Certification Practice Statement of CERTUM's Qualified Certification Services

Version 4.0

Effective date: 1st 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).*

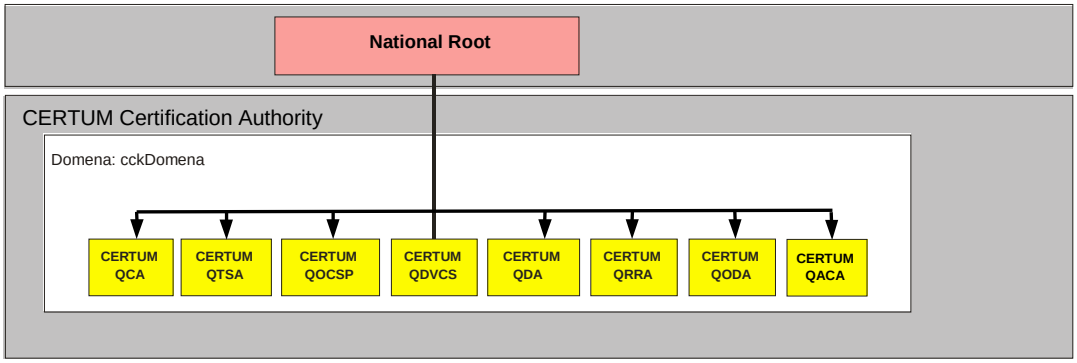

Fig.1.1 The authorities operating within CERTUM qualified services

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: 1.2.616.1.113527.2.4.1.0.1.4.0)[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) 0}
```

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).*