- certificate evidences belonging to 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**, and qualified attribute certificates authority **CERTUM QACA**,
- the list of recommended applications and devices approved by CERTUM,
- the lists of accredited registration authorities or persons confirming identity and attributes,
- Certificates Revocation Lists (CRLs); CRLs are accessible at the so called CRL distribution points, whose addresses are set in every certificate or certificate evidence issued by CERTUM QCA; the basic point of CRLs distribution is repository at: http://crl.certum.pl,
- supplementary information, e.g. announcements and notifications.

2.6.2. 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,
- registration authorities certificates – upon every issuance of new certificates,
- subscribers’ certificates – upon every issuance of new certificates, on subscribers’ prior approval,
- Certificate revocation and suspension lists – see Chapters 4.8.4 and 4.8.9;
- supplementary information – upon every updating of it.

2.6.3. Access to Publications

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

CERTUM service unit has implemented logical and physical mechanisms protecting against unauthorized adding, removing and modifying of the information published in the repository.

2.7. Audit

Audits intend to control the practices of CERTUM service unit or subjects delegated by the unit are compliant with the Integrated Management System which includes the requirements of the standards: PN-EN ISO-9001:2009 and PN ISO/IEC 27001:2007, and the declarations and procedures of CERTUM (including the Certification Policy and the Certification Practice Statement).

CERTUM audit mainly regards Primary Registration Authority and key management procedures. It also concerns all qualified certification authorities providing qualified certification services, registration authorities, and other elements of public key infrastructure, e.g. repository.

CERTUM audit may be carried out by internal units of Asseco Data Systems S.A. (internal audit) and organizational units independent from Asseco Data Systems 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*.

2.7.1. Audit Frequency

An audits checking the consistency with procedural and legal regulations (particularly the consistency with Certification Practice Statement and Certification Policy) is carried out at least once a year.

2.7.2. Identity/Qualifications of the Auditor

An external audit is carried out by an authorized and independent from CERTUM domestic institution or the institution with a representation in Poland. If the audit is carried out on behalf of the Minister in charge of economy, it can only be are carried out by the employees of the ministry's organizational unit which provides support services to the minister in charge of the economy or by employee of the National root (National Center of Certification, NCCert) that generates and issues certificate evidences of certification authorities on behalf the Minister in charge of economy.

An internal audit is carried out by designated unit, operating within Asseco Data Systems S.A. structure.

2.7.3. Topics Covered under the Compliance Audit

External and internal audits are carried out in accordance with the rules specified in the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* and the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)*.. Detailed scope of audit is specifies by authorization issued to auditors by the Minister in charge of economy or an entity acting under the authority of the Minister (in the case

of an audit commissioned by the Minister) or by CERTUM security inspector (in the case of an audit commissioned by the Asseco Data Systems S.A.)

The scope of Web Trust audit includes:

- checking whether the certification service provider's activity meets the requirements of the organizational and legal terms of the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* and the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)*,
- physical security of CERTUM,
- procedures of subscribers' identity verification,
- certification services and procedures of the services delivery,
- security of software and network access,
- security of CERTUM personnel,
- system journals and system monitoring procedures,
- backup copy creation and their recovery,
- archive procedures,
- records of CERTUM's configuration parameters,
- records of software and devices inspection and service.

The vulnerability evaluation is executed according to the principles described in the chapter 4.15.7

2.7.4. Actions Taken as a Result of Deficiency

Records of internal and external audits are submitted to CERTUM **security inspector**. The security inspector is committed to prepare a written opinion concerning the deficiencies specified in the records. Information about deficiencies removal is submitted to the auditing organization.

In the case of an audit commissioned by the Minister in charge of economy, the Minister after reviewing the protocol and reservations as well as the explanations made by CERTUM notifies the auditors of the results of audit and, if necessary, shall fix the time of deficiencies removal not less than 14 days (Art. 40 of the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450*)

2.7.5. Notifying of Audit Results

CERTUM does not publish the results of audit.

2.8. Confidentiality Policy

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

Asseco Data Systems S.A. ensures that third parties are given the access only to the information that is publicly accessible in a certificate or certificate evidence. The other data provided in applications submitted to CERTUM shall never be voluntarily or deliberately revealed to a third party in any circumstances except as specified in *art.12, ∫ 3* of the *the Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450),* at the request of:

- a court or public prosecutor, with respect to pending proceedings,
- a minister in charge of the economy, with respect to his supervision of certification-service-providers,
- other state bodies authorized to obtain the information pursuant to the provisions of separate acts, with respect to proceedings they conduct, concerning the operations of certification service providers.

CERTUM does not copy nor store subscribers private keys, used for signature creation, nor any data which could be used for keys reconstruction.

2.8.1. Types of Information to be Kept Secret

Asseco Data Systems S.A., its employees and entities that perform actual certification activities are committed to keep secret understood as a company secret, during and after the employment. Information regarded as company secret[28] are managed and governed by internal company regulations and in particularly concerns:

- information supplied by subscribers, besides the information that needs to be revealed for appropriate certification services; in other cases the revelation of received information requires a prior written approval of the information beholder or results from exceptions set forth in the *Art.12, ∫ 3* of the *the Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* (see also Chapter 2.8),
- information supplied by/to subscribers (e.g. the contents of agreements with subscribers and requesters, accounts, applications for registration, issuance, renewal, revocation of certificates; a part of the information mentioned above can be made accessible solely upon approval of and in the scope specified by its owner (i.e. subscriber),
- entries of system transactions (the whole of the transactions, as well as **data for control inspection** of transaction, the so called system transactions logs),
- entries of information about events (logs) connected with certification services, stored by CERTUM and registration authorities,
- entries of an internal and external control, if it might cause a threat to CERTUM security (in accordance with Chapter 2.8.2, the majority of this information should be accessible for the public),
- emergency plans,
- information about steps taken in order to protect hardware devices and software, information about administering of certification services and planned registration rules.

[28] A company secret means publicly inaccessible technical, technological, trade, organizational information that an entrepreneur, taking all indispensable action, keeps confident.

Asseco Data Systems S.A. is not obligated to keep secret in relation to a party of the agreement about the delivery of certification services. Persons responsible for keeping secret and obeying the rules concerning information practice bear criminal liability in accordance with the law regulations. The obligation to observe the secrecy shall remain in force for the period of 10 years as of the date of cessation of legal relationships with Asseco Data Systems S.A.

2.8.2. Types of Information Not Considered Confidential and Private

The whole information indispensable for the process of appropriate functioning of certification services is not considered confidential and private. It particularly concerns the information included in a certificate by certificate issuing authorities, in accordance with the description in Chapter 7. It is assumed that a subscriber applying for certificate issuance is aware of what information is included in the certificate and approves of the publication of that information.

A part of information supplied by/to subscribers might be made available to other entities, solely upon the subscriber's approval and within the scope specified in the subscriber's written statement.

The following information, submitted to certification authorities and registration authorities, is accessible for the public:

- 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 of CERTUM with subscribers and relying parties,
- the price list of services,
- guides for users,
- certificates,
- Certificates Revocation List (CRL),
- information about training

2.8.3. Disclosure of Certificate Revocation Reason

If certificate revocation is performed upon request of an authorized party (not the party whose certificate is being revoked), information about revocation and the reasons of it are disclosed to both parties.

2.8.4. Release of Confidential Information under the Article 12 of the *Act on Electronic Signature of 18 September, 2001*

Confidential information might be released to law enforcement officials mentioned in the *Art. 12, § 3* of the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* solely upon the fulfilling of all requirements set by the legal regulations in force in the Republic of Poland.

2.8.5. Release of Confidential Information for Scientific Purposes

The present Certification Practice Statement does not state any conditions in this respect.

2.8.6. Release of Confidential Information upon Owner's Request

The present Certification Practice Statement does not state any conditions in this respect.

2.8.7. Other Circumstances of Release

The present Certification Practice Statement does not state any conditions in this respect.

2.9. Intellectual Property Rights

All trademarks, patents, brand marks, licenses, graphic marks, etc., used by Asseco Data Systems 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 (see Chapter 7.1.1.1) or – in the case of qualified professional certificate – is the property of the represented entity.

2.9.1. Trade Mark

Asseco Data Systems S.A. owns registered trade mark, consisting of graphic mark and inscription, which constitute the following logo:

Fig. 3 CERTUM Logo

The mark and inscription constitute CERTUM logo. The logo is a registered trade mark of Asseco Data Systems S.A. and cannot be used by any other parties without prior written approval of Asseco Data Systems S.A.

CERTUM mark is an additional element of logo of every registration authority, operating on behalf of CERTUM.

2.9.2. Property Rights in the Certification Practice Statement

CERTUM retains all Intellectual Property Rights in and to this Certification Practice Statement.

2.10. 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. The rules are based on particular types of information that is included in certificates and they specify the means indispensable for assuring that the information is precise and credible at the time of issuing a certificate.

The verification is **obligatorily** performed in the stage of subscriber's registration and **on request** of CERTUM in the instance of any other certification service.

Every subscriber submitting a certification request for the first time must be subject to the registration.

Certificate renewal, rekey and certificate modification is possible only if the subscriber is already registered in the system and the subscriber's identity has been verified based on the valid electronic signature used to authenticate the renewal, rekey or certificate modification request

Also, the issuance of the next certificates to the subscriber is only possible when the subscriber is already registered in the system, which means the subscriber has had any valid certificate (even if the certificate is revoked or expired), and the subscriber's identity has been verified in the same way as in the case of initial registration.

CERTUM and subordinate registration authorities confirm the identity of the qualified certificate applicant with a valid identity card or passport in accordance with the provisions of the *Art. 21, § 2 of* the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094).*

3.1. Initial Registration

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

The registration comprises a number of procedures which allow a certification authority – prior to issuing a certificate to a subscriber - to gather authenticated data concerning a given entity or identifying this entity. Confirmation of these data requires a personal contact with a registration authority, a notary or other authorized person confirming identity.

In addition to the Distinguished Name (see Chapter 3.1.3), the subscriber is required to provide in the registration form the following information, which will enable the unambiguous identification of the subscriber, including:

- parents' names,
- the ID card or passport number,
- date of birth,
- contact details.

Every subscriber is subjected to a registration process only once. After the verification of data supplied by a subscriber and making an agreement for the qualified services a subscriber is

included on the list of authorized users of CERTUM services and supplied with a public key certificate.

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.

3.1.1. Registration of subscribers

Before entering into the subscriber agreement with Asseco Data Systems S.A., every subscriber is obligated to familiarize himself/herself/itself with Certification Regulations of CERTUM's Qualified Certification Services.

Registration may takes place only on individual request of subscriber (including requesters). Registration form is filled by means of WWW pages of CERTUM or in the registration authority.

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 (e.g. as an Order) 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,

The detailed terms of reference to act on behalf of someone else should be defined in authorization.

Applicant during registration process is informed, in a clear and generally understandable form, in writing or in the form 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

The subscriber is obliged to confirm, in the *Subscriber Agreement for providing qualified certification services* bearing handwritten signature, his/her/its familiarization with the rules described above. The signing of the *Agreement* also means that:

- the Subscriber agrees that Asseco Data Systems S.A. will process his/her personal data for the purposes necessary for the certification process,
- the Subscriber represents that the information he/she provided is true and have been given voluntarily,
- the Subscriber applying for a certificate is aware of what information is placed in the certificate and agrees to make it publicly available.

The subscriber is also obliged to present to registration authority, notary or to person verifying identity following documents:

- authorizations for creating an electronic signature on behalf of the authorizing entity,
- other documents which are required to verify data provided in an application, e.g. employer's certificate of employment.

Future subscriber agrees on statement:

- to use by CERTUM the data required for verify an electronic signature,
- for processing of personal data by Asseco Data Systems S.A.and registration authority for the purposes of the certification process.

3.1.2. Types of Names

Certificates issued by CERTUM comply with the norm X.509 v3. In particular, it means that a certificate issuer and a registration authority operating on behalf of the issuer approve of subscribers' names that comply with the standard X.509 (with referring to recommendations of the series X.501). Basic names of subscribers and certificate issuers placed in CERTUM certificates are in accordance with Distinguished Names (DNs) – (also known as directory names), created according to the recommendations X.501 and X.520. Within DN, it is possible to define attributes of Domain Name Service (DNS), described in *RFC 2247*. It allows subscribers to use two types of names: DN and DNS simultaneously. It might be substantial in the cases of issuing certificates to servers controlled by the subscriber.

To ensure easier electronic communication with a subscriber, an alternative name of a subscriber is used in CERTUM certificates. The name can also contain subscriber's electronic mail address that is in accordance with the recommendation *RFC 822*.

Tab. 15 Requirements imposed on the name of a certificate subject.

Certificates	Requirements
Qualified certificate	Subject's DN in accordance with X.500 and optionally the alternative name in the case when it is marked as non-critical.
Certificate evidences	Non-empty value of the field **subject** or empty in the case when the field of the alternative name exists (**SubjectAltName**) and it is marked as non-critical[29].
Certificate of infrastructure keys	Subject's DN in accordance with X.500 and optionally the alternative name in the case when it is marked as non-critical

The whole information, submitted in subscriber's application for registration and included in the certificate by a certification authority is accessible for the public. The list of data included in a certificate is in accordance with the recommendation X.509 v.3 and is presented in Chapter 7 (see also Chapter 3.1.3).

3.1.3. Need for Names to be Meaningful

The names included in the Distinguished Name DN allow unambiguous identification of the entity associated with the public key placed in the public key certificate field of issued certificate and have their meaning in Polish or English language.

Distinguished Name structure, approved/assigned and verified by a registration authority, depends on the type of certificate and a subscriber.

DN name may consist of the following fields (descriptions of a field follows its abbreviated name that complies with the recommendation X.501):

- **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

[29] Defined names might contain attributes that are not attributes in X.500 documents; particularly, an attribute defining e-mail address might appear in these fields.

Qualified certificates are issued to natural persons. They can be issued in various categories[30]:

- **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,

If the name and surname of subscriber are made on certificate, the possibility to use a pseudonym in the certificate shall be excluded. If the name of organization is included in subject name the following attributes must be used: ***state or province, locality and address*** *of this organization.*

In the case of infrastructure devices owned by natural persons their DN contains an additional field:

- **field SN** – serial number or identifier of device.

In the case of certificate evidences issued to the minister in charge of the economy or to entity authorized by the minister, the DN must consist following attributes:

- **field C** – international country code (in Poland – **PL**),
- **field O** – organization name,
- **field ST** – state or province,
- **field L** – locality,
- **field CN** – common name,
- **field SN** – serial number containing entry in the register of qualified certification service providers; when the issuer is a minister in charge of the economy the field doesn't exist.,
- **field DC** – domain name used for identifying the objects in the X.500 catalogue available through LDAP protocol.

Subscriber's DN must be confirmed by a registration inspector of Prime Registration Authority (see also chapter 3.1.5)

3.1.4. Rules for Interpreting Various Names Forms

The interpretation of the fields provided in certificates issued by CERTUM is in compliance with certificates profile described in document *Profil certyfikatu kwalifikowanego i CRL*[31]. In creating and interpreting of DNs, the recommendations specified in Chapter 3.1.2 of this document and in the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)* are employed.

30 Certificates in the category I are issued to individual persons, in the category II are issued to employees and in the category III are issued both to the individual persons and employees.

31 *Profil certyfikatu kwalifikowanego i CRL*, wersja 1.3, The Publication of Zespól Podmiotów Świadczących Usługi Certyfikacyjne w Polsce przy Centrum Certyfikacji i Zaufania Centrast S.A., Warszawa, październik 2003

3.1.5. Names Uniqueness

Identification of each entity holding the certificate issued by CERTUM is making under the Distinguished Name.

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

Subscriber's DN is suggested by the subscriber. If the name is in accordance with general requirements stated in Chapter 3.1.2 and 3.1.3 the submitted proposition is initially accepted by the registration authority operator. Within CERTUM qualified domain, the uniqueness of the names of is guaranteed.

If the name proposed by the subscriber violates the rights of other parties to use this name (see Chapter 3.1.4) CERTUM may add additional attributes to the DN and guarantees the uniqueness of this name within the CERTUM domain. The subscriber may, under the provisions of chapter 4.2 reject the proposed name.

Format of global uniqueness of distinguished name of the subscriber is based on serialNumber, name of issuer and name of subscriber. SerialNumber uniquely distinguishes a specific subscriber.

If any subscriber decided to cease using CERTUM's qualified services, the name request which name was used by this subscriber shall be rejected.

CERTUM shall not to register a name of subscriber which was once used by other subscriber even on the basis of his written authorization.

Within CERTUM domain, the uniqueness of the names of directories within the repository is also guaranteed. Applications basing on this property of the names of CERTUM QCA directories and services rendered within them have a guaranteed service continuance, without any risk of service disruption or substitution.

3.1.6. Name Claim Dispute Resolution Procedure

Names that are not owned by a subscriber or a represented entity cannot be used in his/her/its applications. CERTUM does not play a role of an arbiter resolving disputes concerning the property rights to any distinguished name, trademark or trade name.

In disputes concerning name claims, CERTUM is entitled to reject or suspend a subscriber's application without taking liability in virtue of this suspension/rejection. CERTUM is also entitled to take all decisions concerning the syntax of a subscriber's name and assigning the subscriber with the names resulting from it.

3.1.7. Proof of Possession of Private Key

If private keys are not generated by subscribers, they are not obliged to providing the proof of possession of private key. If the subscriber generates its own keys CERTUM may require the proof of possession of private key. Subscribers have the option to generate new keys only if they have a valid qualified certificate issued by CERTUM. Owning a valid qualified certificate shall be deemed to be proof of possession of the private key corresponding to the public key certified by CERTUM.

3.1.8. Authentication of natural person's identity

Verification of the identity of natural person has two purposes. The first purpose is to prove that the data in the request relates to the existing natural person and, secondly, that the applicant is indeed that person who has been mentioned in the application.

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 the case of certificates category II 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

Registration inspectors of Prime Registration Authority, registration authority operators notaries and other persons who confirm subscribers' identity are committed to verify the correctness and truthfulness of all data provided in an application (see chapter 4.1)

Verification procedure of the identity of natural person is based on detailed verification of documents and the request submitted by the subscriber and, optionally, verification of correctness of distinguished name DN.

After successful verification of the request, the registration authority operator or other person who confirm subscriber's identity enter into an agreement with the subscriber on behalf of Asseco Data Systems S.A. In the case of notary's verification, applicant unilaterally signs an agreement that is after transferred to Asseco Data Systems S.A. and shall be signed by the registration authority operator and sent to the address specified by the applicant.

Detailed requirements for the registration inspector, registration authority operator, notary or other person who confirm subscribers' identity are specified in separate document. The status of this document is "non-public".

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.

3.1.9. Authentication of the subscriber's rights and other attributes

The registration inspector of Primary Registration Authority and the registration authority operator are obliged to verify (in accordance with the Art.20 ust.3 of the Act) subscriber's authorizations always in situation, when a subscriber submits the certification request and acts:

a) on behalf of another natural person, legal person or an organizational unit not endowed with legal personality,
b) as a member of a body or as a body of a legal person or an organizational entity not endowed with legal personality
c) as a public authority.

Authentication is a part of procedures of processing of customers' requests for the issuance of the certificate to the individual person representing another person (natural or legal). In this case the issued certificate should be interpreted as confirmation of the rights of the natural person to use a private key on behalf of another person.

The process of checking the authorizations includes authentication of authorized person identity.

The process of checking the authorizations consists in verification of submitted authorization on the basis of:

- submitted documents (e.g. letter of attorney)
- checking the signature created on this documents by entitled person,

- checking of compliance of information in certification application with data included in the submitted documents.

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

Recertification of keys or modification of existed certificate are possible only if the subscriber has a valid qualified certificate issued by CERTUM.

In order to renew a certificate, the subscriber is required to sign (electronically) the addendum to the Subscriber Agreement. Enlargement the scope of the Subscriber Agreement is only to extend the period of provided certification service for another period of validity. No other changes are expected.

Authentication of the identity of subscribers who apply for rekey, renewal or modification of certificates must be performed by an registration inspector of Primary Registration Authority, registration authority operator, a notary or other person who confirm subscribers' identity in the following cases:

- subscriber represents other entity (category II) and the validity period of the certificate exceed the period of validity of the previously submitted authorization to representing the entity indicated in the certificate,
- the data set in the certificate have been modified,
- the request was not electronically signed or certified using the private key that corresponds to the public key included in the valid certificate issued by CERTUM QCA„
- when it concerns key certification resulting in a certificate issued for the first time to a given subscriber according to a new certification policy.

3.2.1. Certification and Rekey

Certification and rekey (key update) occurs when a subscriber requests for:

- additional certificate of the same type or of different type, and
- rekey of currently valid certificate.

In both cases applications contain the request for generating of a new key pair and certificate issuance. The requests have to 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.

Rekey might be performed by a subscriber periodically, on the basis of parameters of a given certificate that is already owned by the subscriber. The result of rekey is a new certificate whose parameters are the same as the parameters of the certificate mentioned in the application, except for a new key, certificate serial number and validity period (see Chapter 4.6)

Verification of the identity of the subscriber requesting rekey is carried out on the basis of electronically signed application for certificate rekey.

Key certification – unlike rekey – is not associated with any valid certificate and concerns issuing any type of certificate (subscriber must be registered, i.e. posses any valid certificate - even if the certificate is revoked or has expired). Identity of the requester applying for key certification must be verified by the registration inspector in Primary Registration Authority, a registration authority operator, by a notary or other person who confirm subscribers' identity.

Subscriber's authentication and identification procedure in key certification or rekey (due to the agreement or declared period of the last direct verification of identity performed by the registration inspector in Primary Registration Authority, a registration authority operator, by a notary or other person who confirm subscribers' identity) is performed analogically to initial registration (see chapter 3.1).

3.2.2. Certificate Modification

Certificate modification means creation of a new certificate on the basis of the certificate that is currently owned by the subscriber. A new certificate has a different public key, a new serial number, and it differs in at least one field (its contents or appearance) from the certificate on the basis of which it is being issued.

Modification might be necessary e.g. in the case of changing the position at work or the name, under the condition that these data were previously stated in the certificate or they should be added. If data that are verified in accordance with subscriber's authentication procedures on the basis of appropriate documents (e.g. certification of the position at work) have been modified, every application must be confirmed in a registration authority (see Chapter 4.7).

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. It is possible to submit application in a non-electronic form.

In the first case, a subscriber must submit an authenticated application for certificate revocation. The subscriber authenticates the application by making an electronic signature on it or by providing previously agreed password on the web page.

A subscriber who has lost an active private key (or it has been stolen) as well as a secret of certificate revocation should submit the application in registration authority. Application for revocation must be certified by a registration authority or certification authority operator. This certification does not have to be electronic.

In both cases, an application needs to enable univocal identification of the subscriber's identity. Application for revocation might concern more than one certificate.

Authentication and identification of a subscriber in a registration authority is performed analogically to initial registration (see Chapter 3.1) or rekey (see Chapter 3.2.1). Authentication of a subscriber in a certification authority consists in verification of application authentication or identity of the requester.

Detailed procedure of revocation is disclosed in Chapter 4.8.3.

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 carried out on the basis of the agreement made between the subscriber and Asseco Data Systems S.A. The subscriber's identity is verified:

- on the basis of an electronically signed agreement and the content of qualified certificate; an electronic signature may be created by the individual person who posses an unexpired qualified certificate,
- by the registration inspector, a notary or other person who confirm subscribers' identity in accordance with the requirements laid down in chapter 3.1 in the case of the subscriber who doesn't posses a qualified certificate or the certificate is expired or revoked.

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 may be connected with the registration of the subscriber of CERTUM's QCA services.

In the case of issuance of the attribute certificates, procedures laid down in Chapters 3.1 (except 3.1.7), 3.2.1 and 3.3 are implemented. If the given rules and procedures apply to the cryptographic key they are ignored, besides the key used by CERTUM QCA for issuance of attribute certificates and attribute certificates revocation list.

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. Submitted applications should contain information necessary for correct identification of the subscriber.

CERTUM provides access to the following basic services:

- issuance of qualified certificates and certificates of infrastructure keys including registration, certification, certificate renewal, rekey, certificate modification and revocation or suspension,
- issuance (certification) and revocation of the certificate evidences in accordance with: *Rozporządzenie Rady Ministrów z dnia 9 sierpnia 2002 r. w sprawie określenia szczegółowego trybu tworzenia i wydawania zaświadczenia certyfikacyjnego związanego z podpisem elektronicznym*,
- time - stamping,
- certificate status verification,
- data validation,
- delivery services,
- object deposit authority,
- registry and repositories authority,
- attribute certificate authority.

Services of issuance of qualified certificates and certificates of infrastructure keys (so called certification services) their revocation, suspension and rekey are described in Chapters 4.1 - 4.7, a time - stamping services are described in chapter 4.8, a certificate status verification services (OCSP) are described in 4.8.11, data validation services are described in chapter 4.9, delivery services are described in 4.11.

CERTUM issues cross certification certificates to the National root (NCCert) and certificate evidences according to procedures for key management (see chapter 6.1). Certificates of CERTUM are issued according to procedures described in chapter 6.1.1.

4.1. Application Submission

Subscriber's applications are submitted indirectly by a registration authority. 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 3.1.8 and 3.1.9), 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. An application for renewal, rekey or modification is submitted by a subscriber only 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) 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 represented entities are notified about this fact.

4.1.4. Processing of applications in registration authority

Verified application with required documents is submitted to Primary Registration Authority.

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.

4.1.5. Processing of applications in certification authority

A certification authority retrieves certification request token out of a request box and then processes its and records these procedures in database and system journals.

4.2. Certificates Issuance

On receiving an appropriate certification request token and processing it (see Chapter 4.1.5), a certification authority **issues a certificate**. Validity periods of the issued certificate depend on the certificate type and the subscriber's category and they are in accordance with periods presented in Table 20 and 21.

Date of issuance is recorded in the event journal and is not later than beginning of the validity period of certificate that is specified in field ***notBefore*** *(see chapter 7.1)*

Every certificate is issued off-line.

In the moment of certificate issuance, subscribers and represented entities are notified about this fact. To download a certificate, the subscriber has to fill in a special form with a cryptographic card number, a social security number (or identification data for foreigners) and the special code received from CERTUM that allows the installation of a certificate on the cryptographic card.

At the same step, before installing / downloading a certificate, the subscriber must get the PUK code, which will be necessary to give the authentication code (PIN).

A certificate can be installed on the cryptographic card automatically - via dedicated JAVA application or can be downloaded and installed using the CETUM's proCertum CardManager software.

Description of the mechanism to automatically download a certificate is as follows:

- a browser launches the Java applet from a web page, and the applet is then executed within a Java Virtual Machine (JVM), then
- a dedicated library that generating keys is started,

(at this point the user must have direct access to the CERTUM services and could not be blocked by a Proxy server).

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

CERTUM can refuse to issue the certificate to any requester without taking any obligations or responsibility that might follow the requester's damages or loss resulting from this denial. The certification authority should immediately refund the requester the certificate fee (if the requester paid it), unless the requester stated false data in his/her/its application.

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 to CERTUM within 14 days of the reception of the 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:

- subscriber's submission of certificate acceptance to the CERTUM 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 Asseco Data Systems 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 on the basis of revocation request.

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. Certificate and Key Usage

Subscribers must use private key and certificates:

- in accordance with their purpose stated in the present Certification Practice Statement and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage** see chapter 7.1),
- in accordance with the optional agreement between the subscriber and Asseco Data Systems S.A.
- only within the validity period (not applicable to certificates for digital signature verification),
- until the certificate revocation; when the certificate is suspended, the subscriber should not use the private key, particularly for creating a signature.

Relying parties, including registration authority operators, must use public keys and certificates:

- in accordance with their purpose stated in the present Certification Practice Statement and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage** see chapter 7.1)

- only upon their status verification and verification of the signature of the certification authority that issued the certificate,
- until the key revocation (applicable to public keys for key exchange, data encryption or key agreement); when the certificate is suspended, the relying party should not use the public key.

4.5. 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.

CERTUM may provides the services of recertification of the same pair of cryptographic keys to the certification authorities in accordance with the chapter 6.1.1. 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 being the subject of the update is not revoked.

4.6. 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.

Rekey request supplied by a subscriber can apply only:

- to a currently valid certificate and certificate not revoked before
- when the subscriber has a private key associated with said certificate for digital signatures creation,

On the other hand, key certification also applies to situations when a subscriber:

- does not have a current and valid private key for digital signatures creation,

- requests an additional certificate of the same type or of different type, but only within the certification policy used for issuance of at least one certificate,

Rekey and certification requests are processed in accordance with Chapter 4.1.4 and 4.1.5.

Certification and rekey procedure can be also applicable for certificate evidences of the certification authorities, although in such a case all customers of the certification authority should be informed about procedure execution.

CERTUM always informs subscribers (at least 14 days in advance) about forthcoming validity period expiry.

4.7. Certificate modification

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, including public key change.

Certificate modification:

- is performed only on subscriber's demand and must be preceded by submission of a suitable certificate modification request, and
- the certificate validity period has not expired or the certificate has not been revoked.

Certificate modification is treated and processed as rekey (certificate renewal) in case of modification of data of lesser sensitivity, such as:

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

or as a certification, when modifying data of greater sensitivity.

Notice:

(a) Modification can be applicable for values, attributes and extensions of particular types of certificates. For example, if the subject of modification is **CERTUM QCA personal** certificate, its contents can be modified only within the structure contained in the issued certificate and specified in a profile of this certificate

(b) Submission of the modification request contains the request for generating of a key pair in the Primary Registration Authority.

Modification request is available in an electronic form via CERTUM WWW site and must be confirmed by registration authority.

Modification requests are processed in accordance with Chapters 4.1.4 and 4.1.5.

4.8. Certificate revocation and suspension

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

Requirements for revocation and suspension of certificates are specified in the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450).* The *Article 31, § 4*

and 5 of the Act is most substantial. According to *§ 4*: the revocation of the certificate evidence of **National root (NCCert)** used for the verification of electronic authentications made by qualified certification service providers **CERTUM QCA, CERTUM QTSA, CERTUM QOCSP**, **CERTUM QDVCS**, **CERTUM QDA**, **CERTUM QODA**, **CERTUM QRRA**, **CERTUM QACA**, results in the invalidity of those authentications, unless it is proved that an authentication was made prior to the revocation of the certificate evidences.

Requirements mentioned above are particularly essential for long term electronic signatures which are verified after expiration of the certificate associated with this signature. Such situation is illustrated in Figure 4[32]. Moreover, the revocation of the certificate evidence, deletion of an entry of authority from the register of qualified certification service providers or in the case of cessation of the certification authority operation shall not result in the invalidity of qualified certificates issued by these authorities before the time point of this revocation.

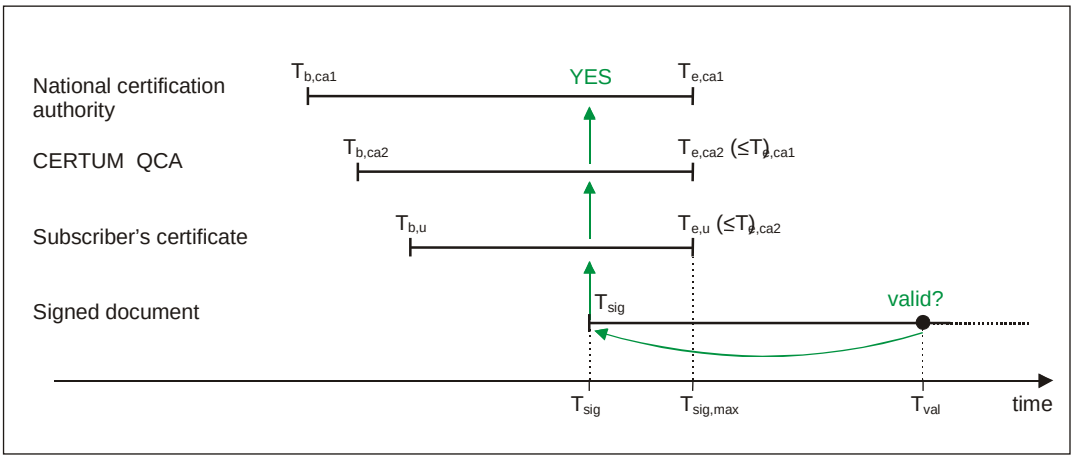

Fig.4 Successful verification of electronic signature based on algorithm described in RFC 3280 recommendations.

The relying party who wants to verify an electronic signature at the T_{sig} moment (this is any moment after T_{sig} moment of the signature creation) should check the signature using a public key included in certificate of the signatory and then should check whether this certificate and all other certificates in a certification path was being valid in the T_{sig} moment in which the document was verified or signed.

During suspension period or shortly after subscriber's certificate revocation, the certificate should be considered as not valid (in state of revocation). Similarly, in the case of certification authority certificate – cancellation of validity of this certificate type means withdrawal of the rights to issue certificates for its owner but does not affect validity of certificates issued by the certification authority when such a certificate was valid.

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

Although certificate suspension is a specific form of revocation, this CPS will distinguish both terms to emphasize the essential difference between them: certificate suspended can be cancelled while revoked – cannot. Once revoked certificate can not be restored.

---

32 Presented scenario derives from *Common ISIS-MailTrust Specifications for Interoperable PKI Applications From T7 & Teletrust ISIS-MTT Specification Optional Profile, SigG-Profile, Version 1.0.2, July 19th 2002*.

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.**

Certification authority revokes these certificates which were not reactivated or revoked within 7 days of suspension.

If a private key, corresponding to a public key, contained in the revoked certificate, remains under the subscriber's control, it should be still protected in a manner guaranteeing its authenticity for a whole period of suspension and it should be stored securely after revocation until it is physically destroyed.

4.8.1. 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 either on subscriber's or authorized representative's of the represented entity. demand.

Certificate revocation may be performed if the following situation occurs:

- when any information within the certificate has changed,
- when a private key, associated with a public key contained in the certificate or media used for storing it has been, or there is a reason to strongly suspect it would be compromised[33]; certificate revocation procedure is in this case executed by a subscriber,
- the subscriber decides to terminate the agreement with Asseco Data Systems S.A., if the subscriber does not request the revocation by himself/herself/itself, a certification authority or a representative of the institution in which the subscriber is employed, has the right to do it,
- on each request of the subscriber or third person indicated in the certificate,
- upon a request from the minister in charge of the economy,
- when a signatory is unable to enter into legal transactions;
- by its issuer, CERTUM, for example when the subscriber does not comply with accepted Certification Policy or resolutions of other documents signed by a certification authority,
- if a certification authority terminates its services, all the certificates issued by this certification authority before expiration of declared period of service termination have to be revoked, along with the certificate of the certification authority,
- the subscriber or the represented entity lingers over fees for services provided by a certification authority or other duties or obligations he/she decided to take,
- a certification authority private key or security of its systems have been breached in a manner directly endangering the certificate reliability,

[33] Private key compromise means: (1) the occurrence of unauthorized access to a private key or a reason to strongly suspect this access, (2) loss of a private key or the occurrence of a reason to suspect such a loss, (3) theft of a private key or the occurrence of a reason to suspect such a theft, (4) accidental erasure of a private key.

- the subscriber, being an employee of an organization, has not returned the electronic cryptographic card, used for storing the certificate and the corresponding private key, when terminating the contract for employment
- other circumstances, delaying or preventing the subscriber from execution of regulations of this Certification Practice Statement, emerging from disasters, computer system or network malfunction, changes in the subscriber's legal environment or official regulations of the government or its agencies.

Revocation request might be submitted (see Chapter 3.3) by means of a registration authority (this requires the subscriber to contact the registration authority). A request is submitted to the Primary Registration Authority where is revoked.

4.8.2. Who can request certificate revocation

The following entities may submit subscriber's certificate request revocation:

- a subscriber who is the subject of a certificate,
- a third person indicated in the certificate,
- an authorized representative of a certification authority (in the case of CERTUM this role is reserved for the security inspector),
- an authorized representative of the represented entity., for example subscriber's employer; the subscriber has to be immediately informed about such fact,
- a natural person who authorizes subscriber to represent its interests,
- the minister in charge of the economy,
- the registration authority operator, which may request revocation on behalf of a subscriber or on its own, if it has information justifying certificate revocation.

Certification authorities are to act with extreme caution when processing revocation requests not submitted by a subscriber and accept only the requests complying with Chapter 4.8.1, and in the case of situations when loss of trust for subjected certificate outreach the subscriber's potential losses which arise from revocation.

When an entity requesting certificate revocation is not an owner of this certificate (i.e. the subscriber), a certification authority has to:

- check whether the requester is authorized to request the revocation,
- submit notification to the subscriber about revocation or initiation of revocation process.

4.8.3. Procedure for certificate revocation

Certificate revocation may be carried out in following manners:

- the first method involves submission of an non-electronic request – paper document;
- the second method involves submission of a request by fax or phone call.

Certificates are revoked or suspended after successful verification of the request. Information about the revoked or suspended certificate is placed on **Certificate Revocation List** (see Chapter 7.2), 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.

Every request for certificate revocation has to provide the means to undeniably identify the certificate being revoked, contain reasons for revocation, and should have been authenticated (signed electronically or a hand-signature).

It is required that requests for revocation have to be authorized by the registration inspector of Primary Registration Authority.

If a certificate being revoked or a private key, corresponding to the certificate, were stored on an electronic cryptographic card, upon certificate revocation, the card may be physically destroyed or securely wiped out. This operation should be carried out by the holder of the card – a private or legal entity (a representative of such an entity).

4.8.4. Certificate revocation grace period

CERTUM guarantees that the maximum grace period[34] 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 (see Chapter 4.8.9).

In the moment of certificate revocation registration authorities' operators and the affected subscribers and applicants are automatically informed about this revocation.

Information about current status of a certificate is available through published Certificate Revocation List, immediately after declared revocation grace period. This service may be requested for example by a relying party, verifying validity of a digital signature on a document submitted by the subscriber.

4.8.5. Circumstances for certificate suspension

Suspension may be carried out solely in case of:

- the data set in the electronic or paper revocation request could raise a reasonable suspicions,
- revocation request was submitted by phone call and the identity of requester can not 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,
- a certificate issued to a subscriber not according to the Certification Practice Statement
- other circumstances that require explanations from subscriber or applicant.

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

[34] Allowable grace period means maximum allowable time between reception of revocation request and the completion of its processing, update in certification authority's database and notification to the subscriber. This period should not be misinterpreted with CRL publication frequency (see Chapter 4.8.9.).

4.8.6. Who can request certificate suspension

Suspension request may be submitted only by the CERTUM personnel.

An application for suspension might not be submitted by the subscriber who is the owner of a certificate. The subscriber has to be immediately informed about fact of suspension.

4.8.7. 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, see chapter 7.2.1)

Certification authority may cancel the certificate suspension if all of conditions specified below are fulfilled:

- the certificate unsuspension should be performed on the basis of a mutual identification of the subscriber, requesting the certificate unsuspension, and certification authority,
- certification authority finds that the reasons for which a certificate was suspended have been resolved or not confirmed.

Certificate suspension requires a request of the security inspector.

In the case of legitimate request the certification authority removes the certificate from the Certificate Revocation List and the certificate becomes a valid certificate, which was before the suspension. The period of the suspension cannot be longer than 7 days. After this period a suspended certificate shall be revoked.

If the qualified certificate has been revoked during the period of suspension or after 7 days of suspension, then the date of the certificate revocation is the same as the suspension beginning date.

4.8.8. 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 4.8.4).

Information concerning certificate suspension (i.e. certificate status) is available through certificate status verification service, immediately after the declared grace period. This service may be requested not only by a subscriber, but also by a relying party verifying validity of a digital signature on the document submitted by the subscriber.

4.8.9. CRL issuance frequency

CERTUM QCA issues Certificate Revocation List.

Every Certificate Revocation List is updated at least once a day[35]. Notwithstanding, the new CRL is published in the repository after every certificate revocation. In the case of

[35] 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**).

revocation of the certificate this certificate is immediately published on Certificate Revocation List.

4.8.10. 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.

Certificate status verification may be based solely on CRL.

When a certificate being verified is placed on a CRL, the relying party is obligated to reject a document associated with the certificate, if the reason for revocation has been one of the following:

```
unspecified          - unknown
keyCompromise        - violation of private key security
cACompromise         - violation of the CA key security
cessationOfOperation – cessation of services associated with the private key
certificateHold      - suspension of the certificate
```

If a certificate was revoked because of the following reasons:

```
affiliationChanged   - data modification
superseded           - amendment of the key
removeFromCRL[36]    - certificate removed from the CRL (unsuspended)
```

The final decision about the certificate trustworthiness sholud be made by a relying party. When making this decision, the relying party should take under consideration that according solely to the above there are no reasons to believe the subscriber's private key was compromised.

4.8.11. 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*[37]. 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:

- **good** – meaning a positive response to the request, which should be interpreted as confirmation of certificate validity[38],
- **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 (i.e. immediately after the certificate revocation)

4.8.12. Requirements for on-line certificate status verification

A relying party is not obligated to verify certificate status *on-line* on the basis of mechanisms and services laid down in Chapter 4.8.11. Notwithstanding above, it is recommended to employ

---

36 Reason for certificate removal from CRL (**removeFromCRL**) is disclosed only in **deltaCRL** lists (see *PKC Certificate and CLR profile*, published by Asseco Data Systems S.A. Certification Authority, 22nd of Oct 2001).

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

38 See **Glossary**.

OCSP service when the risk of forgery of the electronic documents utilizing electronic signature is high or if it is required by other regulations concerning such situations.

4.8.13. Other forms of revocation advertisements availability

In the case of security breach of private keys (their revelation) of the certification authorities within CERTUM, the appropriate information is placed immediately in CRL and (optionally) submitted via electronic mail to every subscriber of the certification authority whose private key has been revealed. The information is submitted to every subscriber whose interests may be (directly or indirectly) endangered.

4.8.14. Checking requirements for other forms of revocation advertisements

Every subscriber is obligated to familiarize himself/herself/itself with electronic mail of the status **urgent**, originating from any certification authority affiliated by CERTUM.

4.8.15. Revocation or suspension of CA certificate (certificate evidences)

The certificate belonging to a certification authority may be revoked or suspended by the National root (NCCert). Such revocation may occur in the following situation:

- the minister in charge of the economy decides to remove entry of certification authority from the register of qualified certification service providers,
- the National root NCCert has reasons to believe that information in issued certificate is false,
- the certification authority private key or its information system were breached in a manner affecting trustworthiness of certificates issued by this authority,
- the certification authority has breached material obligation arising from this Certification Practice Statement.

4.9. 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 proof that data object existed before the date placed in this timestamp. Thanks to this:

- time – stamping authority confirms the existence of data
- time – stamping authority allows to prove that an electronic signature was made prior to the revocation of the key used to signing a document or a message,

Time – stamping ***authority CERTUM QTSA*** *is not a party of transactions referred to and marked with a reliable time.*

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 (timestamp token – TST), which contains serial number, protocol identifier, time from reliable source, application data, data generated by time – stamping authority, binding in a cryptographic manner the time with the digest value, the identifier of the hash function and the session identifier,
- time – stamping authority submits a timestamp token to the requesting entity,
- requesting entity verifies the correctness of timestamp token

Timestamps are issued in accordance with the following requirements:

- trusted time source is synchronized with International Atomic Time (TAI) with an accuracy of 1 second,
- serial number of timestamp token is unique within certification authority domain **CERTUM QTSA,**
- time – stamping authority private keys are generated and stored inside hardware security module complying with FIPS 140-2 Level 3 requirements,
- the time – stamping authority **CERTUM QTSA** owns private key used for creating electronic confirmations of timestamp tokens,

CERTUM QTSA *does not store timestamp tokens.*

4.10. Data Validation Service

Data validation service (also called e-Notarius service) provided by CERTUM QDVCS can be useful to validate the signed documents or certificates and possession or the existence of any data. **CERTUM QDVCS** issues data validation certificate that may be regarded as equivalent to notary token, defined in ISO/IEC 13888-3 standard.

CERTUM QDVCS activity is based on DVCS protocol. CERTUM QDVCS can (RFC 3029):

- confirm validity of digitally signed document (**vsd**) and create on the request certificate (DVC) confirming validity of the signature,
- confirm validity of public key certificates (**vpkc**) and create on the request certificate (DVC) confirming validity of the certificate and its status,
- produce the certificate of possession of data (**cpd**) within a specified time and create on the request certficate (DVC) confirming this fact,
- produce the certificate of claim of possession of data (**ccpd**) and create on the request certificate (DVC) functionally similar to the time-stamp issued by the time-tamping authority..

Qualified data validation and certification server authority **CERTUM QDVCS** can validate following types of tokens and certificates:

- qualified public key certificate,
- qualified and non – qualified electronic signature,
- certificate evidence or certificate,
- timestamp,
- certificate status token (OCSP),
- Evidences of receipt and submission (including Official evidences of receipt and submission),
- data validation token,
- electronic confirmations of data possessing or declaration of data possessing.

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.

If the certification path built for the purpose of verification of qualified certificate or electronic confirmation contains the certificate evidence issued to qualified certification services provider, the result of verification is given as:

1) **properly verified** – secure electronic signature or electronic confirmation is correct according to specification of used cryptographic algorithm and qualified certificate or electronic confirmation are valid in accordance with § 13.1 i § 13.2 (see the Regulation [27]);
2) **negative verified** – secure electronic signature or electronic confirmation is incorrect according to specification of used cryptographic algorithm or qualified certificate or electronic confirmation are invalid;
3) **incomplete verified** - secure electronic signature or electronic confirmation is correct according to specification of used cryptographic algorithm but certification authority cannot confirm validity of qualified certificate or electronic confirmation used to verify this signature, particularly in the case of suspension of certificate.

If none of above mentioned conditions are met, the software used for verification purposes will return the response:

1) **conditionally properly verified** – secure electronic signature or electronic confirmation is correct according to specification of used cryptographic algorithm and non-qualified certificate or electronic confirmation are valid in accordance with § 13.1 i § 13.2 in particular with regard to non-qualified certificate (see the Regulation [27]);

2) **negative verified** – secure electronic signature or electronic confirmation is incorrect according to specification of used cryptographic algorithm or non-qualified certificate or electronic confirmation are invalid;

3) **incomplete verified** – secure electronic signature or electronic confirmation is correct according to specification of used cryptographic algorithm but certification authority cannot confirm validity of non-qualified certificate or electronic confirmation used to verify this signature, particularly in the case of suspension of certificate.

If there is one or more signatures into an electronic document and all are verified properly the ***CERTUM QDVCS*** *supplies information about the certificate status:* ***properly verified.*** *If all signatures or certificates are verified properly but at least one of them has status* ***conditionally properly verified*** *then status of the whole document or token is* ***conditionally properly verified.***

Certification paths built for verification of signatures, certificates and tokens must contain or end in certificates of certification service providers. These entities must be placed on the list of qualified certification services providers registered by Asseco Data Systems S.A. According to *Act*, the list contains all qualified certification services providers established on the territory of the Republic of Poland.

4.11. 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. In the former case, official token is the proof for subscriber that the **CERTUM QDA** has delivered an electronic document into tele-information system of public entity, whereas in the latter one – token is the proof for public entity that the **CERTUM QDA** has delivered an electronic document into tele-information system from that it will be available for recipient. 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.

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.

4.12. 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:

- placing objects in the deposit with the possibility to inform about this fact indicated entities and subscribers; as a result of the service the certification authority shall issue a **token of object deposit entry**,
- releasing object from the deposit (on the basis of entry); objects and entry on the basis of which an objects have been released are removed from deposit; as a result of the service the certification authority shall issue a **token of object release from the deposit,**
- certified releasing object from deposit (including tokens of its authenticity); objects, all validity confirmation data associated with them and the entry on the basis of which object have been released are removed from the deposit; as a result of the service the certification authority shall issue a **certified token of object release from the deposit,**
- downloading entry from the deposit (entries are not removed from the deposit); as a result of the service the certification authority shall issue a **token of download an entry from the deposit,**
- certified downloading entry from the deposit (including tokens of its validity); as a result of the service the certification authority shall issue a **certified token of download an entry from the deposit**,
- downloading object from the deposit (on the basis of entry); as a result of the service the certification authority shall issue a **token of download an object from the deposit,**
- certified downloading object from the deposit (on the basis of entry)) including all authenticity confirmation data associated with the object; as a result of the service the certification authority shall issue a **certified tokens of download an object from the deposit.**

Every token belongs to group of deposits tokens issued by object deposits authority **CERTUM QODA.**

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.

4.13. 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:

- making entry into the registry with optionally objects placement in the repository and, optionally, with the possibility to inform about this fact the subscribers of registry; as a result of the service the certification authority shall issue a **token of registry entry and token of object placement in the repository;**
- downloading registry entries; as a result of the service the certification authority shall issue a **token of download an entry from the registry**;
- downloading objects placed in the repository (download takes place on the basis of object entry); as a result of the service the certification authority shall issue a **token of download an object from the repository,**
- certified downloading registry entry (entry and token of its authenticity are not removed from the repository); as a result of the service the certification authority shall issue a **certified token of download an entry from the registry**,
- certified downloading object from the repository including tokens of its authenticity (entry and token of its authenticity are not removed from the repository); as a result of the service the certification authority shall issue a **certified token of download an object from the repository,**
- registry entry modification; as a result of the service the certification authority shall issue a **token of registry entry modification**,
- repositories object modification; as a result of the service the certification authority shall issue a **token of object modification in the repository**.

Every token belongs to group of registries and repositories tokens issued by registries and repositories authority **CERTUM QRRA.**

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.

4.14. 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.

Services of attribute certificates authority **CERTUM QACA** are provided only to registered users (subscribers) of CERTUM services. If the user is not CERTUM's subscriber, the registration procedure is accomplished in accordance with the procedure laid down in Chapter 4.1.1 and only at the request of the user.

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[39] that should be placed in the attribute certificate
- 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.

[39] 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 issuance of the attribute certificate shall be realized in the manner described in Chapters 4.2 and its acceptance as described in chapter 4.3.

If the user applying for issuance of attribute certificate is a subscriber of CERTUM services and possess a qualified certificate issued by any certification services provider in accordance with the Act, an application might be signed by qualified signature.

The attribute certificate may be revoked but may not be suspended and unsuspended. In the moment of certificate revocation, certificate is published in the **attribute certificates revocation list.**

If the verified certificate is no longer considered valid by the issuing authority and is placed in attribute certificates revocation list and if the reason for revocation has been as follows:

| privilegeWithdrawn - anulowanie uprawnień związanych z atrybutami

the relying party is committed to refuse to perform any actions with respect to this attribute certificate.

Certificate revocation procedure is processed in accordance with rules laid down in Chapter 4.8. If those rules apply to the cryptographic keys, they are ignored, unless it is related to the keys used by CERTUM QACA to issue attribute certificates and attribute certificates revocation list.

The structure of revoked attribute certificates is analogous to the structure of public key certificates revocation list (see Chapter 7.2)

4.15. 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.

It is required that every party – associated in any way with providing certification services – should record information and manage it adequately to their work position and duties. Information records compose event logs and should be retained in a manner allowing authorized parties to access appropriate and required information when resolving disputes between parties or detecting attempts to breach security of CERTUM. Recorded events are subjected to backup procedures. Backup copies are retained outside CERTUM seat.

When applicable, event logs are created automatically. If records cannot be created automatically, paper event logs are used. Every log entry, electronic or handwritten, is retained and disclosed when undergoing an audit.

In CERTUM system, the security inspector is obligated to carry out regular checks of compliance of implemented mechanisms and procedures with regulations of this Certification Practice Statement, as well as to assess effectiveness of existing security procedures.

4.15.1. Types of events recorded

Every activity, critical from the point of CERTUM security, is recorded in event logs and archived. Archives might be encrypted and stored on unrewritable media type to prevent it from modification or forgery.

CERTUM event logs store records of every activity generated by any software component within the system. Such entries are divided into three separate categories:

- **system entries** – record contains information about client's request and server's response (or vice-versa) on the level of network protocol (for example http, https, tcp, etc); Subjects to recordings are: host or server IP address, executed operation (for example: search, edit, write, etc) and its output (for example, amount of entries to database),
- **errors** – record contains information about errors on the level of network protocols and on the level of application modules,
- **audits** – record contains information associated with certification services, for example: registration and certificate request, rekey request, certificate acceptance, certificate and CRL issuance etc.

Event logging is continuous and any interruption is possible only if the affected system is shut down. The above event logs are common for every component installed on an applicable server or workstation and have a capacity set in advance. Upon exceeding this capacity, a new version of the event log is automatically created. The previous event log is archived and erased from the disk.

Every record, automatic or handwritten, includes the following information:

- event type,
- event identifier,
- date and time of the event,
- identifier or other data allowing determination of a person responsible for the event,
- decision whether the event is associated with an successful or erroneous operation,

Recorded entries include:

- alerts generated by firewalls and IDS,
- operations associated with registration, certification, revocation and suspension of certificates, rekey and renewal procedures, issuance of timestamp issuance, data validation, issuance of receipt or submission tokens (including official tokens) or other services provided by an authority issuing certificates,
- every modification to hardware or software structure,
- modification to the network and network connections,
- physical entries to secured areas and their violations,
- changes of passwords, PINs rights and personnel roles,
- successful and unsuccessful attempts to access CERTUM databases and server applications,
- key generation for a certification authority, as well as for other parties, for example subscribers and registration authorities,
- every event related to the update of certificates of certification authority CERTUM QCA and other certification services providers,
- every fact of loss of synchronization between trusted time source and international time source (Coordinated Universal Time - UTC)

- any event related to usage of the private key of any qualified certification authority CERTUM providing certification services,
- every received request and issued decisions in an electronic form, submitted by subscribers or delivered to them as an electronic file or electronic mail; the requirement to record such activities is imposed not only on the certification authorities, but also on the registration authorities,
- history of creating backup copies and informative records archives, as well as databases.

Registered requests, associated with provided services, submitted by subscribers, apart from their usability in dispute resolving and abuse detection, allow calculation of a fee for issuance of a certificate.

Access to event entries (logs) is granted solely to security inspector, system administrators and audit inspector (see Chapter 5.2.1).

4.15.2. Frequency of event logs checking

In order to identify possible illegal activities, the system administrator and audit inspectors should analyze the information laid down in chapter 4.15.1, 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. The result of internal audit should be response to the security requirements. The security inspector records these results in the security logs.

Event log entries should be reviewed in details at least once a month. Every event of significant importance should be explained and described in an event log. Event log review process includes the check against its forgery or modification, and verification of every alert or anomalies disclosed in the logs. Every action executed as a result of detected malfunctions has to be recorded in the logs.

4.15.3. 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.

4.15.4. Protection of event logs

Archives should be electronically signed and marked with time.

An event log may be reviewed solely by the **security inspector**, **system administrator** or an **audit inspector**. Access to the event log is configured in such a way that:

- only authorized entities (i.e. auditors and personnel defined above) have the right to read log entries,
- only the security inspector may archive or erase files (after their archive) containing registered events,
- it is possible to detect every violation of integrity; it assures that the records do not contain gaps or forged entries,

- no entity has the right to modify the contents of the journal.

Additionally, procedures for event logs protection are implemented in a manner that even after the journal archival it is impossible to delete entries or erase the logs before surpassing an estimated period of logs retention (see Chapter 4.16.3).

4.15.5. Procedures for event logs backup

CERTUM security procedures require that the event logs should be subjected to copy in accordance with an established schedule but not less than 4 times a year. These backups are retained in main and alternate site of CERTUM. Backup copies may be signed with a timestamp.

These copies are created by the system operator in the presence of the security inspector.

4.15.6. Notification to event responsible entities

Module for analysis of the event logs implemented in the system allows examination of current events and automatically notifies about suspected or security violating activities. In the case of activities having influence on the system security, the security inspector and system administrator are automatically notified. In other cases, the notification is directed only to the system administrator.

Information transmission to authorized persons about critical – from the point of view of the system security – situations is carried out by other, appropriately secured, means of communication, for example pager, mobile phone, electronic mail.

Notified entities take appropriate actions to prevent the system from detected threat.

4.15.7. Vulnerability assessment

CERTUM classifies and keeps records of all assets according to PN-ISO/IEC 27001: 2007 standard. This Certification Practice Statement requires performing vulnerability assessment analysis of every internal procedures, applications and information system. Requirements for analysis may be also determined by an external institution, authorized to carry out CERTUM audit.

The risk analysis is conducted at least once a year. The decision to proceed with the analysis is undertaken by the Management Board of Asseco Data Systems S.A.

The security inspector is responsible for an internal audit which should control compliance of entries in the security logs, correctness of its backup copy retention, activities executed in the case of threats and compliance with this Certification Practice Statement.

4.16. 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.

4.16.1. Types of data archived

The following data are subjected to archive:

- information from examination and evaluations (arising from an audit) of logical and physical protections of a certification and registration authority, and the repository,
- received requests and issued decisions in an electronic form, submitted by or to the subscriber as files or electronic messages,
- subscribers database, including all the information collected during the registration process.
- certificates database,
- issued Certificate Revocation Lists,
- history of a certification authority key, from its generation to erasure,
- history of the subscribers' keys, from their generation to erasure, if the keys are subjected to archive in certification authority databases,
- internal and external correspondence (paper and electronic) between CERTUM, its subscribers and relying parties in the operation of certificate suspension and unsuspension,
- other documents and data associated with providing certification services.

4.16.2. Frequency of data archive

Data archival is carried out on several levels, in the following period pattern:

- certificate database and subscriber's database are retained on CERTUM media, duplicated by the hardware matrix, for a period of three years (from the time of certificate issuance). For the following three years, archives are stored on magnetic apes or DVD disks, still available *on-line*. In the seventh year (six years after certificate issuance) all information regarding subscribers and their certificates is stored on DVD disk and may be available *off-line (also available online),*
- CRL, electronic correspondence and requests submitted by subscribers, as well as issued decisions are subjected to archive in the same pattern and frequency as for the certificate and subscribers databases,
- information gathered in a paper form related to the subscriber of CERTUM's certification services are subjected to archive six months after the last qualified certificate belonging to him was expired.

4.16.3. Archive retention period

Archived data (in paper and electronic form), described in Chapter 4.16.1, and are retained for the period of minimum 25 years. After expiration of the declared retention period, archived data may be destroyed. In the case of key and certification erasure, an appropriate procedure is executed with particular attention.

4.16.4. Backup procedures

Backup copies allow full restoration (if necessary, for example after system destruction) of data essential to the proper activity of CERTUM. To accomplish the above goal, the following applications and files are subjected to backup:

- installation disks with system applications, for example operating systems,
- installation disks with certification and registration authority applications,
- WWW server and the repository installation disks,
- authorities' keys, certificates and CRL history,
- data from the repository,
- data concerning subscribers and personnel of CERTUM,
- event logs.

Detailed backup copy creation procedures and system recovery after malfunction are disclosed in technical infrastructure documentation. The documentation has a "non-public" status and is available solely to authorized personnel and to auditors.

4.16.5. Requirements for time-stamping of the records

It is recommended that archived data should be signed with a timestamp, created by the time – stamping authority **CERTUM QTSA**, having a certificate issued by the minister in charge of the economy or certification services provider authorized by him.

4.16.6. Access procedures and archived information verification

To verify the integrity of archived information, the data is periodically tested and verified against original data (if still accessible in the system). This activity may be carried out solely overseen by the security inspector and should be recorded in the event logs.

If any damages or modifications to original data are detected, the damages are to be removed as promptly as possible.

4.17. 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.

*From the moment of key changeover, the certification authority **CERTUM QCA** uses only a new private key for signing issued certificates and Certificate Revocation List*

4.18. Key security violation and disaster recovery

This Chapter describes procedures carried out by CERTUM in abnormal situations (including natural disasters) to restore a guaranteed service level. Such procedures are executed in accordance with the accepted plan disclosed in Disaster Recovery Plan.

4.18.1. Corruption of computing resources, software and/or data

Security policy, executed by CERTUM, takes into consideration the following threats influencing availability and continuity of the provided services:

- physical corruption to the computer system of CERTUM, including network resources corruption – this threat addresses corruptions originating from random situations,
- software and application malfunction, rendering data inaccessible – such corruptions address operating system, users' applications and execution of malicious software, for example viruses, worms, Trojan horses,
- loss of important network services, associated with CERTUM interests. It primary addresses power cuts and damages of the network connections,
- corruption of a part of the network, used by CERTUM to provide its services – the corruption may imply obstruction for the customers and denial (unintended) of services.

To prevent or limit results of the above threats, the security policy of CERTUM comprises:

- **Disaster Recovery Plan.** All subscribers and relying parties are informed, as soon as possible and in a manner most appropriate for the existing situation, about every significant malfunction or corruption, associated with any information system or network environment component. Disaster recovery plan includes number of procedures executed in the event any part of the system has been subjected to compromise (corruption, revelation, etc). The following actions are performed:
    - disk images of every server and workstation of CERTUM are created and archived; every backup copy is retained both in main seat and in emergency location outside CERTUM,
    - periodically, following the procedures disclosed in Chapter 4.16.4, a backup copy of the databases and every server full backup copy are created. The copy includes all submitted requests, entries to event logs, issued, renewed and revoked certificates; latest copies are retained both in main seat and in secure location outside CERTUM,
    - CERTUM keys, split according to procedures for secret sharing, are held by trusted individuals in the places known only to themselves,
    - computer replacement is carried out in a manner allowing disk image restoration, on the basis of most recent data and keys (applies to singing server),
    - system recovery procedures after disaster are tested on every system component, at least once a year. These tests are a part of an internal audit.
- **Modification monitoring**. Installation of updated software version in the production system is possible only after carrying out intensive tests in a testing environment, performed in strict accordance with disclosed procedures. Every modification in the

system requires CERTUM security inspector's acceptance. If the newly implemented components, installed in accordance with the above procedures, cause target system corruption, accepted system recovery plans allow swift restoration of the system to the state before corruption occurred.

- **Emergency system**. In the case of corruption restraining CERTUM functionality, revocation service will be able not later than within 24 hours in the alternate site of CERTUM. Within 24 hours an emergency facility will be activated, which should substitute most substantial function of a certification authority until the primary facility is restored to service. Due to regular backup copy and archive creation, unprocessed requests accumulation and hardware-software redundancy, in the case of corruption restraining CERTUM activity, it is possible to:
    - activate emergency facility allowing provision of CERTUM services,
    - process all accumulated and unprocessed revocation requests,
    - process in real-time requests submitted by subscribers until restoration and recovery of the prime facility.
- **Backup copy creation system**. CERTUM system utilizes application, creating backup copy from data, and allowing system recovery at any moment and performance of an audit. Backup copies and archives are created from every data having significant importance on security and normal activity of CERTUM. Copies are created periodically and stored on magnetic tapes, while archives are stored on CD-ROM disks. Backup copies may be protected by a password, while CD-ROM disks are encrypted and may be additionally time-stamped. Backup copies and their archives are retained outside primary facility.
- **Additional services**. To prevent the system from power cuts and to secure service continuity, emergency power sources (UPS) are employed. UPS devices are tested every six (6) months.

4.18.2. Key compromise or suspicion of certification authority private key compromise

In the case of certification authorities (affiliated by the CERTUM) private key compromise or suspicion of such compromise, the following actions should be taken:

- the certification authority generates a new key pair and applies to the National root NCCert for a new certificate,
- all certificate users are immediately informed abut the compromise of the private key, by means of mass media system and electronic mail,
- a certificate evidence of a certification authority corresponding to the compromised key is placed on Certificate Revocation List, along with a suitable reason for revocation ,
- all subscribers's certificates and all certificates in the certification path of the compromised certificate are revoked and a suitable reason for revocation is submitted,
- new certificates for subscribers are generated,
- new certificates for subscribers are submitted to them, without charging a fee for the operation; subscriber may refuse to accept an issued certificate.

4.18.3. Security coherence after disaster

Upon every system recovery after disaster, the security inspector or system administrator executes the following:

- changes all previously used passwords,
- removes and resets all the access rights to the system resources,
- changes all codes and PIN numbers associated with physical access to facilities and the system components,
- if recovery from the accident involves reinstallation of operating system and utility software, all IP addresses of system elements and its subnetworks are changed,
- reviews analysis of the disaster cause, updates to the plan and network security policy of CERTUM and physical access to locations and the system components,
- informs every system user about restoration of the system activity.

4.19. Certification authority termination or service transition

Obligations described below are developed to minimize disruption to subscribers and relying parties, arising from the decision of a certification authority to cease operation, and include obligations to notify in advance all subscribers of the authority that certified the certification authority subjected to termination (if such exists) about the termination, and transition of responsibilities – on the basis of regulations with other certification authorities – for service of its subscribers, database and other resources management.

CERTUM is covered by the civil liability insurance with respect to any damage suffered by certification-service consumers,

4.19.1. Requirements associated with duty transition

Before CERTUM ceases its services, it is obligated to:

- in the case 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** notify the National root (NCCert) about their intention to terminate services as the authorized certification authority; the notification should be made 90 days before the agreed date of the termination,
- notify (at least 90 days in advance) its subscribers who hold active (unexpired and unrevoked) certificates issued by this authority about decision to terminate its services,
- revoke all certificates which remain active (unexpired and unrevoked) in the declared moment of service termination, regardless of the fact that a subscriber has submitted or has not submitted a suitable request,
- notify all subscribers associated with the certification authority about service cessation,

- make commercially reasonable effort to minimize disruptions to interests of subscribers and legal entities engaged in an ongoing process of electronic signature (remaining in usage) verification with public keys certified with the certificates issued by the certification authority being terminated,
- transmist the data, directly connected with certification services, to the minister in charge of the economy or to the entity designated by him,
- pay compensations of issuance fees to the subscriber or the represented entity; compensations should be proportional to remaining validity period of the certificate.

4.19.2. Certificate issuance by the successor of terminated certification authority

Archive of the certification authority ceasing its service has to be turned over to the minister in charge of the economy or to 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.

The successor of the terminated certification authority takes over the rights and obligations of the terminated certification authority related to the management of the event logs and archives for a period specified in chapter 4.16.

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.

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.

5.1.1.1. Site location and construction

CERTUM is located in the Asseco Data Systems S.A. seat, at the following address: ul. Bajeczna 13, Szczecin, Poland .

5.1.1.2. Physical access

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.

Asseco Data Systems S.A. facility and is publicly available every working day within company's working hours. In the remaining time (including non-working days), the facility is available only to persons authorized by the Management of Asseco Data Systems S.A. and known by name and surname by the security inspectorss.

Visitors to areas occupied by CERTUM may access this area only if they are escorted by the authorized personnel of CERTUM.

Areas occupied by CERTUM are divided into:

- computer system area,
- operators and administrators areas,

The computer system area, including location of the hardware security module that stores QCA keys, is equipped with monitored security system built on the basis of motion, fire and flood sensors. Access to this area is granted only to authorized personnel, i.e. the personnel of CERTUM and Asseco Data Systems S.A. Monitoring of the access rights is carried out on the basis of smart cards and access control system, whose terminals are mounted next to the area entry. Every entry and exit from the area is automatically recorded in the event journal. The presence of other individuals (e.g. auditors or service employees) requires presence of authorized personnel and authorization of CERTUM Manager.

Access to the operators and administrators area is enforced through the use of a smart card and access control system. Since all sensitive information is protected by the use of safes, permanently secured to the ground, and to which access is controlled by two keys (two-eye principle), while access to operator's or administrator's terminal requires prior authorization, the employed physical security is assumed as adequate. Keys to the area are accessible only to authorized personnel. The area may be occupied solely by CERTUM personnel and authorized individuals. Additionally, the latter are not allowed to occupy the area unescorted. The only exception concerns the individuals occupying **CERTUM** positions who are classified as **trusted**.

5.1.1.3. Power and air conditioning

In case of main power line failure the system switches to emergency power source (UPS and/or power generators).

Working environment in the computer system area is monitored continuously and independently from other areas.

Each area is air-conditioned.

5.1.1.4. Water exposure

In the computer system area humidity and water detecting sensors are installed. These sensors are integrated with the security system of Asseco Data Systems S.A. building. Reception personnel are notified of the hazards and are obligated to notify appropriate public services, security inspector and one of system administrator.

5.1.1.5. Fire prevention

Fire prevention and protection system installed in Asseco Data Systems S.A. seat complies with local standards and regulations for fire safety. Computer system area is also equipped with fire control system (neutral gas), activated automatically in the case of fire detection in monitored area.

5.1.1.6. Media storage

In accordance with the sensitivity of information held, media containing archives and current data backup are stored in fireproof safes, located in the operators and administrator area and the computer system area. Access to the safe is secured with two keys, being held by authorized individuals. Copies of suitable documents, backups and archives are also retained in emergency facility, within fireproof safes secured to the ground.

5.1.1.7. Waste disposal

Paper and electronic media containing information possibly significant for CERTUM security after expiration of the retention period (see Chapter 4.16) are destroyed in special shredding devices. In the case of cryptographic keys and PIN or PUK numbers, media used for their storage are shredded in DIN-3 class devices (this applies only to the media which do not allow definitive erasure of stored information and their re-usage).

5.1.1.8. Offsite backup storage

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. It enables emergency recovery of most substantial CERTUM function within 48 hours (in CERTUM seat or in the emergency facility).

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

5.1.2.1. Site location and construction

Registration authorities of CERTUM are located in the following sites:

- Primary Registration Authority (PRA) is located in the operators and administrators area in CERTUM (see Chapter 5.1.1.1),
- addresses of other registration authorities are available in repository and by email at the following address: info@certum.pl.

5.1.2.2. Physical access

Access to Primary Registration Authority has to be performed as described in Chapter 5.1.1.2. In the case of other registration authorities, there are no additional restrictions addressing physical access. It is recommended that offices of registration authorities should be separated and rigged with equipment allowing safe storage of data and documents. Access to such areas should be monitored and limited to authorized individuals associated with the activity of the registration authority (registration authority operators, system administrators) and their customers.

5.1.2.3. Power and air conditioning

Primary Registration Authority is connected with Asseco's emergency power source system. Air conditioning is not required. In the case of other registration authorities, there are no restrictions addressing emergency power source and air conditioning.

5.1.2.4. Water exposure

This Certification Practice Statement does not state any conditions in this respect.

5.1.2.5. Fire prevention and protection

This Certification Practice Statement does not state any conditions in this respect.

5.1.2.6. Media storage

Media used for storage of archives and current information backup copies and paper documents are held in the safes located in the Primary Registration Authority area and other registration authorities. Additionally, it is required that copies of the documents used to identity and requests verification must be archived in the Primary Registration Authority. Methods of

protection of the media and data in the registration authorities not affiliated with CERTUM are defined in the agreements between Asseco Data Systems S.A. and administrator of the registration authority.

5.1.2.7. Waste disposal

Paper and electronic media, containing confidential or secret information are, upon expiration of the retention period (see Chapter 4.16.3), destroyed in special shredding devices.

In the case of cryptographic keys and PIN or PUK numbers, media used for their storage are shredded in DIN-3 class devices (this applies only to the media which do not allow definitive erasure of stored information and their re-usage). Hardware security modules are reset end erased according to manufacturer's recommendations. Such devices are erased and reset also prior to their transfer to service or repair.

5.1.2.8. Offsite archive storage

Copies should be retained in safes providing two-factor access.

It is recommended to store archives and current information processed by the computer system backup copy outside location of the registration authority. In the case of the Primary Registration Authority copies are retained in safes in the emergency facility).

5.1.3. Subscriber security

Subscriber has to protect their system access password and personal identification number (PIN). If selected password or PIN is complicated and hard to remember, it might be written down. In this situation, the subscriber has to remember about storage of the written password in the safe, accessible solely to the authorized personnel or encrypted with the algorithm known to the PIN holder.

The password used for protection of the media containing a subscriber's private key should not be stored in the same place as the media itself.

5.2. Organizational security controls

This Chapter presents a list of roles which can be defined for personnel employed in CERTUM. The list is in accordance with the the Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094). The chapter also describes responsibilities and duties associated with each defined role

5.2.1. Trusted roles

5.2.1.1. Trusted roles in CERTUM

Persons who act as trusted roles are subject to special verification. CERTUM verifies information on the qualifications and professional experience as well as clear certificates from the records of criminal convictions.

The following trusted roles which should be manned with one or more individuals are applied by CERTUM:

- **PKI Services Development Team member** – determines direction of CERTUM development, implements and manages Certification Policy as well as Certification Practice Statement,
- **Certification Authority Manager** – responsible for appropriate management of CERTUM, the member of PKI Services Development Team,
- **Security Inspector** – supervises implementing and handling information system security procedures; manages the administrators, initiates and supervises key and shared secret generation; assigns rights in the field of security and user's access privileges; reviews event logs; supervises service tasks,
- **System Operator** – handles standard system operations, including backup copies and transfer of current copies and archives to offsite locations,
- **Registration Inspector** – verifies subscribers' identity and correctness of submitted certification application; authorizes certification request,
- **System Administrator** – installs hardware and software for operating system; initially configures the system and network resources; manages folders of CERTUM available to the public; creates WWW page and manages links,
- **Application Programmer** – creates certification processes and WWW pages,
- **Audit Inspector** – responsible for review, archive and management of event logs (in particular verification of their integrity) and performance of internal audit for compliance of a certification authority operations with this Certification Practice Statement; this responsibility extends also on every registration authority, operating within CERTUM,

Described duties segregation prevents abuses associated with CERTUM system usage. Every user is assigned only the rights arising from the user's role and related responsibility.

The above roles may be combined in limited scope, modified or denied trusted clause. Duties and roles combination could not lead to combination of security inspector role with system administrator or operator, and audit inspector role with security inspector, registration inspector, system administrator or operator.

Access to software supervising operations performed by CERTUM is granted solely to the individuals whose responsibility and obligations arise from the acted role of the system administrator.

5.2.1.2. Trusted roles in registration authority

CERTUM has to be sure that the personnel of a registration authority recognize their responsibility, arising from necessity of credible identification and authorization of subscribers' information. Due to above, at least three following trusted roles have to be defined:

- **System Administrator** – installs hardware and software of operating system; installs application software; configures system and applications; activates and configures security resources; creates operators' accounts and passwords; creates backup copies and archives information; reviews events journals (logs) and (together with registration authority operator) and by the order of the security inspector, erases excessive information;
- **Registration Inspector** – verifies subscriber's identity and correctness of provided request; authorizes requests and provides them to a certification authority; takes part in

certificate generation, submitting information from a request to a certification authority; signs agreements with subscribers concerning services provided by the certification authority; archives (in paper form) requests and issued confirmation,

- **person who verifies identity and/or attributes –** verifies subscriber's identity, attributes placed in the attribute certificate on his/her/its request, correctness of a submitted application. and submits verified applications to the registration inspector,
- **registration authority agent** – is responsible for efficient operation of a registration authority; his/her role is to provide financial support for the personnel, manage operators' and administrators' work, arbitrate disputes, make a decision arising from operations carried out by a registration authority,

A person who verifies identity and/or attributes must be accredited by CERTUM.

5.2.1.3. Subscriber's trusted roles

This Certification Practice Statement does not state any conditions in this respect.

5.2.2. Numbers of persons required per task

Keys generation process for the needs of certificate and CRL signing –is the operation requiring particular attention. Therefore, the generation requires presence of persons, acting as:

- **Security Inspector,**
- **System Administrator (hardware security module operator),**
- **shared secret holder,**
- **observers – (option) representatives of the auditor.**

Detailed procedure of keys generation is described in document entitled „ Certification authorities keys life cycle management procedures". The document has a "non-public" status.

5.2.3. Identification and Authentication for Each Role

CERTUM personnel are subjected to identification and authentication procedure in the following situation:

- inclusion on the list of persons allowed to access CERTUM locations,
- inclusion on the list of persons allowed to physically access system and network resources of CERTUM,
- issuance of confirmation authorizing to perform the assigned role,
- an account and a password assignment in CERTUM information system.

Every confirmation and assigned account:

- has to be unique and directly assigned to a specific person,
- cannot be shared with any other person,
- has to be restricted to function (arising from the role performed by a specific person) carried out solely by means of available CERTUM system software, operating system and controls.

Operations performed in CERTUM that require access through shared network resources are protected with implemented mechanisms of strong authentication and encryption of transmitted information.

Accounts and privileges of employees who are no longer involved in CERTUM's operation are immediately blocked.

Security Inspectors review all accounts on a regular basis - at least quarterly - in compliance with the Information Security Policy and PN-ISO/IEC 27001:2007 standard. All unused accounts are disabled.

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.
- CERTUM personnel, especially those who are classified as trusted roles, are required to comply with the provisions of the *Act on Electronic Signature of 18 September, 2001*.

According to the Information Security Policy, which is the part of the Integrated Management System implemented in Asseco Data Systems S.A., CERTUM implements procedures to manage the permissions of the personnel in the manner required by the PN-ISO/IEC 27001: 2007 standard.

This means, among other things, that the principle of "reasonable knowledge" applies to the information and resources that are classified as sensitive. According to the principle employees access to the protected information or other resources must be justified by the tasks entrusted to them.

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.

Upon completion of the training, participants sign a document confirming their familiarization with presented documentation and acceptance of associated restrictions and obligations.

5.3.2. Retraining Frequency and Requirements

Trainings described in Chapter 5.3.1 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.

5.3.3. Job rotation

This Certification Practice Statement does not imply any requirements in this field.

5.3.4. Sanctions for Unauthorized Actions

In the case of a discovery or suspicion of unauthorized access, the system administrator together with the security inspector (in the case of CERTUM employees) or solely system administrator (in the case of registration authority employees) may suspend the perpetrator's access to CERTUM or the registration authority system. Further disciplinary actions are to be consulted with CERTUM management.

5.3.5. Contract Personnel

Contract personnel (external service, developers of subsystems or software, etc.) are subjected to the same verification procedure as employees of CERTUM and its registration authority (see Chapters 5.3.1, 5.3.2 and 5.3.3). Additionally, contract personnel, when performing their task at CERTUM seat or its registration authority have to be escorted by CERTUM or the registration authority employee.

5.3.6. Documentation Supplied to Personnel

Management of CERTUM and the registration authority agent have to provide their personnel with access to the following documents:

- Certification Policy,
- Certification Practice Statement,
- Certification Regulations of CERTUM's Qualified Certification Services,
- application forms and request templates,
- extracts from documentation corresponding to performed role, including emergency procedures,
- range of responsibilities and obligations associated with the acted role in the system.

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.

Private Keys owned by CERTUM QCA are used to:

- sign subscriber's certificate and CRLs;
-

In addition, the keys of the certification authority CERTUM QCA can be used to sign other electronic confirmations (including cross-certificate) as in the cases specified in Chapter 4.17.

An electronic signature is created by means of RSA algorithm in combination with SHA-1 cryptographic digest, while a key agreement employs Diffie-Hellman[40] 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.

Certification authority keys, time – stamping authority keys, certificate status verification authority keys, data validation authority keys and delivery authority keys are generated in accordance with the accepted by CERTUM procedure for key pair generation. Actions executed while performing key pair generation are recorded, dated and signed by each person present during the generation. The records are retained for the needs of audits and common system reviews.

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.

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

6.1.1.1. Subscriber's keys can be generated by the CERTUM QCA or independently by the subscriber using mechanisms provided by the CERTUM (see Chapter 6.1.2).Procedures of generation of CERTUM QCA initial keys

Procedures of generation of initial **Certum QCA** keys are always deployed during CERTUM system initiation or in the case of suspicion that a subsequent private certification authority key has been compromised. The procedure comprises:

- secure generation of a main key pair for certificate and CRL signing – the main key pair has a form $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, where $\mathbf{K^{-1}_{GPK(1)}}$ – private key, and $\mathbf{K_{GPK(1)}}$ – public key, distribution of private key (according to accepted threshold method),
- generation of the certification request and forward it to the National root (NCCert); the request contains the public key **KGPK (1)** and the proof of possession of complementary private key.

Upon generation of key pair for certificate and CRL signing, private key distribution and its activation in hardware security module, the keys can be used in cryptographic operations until the validity period has expired or the keys have been revealed.

Procedure of generation of initial **Certum QCA** keys comprises:

- generation of key pair $\mathbf{KPW=\{K^{-1}_{KPW}, K_{KPW}\}}$ for message signing or key encryption, where $\mathbf{K^{-1}_{KPW}}$ – private key, and $\mathbf{K_{KPW}}$ – public key,
- the issuance of a certificate of an infrastructure key $\mathbf{K_{KPW}}$, signed with private key $\mathbf{K^{-1}_{GPK(1)}}$.

Generation of initial Diffie-Hellman (DH) key for a key agreement comprises:

- generation of key pair $\mathbf{KDH=\{K^{-1}_{KDH}, K_{KDH}\}}$ for key agreement, where $\mathbf{K^{-1}_{KDH}}$ – private key, and $\mathbf{K_{KDH}}$ – public key,
- issuance of a certificate of an infrastructure key $\mathbf{K_{KDH}}$, signed with private key $\mathbf{K^{-1}_{GPK(1)}}$.

6.1.1.2. CERTUM QCA rekey procedure

CERTUM QCA cryptographic keys have a limited lifetime period; if the period has expired, the keys should be updated.

A particular procedure is applied for update of key pair used for certificate and CRL signing. It is based on the issuance of special certificates by **CERTUM QCA**. The certificates enable subscribers who have already installed an expired self-certificate of **CERTUM QCA** to securely migrate to work with a new self-certificate; new subscribers already possessing a new self-certificate are enabled to securely retrieve expired self-certificate, which may be needed for verification of the data signed in the past (see RFC 2510).

To achieve effect described above, **CERTUM QCA** deploys a procedure, owing to which new key pair generation will secure (authenticate) a new public key with the use of the former (previously used) private key and vice-versa (an old public key is secured with a new private key). It means that as a result of update of the self-certificate of certification authority **CERTUM QCA**, apart from a new self-certificate, two additional certificates are created. After the key update four certificates are created for certificates and CRL signing: the former **self-certificate OldWithOld** (old public key signed with old private key), the new **self-certificate NewWithNew** (new public key signed with new private key), **self-certificate OldWithNew**

(old public key signed with new private key) and **self-certificate NewWithOld** (new public key signed with old private key).

Procedure for **CERTUM QCA** key pair – designated to certificate and CRL signing – update (rekey) is executed as follows:

- generation of a new, succeeding main key pair $\mathbf{GPK_{(i)}=\{K^{-1}_{GPK(i)}, K_{GPK(i)}\}}$, where $\mathbf{K^{-1}_{GPK(i)}}$ – private key, while $\mathbf{K_{GPK(i)}}$ – public key, distribution of the private key (according to accepted threshold method),
- generation of the certification request and forward it to the National root (NCCert); the request consists the public key $\mathbf{K_{GPK(I)}}$ and the proof of possession of complementary private key.
- The National root NCCert creates certificate that consists a new public key **CERTUM QCA,** signed with old private key $\mathbf{K^{-1}_{GPK(i-1)}}$ (**self-certificate NewWithOld**),
- creation of a self-certificate, containing new public key of **CERTUM QCA**, signed with old private key $\mathbf{K^{-1}_{GPK(i-1)}}$ (**self-certificate NewWithOld**),
- deactivation of old private key $\mathbf{K^{-1}_{GPK(i-1)}}$ and activation of new private key $\mathbf{K^{1}_{GPK(I)}}$ – within hardware security module a new private key for certificate and CRL signing is loaded,
- creation of a self-certificate, containing old public key **CERTUM QCA**, signed with new private key $\mathbf{K^{1}_{GPK(I)}}$ (**self-certificate OldWithNew**),
- publication of created certificates in the repository, submission of the information about new available certificates.

After generation and activation of a new private key (it may be executed in any moment within the validity period of the old self-certificate), **CERTUM QCA** authority signs new intermediate certificates solely by means of the new private key.

The old public key (old self-certificate) is available to the public until all subscribers obtain the new self-certificate (new public key) of **CERTUM QCA** (it should be achieved before the expiry date of the old self-certificate).

The end of the validity period of **self-certificate OldWithNew** is the same as the end of date of the old self-certificate.

Validity period of **self-certificate NewWithOld** starts at the generation time of a new key pair and ends at the time by which all the subscribers will obtain new self-certificates (certificate of the new public key) of **CERTUM QCA**. Its expiry date should not be later than the expiry date of the old self-certificate.

Period of use of the **self-certificate NewWithNew** begins at the generation time of a new key pair and expires at least 360 days before the end of its validity period. This requirement means the certification authority **CERTUM QCA** terminates usage of the private key for signing certificates and CRL at least 380 days before the expiry date of the self-certificate corresponding to this private key.

Procedure for **CERTUM QCA** key pair – designated to messages signing and for key agreement – update (rekey), is executed as follows:

- generation of a new key pair – key for RSA message signing or key for DH key agreement and distribution of the private key (according to accepted threshold method),

- creation of a self-certificate for a new public key **CERTUM QCA,** signed with a new private key $\mathbf{K}^{1}_{\mathbf{GPK(1)}}$,
- publication of created certificates in the repository, submission of the information about new available certificates.

6.1.2. Private Key Delivery to Entity

Subscriber's keys are generated by **CERTUM QCA** or independently by the subscriber 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.

New subscribers of qualified services are supplied with personalized cryptographic cards (Secure Signature-Creation Devices). The personalization means that the subscriber's cryptographic keys, PUK security code and the identification number of the card are created on the subscriber's cryptographic card. Codes and numbers are automatically saved to the database. The personalization is done on equipment that is not connected to the network and in a secure room accessible to designated employees performing trusted roles.

Subscribers who hold the qualified certificate on their cryptographic cards and want to renew it, may generate another key pair remotely. Then CERTUM provides to them a dedicated application that generates the keys directly on the subscriber's cryptographic card.

The cryptographic card activation data (PUK/PIN codes) are made available to subscribers separately from issued certificates.

CERTUM guarantees that it employs procedures assuring that in any moment after generation of a key pair on subscriber's demand there will be impossible to use keys for creating an electronic signature by certification authority personnel and that the certification authority will not create conditions for making the signature by any unauthorized entity, except for the owner of the private key.

6.1.3. Public Key Delivery to certification authority

Registration authority operators submit their generated public keys as an electronic request whose format has to comply with protocols supported by a certification authority. It might be format defined in *ISO/IEC 15945* (CMP protocol) standards or format PKCS#10 *Certification Request Syntax*[41] (CRS).

6.1.4. 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:

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

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

In the case of CERTUM certification authority key update (rekey), the repository should contain all additional self-certificates or certificates issued as a result of execution of the procedure laid down in Chapter 6.1.1.2.

6.1.5. Keys Sizes

All qualified certification authorities operating within CERTUM use 2048 bit keys. End-user certificates also have a key length of 2048 bits.

It remains, however, a small amount of subscribers who have cryptographic cards that accept only cryptographic keys of length 1024 bits. The owners of such cards receive certificates provided with key lengths of 1024 bits.

6.1.6. Public Key Generation Parameters

Both when cryptographic keys are generated by CERTUM , and when the subscriber creates them independetly using the mechanisms provided by CERTUM (see Chapter 6.1.2), generating parameters complies with requirements laid down in the *Art. 15 of* the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)*, as well as minimal requirements, laid down in the Appendix 3 of the Regulation: *"Algorithms and Parameters for Secure Electronic Signatures"*, should be fulfilled.

6.1.7. Public Key Quality Checking

The creator of a key is responsible for checking parameter quality of the generated key he/she/it is required to verify:

- ability to execute encryption and decryption operation, including electronic signature creation and its verification,
- key generation process, which should be based on strong random cryptographic number generators – physical sources of white noise, if possible,
- resistance against known attacks (applies to RSA and DH cryptographic algorithms).

Additionally, every certification authority, upon reception or generation (on subscriber's demand) of a public key, subjects to appropriate verification test on compliance with restrictions enforced by the Certification Practice Statement (e.g. module length and exponent).

Parameter quality checking, determining for example whether an input number is prime, should be obligatory in the case of centralized key generation and should be executed according to recommendations listed in *"Algorithms and Parameters for Secure Electronic Signatures"* [25].

6.1.8. Hardware and/or Software Key Generation

In the case of certification authority **CERTUM QCA**, the 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** keys are generated by means of hardware security modules complying with requirements presented in Chapter 6.2.1.

All keys used for data signing, confirmed by CERTUM QCA, are generated in accordance with the requirements presented in Chapter 6.2.1. This requirement particularly applies to the end-users applying to **CERTUM QCA** for qualified certificate issuance.

The keys which are not used for creation of signatures or notifications might be generated using computational method with the usage of pseudorandom number generator in accordance with *ANSI X9.17 - Financial Institution Key Management (Wholesale)* standard, published by the American National Standards Institute.

Tab. 16 Key generation method

Certificates/tokens	Key generation method
Qualified public key certificate	Hardware
Certificate evidences	Hardware
Tokens	Hardware
CA certificates	Hardware
Attribute certificates	Hardware
Certificates of infrastructure keys	Hardware or software

6.1.9. Key Usage Purposes

Allowed key usage purposes are described in **KeyUsage** field (see Chapter 7.1.1.2) of standard extension of a certificate complying with X.509 v3. This field has not to be obligatorily verified by the subscribers' application managing the certificates.

Usage of every bit of **KeyUsage** field has to comply with the following rules (every bit meaning appropriately):

a) **digitalSignature**: certificate intended for verification of electronic signature created for purposes different than the purposes mentioned in b), f) and g),

b) **nonRepudiation**: certificate intended to provide a non repudiation service by private individuals, although for other purposes than described in f) and g). **NonRepudiation** bit may be set only in a public key certificate intended to verify electronic signatures and should not be combined with any other purposes, especially described in points c)-e) and connected with providing confidentiality,

c) **keyEncipherment**: intended to encrypt symmetric algorithm keys, providing data confidentiality,

d) **dataEncipherment**: intended to encryption of subscriber's data, other than described in c) and e),

e) **keyAgreement**: intended for protocols of key agreement,

f) **keyCertSign**: public key is used for electronic signature verification in certificates issued by entities providing certification services,

g) **cRLSign**: public key is used for verification of electronic signatures on revoked and suspended certificates lists issued by the entities providing certification services,

h) **encipherOnly**: may be used solely with **keyAgreement** bit to indicate its purpose of data encryption in key agreement protocols,

i) **decipherOnly**: may be used solely with **keyAgreement** bit to indicate its purpose of data decryption in key agreement protocols,

Certificates used for signature creation may be issued solely to subscribers. Their issuance and management are subjected to requirements defined for certificates intended solely for non-repudiation services (**nonRepudiation** bit).

CERTUM QCA has three different types of keys: for signing certificates and Certificate Revocation List (**keyCertSign** bit and **cRLSign** bit), for signing electronic messages (**digitalSignature** bit) and for key exchange (**keyEncipherment** bit). The last two types of keys are the set of infrastructure keys.

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** and registries and repositories authority **CERTUM QRRA** possess only one type of key, applied to confirm tokens (**digitalSignature** bit and **nonRepudiation** bit).

Attribute certificates authority **CERTUM QACA** possess only one type of key, applied to confirm attribute certificates and entity attribute revocation list EARL (**keyCertSign** bit and **cRLSign** bit**).**

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. Certification authority (see Chapter 6.1.1) generating a key pair on authorized subscriber's demand, has to deliver it securely to the subscriber and notifies the subscriber on rules regarding protection of his/her/its private key (see Chapter 6.1.2).

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 employed 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. In the case of subscriber's using hardware key protection, it is also recommended to comply with FIPS 140-2 or ITSEC (*ITSEC v 1.2 issued by European Committee, Directories XIII/F, 1991*) requirements

Tab. 17 Minimal requirements imposed on hardware security modules

Certificate subject type	Employed security module
Certification authority CERTUM QCA	Hardware, complying with FIPS 140-2 Level 3 or higher

Time – stamping authority CERTUM QTSA	Hardware, complying with FIPS 140-2 Level 3 or higher
Online certificate status protocol authority CERTUM QOCSP	Hardware, complying with FIPS 140-2 Level 3 or higher
Data validation and certification server authority CERTUM QDVCS	Hardware, complying with FIPS 140-2 Level 3 or higher
Delivery authority CERTUM QDA	Hardware, complying with FIPS 140-2 Level 3 or higher
Object deposits authority CERTUM QODA	Hardware, complying with FIPS 140-2 Level 3 or higher
Registries and repositories authority CERTUM QRRA	Hardware, complying with FIPS 140-2 Level 3 or higher
Attribute certificates authority QACA	Hardware, complying with FIPS 140-2 Level 3 or higher
Private or legal entity or their devices (subscribers)	Hardware, complying with FIPS 140-2 Level 2 or higher or ITSEC E3 or higher
Registration Authority	Hardware, complying with FIPS 140-2 Level 2 or higher or ITSEC E3 or higher

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.

6.2.2. Private Key Multi-Person Control

Multi-person control of a private key applies to private keys of all certification authorities

In the case of certification authority **CERTUM QCA** the control applies to a key used for creation electronic confirmations, in the certificates, in the Certificate Revocation List and to the infrastructure keys (to signing messages and to exchange encrypting keys).

CERTUM allows direct and indirect method for private key distribution into multi-person control. In the case of direct method usage, the very private key is subjected to multi-person control, while in indirect method the control applies to a symmetric key used for encryption of private key of certification authority.

In both methods, 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 Table 19

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

Tab. 18 Distribution of shared secrets

Authority providing certification services	Number of shared secrets, required for private key restoration	Total number of distributed secrets
CERTUM QCA	3	5
CERTUM QTSA	2	3
CERTUM QOCSP	2	3
CERTUM QDVCS	2	3
CERTUM QDA	2	3
CERTUM QODA	2	3
CERTUM QRRA	2	3
CERTUM QACA	2	3

Shared secret transfer procedure has to include secret holder presence during key generation and distribution process, acceptance of a delivered secret and resulting responsibility for its storage, and it should state conditions and requirements for shared secret retransmission to authorized personnel.

6.2.2.1. Acceptance of secret shares by its holders

Every shared secrets holder, before receiving his/her secret, should personally observe secret shares creation, verify the correctness of a created secret and its distribution. Each part of the shared secret has to be transferred to its holder on a cryptographic card protected by a PIN number assigned by the holder and known only to him/her. The reception of the shared secret and its appropriate creation in accordance with this document is confirmed by a hand-written signature on an appropriate form whose copy is retained in certification authority.

6.2.2.2. Protection of secret shares

Holders of shared secret have to protect their share from revelation. With the exceptions described below, the holder of the share declares that he/she:

- will not reveal, copy or share the secret with any other party and that he/she will not use the share in an unauthorized manner,
- will not reveal (directly or indirectly) that he/she is the holder of the secret,
- will not store the share in a place rendering emergency usage of the share impossible when the holder is inaccessible.

6.2.2.3. Availability and erasure (transfer) of shared secret

The holder of a shared secret should allow access to his/her share to authorized entities (specified in an appropriate form, signed by the holder upon delivery of the share) only after authorization of secret transmission. This situation should be recorded in the security system as an appropriate transaction log.

In the case of natural disasters (declared by the shared secret issuer) the holder of the secret should attend himself/herself in the emergency recovery site of CERTUM, according to instructions submitted by the share issuer. Before the shared secret holder attends himself/herself in the emergency recovery, site he/she should receive confirmation of a required presence from shares issuer. The shared secret should be delivered by the holder to the

emergency recovery site personally by the holder in a manner allowing share usage for restoration of CERTUM activity to its normal state.

6.2.2.4. Responsibilities of shared secret holder

Shared secret holder should perform his/her duties and obligations according to the requirements of this document and in a deliberate and responsible manner in any possible situation. A shared secret holder should notify the issuer of the share in the case of the secret theft, loss, unauthorized revelation or security violation immediately after the incident occurrence. A shared secret holder is not responsible for neglecting his/her duties because of the reasons that are impossible to control by the holder, but is responsible for inappropriate revelation of the secret or neglecting the obligation to notify the issuer of the secret about inappropriate revelation or security violation of the secret, resulting from the holder mistake, neglect or irresponsibility.

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.

Depending on applicable key distribution method (appropriately direct or indirect, see Chapter 6.2.2), copies of private keys are retained in secret shares or in one piece (after encryption with a symmetric key). Copied keys are stored in hardware security modules. Security module, used for private key storage, complies with requirements disclosed in Chapter 6.2.1. The copy of a private key is entered into module in accordance with procedures described in Chapter 6.2.6.

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 **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** 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.

Private keys of certification authorities used in key agreement operations have to be archived after expiry of the validity date of the associated certificate or upon its revocation for

the period at least 5 years. Archived keys have to be available for 25 years; for the first 15 years they must be accessible *on-line*.

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.

CERTUM applies two methods of securing key – subjected to entry into the cryptographic module – integrity:

- if the key is provided in one piece than outside the module it is not available in plain form, i.e. upon key generation in the module and its export to another cryptographic device, the key is encrypted with a secret key; the secret key is stored in a manner preventing unauthorized access to both parts of the secret (private key and secret key used for its encryption) simultaneously,
- if a key or its password is stored as secret shares, then the very module is able to verify, on shares loading, a potential attack or forgery attempts.

Entry of a private key into hardware security module 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** requires restoration of the key from the cards in the presence of appropriate number of share holders or administrator's card protecting the module containing these private keys (see Chapter 6.2.2). Since every certification authority may posses an encrypted copy of its private key (see Chapter 6.2.4), the keys may be also transferred between the security modules.

A private key of a registration authority is always available in one instance (no copies); therefore there is no need to enter it into the memory of the cryptographic module.

6.2.7. Method of Activating Private Key

Methods of activation of a private key, possessed by various users and subscribers of CERTUM system, apply to the method of key activation before every use of them or beginning of a session (e.g. the internet connection) employing these keys. A once activated key is ready for usage until the moment of the key deactivation.

Activation (and deactivation) of private key procedure execution depends on the type of the entity holding the key (subscriber, registration authority, certification authority, device, etc.), on sensitivity of the data protected by the key, and on, the fact whether the key remains active for the time of one operation, session or for unlimited time.

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.

Activation of a subscriber's private key is carried out similarly to private keys of certification authority operators, regardless whether they are stored on an electronic card or in an encrypted form as a file on a floppy disc or any other media.

6.2.8. Method of Deactivating Private Key

Private key deactivation method applies to key deactivation methods after their usage or upon completion of every session (e.g. network connection) during which the key were used.

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

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.

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

Remaining requirements of this Chapter apply to public key archive procedure and validity period of public and private keys of every subscriber, including a certification authority.

In terms of technology it is possible to use one key pair for both electronic signature creation operation and data encryption. This Certification Practice Statement does not recommend acting in such a manner, except in the cases described in chapter 6.1.9 In the case of qualified this is prohibited.

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 (see Chapter 2.6). 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.

Every authority issuing certificates archives public keys of subscribers whom certificates were issued to. Certification authority public keys are archived together with private keys, in the manner described in Chapter 6.2.5.

Certificates may also be archived locally by subscribers, especially when is required by used application (e.g. electronic mail systems).

Public key archives should be protected in a manner preventing unauthorized addition, insertion, modification or removal of the key to or from the archive. The protection is enforced with authentication of the archiving entity and authorization of their requests.

Within CERTUM, only the keys used for electronic signature verification are subjected to archival. Any other types of public keys (e.g. keys used for encrypting messages) are destroyed immediately after their removal from the repository.

The security inspector performs review of public key archive quarterly , verifying its integrity. The purpose of this verification is to make sure that there are no gaps in the archive, and certificates stored in the archive have not been modified. Mechanisms verifying integrity of the archive take into consideration the fact that the retention period of the archives may be longer than the security means used to creation of the archive.

Public keys are retained in the public key archive for the period of 25 years (see Chapter 4.16.3).

Every archive of a public key or a public key destruction is recorded in the event journal.

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 (see Chapter 7.1). 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 20, while subscriber's certificates are presented in Table 21.

Usage periods of certificates and the corresponding private keys may be shortened in the case of suspension or revocation of a certificate or a key.

For recertification, private key validity period may be longer than the period of validity of the certificate associated with it.

Starting date of the certificate validity period doesn't have to complies with the date of its issuance. It is allowed to set this date in the future but never in the past.

Tab. 19 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	certification authority certificate	–	5 years	–
	private key	–	5 years	–
certification authority certificate	certification authority certificate	–	5 years	–
	private key	–	5 years	–
CERTUM QDVCS	certification authority certificate	–	5 years	–
	private key	–	5 years	–
CERTUM QDA	certification authority certificate	–	5 years	–
	private key	–	5 years	–
CERTUM QODA	certification authority certificate	–	5 years	–
	private key	–	5 years	–
CERTUM QRRA	certification authority certificate	–	5 years	–
	private key	–	5 years	–
CERTUM QACA	certification authority certificate	5 years	–	–
	private key	3 years	–	–

Every user, including a 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*** *can terminate private key usage for electronic signature creation at any time, although the certificate remains currently valid. Notwithstanding, a certification authority, time – stamping authority, online certificate status protocol authority****,*** *data validation and certification server authority and delivery authority are obligated to notify its subscribers of this situation (related for example to key changeover).*

Tab. 20 Maximal usage periods of the qualified certificates

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

Tab. 21 Maximal usage periods of the attribute certificates

Owner and key type	Maximal validity period
Private persons	2 years

6.4. Activation Data

Activation data are used for activation of a private key used by a registration authority, a certification authority or by subscribers. They are usually used on the stage of entity authentication and control of the access to a private key.

6.4.1. Activation Data Generation and Installation

Activation data are used in two basic cases:

- as an element of one- or multi-factor authentication procedure (so called authentication phrase, e.g. password, PIN number, etc),
- as a part of the shared secret, which upon installation allows cryptographic key(s) restoration.

Registration authority and certification authority operators, as well as other persons performing the roles described in Chapter 5.2.1 should operate passwords in the way resistant against the brute force attacks (also called exhaustive attacks).

In the case of the private key activation, it is recommended to use multi-factor authentication procedures, for example a cryptographic token (including an electronic cryptographic card) and an authentication phrase or a cryptographic token and biometric (e.g. fingerprint of the subscriber).

The above authentication phrase should be generated in accordance with the requirements of FIPS-112.

Shared secrets used for certification authority private key protection are generated in accordance with the requirements presented in Chapter 6.2 and retained inside cryptographic tokens. The tokens are protected by a PIN number, created in accordance with the requirements of FIPS 12. Shared secrets become activation data after their activation, i.e. providing the correct PIN number protecting the token.

6.4.2. Activation Data Protection

Activation data protection includes activation data control methods preventing from their revelation. Activation data protection control methods depend on the fact whether they are authentication phrases and whether control is enforced on the basis of private key or its activation data distribution into shares (shared secrets).

In the case of the authentication phrase protection, the recommendations described in FIPS 112 should be enforced, while protection of shared secrets requires implementation of FIPS 140.

Activation data used for private key activation is protected by means of cryptographic controls and physical access controls. Activation data should be biometric data or should be kept securely (not written down) by the entity being authenticated. If the authentication data are written down, the level of their protection should be the same as data protected by the usage of a cryptographic token. Several unsuccessful attempts to access this module should result in token lock. Stored activation data should never be retained together with the token.

6.4.3. Other Aspects of Activation Data

Activation data are stored always as a single copy. A sole exception from this rule are PIN numbers, protecting access to shared secrets – every shared secret holder can create a copy of the PIN number and retain it in the location different than the shared secret

Activation data protecting access to private keys stored on cryptographic tokens can be periodically changed.

Activation data are not archived.

6.5. 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*[42] (ITSEC), at least level E3.

6.5.1. Specific Computer Security Technical Requirements

Technical requirements, presented in this Chapter, apply to single computer security control and installed software control, used for CERTUM system operation. Security means protecting computer systems are executed on the level of operating system, application and physical protections.

[42] Information System Security Controls Assesment Criteria

Computers operated in certification authorities and in their associated components (e.g. registration authorities) are equipped with the following security controls:

- mandatory authenticated registration on the level of operating system and application (in the case of significant importance, e.g. due to the role performed in the system),
- at least, discretionary access control,
- possibility of conducting security audit,
- computers are available only to personnel performing trusted roles in CERTUM,
- employee who act as the trusted role, is obliged to lock his/her workstation ever, if it remains outside his/her supervision,
- forced segregation of duties, arising from the role performed in the system,
- forced log out of user after a period of inactivity,
- identification and authentication of roles and personnel performing these roles,
- cryptographic protection of information exchange session and protection of databases,
- archive of history of operation carried out on the computer and data required by audits,
- a secure path allowing credible identification and authentication of roles and personnel performing these roles,
- key restoration methods (only in the case of hardware security modules) and application and operating system,
- monitoring and alerting means in the case of unauthorized computer resources access.

Assessment of computer security means is carried out in accordance with recommendations presented in ITSEC[43] and related to security level E4.

6.5.2. Computer Security Rating

CERTUM computer system complies with requirements laid down in the *Information Technology Security Evaluation Criteria (ITSEC)*. The above has been confirmed by an independent auditor, performing functionality assessment of CERTUM on the basis of the criteria described in the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* and the WebTrust Principles and Criteria for Certification Authorities. Systems used for issuing and managing certificates are required to fulfil the *CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements, CEN (European Committee for Standardization), January 2003*.

6.6. Technical Controls

6.6.1. System Development Controls

Applications used by CERTUM system are developed and implemented by Asseco Data Systems S.A. developers. Every application is developed and updated in accordance with *Unified Process (RUP)* methodology.

43 *Information Technology Security Evaluation Criteria*

Hardware changes are also monitored and registered. In particular the monitoring guarantees:

- hardware is supplied in a manner allowing its tracing and evaluation of the route of the component to the place of its installation,
- replacement hardware delivery is carried out in a manner similar to delivery of original hardware; replacement is carried out by trusted and trained personnel.

6.6.2. Security Management Controls

The purpose of security management control is to supervise CERTUM system functionality providing assurance that the system operates correctly and in accordance with the accepted and implemented configuration.

Current configuration of CERTUM system, as well as any modifications and updates to its system are recorded and controlled. Controls applied to CERTUM system allow continuous verification of application integrity, their version and authentication and verification of hardware origin.

6.6.3. Life Cycle Security Ratings

This Certification Practice Statement does not imply any requirements in this field.

6.7. 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).

Both segments comply with requirements defined in the *Art 26, § 1* of *the Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094).*

CERTUM's second subnetwork performs the role of a model system, used in development and test operations.

CERTUM computer system is protected against denial of services type attacks and secured by the intrusion detection system. Security controls are developed on the basis of firewall and traffic filtering on the routers and Proxy services.

Network firewall's controls accept only messages submitted with the usage of http, https, and NTP, POP3 and SMTP protocols. Event records (logs) are recorded in the system logs and allow supervision of correctness of the usage of services provided by CERTUM.

Detailed configuration of CERTUM network and its protection means is presented in technical infrastructure documentation. Such documentation has a "non-public" status and is available only to security inspector, system administrator and auditors.

6.8. Cryptographic Module Engineering Controls

Cryptographic module engineering controls include requirements enforced on development, production and delivery of the module process. CERTUM does not define proprietary requirements in this area. However, CERTUM accepts and employs only cryptographic modules complying with the requirements described in Chapter 6.2.

Hardware security modules delivering to CERTUM are always checked whether the module has been tampered with and that the module preserves of its physical and logical integrity. Verification and a written summary of the review is carried only by trusted personnel of CERTUM.

Hardware security modules that are not in use are protected in the special envelopes which make it impossible to open the envelope without leaving traces. Thus prepared modules are stored in safes that are located in the secure zone to which access is limited only to the identified group of people in trusted roles.

6.9. Time stamps as a security control

Request created within CMP and CRS protocol (Chapter 6.1.3) 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*. Note, that in contrast to this time stamps, the time – stamping authority CERTUM QTSA issuing timestamp tokens in accordance with *ETSI TS 101 861* recommendation (see Chapter 1.3.2).

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 the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094)*. 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 Asseco Data Systems S.A. on the basis of requirements defined in the *PN-ISO/IEC 13888-3:1999 Information technology -- Security techniques -- Non-repudiation -- Part 3: Mechanisms using asymmetric techniques.*

Information stated below describes the meaning of respective certificate fields, CRL, timestamp token, applied standard and private extensions employed for the needs of CERTUM.

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 include values of **basic fields** and **extensions** (standard, described by the norm, and private, defined by the certification authority).

Extensions defined in a certificate according to the X.509 v.3 recommendation allow assignation of additional attributes to the subscriber and his/her/its public key and simplify management of hierarchical certificate structure. Certificates issued in accordance with X.509 v.3 recommendation allow definition of proprietary extensions, unique for implementation of the system.

7.1.1.1. Basic fields

CERTUM supports the following certificate basic fields:

- **Version**: third version (X.509 v.3) of certificate format,
- **SerialNumber**: certificate serial number, unique within certification authority domain,
- **SignatureAlgorithm**: identifier of the algorithm applied by a certification authority issuing certificates,
- **Issuer**: distinguished name (DN) of a certification authority,
- **Validity**: validity period, described by the beginning date (**notBefore**) and the ending date (**notAfter**) of the certificate validity period,

- **Subject**: distinguished name (DN) of the subscriber that is the subject of the certificate,
- **SubjectPublicKeyInfo**: value of a public key along with the identifier of the algorithm associated with the key.

In certificates issued by CERTUM values of the above fields are set in accordance with the rules described in Table 23

Tab. 22 Profile of the basic fields of subscriber 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) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Serial Number (SN) =	Entry number: 14
Not before (validity period beginning date)	Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard. CERTUM clock is 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 the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094).* DN profile depends on the type of entity.	
Subject Public Key Info)	Public Key Algorithm	sha1WithRSAEncryption
	RSA Public Key	2048 bits
	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 the *Regulation of the Council of Ministers of 7 August 2002 on determining the technical and organizational conditions for qualified certification service providers, certification policies for qualified certificates issued by these entities and the technical conditions for secure devices for the creation and verification of electronic signatures (Journal of Law 2002, No. 128 item 1094).*	

7.1.1.2. Standard extensions fields

Function of every extension is defined by the standard value of the corresponding object identifier (**OBJECT IDENTIFIER**). Extension, depending of the choice of issuing authority, may be **critical** or **non-critical**. If an extension is defined as critical, the application supporting certificate usage must reject every certificate containing an unrecognized critical extension. On the other hand, extensions defined as non-critical may be omitted.

CERTUM supports the following fields of standard extensions:

- **AuthorityKeyIdentifier**: identifier of a certification authority public key certificate complimentary with a private key, used for signing of issued certificate – **this extension in not critical**,
- **KeyUsage**: allowed key usage – **this extension is critical**. This extension describes the usage of the key, e.g. key for data encryption, key for electronic signature, etc (see below):

```
digitalSignature    (0), -- key for electronic signature creation
nonRepudiation      (1), -- key associated with the non-repudiation
                         -- services
keyEncipherment     (2), -- key for key exchange
dataEncipherment    (3), -- key for data encryption
keyAgreement        (4), -- key for key agreement
keyCertSign         (5), -- key for certificate signing
cRLSign             (6), -- key for CRL signing
encipherOnly        (7), -- key only for encryption
decipherOnly        (8)  -- key only for decryption
```

- **ExtKeyUsage**: definition (constraint) of the key usage – **this extension is critical**. This field defines one or more areas, in addition to standard key usage, defined by **keyUsage** field, of the possible usage of a certificate. This field should be interpreted as constraint of allowed key usage purpose defined in field **keyUsage**. CERTUM issues certificates which may contain one of the following value or combination of such values:

```
serverAuth      - authentication of TLS web server; keyUsage field bits
                  which comply with the fields: digitalSignature,
                  keyEncipherment or keyAgreement
clientAuth      - authentication of TLS Web client; keyUsage field bits
                  which comply with the fields: digitalSignature and/or
                  keyAgreement
codeSigning     – signature of executable code; keyUsage field bits which
                  comply with the field: digitalSignature
emailProtection - Email protection; keyUsage field bits which comply with
                  the fields:  digitalSignature, nonRepudiation and/or
                  (keyEncipherment or keyAgreement)
ipsecEndSystem  – IPSEC protocol protection
ipsecTunnel     - IPSEC protocol tunnelling mode
ipsecUser       - IP protocol protection in user application
timeStamping    – binding of the digest value with the time provided by
                  previously accepted trusted time source; keyUsage field
                  bits which comply with the fields: digitalSignature
                  and/or nonRepudiation
OCSPSigning     – assigns the right to issue certificate status
                  confirmations on behalf of CA; keyUsage field bits
                  which comply with the fields: digitalSignature,
                  nonRepudiation
dvcs            – issuance of  confirmation by a notary authority, on the
                  basis of DVCS protocol; keyUsage field bits which
                  comply with the fields: digitalSignature,
                  nonRepudiation, keyCertSign, cRLSign
```

- **CertificatePolicies –** information of the **PolicyInformation** type (identifier, electronic address) about a certification policy, applied by the issuing authority – **this extension is critical**,

Tab. 23 Policies identifiers and their description

Policy identifier	Certificate policy description
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 1	Identifies certification policy used for issuing qualified certificates.
joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32)	Identifies certification policy used for issuing certificates in accordance with the §7 of the *Regulation of the Minister of Economy of 9 August 2002 on determining the detailed procedure of creating and issuing the certificate of the certification associated with electronic signature (Journal of Laws 2002 No. 128, item 1101, as ammended).*
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 10	Identifies certification policy used for issuing certificates of infrastructure keys.

Certificates issued by certification authorities include both qualifiers, recommended by the *RFC 3280*.

- **PolicyMapping – this field is not critical**; this field contains one or more pairs of OID, defining equivalency of the issuer policy with the subject policy,
- **IssuerAlternativeName**: alternative name of the certificate issuer – **this field is not critical**,
- **SubjectAlternativeName**: alternative name of the certificate subject – **this field is not critical**,
- **BasicContraints – this field is critical**. 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),
- **CRLDistributionPoints**: point of distribution of Certificate Revocation List – **this field in not critical**; the extension defines network addresses hosting current CLR, issued by the **cRLIssuer**,
- **SubjectDirectoryAttributes**: attributes concerning subject directory **– this field is not critical**; The extension contains additional attributes associated with the subscriber and supplementing information described in the field **subject** and **subjectAlternativeName**; this extension contains attributes not included within subject's Distinguished Name,
- **AuthorityInfoAccessSyntax**: access to certification authority information – **this field is not critical**; the field indicates the method of information and service provision by the issuer of the certificate,
- **QCStatements**: declarations of the issuer of the qualified certificate – **this field is not critical,**
- **BiometricSyntax**: information about biometric parameters of the subject of the certificate – **this field is not critical**; two types of biometric information are available:

a hand-written signature and a photo; the certificate contains only the digest of a biometric parameter; the value of the digest is provided in the field **biometricDataHash**, while the identifier of the hash function used for computing the digest is provided in the field **hashAlgorithm**; full biometric information about the subject (his/her/its biometric syntax) is stored in database, whose URI is provided in the field **sourceDataUri**. Effective usage of biometric information in a certificate (its digest) is possible only in the case of comparison of the digest of the syntax stored in database (full information) with the digest collected from the certificate.

7.1.2. Certificate Extensions and issued certificates types

Certificates issued by **CERTUM QCA** may contain various combinations of extensions defined in Chapter 7.1.1.2. Choice of the desired certificate depends mainly on the intended purpose of the certificate and the subscriber whom the certificate is issued.

7.1.2.1. Qualified certificates

The qualified certificates that meet requirements of the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450),* issued to private persons contain extension described in Table 25.

Tab. 24 Extensions of qualified certificates

Extension	Value or Value constraint	Extension status
Authority Key Identifier	SHA1 hash of the public key	Non-critical
Basic Constraints	Subject type = empty (end entity) Path length constraint=none	Critical
Key Usage	Non-repudiation, bit 1	Critical
IssuerAlternativeName	(optionally) Alternative certification authority name	Non-critical
Subject Alternative Name	(optionally) Email: customer@somewhere-in-world.com	Non-critical
CRL Distribution Points	URI: http://crl.certum.pl/qca.crl	Non-critical
Authority Info Access	(optionally) OCSP: http://qocsp.certum.pl	Non-critical
Biometric Info	(optionally) Subscriber's photo, DNA, retinal scan, fingerprint (bit 0) Hand-written signature (bit 1) URI: biometric data location	Non-critical
QCStatements	A statement that the certificate is a qualified certificate [44]. Transaction limit Indication of the authorization	Non-critical

[44] This is the statement of `Asseco Data Systems S.A.` that qualified certificates are issued in accordance with the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450).* `Asseco Data Systems S.A.` 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}.

Extension	Value or Value constraint	Extension status
Certificate Policies	Policies: 1.2.616.1.113527.2.4.1.1 (qualified certificates) CPS: http://www.certum.pl/repozytorium Notice number: depends on certificate type Organisation: Asseco Data Systems S.A.Explicit text: depends on policy identifier (plain text)	Critical
Subject Directory Attributes	(optionally) Additional attributes associated with the entity and an additional information included in field subject and **subjectAlternativeName**.	Non-critical

7.1.2.2. Certificates of certification authority

Certificates of certification authority may contains extensions described in Table 26.

Tab. 25 Minimal extensions of certificates of certification authorities

Extension	Value or Value constraint	Extension status
Basic Constraints	Subject type = CA Path length constraint=none – in the case of **CERTUM QCA**	Critical
Key Usage	Key for certificate signing (keyCertSign), bit 5 Key for CRL signing (cRLSign), bit 6	Critical

7.1.2.3. Cross-certification certificates

Cross-certification certificates may contain extension specified in Table 27

Tab. 26 Extensions of cross-certification certificates

Extension	Value or Value constraint	Extension status
Authority Key Identifier	SHA1 hash of the public key	Non-critical
Basic Constraints	Subject type = CA Path length constraint=none	Critical
Key Usage	Key for certificate signing (keyCertSign), bit 5 Key for CRL signing (cRLSign), bit 6	Critical
Subject Alternative Name	(optionally) URI: http://www. customer-service .pl Client service location	Non-critical
Authority Info Access	(optionally) OCSP: http://qocsp.certum.pl	Non-critical
Certificate Policies	Policies: 2.5.29.32.0 CPS: http://www.certum.pl/repozytorium	Critical

Extension	Value or Value constraint	Extension status
	Notice number: depends on certificate type Organization: Asseco Data Systems S.A. Explicit text: depends on policy identifier (plain text).	

7.1.3. 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.

7.1.4. 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.

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. Mandatory fields identify CRL issuer, while optional fields contain information about revoked certificates and CRL extensions.

The following fields are the contents of mandatory and optional fields of CRL:

- **Version**: CRL format version,
- **Signature**: contains identifier of the algorithm used by a certification authority to sign CRL; CERTUM authorities sign **CRL** by means of **sha1WithRSAEncryption** algorithm,
- **Issuer**: name of the certification authority issuing CRL **(CERTUM QCA)**
- **ThisUpdate**: CRL publication date,
- **NextUpdate**: announcement of the date of the next CRL publication; if the field is present, its value describes non-excessive date of the next CRL update (although the publication may be made prior to this date),
- **RevokedCertificates**: the list of revoked certificates (the field is empty in the case of lack of revoked certificates); the information consist of three sub-fields:

```
userCertificate     - serial number of a revoked certificate
revocationDate      - date of the certificate revocation
crlEntryExtensions  - extended access to CRL (contains additional
                      information about revoked certificates –
                      optional)
```

- **crlExtensions**: extended information about Certificate Revocation List (optional field). Among numerous extensions, the most important are the following ones:

AuthorityKeyIdentifier (see also Chapter 7.1.1.2) allowing identification of a public key corresponding to a private key used for list signing, and **cRLNumber**, containing monotonically increased serial number of the lists issued by a certification authority (by means of this extension, a subscriber is able to define when a specific CRL replaced another list) .

7.2.1. Supported CRL entry extension

Function and meaning of extensions are the same as for certificate extensions (see Chapter 7.1.1.2). CRL entry extensions (**crlEntryExtensions**) supported by CERTUM contain the following fields:

- **ReasonCode**: code of the reason for revocation. This field in **non-critical CRL entry extension**, allowing determination of the revocation reason. The following reasons of certificate revocation are allowed:

```
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; this
                     reason might also mean that the data used for
                     creating electronic signature were compromised
aaCompromise       - applies to attributes certificates; meaning is the
                     same as for withdrawal of privileges;
```

- **HoldInstructionCode**: code of the operation on certificate suspension. This field is **non-critical CRL entry extension** which defines a registered identifier of the instruction determining the operation to be executed upon certificate discovery on Certificate Revocation List with a note (reason for revocation): certificate suspended (**certificateHold**). If the application discovers the code **id-holdinstruction-callissuer**, it should notify the user of necessity to contact CERTUM to verify the reason of the certificate suspension or reject the certificate (assume it is revoked). If the application discovers **id-holdinstruction-reject** code, it should obligatorily reject the respective certificate. The code **id-holdinstruction-none** is semantically equal to omission of **holdInstructionCode** extension; usage of the code in CRL issued by CERTUM is prohibited,

- **InvalidityDate**: date of revocation. This field is **non-critical CRL entry extension** allowing assessment of the confirmed or suspended date of a private key compromise or occurrence of other reason for certificate revocation.

7.2.2. Revoked certificates and CRL

Information about revoked certificates (issued by CERTUM) is included in each list of suspended and revoked certificates, published prior to an expiry date of the certificate's validity period and on the first list published following the expiry of this period..This rule applies also to revoked certificates of a certification authority: certificates have to be included in the succeeding Certificate Revocation Lists, published by the issuer of the revoked certificate (in the case of cessation of the issuer operation, the last published CRL should be transferred to the repository of another, for example supervising, authority issuing certificates (compare Chapter 4.19).

7.2.3. Revoked attribute certificate and CRL

The End Entity Attribute Revocation List (EARL) profile is identical to that described in Chapter 7.2 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.

Revoked attribute certificates remain on the End Entity Attribute Revocation List for the period of their declared validity.

7.3. Timestamp token profile

CERTUM QTSA authority electronically signs issued timestamp tokens with one or more private keys reserved solely for this purpose. According to RFC 3280 recommendation certificates of their complementary public keys contain field constraining allowed key usage (**ExtKeyUsageSyntax**), marked as **critical**. This means the certificate may be used by the time - stamping authority solely for the purposes of signing timestamp tokens issued by this authority.

Time-stamping authority certificate contains information on possible contacts with the authority. Such information is presented in private extension – **AuthorityInfoAccessSyntax** – which is set as non-critical.

Time-stamping authority certificate basic fields profile is described in table 28

Tab. 27 TSA certificate basic fields profile

Field name	Value or its constraint	
Version	Version 3	
Serial Number	Unique value for each certificate issued by the National root NCCert	
Signature Algorithm	sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (Distinguished Name)	Distinguished name DN of the National root NCCert	
Not before (validity period beginning date)	Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard (PPS). CERTUM clock is 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 (PPS). CERTUM clock is known as valid world Stratum I service	
Subject (Distinguished Name)	Common Name (CN) =	Certum Time-Stamping Authority
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Serial Number (SN) =	Entry number: 15
Subject Public Key Info	Encoded in accordance with *RFC 3280*, contains information about RSA public key (key identifier 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.*	
Basic Constraints	Subject type = empty (end entity) Path length constraint=none	Critical
Key Usage	digital signature, bit 0 non-repudiation, bit 1	Critical
Extended Key Usage	Time Stamping Authority (TSA)	Critical
Certificate Policies	Policy: 2.5.29.32.0 CPS: http://www.certum.pl/repozytorium Notice number: depends on certificate type Explicit text: depends on policy identifier (plain text)	Critical
Authority Key Identifier	SHA1 hash of the public key	Non-critical

Timestamp token, issued by Certum Time-Stamping Authority contains (see Fig. 4) information on timestamp (**TSTinfo** structure), located in **SignedData** structure (see RFC 2630), signed by time - stamping authority and embedded in **ContentInfo** structure (see RFC 2630).

TSA authority response (in ASN.1 notation) on timestamp token request has a form:

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

Response status filed (**PKIStatusInfo**) allows submission – to an entity requesting timestamp – of information on occurrence or lack of occurrence of errors in the request. If the error code is equal 0 or 1, it means the response contains timestamp. Any other value means the response does not contain a valid timestamp. The reason of authority not issuing the token is described in **failInfo** field of **PKIStatusInfo** structure.

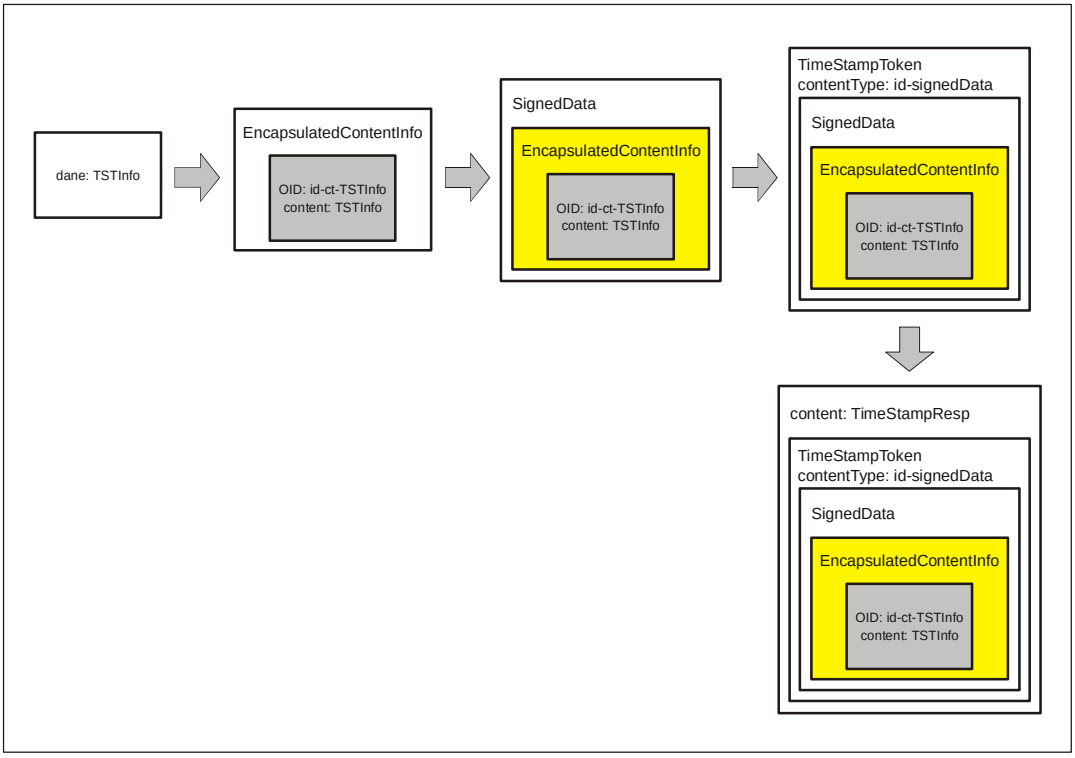

Fig. 5 Timestamp request response encapsulation (see also Technical Report [37])

PKIStatusInfo structure has a following form:

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

Meaning of the fields:

- **status** contains information on response status; basing on RFC 3161 following values were specified:

```
PKIStatus :: INTEGER {
    granted                 (0),
      -- you received what you asked for, i.e. TimeStampToken
    grantedWithMode         (1),
      -- response is similar to what you asked for (TimeStampToken);
      -- the verifier should check the differences
    rejection               (2),
      -- no response was granted, more information in attached message
    waiting                 (3)
      -- the request was not yet proceeded, expect the response later
    revocationWarning       (4)
      -- the message contain warning on approaching revocation
    revocationNotification (5)
      -- confirmation of revocation
}
```

- **statusString** may be used for submitting plain test message (in any language) to the requester. Code of the language used for message construction is described by appropriate tag, described in RFC 1766.

```
PKIFreeText ::= SEQUENCE SIZE (1..512) OF UTF8String
    -- message is encoded as UTF-8 string (warning: each UTF-8 string
    -- should contain tag of the language of the text, complying with RFC
    -- 1766/2044
```

- **failInfo** used for more precise description of error (timestamp token being not issued)

```
PKIFailureInfo ::= BIT STRING (
    badAlg              (0),
      -- unknown or unsupported algorithm identifier
    badMessageCheck     (1),
      -- data integrity error (e.g. signature verification error)
    badRequest          (2),
      -- prohibited or unsupported transaction (request)
    badCertId           (4),
      -- appropriate certificate(s) was not attached to the request
    badDataFormat       (5),
      -- data provided in bad format
    wrongAuthority      (6),
      -- authority selected in the request for issuing the certificate
      -- is not the authority, which received the request
    inccorectData       (7),
      -- data provided in the request are not appropriate for issuing the
      -- response
    missingTimeStamp    (8),
      -- lack of timestamp required in the request
    timeNotAvailable    (14),
      -- TSA time source unavailable
    unacceptedPolicy    (15),
      -- requested TSA policy is not supported by TSA
    unacceptedExtension  (16),
      -- extension provided in the request is not supported by TSA
addInfoNotAvailable  (17),
      -- request for additional information is not recognized or is not
      -- available
    systemFailure       (25),
      -- request could not be proceeded due to system malfunction
}
```

Timestamp token general format complies with ContentInfo format:

```
TimeStampToken ::= ContentInfo
```

Timestamp token cannot contain any other electronic certificates, beside time - stamping authority certificate. TSA certificate identifier must be recognized as signed attribute and located in area of the field **signedAttributes** of **SignedData** structure.

Informative part of the timestamp token is included in **TSTInfo** structure, located in **eContent** field of **EncapsulatedContentInfo** structure (see RFC 2630). **eContent** field type, specified by the value of **eContentType** field for **TSTInfo** is defined as follows:

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

Timestamp informative content has the form:

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

The meaning of most important fields of **TSRInfo** is as follows:

- **policy** – must occur and specify the policy which is used for issuing timestamps by the time - stamping authority; in case of **CERTUM QTSA** the policy identifier has the value:

Policy identifier	Policy name
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1) 2}	CERTUM QTSA Identifies certification policy, used for issuing timestamp tokens

- **messageImprint** contains information submitted by the requester, signed with the timestamp;
- **serialNumber** contains serial number of timestamp token, issued by time - stamping authority. Serial number must contain continuously increasing integers;
- **genTime** field includes date and time of timestamp issued by the authority (with the accuracy of 1 second);
- **accuracy** field specifies the accuracy of time used by the time - stamping authority (**CERTUM QTSA** authority generates time with the accuracy of at least 1 second). If the field is omitted, the default accuracy value is set at 1 second;
- if the field **ordering** is omitted, or its value is set to FALSE, then the field **genTime** discloses only the time of timestamp issuance by the TSA. In this case, ordering of two timestamps issued by this authority or different authorities is possible only, when the difference between **genTime** field value of the first and second token is greater then the cumulative value of the accuracy filed of each token; if the field ordering is present and its value is set to TRUE, then each token issued by this authority may be ordered solely by the value of the filed **genTime**, irrespective of time accuracy. **CERTUM QTSA** authority always set the value of the field to FALSE**;**
- **nonce** field must occur if it was included in the request submitted by the requester and must hale the same value;

- **tsa** field identifies the name of the time - stamping authority. If it occurs, it must comply with subject distinguished name included in the certificate, issued to the TSA by CERTUM QCA and used in token verification

TimeStampToken structure is connected with the set of signed attributes (in field signerInfos of SignedData structure, see Technical Raport [37]). Timestamp token include at least the following attributes:

1. Content type attribute

```
Name:       id-contentType
OID:         { iso(1) member-body(2)
                        us(840) rsadsi(113549) pkcs(1) pkcs9(9) 3 }
Syntax:     id-ct-TSTInfo
values:     id-ct-TSTInfo value is recalled only once
```

2. Message digest attribute

```
Name:       id-messageDigest
OID:         { iso(1) member-body(2)
                        us(840) rsadsi(113549) pkcs(1) pkcs9(9) 4 }
Syntax:     MessageDigest
values:     value of the MessageDigest type is recalled only once

-- hash of the eContent field of EncapsulatedContentInfo structure
MessageDigest ::= Digest
Digest ::= OCTET STRING (SIZE(1..20))
```

3. Signing certificate attribute

```
Name:       id-aa-signingCertificate
OID:         { iso(1)
       member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs9(9)
       smime(16) id-aa(2) 12 }
Syntax:     SigningCertificate
values:     value of the SigningCertificate type is recalled only once

-- Signed attribute of the certificate
SigningCertificate ::= SEQUENCE {
    certs     SEQUENCE OF ESSCertID,
    policies  SEQUENCE OF PolicyInformation OPTIONAL
}

ESSCertID ::= SEQUENCE{
    CertHash       Hash,
    IssuerSerial  IssuerSerial OPTIONAL
}

Hash ::= OCTET STRING -- SHA1 hash of the whole certificate

IssuerSerial ::= SEQUENCE {
    Issuer         GeneralNames,
    SerialNumber   CertificateSerialNumber
}

GeneralNames ::= SEQUENCE SIZE (1..MAX) OF GeneralName
```

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* [40]

8. Certification Practice Statement management

Every version of Certification Practice Statement 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 Practice Statement is supplied for approval. During CPS approval process, new version of the document has the status **under approval**. After completion of the approval procedure, a new version of Certification Practice Statement is marked with the status **valid**.

Beside different versions, Certification Practice Statement has also builds having the same status types as version. The new build of Certification Practice Statement is marked with unique number, placed after the version number of the valid CPS, separated by the dot.

Decision on acceptance of the changes in Certificate Practice Statement version or build number is made by the security inspector.

Rules and requirements concerning Certification Practice Statement management described below also govern Certification Policy management.

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

8.1. Changes introduction procedure

Regardless of audits, there is once a year a review of the current version of the Certification Practice Statement and the Certification Policy. Security inspector, designated by the management of CERTUM, analyze the content of the documents in the direction of their compliance with the implemented procedures and external requirements. Modification to Certification Practice Statement may be a result of observed errors, CPS update and suggestions from the affected parties. Modification proposals may be submitted by regular mail or electronic mail for the contract addresses of CERTUM. Suggestions propositions should describe modifications, their scope and justifications and means of contact the person requesting modification.

Suggestions concerning the current Certification Practice Statement may be submitted by the following authorized entities:

- minister in charge of economy
- auditing entities,
- legal entities, especially when Certification Practice Statement was observed to not to obey laws and regulations in force in the Republic of Poland and may affect subscribers' interests,
- security inspector, system administrator and other CERTUM personnel,
- CERTUM subscribers,
- professionals from the area of information system security.

After introduction of every modification, Certification Practice Statement or Certification Policy date of issuance is updated as well as theirs identifier, version or build.

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 Practice Statement, notification in advance apply to amendments resulting from implementation of editorial modifications, amendments to the contact information of the person responsible for CPS 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 Practice Statement 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 Practice Statement with the status **requested for comment**. Suggested modification may by published in the CERTUM repository and transmitted by the means of electronic mail. Information about implemented modifications is also attached to the new CPS.

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 Practice Statement receives the status **under approval** and is subjected to approval procedure (see Chapter 8.3).

The security inspector may fully accept suggested changes accept with amendments or reject suggested changes after expiration of the allowable period for resubmission of published and posted acceptance questionnaire.

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 Practice Statement. Identifiers of the certification polices applied by authorities issuing certificates may also be subjected to modification. This case may arise particularly as a result of the legislative changes relating to qualified certification service providers.

8.2. Publication

8.2.1. Items not published in CPS

Applied computer system security means are not available to the public. Neither are: authentication procedures and controls and the elements which exposure may affect security protections or suggest possible target of attack. In particular, items not subjected to publication comprise:

- employed hardware-software environment,
- details of applied hardware configuration,
- system emergency recovery plan,
- location of CERTUM key retention stores and their shares and PIN numbers protecting access to them,
- list of individuals being shared secret holders,
- implemented means of personnel protection,
- network protections,
- system logging procedures.

System documentation regarding elements not available to the public is available to the security inspector, the system administrator and the representative of an auditing institution. Documents describing such elements may be reviewed only in CERTUM seat in a specially designated area.

8.2.2. Publication of the new version of Certification Practice Statement

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

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

Three versions (if applicable) of Certification Practice Statement are available (if possible) at the repository and via the email: the currently applicable version, the previous version and the version under approval (see Chapter 8.3). In case of changed to build version of the Certification Practice Statement it is not required to publish previous build.

The document, describing significant differences between the current (still in force) Certification Practice Statement and the CPS subjected to approval should be available at the above addresses.

8.3. CPS Approval Procedures

If within 10 days of the publication of changes to Certification Practice Statement 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 is provided to the PKI Services Development Team for approval. Once it is approved, 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		
V 1.0	12th of October, 2002	Full version of the document. Document approved
V 2.0	15th of February, 2005	The scope of certificate usage clarified (chapter 1.4), circumstances and procedures of certificates modification clarified (chapter 3.2.2 and 4.7), period of validity of certificates was limited only to the period of validity of certification authority certificates (chapter 4.2 and 6.3.2), certificates revocation procedure adapted to the requirement of Article *31of the Act on electronic signature* (chapter.4.8), content of tables revised in chapter 7. Editorial changes.
V 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,)
V 2.2	20th of July, 2005	Change of service name from Unizeto CERTUM – Centrum Certyfikacji to CERTUM – Powszechne Centrum Certyfikacji.
V 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.
V 3.0	15th of July, 2006	New certification services added: certificate status verification services, data validation services, delivery services.
V 3.1	05th of January, 2008	New certification service added: deposits services, registries and repositories services, and relocation of certification authority „CERTUM - Powszechne Centrum Certyfikacji".
V 3.2	17th of September, 2007	New certification service added: issuance of attribute certificates service. Removal of information about certificates of infrastructure keys profile.
V 3.3	1 st of March, 2008	Updating the profiles of certificates
V 3.4	14 th of July, 2008	Updating the information about QDVCS
V 3.5	24th of July, 2009	Updating the information about recertification (renewal)
V 3.6	1st November, 2009	Updating the profiles of certificates
V 3.7	15th of April, 2010	Added information concerning compliance with the requirements of standards AICPA / CICA WebTrust Program for Certification Authorities Version 1.0 and Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements). Updating the Glossary. Removing III category of qualified certificates. Changing of requirements for the validity period of qualified certificates.
V 3.8	15th of May, 2012	Updating CERTUM's logo. Changing the rules of distribution of the shared secrets.
V 3.9	21 st of April, 2015	Adjusting the document to ETSI TS 101 456 requirements.
V 4.0	1st of April, 2016	Transfer of ownership of Unizeto Technologies S.A. Asseco Data System S.A. Adding the information on obligation to maintain certification certificate issued by Unizeto Technologies S.A. Asseco Data System S.A
V4.1	12th of April, 2016	Updating the number of qualified entry.

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	National Object Identifiers Registry (Krajowy Rejestr Identyfikatorów Obiektów)
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)

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, 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 – Asseco Data Systems 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 the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 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= Asseco Data Systems 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 the Art. 3, § *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**.

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 *Art. 23, § 4 or 5* of the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* 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 unauthorised 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 the Art. *2* of the *Act of 17 February 2005 on Informatization of Operation of Entities Performing Public Tasks (Journal of Laws No. 64, item 565, as ammended).*

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 personal certificate – is a qualified certificate issued to a natural person acting on his or her own behalf. Thus, an owner of the certificate is also its user. This certificate, apart from an owner basic identification data such as his or her name and personal ID number, can contain a number of additional information e.g. the owner's date of birth or address. This certificate may be revoked only by its owner (subscriber).

Qualified professional certificate - is a qualified certificate issued to a natural person acting on behalf of another natural person, company, organization or public authority. The owner of the certificate is the represented entity, whereas the agent representing the entity is the certificate's user. Apart from basic user identification data such as the name and personal id number, this certificate also contains information concerning the entity represented by the user. This certificate may be revoked by the subscriber or authorized person (e.g. authorized representative of the represented entity.)

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.

Represented entity – a person or an institution on whose behalf the subscriber uses a qualified certificate. The represented entity is the owner of the certificate and has a right to request its revocation in cases described in the *Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* and the Certification Practice Statement.

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 agreement – the agreement between a subscriber and Asseco Data Systems S.A.; a certificate is ordered by a subscriber and it is used by a subscriber on his/her own behalf or to act on behalf of the represented entity who is the owner of the certificate and has a right to request its revocation, a subscriber is the user of certificate.

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.