Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services

Version 5.6

Effective date: 09.09.2020

Asseco Data Systems S.A.
Podolska Street 21
81-321 Gdynia, Poland
www.assecods.pl/en

Certum
Bajeczna Street 13
71-838 Szczecin, Poland
www.certum.eu

Trademark and Copyright notices

Content

1. Introduction

Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services describes the general rules applicable to the qualified trusted services provided by Certum (full name: Certum – General Certification Authority). This document also fulfills the role of the Certificate Policy for each class of certificate and type of services.

1. the issuance of **public key qualified certificates**[1] **for electronic signatures and seals**, including registration of **subscribers**[2], certification of public keys and rekey,
2. the **revocation** and **suspension** of certificates,
3. the issuance of **electronic timestamp tokens**, **certificate status tokens**, data **validation tokens**[3].

These services are provided in accordance with:

- the Integrated Management System, implemented by Asseco Data Systems S.A., which includes the requirements of the PN-EN ISO 9001:2009 and PN-ISO/IEC 27001:2014,
- the *Regulation of the Ministry of Digitalisation of 5th October 2016 according the National Trust Infrastructure,*
- *the Act on Trust Services and Electronic Identification (Dz.U. 2019 r. poz. 162),*
- standards referred to in the Decision of the Executive Committee (EU) 2016/650 of 25 April 2016 establishing standards for assessment of the safety devices for qualified signature and stamp on the basis of art. 30 paragraph 3 and art. 39 paragraph 2 Regulation of the European Parliament and of the Council (EU) No 910/2014 on electronic identification and trust services in relation to electronic transactions in the internal market,
- the services mentioned above in point 1 – 3: the services of issuing qualified certificates for electronic signature and seal, the qualified time-stamping service and the qualified validation service for qualified electronic signatures and qualified electronic seals are provided in accordance with the requirements of *REGULATION (EU) No 910/2014 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*, hereinafter called *the eIDAS Regulation*.

This Certificate Policy and 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 Certification Policy and Certification Practice Statement is particularly important for a **subscriber** and a **relying party**[4].

The applicability ranges of the qualified certificates, electronic timestamps tokens, certificate status tokens, data validation tokens, 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 9.8.

The structure and contents of Certificate Policy and Certification Practice Statement is in accordance with the recommendation of RFC 3647 *Certificate Policy and Certification Practice*

[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 Policy of qualified validation service is described in the separate document: The Validation Policy of Certum's QESValidationQ Qualified Validation Service for qualified electronic signatures and qualified electronic seals

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

Statement Framework. It fulfils also the requirements of the *ETSI EN 319 411-1 norm Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements* and the requirements of the ETSI EN 319 411-2 *Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 2: Requirements for trust service providers issuing EU qualified certificates*...

This document 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).

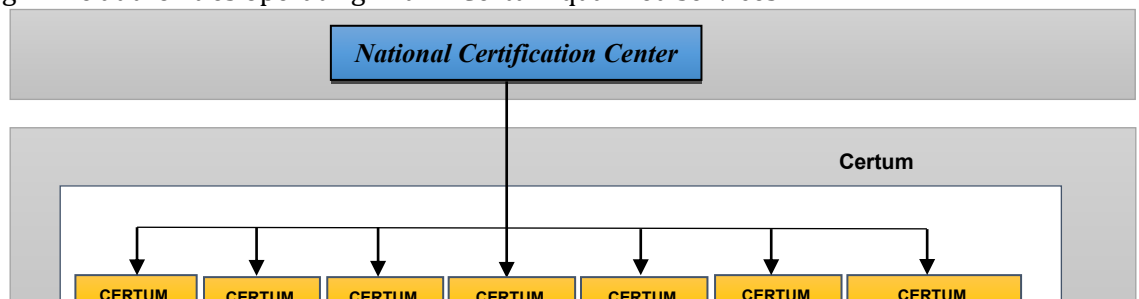
In connection with the transfer of the entire assets of the Unizeto Technologies S.A. company to the Asseco Data Systems S.A. company we declare that Asseco Data Systems S.A. undertakes to maintain the certificate of trust service provider issued to Unizeto Technologies S.A. until the last certificate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

1.1. Overview

Certificate Policy and 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 qualified trust services including: subscriber’s registration, a public key certification and rekey, **certificates revocation** and **suspension,** and issuance of **electronic timestamps tokens**, **certificate status tokens**, **data validation tokens** according to *the Act on Trust Services and Electronic Identification (Dz.U. 2019 r. poz. 162).* The issuance of certificates and tokens is based on trust service providers certificates 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 trust service providers certificates and public key certificates issued by Certum.

The Certum’s qualified certification services are provided within the framework of the separate certification domain with the separate qualified certification authority **CERTUM QCA** and **Certum QCA 2017,** the qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,** the qualified Online Certificate Status Protocol authority **CERTUM QOCSP,** the qualified electronic signatures and qualified electronic seals qualified validation service authority **CERTUM QDVCS** and **Certum QESValidationQ 2017.** These authorities provide services based on the trust service providers certificates issued by the Minister of Digitalisation or an entity authorized by the Minister under the art. 10, item 1 of the *Trust Services and Electronic Identification (Dz. U. 2016 poz. 579)* (Fig.1 issuer of the trust service providers certificates is designated as a **national certification center**).

Fig.1 The authorities operating within Certum qualified services



This document regulates work of the **CERTUM QCA** and **Certum QCA 2017** authority and registration authorities affiliated by the **CERTUM QCA** and **Certum QCA 2017,** the qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,** the qualified online certificate status protocol authority **CERTUM QOCSP,** the qualified electronic signatures and qualified electronic seals qualified validation service authority **CERTUM QDVCS** and **Certum QESValidationQ 2017** and the service recipients – subscribers of qualified certificates, electronic timestamps tokens, certificate status tokens, data validation tokens and all relying parties that use the services or exchange any information with Certum domain.

Certificates and tokens issued by Certum contain the identifiers[5] 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) of every certificate issued by Certum.

Identifiers of certification policies are also placed on tokens issued by the qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,** the qualified online certificate status protocol authority **CERTUM QOCSP,** the qualified electronic signatures and qualified electronic seals qualified validation service authority **CERTUM QDVCS** and **Certum QESValidationQ 2017**.

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 and Certification Practice Statement.

There are many additional documents connected with Certificate Policy and Practice Statement of Certum‘s Qualified Certification Services, which Certum is obliged to use in its activity. They regulate its functioning (see Tab. 1Tab. 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 Certificate Policy and Certification Practice Statement

No.	Document name	Status	Availability
1.	Certification authorities keys life cycle management procedures	Non-public	Locally – only entitled persons and auditor
2.	Personnel book, range of duties and responsibilities	Non-public	Locally – only entitled persons and auditor

[5] 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)

3.	Registration authority book	Non-public	Locally – only entitled persons and auditor
4.	Technical infrastructure book	Non-public	Locally – only entitled persons and auditor
5.	System continuity management system	Non-public	Locally – only entitled persons and auditor
6.	Certum's Security Management v.2.0	Non-public	Locally – only entitled persons and auditor
7.	Certum PKI Disclosure Statement (in a structure according to Annex A ETSI EN 319 411-1)	Public	www.certum.eu
8.	Validation Policy of Certums's QESValidationQ Qualified Validation Service for qualified electronic signatures and qualified electronic seals	Public	www.webnotarius.eu
9.	Terms & Conditions for Certum Qualified Trust Services	Public	www.certum.eu
10.	List of secure devices recommended by Certum, based on art. 31 sec. 2 eIDAS Regulations.	Public	www.certum.eu

Certum is responsible for compliance with the procedures described in this document.

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

1.2. Document Name and its Identification

The present document of Certification Practice Statement is given a proper name of **Certification Policy and Certification Practice Statement of Certum's Qualified Certification Services**; this document is available as an electronic version at: www.certum.eu.

The following registered object identifier is connected with the certification practice statement document (OID: 1.2.616.1.113527.2.4.1.0.1.5.6)[6]:

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(pc)(1) version(5) 6}

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

Certificate Policy and 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 document (described in chapter 7.1 hereinafter). This Certificate Policy and Certification Practice Statement is the main document regulating the provision of qualified trust services by Certum.

[6] The Certificate Policy and Certification Practice Statement Identifier should not be confused with a certification policy identifier (OID) which is provided in a certificate (see **Błąd! Nie można odnaleźć źródła odwołania.**) There is only one Certification Practice Statement Identifier while it could be more than one identifiers of a certification policy.

1.3. Certificate Policy and Certification Practice Statement Parties

Certificate Policy and 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:

- Certum's Certification Authorities,
- Primary Registration Authority (PRA),
- Registration Authorities (RA),
- notaries or persons confirming the identity,
- subscribers,
- relying parties.

Certum provides trust services to all private and legal entities or entities not endowed with legal personality, accepting the regulations of the present document. 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 in its action ensures that none of his clients or relying parties is not directly or indirectly treated less favorably than others, nor subject to restrictions in the exercise of its powers, because of age, color, creed, disability, ethnic origin or national origin, sex, marital status, health, mental health, nationality, physical appearance or political beliefs.

Certum applies specific procedures for the blind and visually impaired persons applying for a qualified electronic signature.

Certum provides the qualified trust services in the range of:

- the issuance of qualified certificates for electronic signature and seal, including:
    - subscribers registration,
    - generating keys and qualified certificates,
    - provides information about the status of certificate based on the Certificate Revocation List,
- revocation and suspension of certificates,
- electronic timestamp,
- online verification of certificate status,
- validation service for qualified electronic signatures and qualified electronic seals.

1.3.1. Trust Services Authorities

Certum as a qualified trust services provider consists of following authorities:

- Qualified certification authority **CERTUM QCA** and **Certum QCA 2017**,
- Qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,**
- Qualified online certificate status protocol authority **CERTUM QOCSP,**
- Qualified electronic signatures and qualified electronic seals qualified validation service authority **CERTUM QDVCS and Certum QESValidationQ 2017.**

1.3.1.1. Qualified Certification Authority CERTUM QCA and Certum QCA 2017

CERTUM QCA and **Certum QCA 2017** (Fig. 1) belongs to Certum which provides qualified certification service and operates on the basis of the entry of the Asseco Data Systems S.A. in the register of qualified trust services providers. The Minister of Digitalization or the entity appointed by the minister (**National Certification Authority NCCert**) supervise over the certification authority **CERTUM QCA** and **Certum QCA 2017** activity.

The authority **CERTUM QCA** and **Certum QCA 2017** issues qualified certificates and certificates of trust service providers according to certification policies (identifiers values are described in **Błąd! Nie można odnaleźć źródła odwołania.** and chapter 7.1).

The authority **Certum QCA 2017** issues qualified certificates and certificates of trust service providers according to certification policies (identifiers values are described in chapter 7) and according to the following requirements:

- *eIDAS Regulation*,
- *Act on the Trust Services and Electronic Identification (Dz.U. 2019 r. poz. 162),*
- the *Regulation of Ministry of Digitalization of 5th October on National Trust Infrastructure (Journal of Law of 2016 item 1632),*
- standards referred to in the Decision of the Executive Committee (EU) 2016/650 of 25 April 2016 establishing standards for assessment of the safety devices for qualified signature and stamp on the basis of art. 30 paragraph 3 and art. 39 paragraph 2 *Regulation of the European Parliament and of the Council (EU) No 910/2014 on electronic identification and trust services in relation to electronic transactions in the internal market*.

*National Certification Authority 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** and **Certum QCA 2017**. A list of qualified service providers, along with information about the provision of trust services is available on the National Certification Center's website at www.nccert.pl (TSL List).*

CERTUM QCA and **Certum QCA 2017** provides trust services to:

- itself (issues and renews self-certificates),
- Minister responsible for informatization or an entity authorized by the Minister which provides certification services,
- natural or legal persons who wish to execute a secure electronic signature using the qualified certificates and electronic seals,
- registration authority operators,
- employees of Certum.

Certum provides, among other services, the services of issuing qualified electronic public key certificates for:

- electronic signature or
- electronic seal.

Qualified certificates are issued by **Certum QCA 2017** in accordance with the NCP+ policy specified in pt. 5.3. of ETSI EN 319 411-1 standards.

Private keys, necessary for using the services mentioned above, may be stored on an electronic card or on a hardware security module (HSM).

In case of a qualified electronic signature certificate, where the subscriber is a natural person, the private key is under his sole control.

In the case of a qualified electronic seal certificate, where the subscriber is a legal person, the private key is under his control.

Private keys on the electronic card are not subjected to deposit operations (see chapter 4.12). When it comes to a hardware security module, the subscriber/entity has exclusive access to the private key that is stored on it when logged into the individual service account.

1.3.1.2. Qualified Electronic Timestamp Authority CERTUM QTSA and Certum QTST 2017

The Certum's Qualified Electronic Timestamp Authority **CERTUM QTSA and Certum QTST 2017**, is a part of Certum infrastructure for qualified services. **CERTUM QTSA** and **Certum QTST 2017** operates on the basis of the entry of the Asseco Data Systems S.A. in the register of qualified trust service providers and based on the certificate evidence issued by the Minister responsible for informatization. The Minister or the entity appointed by the minister (**National Certification Authority NCCert**) supervise over the certification authority **CERTUM QTSA and Certum QTST 2017** activity.

The Certum's Qualified Electronic Timestamp authority **CERTUM QTSA** and **Certum QTST 2017** issues electronic timestamp tokens in accordance with ETSI[7] recommendation. Each electronic timestamp token contains identifier of the policy, under which the token has been issued (identifier value is described in **Błąd! Nie można odnaleźć źródła odwołania.** and chapter 7.3). Electronic Timestamp tokens are signed with a private key issued solely for electronic timestamp service.

The qualified electronic timestamp tokens, issued in accordance with policy described in **Błąd! Nie można odnaleźć źródła odwołania.**, are used primarily for securing long-term electronic signatures[8] and global transactions.

The Certum Qualified Electronic Timestamp Authority applies solutions which guarantee synchronization with international time source (Coordinated Universal Time – UTC) within the accuracy of 1 second.

Time synchronization is based on NTPv4 protocol and consists of continuous synchronization with two labs server in UTC format, that do not provide a service on the global network.

Certum's atomic clocks feature 5-10-12 s. short-term stability, 24-hour stability of ± 22 μs, pulses accuracy of ± 50 ns, and real-time stability in 1-10-12 s with GPS enabled.

Certum QTST 2017 authority provides services in accordance with the requirements of *the eIDAS Regulation*.

Policy of the qualified electronic timestamp authority **Certum QTST 2017** operates in accordance with *ETSI EN 319 411-2*, and indicates a qualified timestamp within the meaning of *the eIDAS Regulation*, the key of this authority is available on the TSL list and indicates a qualified service.

The implemented infrastructure does not allow to issue a timestamp other than a qualified one. Qualified and non-qualified timestamp authorities are separate entities with different

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

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

names and key pairs. Services of these authorities are available from completely separate access points.

1.3.1.3. 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 of qualified trust service providers. Minister of Digitalization or the entity appointed by the minister (**National Certification Authority 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. These confirmations are issued in accordance with the principles set out in this certificate practice statement.

1.3.1.4. Qualified Validation Service for qualified electronic signatures and qualified electronic seals CERTUM QDVCS and Certum QESValidationQ 2017

The Qualified Validation Service for qualified electronic signatures and qualified electronic seals **CERTUM QDVCS and Certum QESValidationQ 2017** issues electronic confirmations (also called qualified validation tokens) to validate a qualified public key certificate, an electronic signature and an electronic seal.

CERTUM QDVCS and **Certum QESValidationQ 2017** operates on the basis of the entry the Asseco Data Systems S.A. in the register of qualified trust services providers. Minister in charge of informatization or the entity appointed by the minister (**National root NCCert**) supervise over the certification authority **CERTUM QDVCS** and **Certum QESValidationQ 2017** activity.

Qualified validation tokens are issued according to the validation policies described in **Błąd! Nie można odnaleźć źródła odwołania.**.

Certum QESValidationQ 2017 authority provides services in accordance with the requirements of *the eIDAS Regulation.*

1.3.2. Primary Registration Authority, Registration authorities and points of the identity verification

CERTUM QCA and **Certum QCA 2017** closely cooperates with Primary Registration Authority, registration authorities and points of the identity verification. Registration authorities and points of identity verification operate on the basis of the authorization by the appropriate certification authorities CERTUM QCA and Certum QCA 2017. The authorization concerns the registration, identification of the identity of subscriber.

Registration authorities receive, verify and approve or reject applications for registration and issuance of a public key certificate and other applications related to the management of certificates (rekey, data 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 identification results from the general requirements described in the Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services (see chapter 3). The scope of duties of registration authorities and points of the identity verification are defined in this document, procedures for registration authorities and the identity confirmation points and Terms & Conditions for Certum Qualified Trust Services.

Identity confirmation points are operated by Certum Partners. The scope of cooperation, rights, duties and obligations are governed by Partner's Authorization Agreements.

Partner agreement imposes obligations on partners and operators to ensure an adequate level of service provision, e.g.:

- each partner is obliged to immediately inform Certum on the cessation of work by the authorized operator and immediately return the Power of Attorney to the address given in paragraph 1.5.2 of this document or to the assigned partner's supervisor,
- partner is obliged to immediately respond to any queries from Certum about operator's current authorizations, queries are sent to partners 2 times a year,
- before obtaining the authority to verify subscribers identity, each operator is obliged to provide declaration of no criminal record, and then confirm it periodically, not later than 12 months after the date of delivery of the previous confirmation,
- before obtaining the authority to verify subscribers identity, each operator is obliged to pass the training and exam related to trust services, identity verification, identity documents and other documents required in the document authentication process and repeat it periodically once a year, no later than 12 months after finishing the previous exam.

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

http://www.certum.eu

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[9] of certificates or certificates of trust services providers. Therefore:

- **RAs** register subscribers that request for qualified certificates; in addition, they provide comprehensive information on digital signatures, including the effects of using it, provide information on the types of attributes, accept the terms of provision of trust services and may sell the certificates and secure devices,
- **PRA** registers registration authorities (RA), notaries and points of the identity 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 Certum is prepared to handle notary's confirmation of the identity 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 and data necessary for the issuance of a public key certificate. Notarized documents with previously accepted terms of provision of trust services

[9] Types of certificates are described in Charter 1.4

are the set of documents and data identifying entity on the basis of which a registry inspector verifies the identity of a subscriber and she/he make a certificate application notification.

Person who verifies the identity of the applicant on behalf of Certum should be authorized to accept the certificate applications and the terms of provision of trust services. The acceptance of the application must be authenticated by this person.

1.3.3. Subscribers

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.

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

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

1.3.4. Relying Parties

Relying party is an entity who uses other subject's qualified certificate for electronic signature or seal in order to verify other party's electronic signature or to secure the confidentiality of information that is being sent.

A relying party, using Certum services can be any entity who accept the qualified electronic signature or electronic seal or other certified electronic confirmation, 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 authority **CERTUM QCA** and **Certum QCA 2017**), or
- connection between electronic signature or electronic seal and electronic timestamp token issued by qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017**, or
- confirmation of validity of certificate issued by qualified data validation and certification server authority **CERTUM QOCSP**, or
- validation token issued by qualified validation service **CERTUM QDVCS** and **Certum QESValidationQ 2017**.

A relying party is responsible for verification of the current status of a subscriber's certificate (including 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 (e.g. identifiers and qualifiers of certification policy) to state whether a given certificate was used in accordance with its declared purpose.

Tab. 2 Users of the Certum qualified certificates, Certum TSP certificates and tokens issued by Certum

Certificate / Certificates of trust service providers / token name	Users
Qualified certificates	A person who signs (a subscriber) and verifies (a relying party) an electronic

	signature or electronic seal.
Certificates of trust service providers	Relying parties who verify an electronic signature or electronic seal.
Electronic Timestamp tokens	Relying parties signing and verifying an electronic signature or electronic seal.
QOCSP tokens	Relying parties verifying status of qualified certificate and used in verifying the validity of electronic signatures equivalent or electronic seal.
Validation tokens	Relying parties signing and verifying an electronic signature and electronic seal.

1.3.5. Other Parties

Independent bodies assessing compliance with the eIDAS Regulation.

Supervisory Body - The Minister of Digitalization or the entity appointed by the minister (National Certification Authority NCCert).

1.4. Certificate and certificate of trust service provider usage

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

Qualified certificates for electronic signature issued by CERTUM QCA and Certum QCA 2017 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.

Qualified electronic seal certificates issued by CERTUM QCA and Certum QCA 2017 may be used only to verify qualified seals which guarantee origin authenticity and integrity of associated data.

Certum does not issue qualified electronic signature certificates and electronic stamps for testing purposes.

Information sensitivity level and information vulnerability to **breach**[10] should be evaluated by a subscriber. Based on this estimate, the subscriber should decide on the desired range of certificate usage (see Tab.10).

The requirements set out by the relying party must be confronted by the subscriber with applicability range (see Tab. 7) and types of certificates (see Tab. 8, Tab. 9 and Tab. 10) issued by CERTUM QCA and Certum QCA 2017.

[10] See **Glossary**

Tab. 3 The applicability ranges of certificates and TSP certificates issued by CERTUM QCA and Certum QCA 2017

Certification policy	Name of certificate type	Description and recommended applicability
CERTUM QCA QC and **Certum QCA 2017 QC**	Qualified electronic sign 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 of qualified electronic signatures. These certificates can be used to authenticate and control the integrity (and authenticity) 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. Qualified certificates cannot be used encrypt data or keys encrypted (in general, in operations in which confidentiality information is generated).
CERTUM QCA QS and **Certum QCA 2017 QS**	Qualified electronic seal certificates	Very high level of the identity of electronic seals certificate. They are issued only to legal persons and organizational units without legal personality. Certificates should be used to submit a qualified electronic seal ensuring that the integrity and authenticity of signed information. Qualified electronic seals certificates are not used to express the will of the entity that uses it.
CERTUM QCA CertEvidences and **Certum QCA 2017 CertEvidences**	Trust service provider certificates	Very high trust level of the identity of a certificate entity. TSP certificates are issued to: (a) The National root NCCert acting under the authority and on behalf of the Minister in charge of informatization, (b) for **CERTUM QCA** and **Certum QCA 2017** keys exchange.

1.4.1. Types of certificates and trust services provider certificates and recommended areas of application

1.4.1.1. Qualified certificates

Certum issues **three basic types of certificates of electronic signatures and electronic seals** (see Tab. 8). Qualified certificates from this list are issued to the subscribers who accepted the terms of provision of trust services by Asseco Data Systems S.A. and the rules of this Certificate Policy and Certification Practice Statement.

Every qualified certificate issued by the **CERTUM QCA** and **Certum QCA 2017** 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 (see chapter 7.1.3.1) and the

second is contained in **QCStatements** extension (see chapter 7.1.3.1). 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 trust services. These indicators may occur together, though the presence of QCStatements extension shall be mandatory.

Tab. 4 Types of qualified certificates and their applicability

Certification policy	Commercial name of certificate type	Description and recommended applicability
CERTUM QCA QC and **Certum QCA 2017 QC**	CERTUM QCA and Certum QCA 2017 Personal (universal)	Qualified electronic signatures of electronic data; certificate contains at least: name of country, name of subscriber and serial number of certificate.
	CERTUM QCA and Certum QCA 2017 Professional (with additional data)	Qualified 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 subject, name of entity and serial number of certificate.
CERTUM QCA QS and **Certum QCA 2017 QS**	Certum QCA 2017 Electronic Seal	Qualified electronic seal certificate can be submitted by legal persons and entities without legal personality. Certified electronic seal includes at least: the name of the country, the name of the legal entity and its registration number, common name and serial number.

1.4.1.2. Trust service providers certificate

TSP certificates are issued by:

- the Minister in charge of informatization or the entity providing qualified certification services under the authority and on behalf of the Minister in charge of informatization,
- **CERTUM QCA** and **Certum QCA 2017** (applicable to keys exchange).

Tab. 5 Types of TSP certificates and their applicability

Certification policy	Commercial name of certificate evidences	Description and recommended applicability
CERTUM QCA CertEvidences and **Certum QCA 2017 CertEvidences**	CERTUM QCA and Certum QCA 2017 Cross-Cert	TSP certificates are issued to the Minister in charge of informatization or to the entity providing certification services under the authority, and on behalf of the Minister in charge of economy.
	CERTUM QCA and Certum QCA 2017 Internal	TSP certificates are issued for the purposes of keys of CERTUM QCA and Certum QCA 2017 exchanging.

1.4.1.3. Electronic timestamps

Electronic Timestamp authority **CERTUM QTSA and Certum QTST 2017** issues electronic timestamp tokens which, in terms of the Civil Code (art. 81*§2 pkt.3)*, produce legal consequences of a certified date. The primary use of electronic timestamps is to mark long-term electronic qualified signatures with reliable time. Electronic timestamp issued by the **CERTUM QTSA and Certum QTST 2017** may also be used in any other cases that require a comparable electronic timestamp service. Time-stamping authority **Certum QTST 2017** issues electronic timestamp tokens in accordance with the *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing electronic timestamps.*

Electronic timestamp service is available to public, however time-stamping authority **CERTUM QTSA and Certum QTST 2017** verifies authenticity of the each request and rejects it when the format of the request is not correct.

1.4.1.4. OCSP Response Tokens Applicability Range

Online certificate status protocol authority **CERTUM QOCSP** issues status tokens of qualified certificates and TSP certificates (issued by qualified certification authorities with accordance to *the eIDAS Regulation*). These tokens are issued after checking if a certificate or a certificate of trust service provider is on revocation list.

1.4.1.5. Data Validation Applicability Range

Qualified Validation Service for qualified electronic signatures and qualified electronic seals. **CERTUM QDVCS and Certum QESValidationQ 2017** issues qualified validation tokens only to validate qualified public key certificate, electronic signature and electronic seal.

Data validation tokens should be collected by entities in order to resolve any disputes, that may arise from discrepancies in the assessment of the validity of qualified signatures or other electronic evidence by various parties.

1.4.2. Prohibited Certificate Uses

It is forbidden to use Certum certificates contrary to their declared purpose referred in this document and in devices that do not meet the requirements of chapter 1.4.1.

1.5. Certificate Policy and Certification Practice Statement Administration

Every version of Certificate Policy and Certification Practice Statement is in force (has a **valid** status) up to the moment of publication and approval of its new version (see chapter 9.10). A new version is developed by Certum personnel and with the status **under review** supplied to approval questionnaire. Upon reception and inclusion of the remarks from the approval questionnaire, the new version of document is supplied for approval to the Certum manager and published. During approval process, the new version of document has the status **under review**. After completion of the approval procedure, the new version of Certificate Policy and Certification Practice Statement is marked with the status **valid**.

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

Decision on acceptance of the changes in Certificate Policy and Certificate Practice Statement version or build number is made by the Certum manager.

Further administration rules for this document are presented in chapter 9.10.

1.5.1. Organization responsible for administrating the document

Asseco Data Systems S.A.

PL 81-321 Gdynia, Podolska Street 21

National Court Register no: 0000421310 District Court in Gdańsk-North in Gdańsk

1.5.2. Contact

Asseco Data Systems S.A.

Certum

PL 71-838 Szczecin, Bajeczna Street 13

E-mail: infolinia@certum.pl

Phone: +48 91 4801 340

1.5.3. Entities determining the validity of the principles contained in the document

The Certum team is responsible for evaluating the timeliness and usefulness of Certificate Policy and Certification Practice Statement and other documents concerning PKI services, provided by Certum, as well as the compatibility between these documents. All inquiries and comments concerning the contents of these documents should be directed to the address in chapter 1.5.2.

1.5.4. Approval Procedures

This Certificate Policy and Certification Practice Statement is in effect from the date indicating the beginning of its validity until the publication of the next valid version.

Comments on suggested modifications may be submitted by the affected parties within 7 working days of their announcement (as presented in chapter 9.12). After this deadline, if there are no significant reservations to the substantive content of the proposed changes, the new version of the Policy becomes valid with the validity date indicated in it.

Decision to approve the new version of Certificate Policy and Certification Practice Statement is taken by Certum manager. All changes made in the document are recorded in **the history of the document**.

1.6. Definitions and abbreviations

Definitions and abbreviations used in this document are at the end of it.

2. Publication and Repository

2.1. Repository

Repository is a collection of publicly available directories containing:

- trust service provider certificates i.e. Certum CA certificate,
- other (see chapter 2.2).

2.2. Information Published by Certum

The www.certum.eu website and the repository are available 24/7 to all customers and relying party. Both services are running simultaneously at the main site and at the alternate one. In case of disruption said services are shifted to another site. Moreover, each site has a static version of content ready to run in case of local disruption of the CMS services.

The information consists of:

- Certification Policy and Certification Practice Statement of Certum‘s Qualified Certification Services,
- Terms & Conditions for Certum Qualified Trust Services,
- Information about Certum public key infrastructure – document is available in PDF/A format, corresponding with ISO 19005, parts 1 to 3,
- templates of agreements with subscribers,
- trust services providers certificates of qualified certification authority **CERTUM QCA** and **Certum QCA 2017,** qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,** qualified online certificate status protocol authority **CERTUM QOCSP,** qualified validation service **CERTUM QDVCS** and **Certum QESValidationQ 2017**,
- the list of qualified secure devices recommended by Certum, based on Art. 31 pt. 2 of *the eIDAS Regulation,*
- the lists of authorized registration authorities or persons confirming identity,
- 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** and **Certum QCA 2017**; the basic point of CRLs distribution are respectively: http://crl.certum.pl and http://qca.crl.certum.pl/qca_2017.crl,
- supplementary information, e.g. announcements and notifications.

There is a possibility of adjusting the contrast ratio between the text and the background on Certum’s website, with minimal ratio of 4.5: 1, with some exceptions.

User also has the option to resize the text, which does not affect the functionality and readability of the web page. Text can be increased by 1 point until it is twice the size of the original font size.

Described facilities have been implemented in accordance with WCAG 2.0 „Web Content Accessibility Guidelines (WCAG) 2.0” (ISO/IEC 40500:2012), developed by W3C organization, which sets standards for website designing. These guidelines are recommended by ETSI EN 301 549 norm.

2.3. Frequency of Publication

Certum publications below are issued with the following frequency:

- Certificate Policy and Certification Practice Statement of Certum‘s Qualified Certification Services and Terms & Conditions for Certum Qualified Trust Services - see chapter 9.12,
- trust services providers certificates of all authorities providing trust services functioning within Certum – upon every issuance of new certificates,
- Certificate revocation and suspension lists - see chapters 4.9.4 and 4.9.7,
- supplementary information – upon every updating of it.

2.4. Access to Publications

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

3. Identification and Authentication

This chapter presents general rules of subscribers' identity verification applied by Certum to certificate issuance.

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

Certum and subordinate registration authorities confirm the identity and other attributes of the natural person or legal entity applying for qualified certificate with a valid identity card or passport or entry in the Business Activity Register or using another method, in accordance with the provisions of the art. 24[11] of *the eIDAS Regulation*.

3.1. Naming

3.1.1. Types of Names

Certificates issued by Certum comply with the norm X.509 v3. In particular, it means that a certificate issuer or trust service provider 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. 6 Requirements imposed on the name of a certificate subject or trust service provider certificate

Certificates	Requirements
Qualified certificate	Subject's DN in accordance with X.500 and ETSI EN 319 412 and optionally the alternative name in the case when it is marked as non-critical.
Trust Service Provider Certificate	Non-empty value of the field **subject** in accordance with X.500 and ETSI EN 319 412.

3.1.2. 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 or trust service providers certificate and have their meaning in Polish or English language.

[11] eIDAS allows the trust service provider to use various methods to confirm the identity of a natural person and the veracity of other relevant data related to the issue and management of a certificate, while providing assurance equivalent to the person's physical presence at the Registration Point.

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

DN name may consist of the following fields (descriptions of a field follows its abbreviated name that complies with the recommendation X.501) DN profile is compliant with ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI) Certificate Profiles; Part 1 – 5:

- **field C** – international abbreviation of the country name (**PL** for Poland),
- **field S** – the region/province where the subscriber lives or runs his/her business,
- **field L** – the city where the subscriber lives or operates,
- **field PostalCode** - postal code of registered office or place of residence of subscriber,
- **STREET field** - street, house number (and possibly apartment number) of registered office or place of residence of subscriber,
- **field SN** – the surname of subscriber (plus possibly maiden or married name),
- **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 serialNumber** and **organizationIdentifier** – a sequence which may include several sequences (separated by spaces), consisting of a 3-character prefix indicating the type of identifier, 2-character country code[12], dash and unique identifier:
    - **field serialNumber** applies for natural persons and may consists prefixes according to paragraph 5.1.3 of ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1: Overview and common data structures;
    - **field organizationIdentifier** applies for legal entities and may consists prefixes according to paragraph 5.1.4 of ETSI EN 319 412-1 Electronic Signatures and Infrastructures (ESI); Certificate Profiles, Part 1: Overview and common data structures.

Qualified certificates for electronic signature are issued to natural persons acting on their own behalf or on behalf of another entity. Qualified certificates for electronic seal are issued for legal entities. They can be issued in various categories:

- **Category I –** electronic signature certificate contains at least the following attributes: name of country, surname and given name, common name and serial number; this category applies to personal qualified signature certificates (universal),
- **Category II –** contains all information of category I and additional data indicating organizationName and organizationIdentifier when a natural person subject is associated with an organization; this category applies to personal qualified signature certificates with additional data indicating link between natural person and represented organization (professional),

[12] Country code according to the international standard ISO 3166, e.g. PL

- **Category III** – contains at least the following attributes: name of country, name (names) of legal entity and organizationIdentifier; this category applies to qualified electronic seals certificates.

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.*

3.1.3. Subscribers anonymity

Qualified certification authority **CERTUM QCA** and **Certum QCA 2017** does not issue qualified certificates containing pseudonyms.

3.1.4. Rules for Interpreting Various Names Forms

The interpretation of the fields provided in certificates or trust service providers certificates issued by Certum is in compliance with certificates profile described in *ETSI EN 319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5*. Within creation and interpretation of DN names the recommendations of chapter 3.1.2 apply.

3.1.5. Names Uniqueness

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

Subscriber's DN is suggested by the subscriber. If the name is in accordance with general requirements stated in chapter 3.1.1 and 3.1.2 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 4.4 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** and **Certum QCA 2017** directories and services rendered within them have a guaranteed service continuance, without any risk of service disruption or substitution.

3.1.6. Recognition, Authentication and Role of Trademarks

Certum does not include trademarks in certificates. At the same time it is prohibited to use the names that are not owned by the subscriber.

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.

3.2. Initial Registration

Subscriber's registration takes place when a subscriber applying for qualified certificate of electronic signature or electronic seal is registered for the first time in **CERTUM QCA** and **Certum QCA 2017**.

The registration comprises a number of procedures which allow a certification authority – prior to issuing a certificate for qualified electronic signature or seal to a subscriber – to gather authenticated data concerning a given entity or identifying this entity. Confirmation of these data requires contact with a registration authority, a notary or other authorized person confirming identity (in accordance with art. 24.1 of *eIDAS Regulation*). In addition to the Distinguished Name (see chapter 3.1.2), the subscriber is required to provide in the registration form the following information, which will enable the unambiguous identification of the subscriber, including:

- citizenship,
- the ID card or passport number and date of expiry,
- place and date of birth,
- contact details.

Each subscriber is subjected to a registration process only once. After filling the electronic form, verification of data supplied by a subscriber and accepting the terms of provision of trust services a subscriber is included on the list of authorized users of Certum services and supplied with a public key certificate.

Before accepting the terms of provision of trust services by Asseco Data Systems S.A., each subscriber is obligated to familiarize himself/herself/itself with Terms & Conditions for Certum Qualified Trust Services and the terms of the services provided set out in this document.

Registration may takes place only on individual request of subscriber (including requesters). Registration can be performed via website or in the registration point.

Every subscriber, including Asseco Data Systems S.A. employees, requesting public key infrastructure services and applying for certificate or trust services provider 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,
- indicate type of an certificate.

The detailed scope of the powers to act on behalf of someone else should define the power of attorney or other document authorizing to act on someone else's behalf.

Issuing certificates for Asseco Data Systems S.A. employees Certum applies the same registration procedures, identity verification and certification as for all other subscribers.

Applicant, during registration process is informed, in a clear and generally understandable form, in writing or in the form of an electronic document, about:

- conditions of use of qualified services,
- liabilities of the subscriber,

- information for relying parties,
- information about the data backup,
- the scope and limitations of liability of Asseco Data Systems S.A.,
- the scope and limitations of providing qualified services,
- compatibility of services with *the eIDAS Regulation* and *the Act*,
- complaints and disputes settlement,
- method of auditing qualified services,
- Certum contact information,
- availability of services,
- revocation procedure for qualified certificates.

All issues listed above are contained in the Terms & Conditions for Qualified Trust Services document which is available at www.certum.pl.

The subscriber is obliged to confirm his/her/its familiarization with the rules described above by accepting the terms of provision of trust services.

Certum guarantees documents in Polish and English language of information listed above which cover an area of interest in the language of our customers. The documents are downloadable in PDF format through the repository of Certum.

The acceptance of the terms of provision of trust services 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 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.

If the subscriber is presenting a power of attorney, the entity providing it is also required to sign contained in power of attorney additional components constituting the second part of the consent for the provision of qualified trust services, comprising the following in accordance with section 6.3.4 e) ETSI EN 319 411-1:

- consent to the terms of provision of trust services ,
- a statement of reviewing the terms of service contained in Terms & Conditions for Qualified Trust Services,

- agreed to store the registration data used in the registration process for a period required by *the Act.*

3.2.1. 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.

3.2.2. 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 subscriber's authorizations always in situation, when a subscriber submits the certification request for:

- Qualified signature certificate issue, containing an indication of whether subscriber acts on behalf of another entity, whose data are included in the application
- Electronic seal issue.

Authentication is a part of procedures of processing of customers' requests for the issuance of the qualified electronic signature certificate to the individual person representing another person (natural or legal) or electronic seal. 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.

3.2.3. 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.

If the subscriber is a natural person (an employee of the organization or its representative) for whom a category II and category III certificate is issued, the verification may be carried out additionally on the basis of:

- appropriate authorization issued by the organization to represent its interests and to include the organization's details in the certificate,
- recent extract from the National Court Register or Central Records and Information on Business Activity.

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 (except notary) accepts on behalf of Asseco Data Systems S.A. the terms of provision of trust services. After completing the registration process of the applicant, the operator of the registration authority is obliged to send documents, if they are in paper form, to Certum's Prime Registration Authority at Bajeczna Street 13 in Szczecin not later than on the next business day. Documents shall be sent via the registered mail of the Polish Post or courier company. In the case of electronic documents prepared in the Certum IT system, no separate shipment is required.

In the case of notary's verification, applicant unilaterally accepts the terms of provision of trust services, which after the transfer to Asseco Data Systems S.A. are accepted by the registration authority operator and sent back to the address specified by the applicant.

3.2.3.1. Identity verification by an authorized representative of Certum

Confirmation of the subscriber's identity is based on a valid identity card or passport via the Registration Point or Identity Confirmation Point. Confirmation of the subscriber's identity can be done in three ways:

- through personal appearance at a Registration Point or Identity Confirmation Point,
- by a visit of an authorized Certum representative to the location where the subscriber is currently staying,
- remotely, through secure electronic communication means, ensuring constant voice and visual contact of the person confirming identity with the subscriber.

In the case of a remote verification process, the subscriber's identity is confirmed by two additional independent methods implemented during the ongoing process:

- authentication of the applicant in an external reliable electronic identification system using electronic identification means issued in that system, i.e. by making a bank verification transfer via the Blue Media service,
- independent video verification path provided by the AriadNEXT service, which additionally serves to check the originality of the presented identity document and to compare the image of a person with a photo that is contained the presented document.

The information obtained through verification using an electronic identification means and an independent video channel is an attachment to the certificate application and is registered and archived in accordance with Chapter 5.5.2.

In the case of running an identity confirmation point by a partner, which is an entity from the financial sector obliged under the provisions of Directive 2005/60 / EC (AML) and applies a sufficiently high level of credibility of verification of identity of natural persons, the operator of this point may use the means of identity verification used by that entity. At the same time, the whole process must be thoroughly described in the procedure and approved by Certum.

3.2.3.2. Identity verification by a notary public

Certum accepts certificate applications signed by the subscriber in the presence of a notary public who confirms this fact.

3.2.3.3. Identity verification based on a qualified electronic signature

In a special cases, when a person applying for a qualified certificate has a valid qualified certificate, their identity is confirmed on the basis of a certification application bearing the qualified signature of that person.

3.2.4. Non-Verified Subscriber Information

Certum verifies all information contained in the subject name (DN) of certificate.

3.2.5. Validation of Authority

In case the certification application contains the name of the organization, it should be seen as an entitlement of that person to act on behalf of the organization. This also means that the Certum verifies whether a natural person who has applied for certification was at the time of issuance of the certificate the employee organization or its associate and has the right to act on behalf of the organization; entitlements and period of validity may be regulated by separate laws, data of the individual and rights of Certum to check in available records or databases.

3.2.6. Interoperability criteria

Not applicable.

3.3. Subscriber's Identity Authentication for Certificate Rekey or Certificate Data Modification requests

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

- subscriber represents other entity 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,
- applicant makes a request for an electronic seal, and obtained electronic seal exceeds period of validity of previously submitted attorney entitlement to apply for electronic seal on behalf of represented entity,
- 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** and **Certum QCA 2017**,
- when it concerns key certification resulting in a certificate issued for the first time to a given subscriber according to a new certification policy.

3.3.1. Identification and authentication in a standard rekey

3.3.1.1. 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. Certum checks if the applied cryptographic security will be sufficient for the new certificate period to ensure that the key has not been compromised or has been revoked as a result of a security breach. 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 4.7).

Identity validation of the subscriber requesting certificate rekey is carried out on the basis of qualified signature that was used to sign certificate rekey request.

Key certification – unlike rekey – is not associated with any valid certificate and concerns issuing any type of certificate (subscriber must be registered, i.e. possess 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 accepted terms of provision of trust services 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 3.2).

3.3.1.2. Certificate Data Modification

Certificate data 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.

Certum does not offer a certificate modification.

Modification might be necessary e.g. in the case of changing the position at work or the e-mail address, 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 4.8).

After new certificate issuance, Certum revokes the certificate whose data has become outdated - i.e. the certificate based on which the modification procedure was carried out.

3.3.2. Authentication for issuing a certificate after revocation

A Certification requests following certificate revocation are verified in the same way as applications made for the first issue of the certificate.

3.3.3. Registration of other Certum services users

Registration of users of services provided by the electronic timestamp authority CERTUM QTSA and Certum QTST 2017, online certificate status protocol authority CERTUM QOCSP, qualified validation service CERTUM QDVCS and Certum QESValidationQ 2017 is carried out on the basis of the acceptance by the subscriber and Asseco Data Systems S.A. of the terms of provision of trust services . The subscriber's identity may be 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 possess 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 3.2 in the case of the subscriber who doesn't possess a qualified certificate or the certificate is expired or revoked.

Registration may be connected with the registration of the subscriber of CERTUM QCA and Certum QCA 2017 services. Registration of users of the qualified electronic timestamp service CERTUM QTSA and Certum QTST 2017, QOCSP service and qualified validation service CERTUM QDVCS and Certum QESValidationQ 2017 is optional.

3.4. Subscriber's Identity Authentication for Certificate Revocation

Revocation requests can be submitted by mail, phone, fax or directly to a Registration Authority.

In case of revocation by mail, telephone or fax, the subscriber submits revocation application directly to the Prime Registration Authority. By calling the phone number indicated in the revocation order, the registration inspector verifies the data contained in the application. In case of inconsistency of the verified data, the certificate is suspended until the inconsistencies are clarified.

In case of submitting revocation application trough the Registration Point, the operator will identify and authenticate the subscriber. The identification and authentication process is identical to that of the initial registration (see chapter 3.2). Then revocation application and identity authentication is sent by the operator to the Prime Registration Authority, where the registration inspector revokes the certificate based on received documents.

Detailed procedure of revocation is disclosed in chapter 4.9.3.

4. Certificate Life-Cycle Operational Requirements

Trust services procedures are presented below. Every procedure starts with a subscriber's submitting a suitable application to a registration authority, electronic timestamp authority, certificate status verification authority and data validation 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.

4.1. Application Submission

4.1.1. Who can apply for certificate

Any entity belonging to one of the following categories may submit an application for a certificate:

- a natural person who is or will be the subject of a certificate,
- authorized representative of a legal person or institution without legal personality,
- authorized representative of Certum.

Certum does not issue certificates to entities carrying out business activities in countries with which Polish law forbids doing business.

4.1.2. Application process and related responsibilities

4.1.2.1. Certification Application

Application for certification can be submitted by an applicant personally in Registration Point, Partner Identity Confirmation Point or via electronic form (in that case identity validation has to be carried out by a notary public or any other person authorized to confirm subscriber's identity).

4.1.2.2. Certificate rekey or certificate data modification application

An application for rekey or data modification is submitted by a subscriber only in electronic form.

4.1.2.3. Certificate revocation or suspension application

An application for certificate revocation can be submitted only by authorized persons (see chapter 4.9.2 and 4.9.14):

- personally in Registration Point,
- by phone call,
- by fax
- by registered mail.

Applications must be confirmed by registration inspector.

Application form is published at www.certum.eu.

Subscriber and authorized entity, whose data is included in the certification application are notified about certificate revocation or suspension.

4.2. Applications processing

Upon authentication of the identity of the subscriber by a registration authority operator, a notary or other person who confirm subscriber's identity (see chapters 3.2.3 and 3.2.2), an application is submitted to the Primary Registration Authority where a **certification request token** is prepared and submitted to the certification authority.

4.2.1. Identification and authentication function

Identification and authentication functions of all required subscriber data are carried out by Primary Registration Authority, cooperating Registration Points and Identity Confirmation Points in accordance with the conditions set out in 1.3.2.

4.2.2. Acceptance or rejection of application

4.2.2.1. Application processing

Registration Point or Identity Confirmation Point accepts and verifies the certificate application and, together with the required set of documents, passes it to the Primary Registration Point.

In the case of electronic processing of rekey application the registration inspector or person who confirm subscriber's identity shall confirm, according to this document and Certum internal requirements, the subscriber's identity.

4.2.2.2. Rejection 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**,
- validity date of the applicant's identity document, whose data (number and series number) included in the certificate is shorter than the certificate's validity date,
- if there is suspicion or certainty that the subscriber falsified the data or stated false data,
- if the applicant fails to deliver the required set of formal documents, constituting as an attachment to the application,
- in case of detection of hand-written corrections or modifications in submitted formal documents,
- if the validity date of submitted documents is exceeded - the documents whose date of signature exceeds 3 months in the moment of its reception in Certum (in electronic or paper form),
- if the validity date of certificate application is exceeded - the applications whose filling date exceeds 3 months in the moment of its reception in Certum (in electronic or paper form),
- from other reasons not specified above, upon prior notice of **security inspector**.

If the required set of formal documents is not provided, the required set of documents of the entity (in case of certificates with the entity's data) Certum reserves the right to send them back within 3 months from the date of receipt.

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.

4.2.3. Certificate Issuance Awaiting

Certum makes every efforts to ensure that on receiving application for registration and certification, rekey or certificate data modification, the authority examines the application and issues a certificate as soon as possible.

If the reasons for which there may be possible delays in issuing the certificate lie solely with Certum, this time should not exceed 7 days from the moment of accepting the terms of provisioning trust services between Asseco Data Systems S.A. and the subscriber.

4.3. Certificates Issuance

4.3.1. Authority activities during certificate issuance

On receiving an appropriate certification request token and processing it (see chapter 4.2), a certification authority **issues a certificate**.

Date of issuance is recorded in the event log 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. Authority provides subscriber form to download the certificate. Credentials allowing to use the form are sent to the subscriber separately.

4.3.2. Subscriber notification of certificate issuance

Subscriber and authorized entity, whose data is included in the certificate application are informed about certificate issuance.

Certum Certification Authority have mechanism to inform subscriber about certificate issuance via e-mail, it involves sending information that will allow subscriber to download a certificate. Authorized entity, whose data is included in the certificate application receive information about certificate issuance, sent to a given e-mail address.

To download a certificate, the subscriber has to fill in a special form with 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 issue the authentication code (PIN). In case of a remote signature or seal service, the subscriber himself/herself issues both the PUK code and the PIN.

A certificate can be installed on the cryptographic card automatically – via dedicated JAVA application or can be downloaded and installed using the Certum’s proCertum CardManager software.

4.4. Certificate Acceptance

4.4.1. Confirmation of 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. In its place, based on the required new set of documents, a new one will be issued.

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 the terms of provision of trust services by Asseco Data Systems S.A.

Lack of certificate acceptance for reasons other than resignation from services means need to revocation of the certificate and to issue a new certificate on the basis of the new certificate request and new acceptance of the terms of provision of trust services.

4.4.2. Certificate publication

Not applicable .

4.4.3. Informing other entities about certificate issuance

Certum may inform Registration Authority, authentication points, which confirmed data contained in the subscriber's application. Information regarding certificate issuance can be send also to authorized entity, whose data is included in the certificate application.

4.5. Certificate and Key Usage

4.5.1. Subscribers certificates and keys usage

Subscribers are required to use private key and certificates:

- in accordance with their purpose stated in the present Certificate Policy and Certification Practice Statement and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage** see chapter 7.1),
- in accordance with the content of accepted by subscriber terms of provision of trust services by Asseco Data Systems S.A.,
- only within the validity period,
- until the certificate revocation; when the certificate is suspended, the subscriber should not use the private key, particularly for creating a signature.

4.5.2. Relying parties certificates and keys usage

Relying parties must use public keys and certificates:

- in accordance with their purpose stated in the present Certificate Policy and Certification Practice Statement and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage** see chapter 7.1),
- only upon their status verification,
- 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.

4.6. Recertification

Certum does not provide recertification services for qualified electronic signature certificates, electronic stamps and trust service provider certificates.

4.6.1. Circumstances for certificate renewal

Not applicable.

4.6.2. Who can apply for certificate recertification?

Not applicable.

4.6.3. Processing recertification application

Not applicable.

4.6.4. Informing subscriber about certificate issuance

Not applicable.

4.6.5. Acceptance of a renewal certificate

Not applicable.

4.6.6. Publication of the renewal certificate

Not applicable.

4.6.7. Informing other entities about certificate issuance

Not applicable.

4.7. 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, (however, the subscriber should be registered in the system, i.e. have at least one certificate – even if it has been revoked or it expired),
- **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.

4.7.1. Circumstance for 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 the currently valid certificate.

In both cases applications contain the request for generating 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.

4.7.2. Who can apply for a new public key?

Certification or rekey is performed only on subscriber's demand and must be preceded by the submission of the application.

4.7.3. Processing an application for certification and rekey

Rekey request supplied by a subscriber can apply only:

- to a currently valid certificate,
- when the subscriber has a private key associated with the certificate.

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 or seal 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 3.3.

Certification and rekey procedure can be also applicable for trust service providers certificates. 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.

4.7.4. Informing subscriber about new certificate issuance

Subscriber and authorized entity, whose data is included in the certificate application is informed about issuance of certificate.

4.7.5. Acceptance of new certificate

See chapter 4.4.1.

4.7.6. Publishing new certificate

See chapter 4.4.2.

4.7.7. Informing other entities about certificate issuance

See chapter 4.4.3.

4.8. Certificate data modification

Data modification means replacing the currently used (**currently valid**) certificate with a new certificate, in which – with relation to the replaced certificate – some information included in it, including the public key, may be changed.

Certum does not offer a certificate modification.

The process of data modification in a certificate means that a new certificate has been created based on a certificate that is currently in the subscriber's possession, has not been revoked and has not expired. New certificate has a new public key, a new serial number, and differs in at least one of the other certificate fields. Certification policy identifier, according to which the certificate was issued, can't be modified.

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

4.8.1. Circumstance for certificate data modification

Modification can be applicable only for values and extensions of particular types of certificates. Certificate content can be modified only within the structure contained in the issued certificate and specified in a profile of this certificate (see chapter 7).

Certificate data modification:

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

The need for certificate data modification may occur, for example, if there is a change of job position or change of email address, provided that the data was previously included in the certificate or should be added.

Following data can be modified:

- the name of position at work or the name of performing role (authorization, confirmation of job position required),
- postal address, e-mail address and telephone number,
- name or address of represented entity (appropriate documents required),
- other changes of certificate's extensions.

4.8.2. Who can apply for a certificate data modification

Certificate data modification is performed only on subscriber's demand and must be preceded by the submission of the application.

4.8.3. Processing Certificate Data Modification Requests

Procedure of processing application for certificate data modification is the same as application for new certificate and requires verification of all information in accordance with chapter 3.2.

4.8.4. Informing subscriber about certificate data modification

Subscriber and the entity represented by the subscriber is informed about issuance of the new certificate.

4.8.5. Acceptance of modified data certificate

See chapter 4.4.1.

4.8.6. Publishing modified data certificate

See chapter 4.4.2.

4.8.7. Informing other entities about certificate issuance

See chapter 4.4.3.

4.9. Certificate revocation and suspension

Certum provides a 24/7 capability to submit revocation request.

Requirements for revocation and suspension of certificates or trust service providers certificate are specified in *the eIDAS Regulation*, *the Act and Regulation on National Trust Infrastructure of 5th October 2016*. In the case of the revocation of the **National Root (NCCert)** certificate, the certificates and tokens issued by **CERTUM QCA** and **Certum QCA 2017, CERTUM QTSA** and **Certum QTST 2017, CERTUM QOCSP**, **CERTUM QDVCS** and **Certum QESValidationQ 2017**, do not lose the validity if it is proved that these certificates or tokens had been issued before the National Root certificate revocation.

Requirements mentioned above are particularly essential for long term electronic signatures and seals which are verified after expiration of the certificate associated with this signature. Such situation is illustrated in Figure 2[13]. Moreover, the revocation of trust service providers certificate, 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.

[13] 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*.

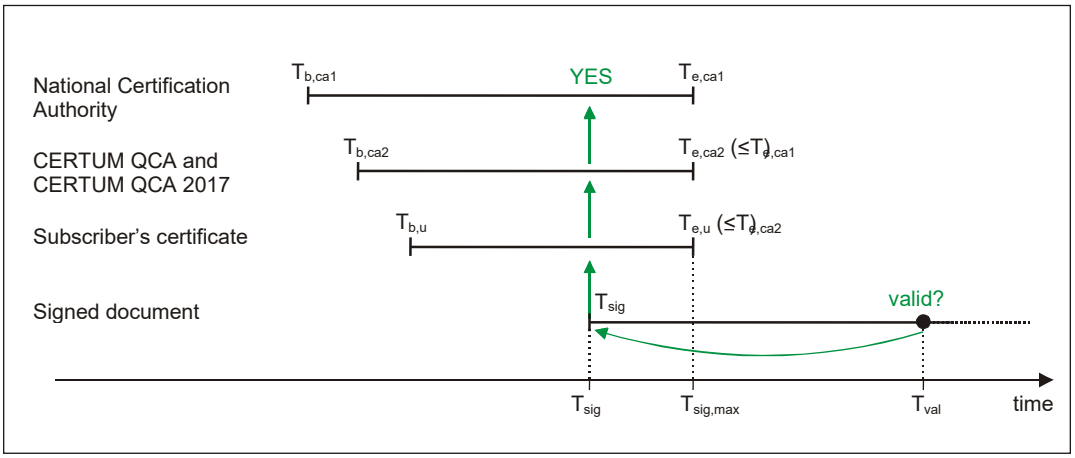


Fig.2 Successful verification of electronic signature based on algorithm described in RFC 5280 recommendations

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 trust service providers 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 or trust service providers when such a certificate was valid.

Certificate revocation is equivalent to the loss of certificate validity and results in the termination of the contract between the subscriber and Certum.

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 cannot be restored (however, where this is not clearly stated, the word revocation will also include suspension of the certificate).

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 (otherwise certificate will be revoked).**

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.

4.9.1. 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 and Certification Practice Statement

by the subscriber. Revocation is performed either on subscriber or authorized representative 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[14]; certificate revocation procedure is in this case executed by a subscriber,
- the subscriber resigns from services provided by 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,
- upon a request from authorized entity, whose data is included in the certificate application,
- upon a request from Minister of Digital Affairs,
- 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 and Certification Practice Statement,
- 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,
- 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 Certificate Policy and 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 can be submitted trough Registration Authority (see chapter 3.4). After verification of applicant's identity – revocation application is sent to the Primary Registration Authority, which revokes the certificate based on received documents.

Revocation request submitted on request of the third person indicated in certificate request applies to all qualified certificates issued by Certum.

4.9.2. Who can request certificate revocation

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

[14] 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.

- a subscriber who is the subject of a certificate,
- authorized entity, whose data is included in the certificate application,
- an authorized representative of a certification authority (in the case of Certum this role is reserved for the security inspector),
- Minister of Digital Affairs,
- the registration authority operator, registration inspector 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 4.9.1, 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.

4.9.3. Procedure for certificate revocation

Certificate revocation may be carried out in following manners:

- submission of an non-electronic request – paper document,
- submission of a request by fax or phone call.

Upon successful verification of a revocation request by the certification authority, the certificate is revoked. Information about the revoked certificate is published on the **Certificate Revocation List** (see chapter 7.2), issued by the certification authority.

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

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 should 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).

4.9.4. Certificate revocation grace period

Certum guarantees that the maximum grace period[15] for revocation request is 24 hours 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 4.9.8).

[15] 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 4.9.8).

Subscriber and authorized entity, whose data is included in the certificate application are informed about the certificate 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.

4.9.5. Maximum time of processing revocation application

Certificate revocation application is processed by Certum within 24 hours of its acceptance.

4.9.6. Obligatory revocation check

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.

The revoked certificate remains on the Certificate Revocation List at least until the end of its validity period.

The final decision about the certificate trustworthiness should 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.

Certum guarantees uninterrupted access to certificate's status information for 24/7 (24 hours / 7 days a week).

4.9.7. CRL issuance frequency

CERTUM QCA and **Certum QCA 2017** issues Certificate Revocation List.

Every Certificate Revocation List is updated at least once a day[16]. Notwithstanding, the new CRL is published in the repository after every certificate revocation. In the case of revocation of the certificate this certificate is immediately published on Certificate Revocation List. The same rules are for revocation of trust service provider certificate, this certificate is immediately published on Certificate Revocation List.

4.9.8. Maximum delay of publishing Certificate Revocation List

Every Certificate Revocation List is published immediately after being created (usually it is done automatically in a few minutes).

4.9.9. On-line certificate status verification availability

Certum provides real-time certificate status verification service. The service also allows to obtain information about the certificate revocation beyond its validity period. The QOCSP service is based on the protocol shown in *RFC 6960*[17]. Using OCSP, it is possible to acquire more frequent and up-to-date information (in comparison to sole CRL usage) about a certificate status.

[16] 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**).

[17] RFC 6960 *Internet X.509 Public Key Infrastructure: Online Certificate Status Protocol – OCSP.*

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[18],
- **revoked** – meaning the certificate has been revoked,
- **unknown** – meaning that the validity period of the verified certificate has expired or the certificate has not been issued by qualified certification authority CERTUM QCA and Certum QCA 2017.

Certificate's status information is public. The address of service is included in the issued certificate (see chapter 7.1.3.1)

Certificate's status is retrieved from the certification authority server and is available not later than 60 seconds after certificate revocation.

CRLs published by Certum as well as responses from QOCSP service are electronically signed by their issuing authorities, so Certum guarantees their integrity and authenticity.

4.9.10. 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 4.9.9. Notwithstanding above, it is recommended to employ 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.

4.9.11. Other forms of revocation advertisements availability

Not applicable.

4.9.12. Special duties in case of rekey security breach

Not applicable.

4.9.13. Circumstances of certificate suspension

Suspension of certificate may occur under the following circumstances:

- data contained in the revocation request rise justified suspicion,
- revocation request was made by phone, and was not possible within 24 hours since receiving request, to confirm the identity of applicant, but also negate the correctness of the submitted application,
- there is a suspicion that the person using electronic signature has lost his or her full legal capacity,
- certification authority may immediately suspend the certificate if reasonably suspects that the certificate has been issued without complying with the provisions of this Certificate Policy and Certification Practice Statement; certificate may remain suspended until the certification authority finds the grounds for the revocation of the certificate, but no longer as 7 days,
- other circumstances requiring clarification from the subscriber or the applicant.

[18] See **Glossary**.

Information contained in the certificate suspension application are similar to those in revocation application.

4.9.14. 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.

4.9.15. Procedure of certificate suspension and unsuspension

The suspension procedure is carried out analogically to revocation procedure (see chapter 4.9.3). 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 (by restoring it to its normal state) 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 authorized employee of Certum.

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 (that means, it cannot be the date of the end of suspension).

4.9.16. 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 4.9.4).

That period does not include the time of receiving the confirmation of certificate suspension and publishing suspended certificate on Certificate Revocation List (see chapter 4.9.7).

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.

4.9.17. Revocation or suspension of the Trusted Service Provider certificate

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

- Minister of Digital Affairs decides to remove entry of certification authority from the register of qualified trust 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 Certificate Policy and Certification Practice Statement.

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 mandatory 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.

4.10. Other services – Certificate status services

4.10.1. Operational characteristics

4.10.1.1. Electronic timestamp service

The primary objective of electronic timestamp service, provided by the electronic timestamp authority **CERTUM QTSA** and **CERTUM QTST 2017** is to mark an electronic documents, electronic signatures, electronic transactions, etc. with a reliable time. Electronic timestamp is proof that data object existed before the date placed in this electronic timestamp. Thanks to this:

- electronic timestamp authority confirms the existence of data,
- electronic timestamp 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.

*Electronic timestamp authority **CERTUM QTSA** and **CERTUM QTST 2017** is not a party of transactions referred to and marked with a reliable time.*

Procedure of obtaining a time – stamp issued by electronic timestamp 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 electronic timestamp token issuance; the format of issuance is default in the case of lack of identifiers,
- electronic timestamp authority verifies completeness and correctness of application,
- electronic timestamp authority generates an electronic timestamp (electronic timestamp token – TST), which contains serial number, protocol identifier, time from reliable source, application data, data generated by electronic timestamp authority, binding in a cryptographic manner the time with the digest value, the identifier of the hash function and the session identifier,
- electronic timestamp authority submits an electronic timestamp token to the requesting entity,
- requesting entity verifies the correctness of electronic timestamp token.

Electronic 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 electronic timestamp token is unique within certification authority domain **CERTUM QTSA** and **CERTUM QTST 2017**; this feature is also retained in the event of a resumption of service after a failure,
- electronic timestamp authority private keys are generated and stored inside hardware security module complying with FIPS 140-2 Level 3 requirements,
- the electronic timestamp authority **CERTUM QTSA** and **CERTUM QTST 2017** owns private key used for creating electronic confirmations of electronic timestamp tokens.

4.10.1.2. Qualified Validation Service for qualified electronic signatures and qualified electronic seals

Qualified validation service provided by **CERTUM QDVCS** and **Certum QESValidationQ 2017** can be useful to validate the signed documents or certificates. **CERTUM QDVCS** and **Certum QESValidationQ 2017** issues data validation certificate that may be regarded as equivalent to notary token, defined in ISO/IEC 13888-3 standard.

CERTUM QDVCS and **CERTUM QESValidationQ 2017** activity is based on DVCS, OASIS DSS, XKMS protocols. **CERTUM QDVCS** may:

- 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.

Qualified validation authority **CERTUM QDVCS** and **Certum QESValidationQ 2017** can validate following types of tokens and certificates:

- qualified public key certificate,
- qualified electronic signature,
- qualified electronic seal.

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 authority server verifies format of the request, downloads type of validation and identifier of certification policy,
- a data validation authority server creates token and sends it to applicant,
- an applicant checks the correctness of the token, and if the token does not raise any suspicions, she/he remembers it together with the data involved.

The detailed validation policy is descripted in *Validation Policy of Certum's Qualified Validation Service for qualifies electronic signatures and qualified electronic seals*.

4.10.2. Additional options

Time stamping services and validation services for qualified electronic signatures and qualified electronic seals are available 24/7 (without any planned outages).

4.10.3. Optional functions

Not applicable.

4.11. End of subscription

The end of the subscription occurs in the following cases:

- subscriber certificate validity period has passed and subscriber has not taken action to update or modify his/her key,
- subscriber's certificate was revoked and replaced by another certificate.

4.12. Key escrow and restoration

Private keys of certification authorities, or other subscribers, for which Certum generates keys or that are available are not subject key escrow.

The exception is the remote signature or seal service, where the private keys of the subscribers are stored on the hardware cryptographic module (HSM) meeting the FIPS 140-2 Level 3 and are available only to the subscriber / entity after logging to the individual service account in accordance with the internal Certum procedure.

4.12.1. Principles and of key escrow and restoration

Not applicable.

4.12.2. Session key encapsulation, restoration policy and practice

Not applicable.

5. Facilities, Management and Operational 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 and trust service providers certificate issuance and publication, certificate and trust service providers certificate revocation, audit and backup copy creation.

5.1. 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. System logs record each entrance and leaving. Stability of power supply, temperature, and humidity is tested.

5.1.1. Site location and construction

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

5.1.2. Physical access

Physical access to the building and Certum rooms 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.

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 Trust and Security Division Director.

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**.

5.1.3. 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.

5.1.4. 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. buildings at Bajeczna Street 13 in Szczecin and Narutowicza 136 Street in Łódź. Reception personnel are notified of the hazards and are obligated to notify appropriate public services, security inspector and one of system administrator.

5.1.5. Fire prevention

Fire prevention and protection system installed in Asseco Data Systems S.A. buildings at Bajeczna Street 13 in Szczecin and Narutowicza 136 Street in Łódź 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.

5.1.6. 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.

Media storage of archives, current data copies and paper documents are stored in Certum rooms.

5.1.7. Waste disposal

Paper and electronic media containing information possibly significant for Certum security after expiration of the retention period (see chapter 5.5.2) 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).

Hardware cryptographic modules are reset according to the manufacturer's documentation. Resetting modules also takes place before sending them for service/repair to the manufacturer.

5.1.8. Offsite backup storage

Copies of passwords, PIN numbers and cryptographic cards are stored in two localizations of Asseco Data Systems S.A.

In the building of Asseco Data Systems S.A. also archives, current copies of information processed by the system and full installation version of Certum applications are stored. It enables emergency recovery of most substantial Certum function within 48 hours (in Certum building or in the emergency facility).

5.1.9. 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 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.

5.1.9.1. 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),
- addresses of other registration authorities are available in repository at www.certum.eu.

5.1.9.2. Physical access

Access to Primary Registration Authority has to be performed as described in chapter 5.1.2. 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.

5.1.9.3. Power and air conditioning

Primary Registration Authority is connected with ADS'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.

5.1.9.4. Water exposure

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

5.1.9.5. Fire prevention and protection

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

5.1.9.6. 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.

5.1.9.7. Waste disposal

Paper and electronic media, containing confidential or secret information are, upon expiration of the retention period (see chapter 5.5.2), 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.

5.1.9.8. 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).

5.1.10. 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.

Certificate holder should not leave the workstation and software installed on it unattended when it is in a cryptographically unsecured state, i.e. a password, PIN, or private key has been entered.

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

Certum is a service unit of Asseco Data Systems S.A., providing nonqualified and qualified trust services. Certum teams related to the generation and revocation of certificates have a documented structure that secures the impartiality of the operation. A thorough description of the roles and tasks assigned is governed by the internal Certum procedure. Certum teams are fully independent from other divisions for decisions regarding the: creation, provision, maintenance and suspension of services in accordance with the applicable certification policy. In particular, management staff, specialist staff, and staff in trusted roles are not subjected to commercial pressure that could negatively affect the trust in provided services.

This chapter presents a list of roles which can be defined for personnel employed in Certum. The list is compliant with ETSI EN 319 401 *Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers*. 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 criminal record.

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

- **Certification Authority Manager –** responsible for appropriate management of Certum, defines the directions of Certum development, implements and manages the Certification Policy and Certification Practice Statement,
- **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; 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,
- **Audit Inspector** – responsible for review, archive and management of event logs (in particular verification of their integrity), reviews event logs 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.

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, the following trusted roles have to be defined:

- **person who verifies identity** – verifies subscriber's identity and correctness of a submitted application and behalf of Asseco Data Systems S.A. accepts the terms of provision of trust services,
- **partner establishing registration authority** – is responsible for efficient operation of a registration authority; his/her role is to provide financial support for the personnel, manage operators' work, A person who verifies identity must be accredited by Certum.

Person confirming the identity of applicants must be accredited by Certum. Based on the authorization (received at hers/his request or the partner's authorized registration authority) she/he can confirm the identity of the applicants, both at the point of registration as well as in the place of residence of the applicant.

5.2.1.3. Subscriber's trusted roles

The present Certificate Policy and 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 – (optional) i.e. 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,
- issuance of certificate enabling access to Certum systems (cryptographic card).

All accounts associated with issuing, renewing, revoking a certificate require multi-component authentication, realized through login and password, and a cryptographic card with a certificate.

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 27001:2014 standard. All unused accounts are immediately disabled, Certum systems access certificates are revoked accordingly with internal procedures.

5.2.4. Roles that cannot be combined

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.

5.3. Personnel controls

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 27001:2014 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. Qualifications, experience and authorization

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 eIDAS Regulation* and *the Act*.

5.3.2. Personnel verification procedure

Control of preparation for job binded with trusted role is carried out for each new employee, before allowing him/her to perform his/her duties and is preceded by appropriate training. Control of the preparation includes:

- proof of the efficacy of previous employment,
- check references and professional qualifications,
- confirming level of education suitable to perform trusted role,
- declaration of no criminal record from candidate.

In certain information availability absence (e.g. due to applicable law), Certum may use other – allowed by law – techniques that will allow to obtain information similar to the above.

Certum may reject a candidate for the position associated with trusted role or take action against a person already employed in such a position in the event of, among others, the following facts:

- misrepresentation by the candidate to perform trusted role or a person holding such a role already,
- highly unfavorable or unreliable references and professional qualifications,
- criminal past of a candidate or those already employed.

In case of any of the above facts, further operations are carried out in accordance with Asseco Data Systems S.A. safety procedures and applicable law.

5.3.3. 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 Policy and Certification Practice Statement of Certum‘s Qualified Certification Services,
- regulations of Terms & Conditions for Certum Qualified Trust 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,
- the existing and emerging threats to the PKI technology and the critical role they play in mitigating them.

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

5.3.4. Retraining Frequency and Requirements

Trainings described in chapter 5.3.3 have to be repeated or supplemented at least once a year and always in situation when significant modification to Certum or its registration authority operation is executed or when new version of Certification Policy and Certification Practice Statement is introduced.

5.3.5. Job rotation

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

5.3.6. 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.

In the case of the personnel actions that violate the provisions of *the Act*, penalties resulting from chapter 6 of *the Act* are provided.

5.3.7. 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 5.3.3 and 5.3.4). 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.

5.3.8. Documentation Supplied to Personnel

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

- Certification Policy and Certification Practice Statement,
- Terms & Conditions for Certum Qualified Trust 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.

5.4. Events recording, security incidents management 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.

In case of detecting a susceptibility Certum should:

- report safety event,
- perform risk analysis for the detected susceptibility and concerned resources and classify susceptibility,
- define owned security, estimate the impact and accept the risk, or define a proposal to proceed to compensate for the risk,
- plan corrective actions to remove the susceptibility,
- removal of detected susceptibility depends on the type of susceptibility, all efforts are made to remove susceptibility within 48 hours from the moment of its detection. It is permissible for a situation where the vulnerability is removed in the long run in accordance with the risk management plan.

Dealing with the detected vulnerability is carried out in accordance with the internal incidents management procedure.

It is required that every party – associated in any way with providing trust 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 both in the main and the alternate Certum sites.

Event logs are created automatically. Every log entry is retained and disclosed when undergoing an audit.

Activity of servers in teleinformatic network, including cryptographic modules devices, is monitored 24/7. In case of a failure of one of the elements of the teleinformatic network, the service personnel is immediately informed of this fact. In addition, monitoring systems analyze the performance of services such as time stamp issuance, an OCSP token, or DVCS confirmation issuance. In the event of problems with a given service, the IT system is immediately informed.

Certum's Compliance and Quality Team regularly carries out internal audit regarding compliance of implemented mechanisms and procedures with regulations of this Certificate Policy and Certification Practice Statement, as well as effectiveness of existing security procedures.

5.4.1. 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 trust services, for example: registration and certificate request, rekey request, certificate acceptance, certificate and CRL issuance, electronic seals 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.

Certum's service servers log events related to data processing in business process. Logs are send to central log servers, storing event logs of all devices working in the teleinformatic network.

Recorded entries include:

- operations associated with registration, certification, revocation and suspension of certificates and rekey procedures, electronic timestamp issuance, data validation, verification of certificate status or other services provided by an authority issuing certificates,

  - particular registration of events is subjected to the handling of applications for the issuance of qualified signatures and stamps, where all the events related to the certificate life cycle and its rekeying are recorded: e.g. the registration of the application by the Primary Registration Authority, its operation within Primary Registration Authority, the generation of the certificate, the date and time the certificate was downloaded by the applicant, as well as all activities related to certificate revocation,

- all events related to the use of the subscriber's private key stored on the hardware cryptographic module,
- 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,
- alerts generated by firewalls and IDS,
- key generation for a certification authority, as well as for other parties, for example subscribers and registration authorities,
- information related to the process of starting and stopping event logging on service servers,
- every event related to the usage of trust service providers certificate of certification authority and other trust services providers,
- record of synchronization, using the NTP, to trusted source of Coordinated Universal Time (UTC),
- every act of loss of synchronization between trusted time source and international time source (including exceeding the limit timing accuracy (one second); in such case, the service ceases to be provided,
- any event related to usage of the private key of any qualified certification authorities of Certum providing trusted services,
- all events related to the preparation of the subscribers' and employees' cryptographic cards (physical and virtual QSCDs),
- 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,
- notification and alerts for exceeded systems capacity and availability limits,
- every startup and shutdown of any of Certum's services.

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 5.2.1.1).

The configuration of the Certum Qualified IT Systems are regularly checked for changes which could violate a security policy. Reports from the system integrity service (Host Based IDS) are analyzed by our staff at least once every 5 days. Every unauthorized change get detected, reported and investigated immediately.

5.4.2. 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 5.4.1, at least once a working day.

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.

5.4.3. Event journals retention period

Records of registered events are stored in files on system disk for 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 20 years.

5.4.4. 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 5.5.2).

5.4.5. 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 an electronic timestamp.

5.4.6. Collecting data for internal and external audit

Module for analysis of the event logs implemented in the system allows examination of all 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.

5.4.7. Notification to event responsible entities

Certum manages security incidents according to the incidents management procedure applied over Asseco Data Systems S.A.

This procedure complies with the requirements of art. 19.2 of *the eIDAS Regulation*.

When determining that recognized incident has a significant impact on the provided trust services, Certum notify the supervisory body within 24 hours after having become aware of it. Notification is sent by fax.

The notified supervisory body inform the Inspector General for Personal Data Protection or the competent national body for information security, where it determines, that disclosure of the breach of security or loss of integrity has a significant impact on the trust services provided by Certum.

Where determining that the breach of security or loss of integrity is likely to adversely affect a natural or legal person to whom the trusted service has been provided, Certum notify the natural or legal person of the breach of security or loss of integrity without undue delay.

5.4.8. Vulnerability assessment

Certum classifies and keeps records of all assets according to PN-ISO/IEC 27001:2014 standard. This Certificate Policy and 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.

Risk analysis for Certum is conducted at least once a year or when introducing new services, major changes in Certum systems or as a result of a security incident.

Certum assets and Information Security Policy, which is part of the implementation of Asseco Data Systems S.A. The Integrated Management System is subjected to annual reviews and approval of the Certum Director.

Certum informs its subscribers, third parties, regulatory bodies and assessment bodies about changes in Information Security Policy.

In accordance with the to risk management plan, each risk analysis begins with the identification and verification of the asset list.

The list of assets is sent for verification to the team conducting the analysis. Verified lists are sent to the analysis manager, who consolidates received information and creates a current asset list.

The risk assessment process is carried out if:

- new group of information will be created,
- new assets will appear,
- new threat/risk will appear,
- new cycle of analysis will begin, no later than 11 months after the end of the previous analysis.

Low level risks are accepted by the Certum Director. For the risks above acceptable level, risk management plans are being developed that also require the approval of Certum Director.

5.5. 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 authorities, in accordance with art. 17 of *the Act* is archived.

Archive contains certificates issued up to 25 years back.

The archive also contains paper documents used to provide trust services.

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

Archived paper and electronic documents are retained for 20 years.

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.

Data obtained in the process of remote verification of subscribers identity are also stored by service providers through which the service is provided, i.e. Blue Media S.A and AriadNEXT.

Data from the bank verification transfer are stored by Blue Media S.A. for 30 days. They may also be removed on the basis of a subscriber's request made via Certum.

Data obtained during the video verification path is stored by AriadNEXT for a period of 15 days. They may also be removed on the basis of a subscriber's request made via Certum.

5.5.1. 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,
- subscribers, subjects certifications requests, documents issued by the registration point operator, notary or other person authorized to confirm subscriber’s identity,
- accepted by subscribers terms of provision of trust services,
- data from bank verification transfer obtained in the process of remote identification of subscribers - a report containing the name of the subscriber,
- data obtained during the video verification path in the process of remote identification of subscribers - a report containing a photo of an identity document along with its data and a photo of the subscriber,
- video call records obtained in the process of remote identification of subscribers,
- subscribers database, including all the information collected during the registration process,

- Certum-managed certificate lifecycle events on behalf of subscribers (related to remote signing / sealing services),
- certificates database,
- issued Certificate Revocation Lists,
- history of a certification authority key, from its generation to erasure,
- internal and external correspondence (paper and electronic) between Certum, its subscribers and relying parties in the operation of certificate revocation, suspension and unsuspension,
- other documents and data associated with providing trust services.

5.5.2. Archive retention period

Archived data (in paper and electronic form), described in chapter 5.5.1, and are retained for the period of 20 years (does not apply to video records obtained in the process of remote identity verification). After expiration of the declared retention period, archived data may be destroyed. In the case of key and certification erasure, according with the internal procedure.

Records of video calls obtained in the process of remote identity verification are stored for a period of 14 days, after this time the records are destroyed.

5.5.3. Archive protection

Access to archive have only authorized persons performing trusted roles in Certum. Archive is stored on a system that meets standards requirements referred to in the Commission Implementing Decision (EU) 2016/650 of 25 April 2016 laying down standards for the security assessment of qualified signature and seal creation devices pursuant to Articles 30(3) and 39(2) of Regulation (EU) No 910/2014 of the European Parliament and of the Council on electronic identification and trust services for electronic transactions in the internal market. System shall protect archive from unauthorized viewing, modification, removal or tampering. Media on which archives are stored and applications for archives processing must be maintained in such condition to ensure declared access period to the archives.

5.5.4. 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,

Backups are performed by trusted Certum personnel. Backups are subjected to periodic verification, restoration accordingly to internal Certum procedures.

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.

Backups contain information related to applications for certificates issue/revocation, data for audit and records in a database of all issued certificates. They are stored outside the place of their creation and must be available for any request of authorized persons.

Copies of private keys of certification authorities and other trust service providers are created and managed in accordance with the principles set out in chapter. 6.2.4.

Certum maintains copies of above information for their own CA and trust service providers.

5.5.5. Requirements for electronically timestamping of the records

The archived data is signed with an electronic timestamp, created by the time – stamping authority **CERTUM QTSA and Certum QTST 2017**.

5.5.6. Collecting of archival data (internal and external)

Archives collection is an Certum internal system.

5.5.7. Procedures to obtain and verify archive information

Access to archive is granted only to people performing trusted roles in Certum and is possible only after a successful authentication.

To verify the integrity of archived information, the data is periodically tested and verified against original data. This activity may be carried out under the control of the system administrator 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.

5.6. Key changeover

Procedure for key changeover applies to the keys of certification authorities **CERTUM QCA** and **Certum QCA 2017** and other authorities providing trusted services and it describes procedure for key update (rekey) for a certificate, CRL, electronic timestamps, verified certificate status, validated data and receipt or submission tokens signing (including official tokens), which replaces a currently used key.

Rekey procedure for the mentioned above authorities requires a request to **National certification authority (NCCert)** for a new trust service provider certificate. If the request concerns the keys for **CERTUM QCA** and **Certum QCA 2017**, then upon receipt of the certificate, that authority issues to **National certification authority** a mutual certificates of trust service providers.

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

*From the moment of key changeover, the certification authority **CERTUM QCA** and **Certum QCA 2017** uses only a new private key for signing issued certificates and Certificate Revocation List.*

5.7. 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.

5.7.1. Procedures for handling incidents and respond to threats

Incidents handling and responding to threats are regulated by Certum Business Continuity Plan. At least once a year Certum tests the effectiveness of the procedures covered by the Business Continuity Plan.

5.7.2. Key security violation and disaster recovery

All information on failure cases of computing resources, software or data are transmitted to safety inspector, who ordered to take action in accordance with developed procedures. These procedures are designed to analyze the intensity of the attack, investigate the incident, to minimize its effects and to eliminate it in the future. If necessary actions taken must be provided for disclosure of Certum authority public key or running procedures related to planned system recovery after disaster.

5.7.3. 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 about the compromise of the private key, by means of mass media system and electronic mail,
- trust service provider certificate of a certification authority corresponding to the compromised key is placed on Certificate Revocation List, along with a suitable reason for revocation,
- all subscribers 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,
- In the case of a compromise, or suspected compromise of CERTUM QTSA or Certum QTST 2017 keys, or loss of correct time, Certum will make available to all subscribers and relying parties information which may be used to identify the time-stamps which may have been affected, unless this publication breaches the privacy of the subscribers or the security of Certum services. The information includes, among others: the name of affected qualified time stamp authority and the period of time during which incorrect timestamps were issued.

5.7.4. Business continuity capabilities after a disaster

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 5.5.4, 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 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 48 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. Backup copies and their archives are retained outside primary facility. Periodically, the process of checking the durability of stored data carriers is carried out in accordance with internal Certum procedures.
- **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.

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.

5.8. Certification authority termination or service transition

Obligations described below are developed to minimize disruption to subscribers and relying parties, arising from the Certum's decision to cease operation, and include obligations to notify in advance the supervisory body, subscribers, contractors and Partners about the termination of trust services, and transfer to the supervisory body all documents and data relating to the provision of trusted services. The detailed procedure for the termination is described by the Certum's termination plan, which is the internal procedure of Certum.

Supervisory body is informed about Certum's plans for termination and every time it changes.

5.8.1. Requirements associated with duty transition

When Certum terminates its services, it is obligated:

- to notify the National root (NCCert) at least 90 days before the agreed date of the termination that Certum is going to terminate services as the qualified trust service provider,
- to 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,
- to notify its contractors, trading partners and partners having points of the identity verification,

- to revoke all issued authorizations for verification of subscribers' identity and all authorizations to sign qualified trust services agreements on behalf of Asseco Data Systems S.A.,
- to notify the other entities with whom Certum is linked by agreements for the provision of qualified trust services,
- to notify all subscribers associated with the certification authority about service cessation,
- to 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,
- to transmit the data, directly connected with trust services, to the supervisory body or to the entity designated by him, including Trusted Service Provider's keys, subscribers' certificates, documentation about the registration of entities and subscribers, information about the event logs and CRLs, including obligations to make them available for reasonable period (for period of 20 years from the time of their creation),
- to sign the contracts necessary for the proper transfer of data and services (mentioned above) to the transferees, containing the obligation to keep them for the period indicated by law, i.e.: for a period of 20 years from their creation,
- to transfer to destroy or to decommission trust services keys and their backups, if further use of this data have not been foreseen or if trust services provider certificate associated with these services have been revoked,
- to pay compensations of issuance fees to the subscriber or the represented entity; compensations should be proportional to remaining validity period of the certificate.

5.8.2. Dealing with a terminated certification authority

The detailed procedure for ending Certum activity is described in Business Continuity Plan, which is the internal document.

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** and **Certum QCA 2017**, electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017**, online certificate status protocol authority **CERTUM QOCSP,** data validation authority **CERTUM QDVCS** and **Certum QESValidationQ 2017**, have to be revoked and keys destroyed.

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 and installation

6.1.1. 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 and **Certum QCA 2017** 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** and **Certum QCA 2017** are used to sign subscriber's certificate and CRLs.

In addition, the keys of the certification authority **CERTUM QCA** and **Certum QCA 2017** can be used to sign other electronic confirmations of trust service provider certificates (including cross-certificate) as in the cases specified in chapter 5.6.

An electronic signature is created by means of RSA algorithm in combination with SHA-1 or SHA-2 cryptographic digest, while a key agreement employs Diffie-Hellman[19] algorithm.

6.1.1.1. Key pair generation

Certum has a documented internal procedure for generating certification authority keys. This procedure defines the role of participants in the ceremony (trusted persons roles participating in the ceremony), the next steps to be taken by each person, accordingly to the principle of double checking, responsibility for the performance during the ceremony and its completion, and documentation requirements for generating the certification authority keys (protocol, report).

Certum certification authority keys are generated within Certum building, 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 electronic timestamp tokens issuance. 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, electronic timestamp authority keys, certificate status verification authority keys, data validation 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.

Subscriber's keys can be generated by the **CERTUM QCA** and **Certum QCA 2017** or independently by the subscriber using mechanisms provided by the Certum (see chapter 6.1.2).

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

6.1.1.1.1. Procedures of generation of CERTUM QCA and Certum QCA 2017 initial keys

Procedures of generation of initial **certification authorities** 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 trust service 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.

6.1.1.1.2. CERTUM QCA and Certum QCA 2017 rekey procedure

CERTUM QCA and **Certum QCA 2017** cryptographic keys have a limited lifetime period, before expiration date the keys should be updated, updates must be performed at least two years and three months before their expiry date.

A particular procedure is applied for update of key pair used for certificate and CRL signing. It is based on the issuance of special trust service providers certificates by **CERTUM QCA** and **Certum QCA 2017**. The certificates enable subscribers who have already installed an expired self-certificate of **CERTUM QCA** and **Certum QCA 2017** 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** and **Certum QCA 2017** 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** and **Certum QCA 2017**, 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** and **Certum QCA 2017** 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 $\mathbf{K_{GPK(1)}}$ and the proof of possession of complementary private key,
- The National root NCCert creates certificate that consists a new public key **CERTUM QCA** and **Certum QCA 2017,** 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** and **Certum QCA 2017**, 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 $\mathbf{K^{1}_{GPK(1)}}$ – 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** and **Certum QCA 2017**, signed with new private key $\mathbf{K^{1}_{GPK(1)}}$ (**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** and **Certum QCA 2017** 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** and **Certum QCA 2017** (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** and **Certum QCA 2017**. 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** and **Certum QCA 2017** 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** and **Certum QCA 2017** 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** and **Certum QCA 2017,** signed with a new private key $\mathbf{K^{1}_{GPK(1)}}$,
- 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** and **CERTUM QCA 2017** 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.

Certum allows subscribers to use their keys only with devices officially listed as Certified Qualified Signature Creation Devices and notified by certification designated bodies under Article 30(2), 39(2) and 39(3) of *the eIDAS Regulation*[20].

[20] It also applies to Secure Signature Creation Devices benefiting from the transitional measure set in article 51(1) of Regulation 910/2014

New subscribers of Certum qualified services are supplied with personalized cryptographic cards (Secure Signature-Creation Devices). The personalization means that the subscriber's cryptographic keys – 3 pairs for future subscribers, PUK security code and the identification number of the card are created on the subscriber's cryptographic card. All these data are automatically saved to the database. Personalization is done on equipment that is not connected to the network and in a secure room accessible to designated employees performing trusted roles. The card number is then entered by the subscriber/entity in the registration form, into which the data is entered into her/his certificate and permanently binded in the database with the user's certificate data. Based on the registration form data, an end-user certificate is generated. These data are also permanently bound to the one pair of keys.

New Certum subscribers may also receive access to the personalized card on the HSM device. Cards personalization means – preparing the card for use by setting up the main card structure, creating profiles, generating and printing a unique card number. Card, created this way, is a secure device that will hold an end-user certificate. Card personalization process is performed in a secure room, which is accessible only to trusted employees who act as the trusted roles. Subscribers cryptographic keys and card identification numbers are generated on cards and automatically saved to database, cards are not initialized what it means that they do not have PUK and PIN security codes. Card personalization is performed on devices not connected to the network.

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, i.e. PUK code, needed to issue an authenticating PIN code are made available to subscribers separately from issued certificates or issued by subscribers on their own when HSM device stores cards. Data needed to activate the hardware cryptographic module are also supplied separately.

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 or seal 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

No stipulation.

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 trust service providers certificates complying with ITU-T X.509 v.3 recommendations. Certum's trust service provider certificates are issued by the National root NCCert.

Certum certification authorities distribute their certificates in two different methods:

- in the publicly available at:

  www.certum.pl/repozytorium

- distributing together with a dedicated software (e.g. web browsers, e-mail clients, etc.), which allows usage of services offered by Certum.

In the case of Certum certification authority key update (rekey), the repository should contain all additional trust service provider certificates issued as a result of execution of the procedure laid down in chapter 6.1.1.1.2.

6.1.5. Keys Sizes

Certum uses cryptographic algorithms and minimum key sizes that comply with the requirements of the ETSI TS 119 312 standard.

All certificates issued to end-users under a qualified certification authority have a 2048 bits key length and a SHA-2 hash function.

6.1.6. Public Key Generation Parameters and quality checking

Both when cryptographic keys are generated by Certum, and when the subscriber creates them independently using the mechanisms provided by Certum (see chapter 6.1.2), generating parameters complies with requirements laid down in ETSI EN 319 401 and 319 411-2.

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].

6.1.7. Key Usage Purposes

Allowed key usage purposes are described in **KeyUsage** field 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 trust services,

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

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

CERTUM QCA and **Certum QCA 2017** has keys for signing certificates and Certificate Revocation List (**keyCertSign** bit and **cRLSign** bit).

Electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017**, online certificate status protocol authority **CERTUM QOCSP,** data validation authority **CERTUM QDVCS** and **Certum QESValidationQ 2017** possess of the key applied to confirm tokens (**digitalSignature** bit and **nonRepudiation** bit).

In terms of technology it is possible to use one key pair for both electronic signature creation operation and data encryption. This Certificate Policy and Certification Practice Statement does not recommend acting in such a manner. In the case of qualified certificates for electronic signature and electronic seal this is prohibited.

6.1.8. Hardware and/or Software Key Generation

In the case of certification authority **CERTUM QCA** and **Certum QCA 2017**, the electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017**, online certificate status protocol authority **CERTUM QOCSP,** data validation authority **CERTUM QDVCS** and **Certum QESValidationQ 2017** keys are generated by means of hardware security modules complying with requirements presented in chapter 6.2.1.

All keys used for electronic signatures, whose public part in the form of a certificate or trust service provider certificate is confirmed by **CERTUM QCA** and **Certum QCA 2017**, 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** and **Certum QCA 2017** for qualified certificate issuance.

Acceptable ways of generating key depend on their usage and are shown in Tab. 7.

Tab. 7 Key generation method

Certificates / trust service providers certificates / tokens	Key generation method
Qualified public key certificate	Hardware
Trust service providers certificate	Hardware
Tokens	Hardware

6.2. Private key protection

Every subscriber and certification 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).

6.2.1. Standards for Cryptographic Modules

Hardware security modules used by Certum certification authorities and subscribers are compliant with FIPS 140, Common Criteria EAL 4+ or ITSEC E3.

Tab. 8 Minimal requirements imposed on hardware security modules

Certificate subject type / Trust service providers certificates	Employed security module
Certification authority CERTUM QCA and Certum QCA 2017	Hardware, complying with FIPS 140-2 Level 3 or higher
Electronic timestamp authority CERTUM QTSA and Certum QTST 2017	Hardware, complying with FIPS 140-2 Level 3 or higher/EAL 4+
Online certificate status protocol authority CERTUM QOCSP	Hardware, complying with FIPS 140-2 Level 3 or higher/EAL 4+
Data validation authority CERTUM QDVCS and Certum QESValidationQ 2017	Hardware, complying with FIPS 140-2 Level 3 or higher/ EAL 4+
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 signature or seal),

- **inactive** – the key may be used for e-signature validation or decryption only (the subscriber cannot use the private key for creating a signature or seal – 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 trust service authorities.

In the case of certification authorities the control applies to a key used for creation electronic confirmations, in the certificates, trust service providers certificates, in the Certificate Revocation List. 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 Tab. 9.

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

Tab. 9 Distribution of shared secrets

Authority providing certification services / Trust services	Number of shared secrets, required for private key restoration	Total number of distributed secrets
CERTUM QCA and Certum QCA 2017	3	5
CERTUM QTSA and Certum QTST 2017	3	5
CERTUM QOCSP	3	5
CERTUM QDVCS and Certum QESValidationQ 2017	3	5

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

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

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.

6.2.2.2. 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 only after authorization of secret transmission.

In the case of natural disasters 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.

The exception is the remote signature or seal service, where the private keys of the subscribers are stored on the hardware cryptographic module (HSM) and are available only to the subscriber / entity after logging to the individual service account in accordance with the internal Certum procedure.

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.

Timestamp signing keys are stored within several hardware cryptographic modules, and the corresponding electronic timestamp device is associated with the same certificate. At the time, only one signing key is used to sign timestamp tokens.

Certum does not retain copies of subscriber's private keys.

6.2.5. Private Key Archival

Private key of certification authority **CERTUM QCA** and **Certum QCA 2017**, electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017**, online certificate status protocol authority **CERTUM QOCSP,** data validation authority **CERTUM QDVCS** and **Certum QESValidationQ 2017** 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 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,
- in the case of creating and using private keys stored in HSM device,
- 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 three 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 the 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,
- when keys are available remotely to subscriber the security code PIN and PUK are assigned by subscribers on their own and they are known only to her/him.

Entry of a private key into hardware security module of certification authority **CERTUM QCA** and **Certum QCA 2017**, electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017**, online certificate status protocol authority **CERTUM QOCSP,** data validation authority

CERTUM QDVCS and **Certum QESValidationQ 2017** requires restoration of the key from the cards in the presence of appropriate number of shareholders or administrator's card protecting the module containing these private keys (see chapter 6.2.2). Since every certification authority may possess an encrypted copy of its private key (see chapter 6.2.4), the keys may be also transferred between the security modules.

6.2.7. Private Key Storage in Cryptographic Module

Depending on cryptographic module type private keys can be stored in the module in the plain or encrypted form. Regardless of private key storing form it is not accessible from outside cryptographic module for unauthorized entities.

6.2.8. 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, electronic timestamp 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** and **Certum QCA 2017**, electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017**, online certificate status protocol authority **CERTUM QOCSP,** data validation authority **CERTUM QDVCS** and **Certum QESValidationQ 2017**, 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.

Subscribers private keys are activated after authentication (administration PIN) and only for the duration of cryptographic operations using the key. After completion of this operation the private key is automatically deactivated and must be reactivated before the next operation on an electronic card or other qualified signature or seal creation device (i.e. HSM device).

6.2.9. 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 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.

6.2.10. Method of Destroying Private Key

Erasure of private keys of subscriber 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.

Destroying private keys of Certum certification authority, timestamp authority, online certificate status protocol authority, data validation authority means physical destruction of the electronic cards and/or other media or their safe erasure from the media (from electronic card, hardware security module, etc.) used for storage of copies or archives of shared secrets.

6.2.11. Cryptographic Modules ratings

See chapter 6.2.1.

6.3. Other Aspects of Key Pair Management

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

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). It is extremely important in the case of providing of non-repudiation services, such as an electronic 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, electronic timestamp authority 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.

Public keys are retained in the public key archive for the period of 25 years (see chapter 5.5.2).

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 or trust service provider certificate (see chapter 7.1). Validity period of a service private key is shorter than validity period of trust service provider certificate (which results from the possibility to cease private key usage at any time).

The electronic timestamp service provided by Certum recognizes this possibility and constantly checks the validity period of the private key. If it's unable to verify, it blocks the issuing of timestamp tokens.

Standard values of maximal usage period of trust service provider certificate certification, electronic timestamp authority, online certificate status protocol authority**,** data validation are described in Tab. 10, while subscriber's certificates are presented in Tab. 11.

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

Starting date of the trust service provider certificate validity period don't have to comply with the date of its issuance. It is allowed to set this date in the future but never in the past.

Tab. 10 Maximal usage periods of trust service provider certificates

Owner and key type		Main key usage	
		RSA for certificate and CRL signing	RSA for token signing
CERTUM QCA	authority certificate	5 years	–
	private key	3 years	–
Certum QCA 2017	authority certificate	11 years	–
	private key	8 years	–
CERTUM QTSA	authority certificate	–	4 years
	private key	–	4 years
Certum QTST 2017	authority certificate	–	11 years
	private key	–	11 years
CERTUM QOCSP	authority certificate	–	4 years
	private key	–	4 years
CERTUM QDVCS	authority certificate	–	11 years
	private key	–	11 years
Certum QESValidationQ 2017	authority certificate	–	11 years
	private key	–	11 years

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

Tab. 11 Maximal usage periods of the qualified certificates for electronic signature and electronic seal

Owner and key type		Main key usage
		RSA for secure electronic signatures
Private persons, legal entities	Qualified certificate	3 years
	Private key	3 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 trust services 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 112. 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 other 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*[21] (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.

Computers operated within Certum 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),
- discretionary access control based on login credentials (login name, password and cryptographic smart card),
- possibility of conducting security audit,
- 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,

[21] Information System Security Controls Assessment Criteria

- 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,
- monitoring and alerting means for exceeded systems capacity and availability limits.

Assessment of computer security means is carried out in accordance with recommendations presented in ITSEC[22] 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 eIDAS Regulation* and *the Act.* Systems used for issuing and managing certificates are required to fulfil the *standards referred to in the Decision of the Executive Committee (EU) 2016/650 of 25 April 2016 establishing standards for assessment of the safety devices for qualified signature and stamp on the basis of art. 30 paragraph 3 and art. 39 paragraph 2 Regulation of the European Parliament and of the Council (EU) No 910/2014 on electronic identification and trust services in relation to electronic transactions in the internal market* Technical Controls.

6.6. Technical control

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 internal procedure which is available in the Certum collaborative workspace.

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.

Control of the cryptographic modules creation includes requirements imposed on design, manufacture and delivery of cryptographic modules. Certum does not define its own requirements in that matter. Certum only accepts cryptographic modules which meet the requirements described in chapter 6.2.1.

Hardware security modules delivered to Certum are checked every time if there was any violation of the shipment and if the module preserves physical and logical integrity. The verification (from which the report is made) is conducted by trusted Certum personnel. Hardware security modules that are not in use are protected in envelopes which can't be opened without leaving a mark. Prepared that way modules are stored in safes located in secured rooms accessible only to group of persons acting as trusted roles.

[22] *Information Technology Security Evaluation Criteria*

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.

Although the administrative work and changes in the Certum systems are recorded, each of them require further verification and acceptance by at least two administrators. Change control system notify eligible employees of the occurrence of modifications in the system and requires to verify it by a different person than the one who introduced the change.

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

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

6.7. Network Security Controls

Certification Authority Networks are divided into several logically separated segments:

- demilitarized area (DMZ) that contains and exposes Certum's external-facing, public service servers (frontend),
- protected area including application servers, databases, logs (backend),
- protected area of the operators workstations,
- protected area of the administrators workstation,
- protected area of the certification authority including the key servers, certificate issuance servers and the time stamping servers.

Each of the above area have a separate traffic policy filtering policy. Network traffic registries are additionally analyzed by skilled, trustworthy employees.

At least once a year, penetration tests covering Certum systems are conducted. In addition, Certum runs at least four vulnerability scans per year (one per quarter). Both types of tests are performed by a professional service provider. The results of penetration tests and vulnerability scans are reported to Certum and analyzed by Certum qualified personnel who act as the trusted role. Risks resulting from reported vulnerabilities are evaluated and, when appropriate, changes are made to the systems.

Communication from the protected area of the certification authority to the public servers zone is possible through the internal and external security locks. These firewalls accept only packets coming out of the protected area of the certification authority. Communication between the protected zone and the backend server protection zone is based on a queue system. Certum has its own, autonomous intrusion and DDoS attacks detection system. In addition, all servers are subject to periodic data integrity checks.

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). This means that both the certification request token and the user registration process are processed in a closed internal zone (the operator work station) with no

access from the global network, transition areas or even from the internal network of Asseco Data Systems S.A.

Certum centers have redundant internet connection. All network devices are redundant to ensure high network infrastructure reliability. Server access to the LAN is provided through redundant connections (2 network cards each) from each server to the switches to provide single device or connection failure protection. Certum Firewalls are working in HA clusters. Its task is to ensure continuous availability of the network in case of one of the pair failure.

All Certum system accounts and user permissions are reviewed on regular basis and at the request of Certum executives. Any system, services and network accounts that are not used are blocked or deactivated.

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.

In addition, security functions are implemented on the basis of virtualization, the use of reliability clusters and redundancy of the equipment such as power supplies, SAN arrays etc.

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.

Any changes in Certum network devices require the prior approval of Security Inspector. The change is implemented only after verification by the administrator who did not take a direct part in creation of changes.

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. Electronic Timestamps 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 timestamps.

Electronic timestamps for internal needs can be created within Certum system in accordance with the recommendation *RFC 3161*. Note, that in contrast to this electronic timestamps, the electronic timestamp authority CERTUM QTSA and Certum QTST 2017 issuing electronic timestamp tokens in accordance with *ETSI EN 319 422* recommendation (see chapter 1.3.1.2).

7. Certificate, CRL, and OCSP Profile

Qualified certificates profiles for electronic signature and electronic seal, trust service providers certificates profile and Certificate Revocation List profile provided by Certum QCA 2017 comply with the format described in ITU-T X.509 v.3 and profiles included in the ETSI EN *319 412 Electronic Signatures and Infrastructures (ESI); Certificate Profiles; Part 1 – 5.* The profile of OCSP token complies with the requirements of *RFC 2560*, while the profile of timestamp token complies with *ETSI EN 319 422 Time-stamping protocol and time-stamping profiles.* The profile of data validation tokens complies with the requirements of *RFC 3029*.

Information stated below describes the meaning of respective certificate fields, CRL, electronic timestamp, 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. Certificate content

The contents of a certificate or trust service provider 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 or trust service providers certificates structure. Certificates or trust service providers certificate issued in accordance with X.509 v.3 recommendation allow definition of proprietary extensions, unique for implementation of the system.

Basic Certificate Fields

Certum supports the following certificate or trust service provider certificate basic fields:

- **Version**: third version (X.509 v.3) of certificate or trust service provider certificate format,
- **SerialNumber**: certificate or trust service provider certificate serial number, unique within certification authority domain,
- **SignatureAlgorithm**: identifier of the algorithm applied by a certification authority issuing certificates or trust service provider 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 or trust service provider certificate validity period,
- **Subject**: distinguished name (DN) of the subscriber that is the subject of the certificate or trust service provider certificate,
- **SubjectPublicKeyInfo**: value of a public key along with the identifier of the algorithm associated with the key.

In certificates or trust service provider certificate issued by Certum values of the above fields are set in accordance with the rules described in Tab. 12.

Tab. 12 Profile of the basic fields of the trust service provider certificate

Field name	Value or value constraint	
Version	3	
Serial Number	Unique value for all certificate issued by certification authorities within National Certification Center (Narodowe Centrum Certyfikacji)	
Signature Algorithm	CERTUM QCA: SHA-1 with RSA encryption sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) SHA-512 with RSA encryption Certum QCA 2017: sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)	
Issuer: National Certification Center (Narodowe Centrum Certyfikacji, NCCert) (for CERTUM QCA)	Common Name (CN) =	Narodowe Centrum Certyfikacji (NCCert)
	Organization (O) =	Minister właściwy do spraw gospodarki
	Country (C) =	PL
Issuer: National Certification Center (Narodowe Centrum Certyfikacji, NCCert) (for Certum QCA 2017)	Common Name (CN) =	Narodowe Centrum Certyfikacji (NCCert)
	Organization (O) =	Minister właściwy do spraw gospodarki
	Country (C) =	PL
	Organization Identifier (2.5.4.97) =	VATPL-5250008198
Subject CERTUM QCA:	Common Name (CN) =	CERTUM QCA
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	SERIAL NUMBER =	Entry number: 14
Subject Certum QCA 2017:	Common Name (CN) =	Certum QCA 2017
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Organization Identifier (2.5.4.97)	VATPL-5170359458
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.	

Field name	Value or value constraint	
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 Public Key Info	Algorithm	RSA encryption RSA encryption (OID: 1.2.840.113549.1.1.1)
	Public Key	2048 bits or 4096 bits
	Public Key value	Value is expressed in the form of a string of bytes.
Signature	Certificate signature is generated and coded: • according to the "Signature algorithm" field, • by the Issuer in order to confirm the relationship of the public key with the Subject.	

Certificate extensions

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 trust service provider certificate public key certificate complimentary with it's private key – **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 and trust service
  -- providers 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 or trust service provider certificate. This field should be interpreted as constraint of allowed key usage purpose defined in field **keyUsage**. Certum issues certificates or trust service provider certificate 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 policies, applied by the issuing authority – **this extension is critical**.

Tab. 13 Policies identifiers and their description

Policy identifier	Certificate policy description
joint-iso-ccitt(2) ds(5) id-ce(29) id-ce-certificatePolicies(32)	Identifies certification policies used for issuing qualified certificates.
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-cck(4) id-cck-certum-certPolicy(1)	Identifies Certum's certification policies used for issuing trust service provider certificates.

Certificates or trust service provider certificate issued by certification authorities include both qualifiers, recommended by the *RFC 5280*.

- **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 or trust service provider 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**; claims that the certificate is an EU qualified certificate that is issued according to *the eIDAS Regulation*, declares that the private key related to the certified public key resides in a Qualified Signature / Seal Creation Device (QSCD) according to the Regulation (EU) No 910/2014 and declares that qualified certificate is issued as one or more specific types. **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. Version number

All Certum certificates are issued in accordance with X509 third version (X.509 v.3).

7.1.3. Certificate Extensions and issued certificates or trust service providers certificates types

Certificates or trust service providers certificates issued by **CERTUM QCA** and **Certum QCA 2017** may contain various combinations of extensions defined in chapter 7.1. Choice of the desired certificate or trust service providers certificate depends mainly on the intended purpose of the certificate or trust service providers certificate and the subscriber whom the certificate or trust service providers certificate is issued.

7.1.3.1. Qualified certificates

The qualified certificates that meet requirements of *the Act,* issued to private persons contain extension described in Tab. 144.

Tab. 14 Extensions of qualified certificates for electronic signatures and seals

Extension	Value or Value constraint	Extension status
Authority Key Identifier	SHA1 hash of the public key (OID: 2.5.29.35)	Non-critical
Subject Key Identifier	SHA1 hash of the public key (OID: 2.5.29.14)	Non-critical
Basic Constraints	Subject type=empty (end entity) Path length constraint=none (OID: 2.5.29.19)	Critical
Key Usage	Digital Signature, bit 0 Content commitment[23], bit 1 (OID: 2.5.29.15)	Critical
Subject Alternative Name	(optionally) E-mail: customer@somewhere-in-world.com	Non-critical
CRL Distribution Points	Certificates issued by Certum QCA: http://crl.certum.pl/qca.crl Certificates issued by Certum QCA 2017: http://qca.crl.certum.pl/qca_2017.crl	Non-critical
Authority Information Access	Online Certificate Status Protocol (OCSP) https://qca-2017.qocsp-certum.com (OID: 1.3.6.1.5.5.7.48.1) Certification Authority - issuer https://repository.certum.pl/qca_2017.cer (OID: 1.3.6.1.5.5.7.48.2)	Non-critical
QCStatements	A statement that the certificate is an european qualified certificate[24]: id-etsi-qcs-QcCompliance (0.4.0.1862.1.1) A statement that the private key associated with the certificate resides in a qualified signature/seal creation device: id-etsi-qcs-QcSSCD (0.4.0.1862.1.4) Reference to the information on Certum QCA and Certum QCA 2017 public key infrastructure:	Non-critical

[23] In the ITU-T X.509 standard, this bit has been renamed from "nonRepudiation" to "contentCommitment"

[24] This is the statement of Asseco Data Systems S.A. that qualified certificates are issued in accordance with *the eIDAS Regulation* and *the Act of Trust Services*. Asseco Data Systems S.A. declares the consistency of the issued qualified certificates with the *ETSI TS 319 422* 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
	id-etsi-qcs-QcPDS (0.4.0.1862.1.5) EN: https://repository.certum.pl/PDS/Certum_QCA-PDS_EN.pdf PL: https://repository.certum.pl/PDS/Certum_QCA-PDS_PL.pdf Indication that the certificate is used for the purposes of electronic signatures or seals: id-etsi-qct-esign (0.4.0.1862.1.6.1) or id-etsi-qct-eseal (0.4.0.1862.1.6.2)	
Certificate Policies	1.2.616.1.113527.2.4.1.1 (qualified certificates before 1st July 2016), 1.2.616.1.113527.2.4.1.11 (qualified certificates after 1st July 2016), 1.2.616.1.113527.2.4.1.12.1, 0.4.0.194112.1.2 (qualified certificates for e-signature (*eIDAS* structure) card), 1.2.616.1.113527.2.4.1.12.2, 0.4.0.194112.1.2 (qualified certificates for e-signature (*eIDAS* structure) HSM) 1.2.616.1.113527.2.4.1.13.1, 0.4.0.194112.1.3 (qualified certificates for eSEAL (*eIDAS* structure) card) 1.2.616.1.113527.2.4.1.13.2, 0.4.0.194112.1.3 (qualified certificates for eSEAL (*eIDAS* structure) HSM) CPS: http://www.certum.pl/CPS Notice number: depends on certificate type Organization: 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

7.1.3.2. Certificates of trust service providers

Certificates of trust service providers may contains extensions described in Tab. 15.

Tab. 15 Minimal extensions of certificates of certification authorities

Extension	Value or Value constraint	Extension status
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

7.1.3.3. Cross-certification trust service providers certificates

Cross-certification trust service providers certificates may contain extension specified in Tab. 16.

Tab. 16 Extensions of cross-certification trust service providers certificates

Extension	Value or Value constraint	Extension status
Authority Key Identifier	SHA1	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/CPS Notice number: depends on certificate type Organization: Asseco Data Systems S.A. Explicit text: depends on policy identifier (plain text).	Critical

7.1.4. 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 or trust service providers certificate. In the case of Certum - RSA with SHA-2.

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

7.1.5. Name forms

Certum issues certificates containing name of issuer and entity created in accordance with the principles described in the chapter. 3.1.1.

7.1.6. Names restrictions

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

7.1.7. Certification Policy Identifiers

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

Certificates or trust service provider certificate issued by certification authorities include both qualifiers, recommended by the *RFC 5280*.

Tab. 17 The Certification policy identifiers included in the certificates issued by **CERTUM QCA** and **Certum QCA 2017**

Name of certificate / certificates of trust service providers	Certification policy identifier
Qualified certificates (before 1st July 2016)	1.2.616.1.113527.2.4.1.1
Qualified certificates (after 1st July 2016)	1.2.616.1.113527.2.4.1.11
Qualified certificates for eSignature (*eIDAS* structure) card	1.2.616.1.113527.2.4.1.12.1
Qualified certificates for eSignature (*eIDAS* structure) HSM	1.2.616.1.113527.2.4.1.12.2
Qualified certificates for eSeal (*eIDAS* structure) card	1.2.616.1.113527.2.4.1.13.1
Qualified certificates for eSeal (*eIDAS* structure) HSM	1.2.616.1.113527.2.4.1.13.2
Certificates of TSP	2.5.29.32.0

Tab. 18 The identifier for the Certum Qualified Electronic Timestamp Authority policy included in timestamp tokens issued by CERTUM QTSA and Certum QTST 2017

Token name	Certification Policy Identifier
Qualified timestamp token QTSA	1.2.616.1.113527.2.4.1.2
Qualified timestamp token QTST 2017	1.2.616.1.113527.2.4.1.14

Tab. 19 The certification policy identifiers for validation included in data validation tokens

Token name	Certification Policy Identifier
Qualified validation token of qualified electronic signature[25]	1.2.616.1.113527.2.4.1.3.2.c[26]
Qualified validation token of qualified electronic seal	1.2.616.1.113527.2.4.1.3.5.c – 1.2.616.1.113527.2.4.1.3.9.c, 1.2.616.1.113527.2.4.1.3.11.c
Qualified validation token of qualified certificate[27]	1.2.616.1.113527.2.4.1.3.4.c

7.1.8. Certification Policy Identifiers Extensions usage on defining politics restrictions

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

7.1.9. Policy qualifiers syntax and semantics

In most cases, the certificates issued by Certum contain two qualifiers of certification policy, placed in the extension policyInformation. The first qualifier provides an indication of the Certification Practice Statement (ang. CPS Pointer). The second qualifiers – note addressed to the relying party – contains a number of notes and its contents. Note number clearly defines the type of certificate issued under the certification policy, and the content of notes – contains name of the commercial type certificate (see Tab. 4).

7.1.10. Processing semantics critical extension of the certification policy

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

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

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

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

[27] These are certificates which are issued by registered (i.e. qualified) 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.

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 or trust service providers 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, trust service providers 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 QCA authority sign **CRL** by means of **sha1WithRSAEncryption** algorithm, and Certum QCA 2017 – by means of **sha512WithRSAEncryption,**
- **Issuer**: name of the certification authority issuing CRL (**CERTUM QCA** and **Certum QCA 2017**),
- **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 or trust service providers certificates (the field is empty in the case of lack of revoked certificates or trust service providers certificates); the information consist of three sub-fields:

  userCertificate - serial number of a revoked certificate or trust service providers certificate
  revocationDate - date of the certificate or trust service providers certificate revocation
  crlEntryExtensions - extended access to CRL (contains additional information about revoked certificates or trust service providers certificate – 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) 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).

CRL's profiles list is conformant with IETF RFC 5280.

7.2.1. Version number

CRLs versions published by Certum vary depending on the certification authority to which they relate. They include the name of the certification authority that issued it, the date of the present and next publication and the serial number, date and reason of revocation (or suspension). CRLs are published at certain intervals, or each time after the suspension or revocation of one of the issued certificates.

7.2.2. Supported CRL entry extension

Function and meaning of extensions are the same as for certificate or trust service providers certificate extensions (see chapter 7.1). 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 or trust service providers 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 or trust service providers certificate renewal;
  cessationOfOperation - cessation of certificate usage;
  certificateHold - suspension of certificate or trust service providers certificate;
  removeFromCRL - certificate or trust service providers certificate removal from CRL;
  privilegeWithdrawn - certificate was revoked due to canceling of authorization associated with the attributes and included in the public key certificate or the attribute certificate;
  aaCompromise - applies to attributes certificates; meaning is the same as for withdrawal of privileges

- **HoldInstructionCode**: code of the operation on certificate or trust service providers 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 or trust service providers certificate discovery on Certificate Revocation List with a note (reason for revocation): certificate or trust service providers 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 or trust service providers certificate suspension or reject the certificate or trust service providers certificate (assume it is revoked). If the application discovers **id-holdinstruction-reject** code, it should obligatorily reject the respective certificate or trust service providers 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.

7.2.3. Revoked certificates and CRL

Information about revoked certificates is included in each list of revoked certificates or trust service providers 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 or trust service providers certificates of a certification authority: certificates or trust service providers certificates have to be included in the succeeding Certificate Revocation Lists, published by the issuer of the revoked certificate or trust service providers certificates (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 (also see chapter 5.8).

7.3. OCSP profile

OCSP profile of **CERTUM QOCSP** has a structure that complies with RFCs 6960 X.509 *Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP*. CERTUM QOCSP authority verifies the certificate status (OCSP) as recommended by RFC 6960.

Tab. 20 Basic fields profile of the Trusted Services Provider Certificate

Field name	Value or its constraint	
OCSP Response Status	The field assumes one of the values: successful malformedRequest internalError tryLater sigRequired unauthorized	
Response Type	Field assumes the value: Basic OCSP Response	
Version	Field assumes the value: Version 1	
Responder Id	Identifier of the responder issuing the token OCSP.	
Produced At (date of issue)	Date and time the OCSP response was signed by the responder.	
Certificate ID	Hash Algorithm	The algorithm used to calculate the two values below. The field assumes the value sha1 (OID: 1.3.14.3.2.26).
	Issuer Name Hash	A shortcut of the distinguished name of a certificate issuer who is the subject of an OCSP query.
	Issuer Key Hash	Public key excerpt from certificate issuer being the subject of the OCSP inquiry.
	Serial Number	Serial number of certificate being the subject of the OCSP inquiry.
Cert Status (certificate status)	Certificate status. The field can assume one of the values: good revoked unknown	
This Update (update date)	Date from which OCSP response status should be considered correct.	
Next Update (next update date)	Date to which OCSP response status should be considered correct.	
Response Extensions	OCSP Nonce (non-critical, optional).	Random value allowing the cryptographic binding of the request and response.

Field name	Value or its constraint
Signature Algorithm	The algorithm used to sign the OCSP response. Field assumes the value sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.13).
Certificate	Certificate signing OCSP response.

7.3.1. Version number

Version – Field assumes the value: Version 1 (tab. 20).

7.3.2. Supported Extensions

Response Extensions – Random value allowing the cryptographic binding of the request and response (tab. 20).

7.4. Other profiles

7.4.1. Electronic timestamp token profile

CERTUM QTSA and **Certum QTST 2017** authority electronically signs issued electronic timestamp tokens with one or more private keys reserved solely for this purpose. According to RFC 5280 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 electronic timestamp authority solely for the purposes of signing electronic timestamp tokens issued by this authority.

The Time-Stamp Token remains valid as long as all the algorithms used for its issuance are considered secure.

Otherwise TST shall be renewed based upon the new algorithms. The TST verification should be carried on by means of the IETF RFC 3161 compliant software all the time.

Electronic timestamp authority certificate basic fields profile is described in Tab. 21.

Tab. 21 Certum QTSA and Certum QTST 2017 certificate basic fields profile

Field name	Value or its constraint
Version	Version 3
Serial Number	Unique value for each trust service provider certificate issued by the National root NCCert
Signature Algorithm	Certum QTSA: sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) Certum QTST 2017: sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13)
Issuer (Distinguished Name)	Distinguished name DN of the National root NCCert – provider of trust service certificate for CERTUM QTSA and Certum QTST 2017.
Not before (validity period	Universal Time Coordinated based. Certum owns satellite clock controlled by Atomic Frequency Standard (PPS). Certum clock is

beginning date)	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: Certum QTSA	Common Name (CN) =	CERTUM QTSA
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	Serial Number (SN) =	Entry number: 15
Subject: Certum QTST 2017:	Common Name (CN) =	Certum QTST 2017
	Organization (O) =	Asseco Data Systems S.A.
	Country (C) =	PL
	2.5.4.97 =	VATPL-5170359458
Subject Public Key Info	Encoded in accordance with *RFC 5280*, contains information about RSA public key (key identifier and value of the public key). Certum QTSA: Key length: 2048 bits Certum QTST 2017: Key length: 4096 bits	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280.	
Authority Key Identifier	SHA2 hash of the public key	Non-critical
Basic Constraints	Subject type=empty (end entity) Path length constraint=none	Critical
Key Usage	digital signature, bit 0 content commitment, bit 1	Critical
Extended Key Usage	Time Stamping Authority (TSA)	Critical
Certificate Policies	Policy: 2.5.29.32.0 CPS: http://www.certum.pl/CPS Notice number: depends on certificate type Explicit text: depends on policy identifier (plain text)	Critical

CERTUM QTSA and Certum QTST 2017 accepts electronic timestamp requests that meet the IETF RFC 3161 specification and ETSI EN 319 422 requirements with the provision that:

- a request for electronic timestamp must point algorithm hash function SHA-2,
- a request for electronic timestamp may not indicate a policy identifier except for the CERTUM QTSA and Certum QTST 2017 policy OID (see chapter 1.3.2).

Electronic timestamp token, issued by Certum Electronic Time Stamp Authority contains (see Fig. 3) information on electronic timestamp (**TSTinfo** structure), located in **SignedData** structure (see RFC 2630), signed by time-stamping authority and embedded in **ContentInfo** structure (see RFC 2630).

Time stamp validation software must comply with IETF RFC 3161.

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

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

Response status filed (**PKIStatusInfo**) allows submission – to an entity requesting electronic 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 electronic timestamp. Any other value means the response does not contain a valid electronic timestamp. The reason of authority not issuing the token is described in **failInfo** field of **PKIStatusInfo** structure.

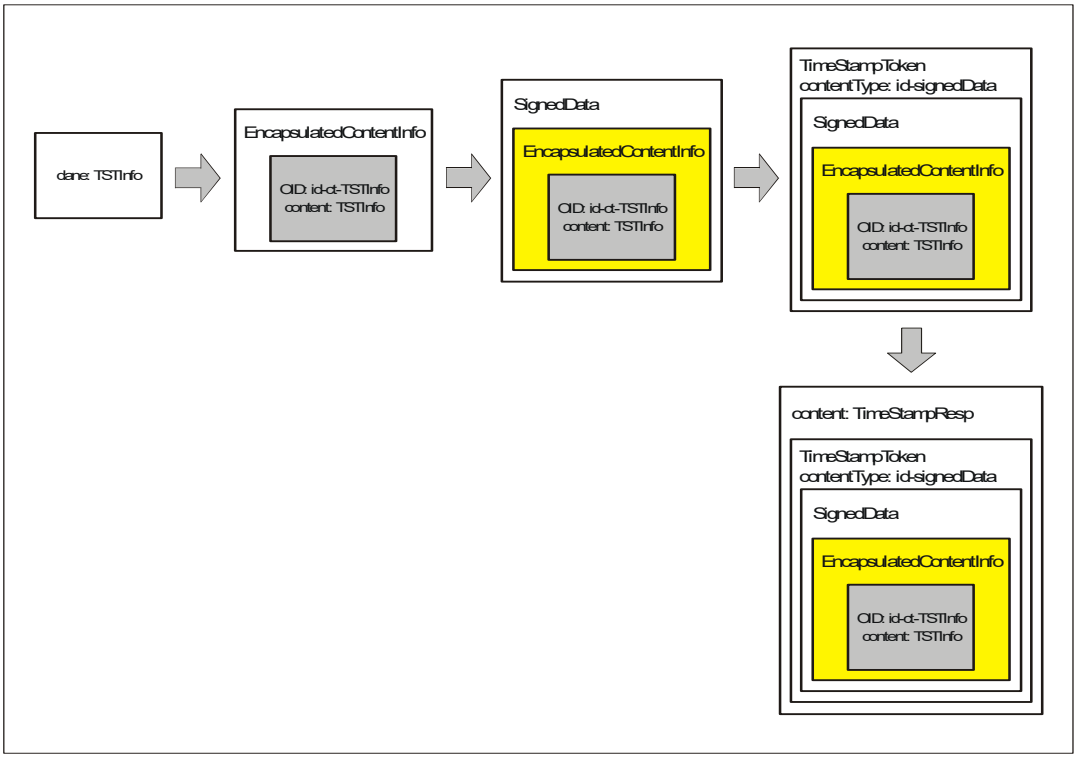


Fig.3 Electronic timestamp request response encapsulation (see also Technical Report [37])

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 (electronic 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 electronic 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
}
```

Electronic timestamp token general format complies with ContentInfo format:

```
TimeStampToken ::= ContentInfo
```

Electronic timestamp token cannot contain any other electronic certificates, beside electronic timestamp 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}
```

Electronic 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 electronic timestamps by the time-stamping authority; in case of **CERTUM QTSA and CERTUM QTST 2017** 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 and Certum QTST 2017 Identifies certification policy, used for issuing electronic timestamp tokens

- **messageImprint** contains information submitted by the requester, signed with the timestamp;
- **serialNumber** contains serial number of electronic timestamp token, issued by electronic timestamp authority. Serial number must contain continuously increasing integers;
- **genTime** field includes date and time of electronic 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** and **Certum QTST 2017** 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 electronic timestamp issuance by the TSA. In this case, ordering of two electronic 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 than 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** and **Certum QTST 2017** 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 have the same value;

- **tsa** field identifies the name of the electronic timestamp authority. If it occurs, it must comply with subject distinguished name included in the certificate, issued to the TSA by **CERTUM QCA** and **Certum QCA 2017** and used in token verification.

Time Stamp Token structure is connected with the set of signed attributes. Electronic 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/SHA2 hash of the whole certificate

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

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

7.4.2. Qualified validation tokens profiles

The qualified validation service provided by **CERTUM QDVCS** and **Certum QESValidationQ 2017** electronically certifies issued electronic timestamps with one or more private keys reserved for this purpose. In accordance with the recommendation RFC 3029, the public key certificates (which complements the private key) contain a field specifying the permitted usage of the key (**ExtKeyUsageSyntax**) marked as **critical**. This means that the trust service provider certificate may be used by the qualified validation services only for the issuance of electronic credentials in the validation tokens.

For each of the available communication protocols the validation token is structured in accordance with the selected protocol:

- for DVCS protocol according to RFC 3029 (chapter 9),
- for XKMS protocol according to the protocol XKMS 2.0,
- for OASIS protocol according to the protocol OASISS-DSS.

The report of validation is available on demand and it is provided in the human-readable form as a PDF document which is electronically signed.

Detailed descriptions of the protocols are internal documents.

7.4.3. OCSP response token profiles

The profiles of on-line certificate status verification (OCSP) tokens and data validation tokens issued by Certum certification authorities are described in Certum’s internal documents.

8. Compliance audit

Audits intend to control the practices of Certum service unit or subjects delegated by the unit are compliant with the Integrated Management System, in terms of Quality and Information Security, which includes the requirements of the standards: PN-EN ISO 9001:2009 and PN-ISO/IEC 27001:2014, and the declarations and procedures of Certum (including Certification Policy and Certification Practice Statement).

Audits carried out concern Certum's qualified trust services.

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**).

8.1. 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 on the basis of art. 20 Sections 1 and 17.4. of *the eIDAS Regulation*. Not less than once a year. According to provisions of chapter 7 of the ETSI EN 319 403 standard Compliance audit service providers trust – regulations for entities conformity assessment bodies assessing trust service providers the certification audit is carried out once every two years, and it is recommended that at least one surveillance audit was carried out between the two certification audits.

An external audit may also be carried out at the request of the Minister of Digitalization under the Art. 31 of *the Act* in relation to art. 20 Sections 1 and 17.4. of *the eIDAS Regulation.*

8.2. Identity/Qualifications of the Auditor

External audit is performed by an authorized and independent from Certum the national or European agency possessing the accreditation in Poland given by the Accreditation Centre in Poland or by an accrediting conformity assessment body within European Union. The system of accreditation and competence of the auditor are defined by the *Regulation WE 765/2008 setting out the requirements for accreditation and market surveillance relating to the marketing of products and repealing Regulation EEC 339/93* and regulated by the *ISO 17065 Conformity assessment – Requirements for bodies certifying products, processes and services*. Supervisory authority may at any time carry out an audit – or ask the conformity assessment body to carry out conformity assessment. An internal audit is carried out by designated unit, operating within Asseco Data Systems S.A. structure.

8.3. Auditor relationship with audited entity

See chapter 8.2.

8.4. Topics Covered under the Compliance Audit

Certum provides qualified services in accordance with the rules specified in *the Act* and *the eIDAS Regulation* as confirmed by independent auditors conducting Certum assessment on the basis of the ETSI EN 319 403 norm *Trust Service Providers Conformity Assessment.* Detailed scope of audit is specifies by authorization issued to auditors by the Minister of digitalization or due to the type of services provided by a qualified certification service provider in connection with the provisions above *the eIDAS Regulation* and issued decisions implementing it.

The scope of audit includes:

- checking whether the certification service provider's activity meets the requirements of the organizational and legal terms of *the Act* and *the eIDAS Regulation* and issued decisions implementing it,
- physical security of Certum,
- procedures of subscribers' identity verification,
- trust 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.

8.5. Actions Taken as a Result of Deficiency

Records of internal and external audits are submitted to Certum **Quality Team**. The Quality Team 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 Minister of Digital Affairs, 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. 34 of *the Act.*).

8.6. Notifying of Audit Results

The certificates of compliance with the requirements of the services are published at www.certum.eu.

9. Other Business and Legal Matters

9.1. Fees

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

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 electronic timestamp services and certificate status verification by means of OCSP protocol, data validation
- **indirect sale** – fees are charged for every service unit from a customer who renders services established on the basis of Certum infrastructure.

9.1.1. Certificate issuance fees

Certum charges a fee for issuance of a certificate.

9.1.2. Certificates and trust service providers certificate access fees

Certum does not charge a fee for access to certificates and trust service providers certificate.

9.1.2.1. Timestamps and tokens fees

Certum charges a fee for issued timestamps, certificate status tokens (OCSP response tokens), data validation tokens.

9.1.3. Qualified certificate revocation and status information access fees

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

9.1.4. 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.

9.1.5. 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 terms of provision of trust services or this document.

Contract termination due to certificate revocation does not result in reimbursement of costs incurred by the Subscriber that arise from the subject of the contract.

Fees refund claims should be submitted to the addresses stated in chapter 1.5.2.

9.2. Financial Responsibility

Asseco Data Systems S.A. responsibility is through its organizational unit, operating under Certum name and the parties connected by services provided by this unit as a results from routine activities performed by these entities or actions of third parties. The responsibility of every entity is stated in mutual agreements or arises from statements of will.

Certum is responsible for existence of the situations listed in chapter 9.9 of this document.

Certum is financially responsible to trust services subscribers and relying parties who are beneficiaries of the guarantee. These entities will be referred to hereinafter entities that are beneficiaries of the guarantee.

Certum does not have financial responsibility defined in this document to other third parties not included in chapter 9.2 this document.

Financial responsibility of Certum is for beneficiaries of the guarantee only if damages are the fault of Certum or fault of the parties with whom Asseco Data Systems S.A. has such agreements that the fault is transferred to Certum.

When damage is found beneficiaries from the guarantees must report its occurrence within 30 days of its occurrence. In the case of notification of a claim at a later date Certum no obligation to examine the damage.

Certum is financially responsible to beneficiaries of the guarantee only if damage occurred during the period of validity of the certificate to which it relates.

If damage is confirmed by Certum employees, Asseco Data Systems S.A. undertakes to pay compensation. The amount of compensation for a single entity which is beneficiary of the guarantee as part of a reported loss for the type certificate issued by a particular certification policy, cannot be higher than the limit of the financial guarantee for a single damages. Size of compensation paid will not be higher than proven by the entity benefiting from the guarantee amount of damage.

Asseco Data Systems S.A. undertakes for all cases of damage to pay the total compensation of up to the total limit of the financial guarantee in relation to one certificate during the entire period of its validity, total for all the beneficiaries of the guarantee.

Asseco Data Systems S.A. pays compensation to reported damages in order of receipt of a claim by beneficiaries of the guarantee. If the limit of the financial guarantee is reached, Asseco Data Systems S.A. has no obligation to pay further compensation to the next of reportable injuries by following the beneficiaries of the guarantee for the certificate.

9.2.1. Insurance coverage

Asseco Data Systems S.A. has a civil liability insurance policy that meets the requirements set by the *Regulation of the Minister of Development and Finance of 19 December 2016 regarding compulsory third party liability insurance of a trust service provider*.

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.

9.2.2. Other assets

Certum has sufficient financial resources necessary for conduct of business and discharge of their duties and to provide guarantees for subscribers and relying parties.

9.2.3. Extended warranty coverage

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

9.3. 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 Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

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. 15, § 4* of *the Act,* at the request of:

- a court or public prosecutor, with respect to pending proceedings,
- Minister of Digital Affairs, with respect to his supervision of trust 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 trust 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.

9.3.1. 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 trust 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. 15, § 4* of *the Act on Electronic Signature of 18 September, 2001 (Journal of Law 2001 No. 130 item 1450)* (see also chapter 9.3),

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

- information supplied by/to subscribers (e.g. the contents of agreements with subscribers and requesters, accounts, applications for registration, issuance, rekey, 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 trust services, stored by Certum and registration authorities,
- entries of an internal and external control,
- emergency plans,
- information about steps taken in order to protect hardware devices and software, information about administering of trust services and planned registration rules.

Asseco Data Systems S.A. is not obligated to keep secret in relation to a party that accepted the terms of provision of trust 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. based on art. 15.5 the Act.

9.3.2. Types of Information Not Considered Confidential and Private

The whole information indispensable for the process of appropriate functioning of trust 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. Electronic documents containing electronic signatures will be treated equally to those in written form.

The following information shall be treated as generally available through Certum website available at www.certum.eu:

- Terms & Conditions for Certum Qualified Trust Services,
- Certification Policy and Certification Practice Statement of Certum‘s Qualified Certification Services,
- Certum PKI Disclosure Statement,
- document templates,
- the price list of services,
- guides for users,
- trust service providers certificates,
- Certificates Revocation List (CRL),
- information about training.

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.

9.3.3. Obligation to protect confidentiality of information

Certum protect private information from being disclosed and available to third parties.

9.4. Privacy of Personal Information

9.4.1. Privacy Policy

Private data transferred to Certum by subscribers are protected defined by *the Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Scope of the personal data collected and processed by the CA meets the objectives for which these data are necessary. The consent of the subscriber / representative of the organization to processing of personal data is contained in the terms of provision of trust services and is mandatory.

Private data are used only for provision of trust services.

Private data are protected in accordance with privacy principles contained in the Asseco Data Systems S.A. security policy.

9.4.2. Information considered as private

Any information concerning subscriber identity, which is not publicly available in issued certificate in the repository and in CRL is considered private information.

9.4.3. Information not considered as private

All the information publicly available in certificate are not considered as private information, as long as this rule does not affect the requirements of *the Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

9.4.4. Responsibility to protect private information

Each Certum employee or user, which gained access to private information must protect it from disclosure and available to third parties. Apart from this, access to private information must comply with the requirements of *the Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.*

9.4.5. Reservations and permission to use private information

Unless otherwise erected in this CPS, in their respective privacy policy or the terms of provision of trust services, private information cannot be used without the consent of the party to whom the information relates.

Reservations and permits cannot violate the requirements of *the Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of*

natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC.

9.4.6. Sharing information in accordance with a court order or administrative

Classified information may be released to the competent authorities mentioned in art. 15 paragraph 4 of *the Act* only after meeting all the requirements of the applicable laws in the Republic of Poland.

9.4.7. Other circumstances disclosure

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

9.5. 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.

Each 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).

9.5.1. Trade Mark

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

Fig.4 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.

9.6. Commitments and guarantees

This chapter describes obligations/guarantees and liability of Certum, registration authorities (including points of the identity verification), subscribers and relying parties. The obligations and liability are governed by mutual agreements made by the parties mentioned above. Figure 5 presents the parties (entities) associated with trust 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.

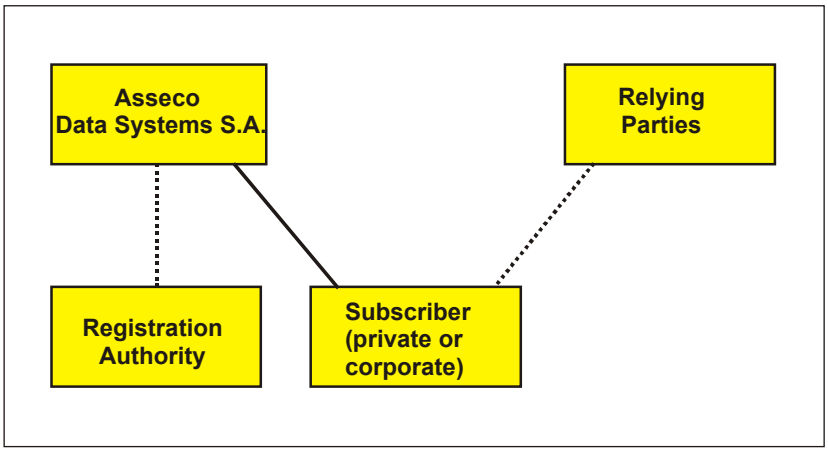


Fig.5 Agreements between parties

Asseco Data Systems S.A. agreements with subscribers describe types of qualified certification services provided by Certum, mutual obligations and liabilities (including financial ones). Detailed description is included in Terms & Conditions for Certum Qualified Trust Services.

9.6.1. CERTUM obligations and guarantee

Certum providing qualified certification services ensures that:

- its commercial activity is based on reliable devices standards referred to in the *Decision of the Executive Committee (EU) 2016/650 of 25 April 2016 establishing standards for assessment of the safety devices for qualified signature and stamp on the basis of art. 30 paragraph 3 and art. 39 paragraph 2 Regulation of the European Parliament and of the Council (EU) No 910/2014 on electronic identification and trust services in relation to electronic transactions in the internal market*,
- its activity and services are in accordance with the law; in particular they do not violate *the eIDAS Regulation*, *the Act*, included copyrights and licensed third parties rights,
- its services are in accordance with widely accepted standards or specifications:
    - trust services – with *ITU-T X.509 (ISO/IEC 9594-8), ISO/IEC 15945* (CMP protocol) and PKCS#10, PKCS#7, PKCS#12 standards,
    - electronic timestamp services – with ETSI EN 319 422 *Time-Stamping protocol and time-stamp profiles* and RFC 3161 recommendations,
    - certificate status verification (OSCP) – with *RFC 6960* recommendation,
    - validation services (DVCS) – with *Policy of Certum's Qualified Validation Service for qualified electronic signatures and qualified electronic seals*,
- it complies with and exacts the procedures described in the present document,
- 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,
- it secures personal data protection in accordance with *the Regulation (EU) 2016/679 Of The European Parliament And Of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* including its later changes and accomplishing regulations,
- it does not copy or store private keys of its customers, except for private keys stored in HSM devices,
- it hires employees who possess a knowledge, a qualifications and an experience appropriate to providing trust services, particularly in the area of:
    - automatic data processing in telecommunication networks and systems,
    - network and systems security mechanisms,
    - cryptography of electronic signatures and seals 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 and publish a list of recommended software and devices, and monitor on a quarterly basis the list of certified qualified signature/seal creation devices, published by the European Commission, in accordance with art. 31 of *the eIDAS Regulation*. When a device, which is used by Certum, is removed from the list, Certum immediately withdrawn the device from use,
- keep information secret relating to Certum's trust 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. 15 pkt.3 of *the Act,* and to protect of data used in confirmation processes for an indefinite period, and to:
    a. retain for 20 years:
        - qualified certificates issued by Certum,
        - Certificate Revocation Lists issued by Certum,
        - agreements,
    b. retain of every event logs for 3 years in a manner allowing authorized parties to access appropriate and required information.

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.

9.6.1.1. Electronic timestamp authority obligations

Electronic timestamp authority **Certum QTST 2017** provides electronic timestamp services in accordance with requirements defined in *the eIDAS Regulation* and *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI).*

CERTUM QTSA and **Certum QTST 2017** 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 *ETSI TS 119 312 Electronic Signatures and Infrastructures (ESI); Cryptographic Suites,*
- 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 electronic timestamp tokens is provided with the accuracy of 1 second.

Additionally, **CERTUM QTSA** and **Certum QTST 2017** commits itself to:

- provide continuous 24/7/365 access to supporting services except for technical breaks,
- use in the electronic 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: *ETSI EN 319 421 Electronic Signatures and Infrastructures (ESI); Policy and Security Requirements for Trust Service Providers issuing Time Stamps,*
- conduct its activity and services in accordance with the law; in particular they do not violate copyrights and licensed third parties rights,
- issue electronic timestamp tokens in accordance with *ETSI EN 319 422 Time-stamping protocol and time-stamp profiles*,
- retain, under *the Act*, the every recorded event logs for three (3) years,
- issue electronic timestamp tokens that do not contain errors or inaccurate information.

9.6.1.2. Certificate status authority and data validation authority obligations

Online certificate status protocol authority **CERTUM QOCSP** and data validation authority **Certum QESValidationQ 2017** provide their services in accordance with the requirements defined in *the eIDAS Regulation* and this Certificate Policy and Certification Practice Statement.

CERTUM QOCSP and **Certum QESValidationQ 2017** ensure that they:

- use operational procedures and security management procedures, which preclude any possibility of manipulating the certificates, trust service providers certificates or data status,
- verify validity of qualified signature certificates and electronic seals used according to the requirements of *the eIDAS Regulation,*

- **CERTUM QOCSP** verify certificate status in accordance with *RFC 6960 Online Certificate Status Protocol (OCSP)* recommendation,
- **Certum QESValidationQ 2017** service certifies the validation of qualified certificates, qualified electronic signatures and qualified electronic seals certificates.

CERTUM QDVCS service certifies the validation of qualified certificates, qualified electronic signatures and qualified electronic seals certificates and ensures that it uses operational procedures and security management procedures, which preclude any possibility of manipulating the certificates, trust service providers certificates or data status.

CERTUM QDVCS and **Certum QESValidationQ 2017** service certify the validation of qualified certificates, qualified electronic signatures and qualified electronic seals certificates.

9.6.1.3. Repository Obligations

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

- publish and archive certificate evidences of qualified trust service providers certificates **CERTUM QCA** and **Certum QCA 2017**, qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,** qualified online certificate status protocol authority **CERTUM QOCSP,** qualified validation service **CERTUM QDVCS** and **Certum QESValidationQ 2017**,
- publish and archive Certificate Policy and Certification Practice Statement of Certum‘s Qualified Certification Services and Terms & Conditions for Certum Qualified Trust 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, 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 Certificate Policy and Certification Practice Statement.
- guaranteed and uninterrupted access to certificate’s status information for 24/7 (24 hours / 7 days a week).

9.6.2. Registration authorities obligations and guarantee

Regarding registration authorities operating within 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 document, 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.

9.6.3. Subscriber obligations and guarantee

By applying for the certificate issuance and accepting the terms of provision of trust services by Asseco Data Systems S.A., a subscriber agrees to enter the certification system on the conditions stated in the terms of provision of trust services, Certificate Policy and Certification Practice Statement of Certum‘s Qualified Certification Services and Terms & Conditions for Certum Qualified Trust Services.

Subscriber is committed:

- to comply with the terms of provision of trust services by Asseco Data Systems S.A.,
- to state true data in applications submitted to a registration authority,
- to submit or present copies of required documents confirming the information included in a submitted application according to the requirements of the Certification Policy and Certification Practice Statement,
- to immediately inform Certum about any errors, defects or changes in the certificate,
- to use his/her/its own key pair and the public keys of other trust services users only for the purposes stated in Certificate Policy and 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,
    - immediately inform Primary Registration Authority about the certificate card loss or PIN number loss,
- to control the access to this software, media, and devices on which the keys or passwords are stored,
- to treat 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),
- to discontinue using the revoked, suspended or expired certificate,
- to start a procedure of revocation in the case of security violation (or security violation suspicion) of their private keys,
- to use 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.

Electronic signature usage constraints:

- not to create electronic signature or electronic seal with its private key if the validity period of certificate has expired and certificate has been revoked or suspended,
- not to store the cryptographic card containing the private key together with a personal identification number (PIN),
- not to share and communicate her/his private keys and passwords to third parties.

9.6.4. Relying Party Obligations and Guarantee

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 Asseco Data Systems S.A. and a subscriber or they might have the character of acceptance of the terms of provision of trust services.

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

- thoroughly verify[29] every electronic signature or confirmation made on a document or certificate, electronic timestamp token, certificate status token, validation token submitted to him/her/it. In order to verify the signature a relying party should:
    - specify a **certification path**[30] containing all trust service providers 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 trust service providers certification, because it is possible that there is more than one certification path leading from certificate or confirmation to trusted certification authority,
    - check whether neither of trust service providers 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 trust service providers certificates belonging to a certification path belong to certification authorities and if they are authorized to sign other trust service providers 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 an electronic timestamp issued by an electronic 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,
- 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

[29] 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.

[30] See **Glossary**

document (including electronic confirmations in public key certificate) submitted to him/her/it.

If an electronic document is marked with time or associated with other tokens, confirmations 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 were correctly electronically certified and verifies whether the private key used by qualified electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,** qualified online certificate status protocol authority **CERTUM QOCSP,** qualified validation service **CERTUM QDVCS** and **Certum QESValidationQ 2017** to issuance of token was not disclosed until the token 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 electronic timestamp tokens, certificate status token, data validation token described in this Certificate Practice Statement and stated in the terms of provision of trust services by Certum.

9.6.5. Other Users Obligations and Guarantee

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

9.7. Warranty Disclaimer

Certum guarantees are based on the general principles contained in this Certification Practice Statement and comply with applicable in the Republic of Poland overriding legal acts. Certum warranty disclaimer is placed in the terms of provision of trust services by Certum.

9.8. Liability

Certum acting within authorization of Asseco Data Systems S.A., bears liability for the consequences of the actions of certification authority **CERTUM QCA** and **Certum QCA 2017**, electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017,** online certificate status protocol authority **CERTUM QOCSP,** qualified validation service **CERTUM QDVCS** and **Certum QESValidationQ 2017,** 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 the terms of provision of trust services or resulting from separate law regulations.

9.8.1. Certum liability

9.8.1.1. Certification authority CERTUM QCA and Certum QCA 2017 liability

CERTUM QCA and **Certum QCA 2017 certification authority bears** liability for cases when direct or indirect damages suffered by a subscriber or a relying party have arisen despite compliance with the rules set out by Certificate Policy and Certification Practice Statement of Certum's Qualified Certification Services, Terms & Conditions for Certum Qualified Trust Services:

- 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 9.6.1.

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 trust services on behalf of Certum.

Certum does not use outsourcing services or outsource any part of its activities to external entities.

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 other than those provided by Certum,
- 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.

9.8.1.2. Electronic timestamp authority liability

Electronic timestamp authority **CERTUM QTSA** and **Certum QTST 2017** 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 Certificate Policy and Certification Practice Statement,
- result from mistakes made by **CERTUM QTSA** and **Certum QTST 2017**, particularly concerning inappropriate security of the private key used to confirm validity of the electronic timestamp tokens,
- occurred as a result of the violation of other **CERTUM QTSA** and **Certum QTST 2017** warranties, specified in chapters 9.6.1.1.

9.8.1.3. Online certificate status protocol authority, qualified validation service authority liability

Online certificate status protocol authority **CERTUM QOCSP,** qualified validation service **CERTUM QDVCS** and **Certum QESValidationQ 2017** 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 Certificate Policy and Certification Practice Statement,

- result from mistakes made by **CERTUM QOCSP**, **CERTUM QDVCS** and **Certum QESValidationQ 2017**, particularly concerning inappropriate security of the private key,
- occurred as a result of the violation of **CERTUM QOCSP**, **CERTUM QDVCS** and **Certum QESValidationQ 2017**, warranties, specified in chapter 9.6.1.2.

9.8.1.4. Repository liability

The liability for functioning of the repository and results of its functioning is taken by Certum (see chapter 9.6.1.3).

9.8.1.5. Subscriber liability

Described in chapter 0.

9.8.1.6. Relying party liability

Relying party responsibility results from the obligations and warranties stated in Chapter 9.6.4. The liability conditions are also governed by an agreement with subscribers and Asseco Data Systems S.A or an acceptance of the terms of provision of trust services.

It's required that relying parties have confirmed that they have sufficient amount of information to make an informed decision about acceptance or rejection of signature/electronic credentials at the time of submission.

9.9. Compensations

9.9.1. Subscribers civil liability compensation

Subscribers civil liability compensation results from the obligations and warranties stated in Chapter 0 in this document.

9.9.2. Relying party civil liability compensation

Relying party civil liability compensation results from the obligations and warranties stated in chapter 9.6.4 in this document.

9.10. Certificate Policy and Certification Practice Statement validity period

9.6.1. Validity period

This Certificate Policy and Certification Practice Statement is in effect from the moment of changing its status to valid and publication in Certum's repository until the publication of the next valid version.

9.6.2. Expiration

This document is valid until it is replaced with a new version. The starting date of the validity of the new version of the Certificate Policy and Certification Practice Statement is also the expiry date of this Policy.

9.6.3. Certificate Policy and Certification Practice Statement expiry effects

Users of Certum certificates issued during the period of this document's validity are further limited by the provisions of this document until the certificate is expired.

9.11. Users notification and communication

The parties mentioned in the present Certificate Policy and Certification Practice Statement can state, by means of the terms of provision of trust services, 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 Certum's private key, and to any changes to parameters of certificates issued by Certum.

9.12. Changes introduction procedure

Regardless of audits, there is once a year a review of the current version of Certificate Policy and Certification Practice Statement. Certum's employees, 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. If, as a result of the review, changes were made to the content, then a new version of the document will be published on the terms set out in Chapter 1.5.4.

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

9.12.1. Modification introduction procedure

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 Certificate Policy and Certification Practice Statement may be submitted by the following authorized entities:

- Minister of Digital Affairs,
- auditing entities,
- legal entities, especially when Certificate Policy and Certification Practice Statement was observed to not to obey laws and regulations in force in the Republic of Poland and may affect subscribers' interests,
- quality team, 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.

9.12.1.1. Items that can be changed without notification

The only items not requiring notification in advance apply to amendments resulting from implementation of editorial modifications, amendments to the contact information of the person responsible for the document 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.

9.12.2. Notification mechanism of and comment period

After notification in advance, each and every item of Certificate Policy and 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 Certificate Policy and Certification Practice Statement. Suggested modification may be published in the Certum repository and transmitted by the means of electronic mail. Information about implemented modifications is also attached to the new CPS document.

9.12.2.1. Comment period

Comments on suggested modifications may be submitted by the affected parties within 7 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 Certificate Policy and Certification Practice Statement is subjected to approval procedure (see chapter 1.5.4) receives the valid status.

Certum 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.

9.12.3. Changes requiring new identifier

In the case of amendments which may have influence on extensive group of trust service users, the security inspector may assign a new identifier (Object Identifier) for a modified document of Certificate Policy and 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 trust service providers.

9.12.4. Publication of the new version of Certificate Policy and Certification Practice Statement and Terms & Conditions for Qualified Trust Services

Certification Policy and Certification Practice Statement and Terms & Conditions for Qualified Trust Services documents are available in an electronic form via:

- WWW site at the address: www.certum.eu
- e-mail at the address: infolinia@certum.pl

Certum provides information to all subscribers about the intended changes to the Certificate Policy and Certification Practice Statement via mailing system, information includes the date and manner of submitting comments to its content.

Information about changes to the Terms & Conditions for Qualified Trust Services is distributed to subscribers and entities via mailing system. No comments from subscribers (by

email to infolinia@certum.pl) on the content of the revised document is equivalent to its acceptance.

The current and all previous versions of Certificate Policy and Certification Practice Statement are available in Certum repository. Lack of comments to email address infolinia@certum.pl constitutes acceptance of the document by subscribers and relying parties. If subscribers do not accept the amended provisions of the document then it is possible to resign from Certum services by submitting revocation request as defined in chapters 4.9.1 and 4.9.3 of this document.

Information on the scope of the changes is in the document history.

9.12.5. Items not published in Certificate Policy and Certification Practice Statement

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.

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.

9.13. Disputes Resolution, complaints

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

Disputes or complaints following the usage of certificates, certificate evidences, electronic timestamp tokens, certificate status tokens and data validation tokens delivered by Certum will be resolved by mediation on the basis of written information. Complaints should be directed to the following address:

Asseco Data Systems S.A.

Bajeczna Street 13

71-838 Szczecin, Poland

Disputes related to Certum’s qualified trust services will be first settled through conciliation.

Complaints are subjected to written examination within 21 days from the date of delivery to the address indicated above. If the complaint is not settled within 45 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 local 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.

9.14. Governing law

9.6.1. Resolution Survival

The resolutions of the present Certificate Policy and Certification Practice Statement are valid of the date of the approval by Certum manager 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 9.12.

If the agreement made on the grounds of the present document 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 Certificate Policy and Certification Practice Statement resolutions cannot be transferred to third parties.

9.6.2. Provision references

This Certificate Policy and Certification Practice Statement and agreements may contain references to other provisions, provided that: it has been expressed in the form of a clause in this document or contract.

9.15. Accordance with applicable law

Certum functioning is based on the principles contained in this Certificate Policy and Certification Practice Statement and applicable law in the territory of Poland.

9.16. Other laws

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

9.6.3. Contracts completeness

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

9.6.4. Conveyance

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

9.6.5. Resolution severability

On event present in document or agreements made on its basis of as violating applicable law or against the law, court may order the respect of the remaining part of Certificate Policy

and Certification Practice Statement or agreements already made, unless questioned parts are not significant from the point of view of the agreed between the parties exchange (e.g. commercial transaction).

Resolution severability is particularly crucial in the contracts signed with the subscriber.

9.6.6. Enforcement clause

Any waiver or lack of immediate implementation of any right under this document does not create a continuing waiver of such right or authorizes expectations withdraw from its implementation.

9.6.7. Force majeure

Certum is a party exempt from liability in case of unforeseen events beyond its control, which prevents it from performing its obligations under the provisions of this document (see chapter 9.6). This type of disclaimer must be included in the terms of provision of trust services.

9.17. Additional provisions

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

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, 2006	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, 2007	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	1st of March, 2008	Updating the profiles of certificates
V 3.4	14th 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	21st 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 Systems S.A. Adding the information on obligation to maintain certification certificate issued by Unizeto Technologies S.A. Asseco Data Systems S.A.
V 4.1	12th of April, 2016	Updating CERTUM registry number in the qualified certification services provider registry.
V 4.2	1st July, 2016	Adaptation to the requirements of the Regulation UE 910/2014 *eIDAS*
V 4.3	23 rd of December, 2016	Update on legislation.
V 5.0	26th June 2017	Adjusting the document to the requirements of RFC 3647. Removed information about compliance with WebTrust, Determining the compliance with *the eIDAS Regulation*. Merging Certificate Policy and Certification Practice Statement into the one document. Deleting records of key infrastructure or services regulated on country/local level: CERTUM QDA, CERTUM QODA, CERTUM QRRA, CERTUM QACA.
V 5.1	1 August 2017	Change to the address of Asseco Data Systems S.A.
V 5.2	29 June 2018	Change of entries in relation to services and their compliance with eIDAS Regulation. "Signed agreement" was changed to "acceptance of terms of provision". Change in the structure of Distinguished Name DN - adaptation to eIDAS requirements. Change in the location of the backup center. Change in the maximal usage period of qualified certificate to 3 years. Added possibility of revoking certificate by third parties indicated in the certification request on the basis of entries in dedicated contracts.
V 5.3	1 October 2018	Change in the maximum time allowed for revocation of certificate
V 5.4	27 June 2019	Expanding the catalog of cases resulting in the refusal of certificate issuance
V 5.5	26 March 2020	Corrections after eIDAS compliance auditor notes and other editorial changes
V 5.6	9 September 2020	Added remote identity verification path for subscribers, added editorial corrections

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
DH	Diffie–Hellman key exchange, a specific method of securely exchanging cryptographic keys over a public channel named after Whitfield Diffie and Martin Hellman. This method allows two parties that have no prior knowledge of each other to jointly establish a shared secret key over an insecure channel
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	Electronic 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.

Act (the) – *the Act of 5 September 2016 on trust services and electronic identification (Journal of Laws No. 2019 item 162)*

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

Certificate 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).

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.

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 (CPS) – 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 trust 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 trust 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*.

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.

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.

eIDAS Regulation (the) - *Regulation (EU) no 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC*.

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 Act.*

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).

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).

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.

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 informatization or an entity appointed by the minister according to the art. 11 of *the Act* to issuing certificates used for verifying electronic authentications of certification authorities.

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

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

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

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

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

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

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

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

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

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

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

Public entity – every entity complies with 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 amended)*.

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 (PKC) – 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 trust services, as well as other services e.g. electronic timestamp.

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

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

Qualified certification service provider – certification service provider who has been entered in the register of qualified certification service providers.

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 by its owner (subscriber) or an entity indicated by him/her in the certificate application.

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).

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* 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) possess a private key associated with the certificate issued to the entity and (3) does not issue certificates to other parties.

Terms & Conditions for Certum Qualified Trust Services – a document regulating basic rights and obligations of the parties to the certification service agreement.

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.

Electronic Timestamp 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.