# Certification Practice Statement of CERTUM's Certification Services

**Version 5.1**
**Date: 07 March, 2018**
**Status: archive**

Asseco Data Systems S.A.
Podolska Street 21
81-321 Gdynia, Poland
Certum - Powszechne Centrum Certyfikacji
Bajeczna Street 13
71-838 Szczecin, Poland
http://www.certum.pl

# Trademark and Copyright notices

# Content

# 1.Introduction

**Certification Practice Statement**[1] **of CERTUM's Certification Services** (further referred to as **Certification Practice Statement** or **CPS**) details rules of certification practice stated in **Certification Policy of CERTUM's Certification Services** (further referred to as **Certification Policy** or **CP**) and describes the process of public key certification and the applicability range of certificates resulting from this certification. The nature, aim and role of the Certification Practice Statement is particularly important from the point of view of a **subscriber**[2] and a **relying party**[3]**.**

The Certification Policy states what level of trust can be applied to a given type of the certificate issued by CERTUM providing **non-qualified certification services**. The Certification Practice Statement – on the other hand – describes how CERTUM secures the level of trust guaranteed by the policy.

*The Certification Policy and the Certification Practice Statement were defined by CERTUM, which is the supplier of certification services rendered on the basis of the CP and the CPS. The procedure of defining and updating of the Certification Policy and the Certification Practice Statement is in accordance with the rules stated in chapter9.12.*

The Certification Practice Statement describes a set of certification policies[4] applied by CERTUM to issuance of certificates to authorities and to end-users. These policies represent different levels of credibility[5] corresponding to public key certificates. The applicability ranges of certificates issued in compliance with the policies might be the same. However, responsibility (also legal) of a **certification authority** and certificate users is different.

Structure and contents of the Certification Practice Statement are in accordance with the recommendation of RFC 3647 *Certificate Policy and Certification Practice Statement Framework*.

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

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

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

[2] The subject of a certificate who is the initiator of a message and signs it using a private key corresponding to a public key contained within the certificate.

[3] The receiver who acts basing on reliance upon a certificate and an electronic signature.

[4] Information (identifier, address) on certification policy used by CERTUM. Terms Certification Policy – the document – and certification policy – a set of parameters unique for a given type of certificate – have to be distinguished.

[5] The term of *credibility* refers to what extent a relying party can be certain that the correspondence between a public key and a private or legal entity, or device (the subject of a certificate), whose data were stated in the certificate is univocal. Additionally, the credibility reflects: (a)relying party's belief that the subject of a certificate controls the usage of a private key corresponding to a public key in the certificate and (b)the level of security in the procedure of supplying the subject with a public key when it is generated also by the system creating public key certificates

# 1.1. Introduction

The Certification Practice Statement describes and is the basis for functioning of CERTUM and associated certification authorities, the Primary Registration Authority, Registration Points, subscribers and relying parties. It also specifies rules of certification services delivery, such as subscribers' registration, public key certification, rekey and certificates renewal and certificates revocation.

CERTUM's non-qualified certification services forms a separate certification domains: **certum** and its root certification authority **Certum CA** and **ctnDomena** domain and its root certification authorities **Certum Trusted Network CA**, **Certum Trusted Network CA 2**[6] and **Certum Trusted Network CA EC.** The root certification authorities are independent from the each other and issue the so called self-certificates[7] to itself. In terms of hierarchy, there are certification authorities subordinate to the root certification authorities.

This Certification Practice Statement refers to all certification authorities, Registration Points, subscribers and relying parties that use the service or exchange any information within **certum** domain or **ctnDomena** domain.

Certificates issued by CERTUM within **certum** and **ctnDomena** domains contain the identifiers[8] of certification policies, enabling relying parties to state if the application of 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** (of each certificate issued by CERTUM.

There are many additional documents connected with the Certification Practice Statement. They are used in CERTUM and regulate its functioning (see Table 1.1). 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.1.1 Important document connected with the Certification Practice Statement

| | Document name | Status | Availability |
|---|---|---|---|
| 1. | Certification Policy of CERTUM's Certification Services. | public | http://www.certum.eu |
| 2. | Certum Time-Stamping Authority Policy. | public | http://www.certum.eu |
| 3. | Personnel documentation, range of duties and responsibilities | Non-public | Locally – only entitled persons and auditor |
| 4. | The Primary Registration Authority documentation. | Non-public | Locally – only entitled persons and auditor |
| 5. | Technical infrastructure documentation. | Non-public | Locally – only entitled persons and auditor |
| 6. | Business continuity plan. | Non-public | Locally – only entitled persons and auditor |
| 7. | Identity verification instruction. | Non-public | Locally – only entitled persons and |

[6] All information in this document that refer to Certum Trusted Network CA also apply to Certum Trusted Network CA 2.

[7] **Self-certificate** – any public key certificate used for the verification of a signature made on a certificate in which the signature is verifiable by means of a public key contained in the field **subjectKeyInfo**; the contents of the fields **issuer** and **subject** are the same, the field **cA** of the extension **BasicConstraints** is set to true (see chapter 7.1.1.2)

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

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

| | | | |
|---|---|---|---|
| | | | auditor |

Additional information and service are available at: info@certum.pl.

# 1.2. Document Name and its Identification

The present document of Certification Practice Statement is given a proper name of **Certification Practice Statement of CERTUM's Certification Services**; the document is available as an electronic version at the repository at: http://www.certum.eu,

The following registered object identifier is connected with the certification policy document (OID: 1.2.616.1.113527.2.2.0.1.5.1):

```
id-ccert-kpc-v3  OBJECT IDENTIFIER::= { iso(1) member-body(2) pl(616)
        organization(1) id-unizeto(113527) id-ccert(2) id-certum(2)
        id-certPolicy-doc(0) id-ccert-kpc(1) version(5) 1}
```

in which the two last numeric value corresponds to the current version and subversion of this document.

The Certification Practice Statement Object Identifier is not included in the contents of issued certificates. Only certification policies identifiers belonging to the collection of certification policies incorporated by the Certification Policy are included in the certificates issued by CERTUM.

# 1.3. Certification Practice Statement Parties

The 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:

- the certification authorities within **certum** domain, certification authorities within **ctnDomena** domain and any other authority established in accordance with the rules stated in the present Certification Practice Statement,
- **Primary Registration Authority (PRA),**
- **Registration Points**,
- **subscribers**,
- **relying parties**.

CERTUM provides certification services to all private and legal entities accepting the regulations of the present Certification Practice Statement. The purpose of these practices (including key generating and certificate issuance rules as well as information system security) is to convince the users of CERTUM services that declared credibility levels of issued certificates are the reflection of certification authorities' practices.

## 1.3.1. Certification Authorities

There are the following root certification authorities of CERTUM (Root CAs):

- **Certum CA**
- **Certum Trusted Network CA**,
- **Certum Trusted Network CA 2** and
- **Certum Trusted Network CA EC**

All intermediate certification authorities are subordinated to their roots.

At present, **Certum Trusted Network CA 2** and **Certum Trusted Network CA EC** roots do not provide certification services.

#### 1.3.1.1. CERTUM Root Certification Authorities

CERTUM root certification authorities can register and issue certificates only to the subordinate certification authorities and the authorities issuing electronic confirmation of non-repudiation.

**Certum CA**, **Certum Trusted Network CA, Certum Trusted Network CA 2** and **Certum Trusted Network CA EC** operate on the basis of the self-certificates issued by themselves. In such self-certificate, the extension **certificatePolicies** is not placed, which should be interpreted as lack of limits to the set of **certification paths**[9], to which **CERTUM root** certificates can be attached.

**Certum CA, Certum Trusted Network CA, Certum Trusted Network CA 2** and **Certum Trusted Network CA EC** provide certification services to:

- themselves (issues and renews self-certificates),
- subordinated certification authorities
- **,**the entities delivering on-line certificate status verification (OCSP) services and other entities providing services of non-repudiation (e.g. time-stamping service).

[9] See **Glossary**

### 1.3.1.2. Intermediate Certification Authorities

Intermediate certification authorities issue certificates to its subscribers in compliance with the policies which identifiers are stated in Table 1.3.

| Certification policy | Certification policy identifier |
|---|---|
| Certum Level I CA | 1.2.616.1.113527.2.2.1 |
| Certum Level II CA | 1.2.616.1.113527.2.2.2 |
| Certum Level III CA | 1.2.616.1.113527.2.2.3 |
| Certum Level IV CA | 1.2.616.1.113527.2.2.4 |
| Certum Global Services CA | 2.5.29.32.0 (anyPolicy)10 lub<br>1.2.616.1.113527.2.2.911 |
| Certum Global Services CA SHA2 | 1.2.616.1.113527.2.5.1.9 |
| Certum Extended Validation CA,<br>Certum Extended Validation CA SHA2 | 1.2.616.1.113527.2.5.1.1 |
| Certum Organization Validation CA SHA2 | 1.2.616.1.113527.2.5.1.2 |
| Certum Digital Identification CA SHA2 | 1.2.616.1.113527.2.5.1.6.11<br>1.2.616.1.113527.2.5.1.6.12<br>1.2.616.1.113527.2.5.1.6.13<br>1.2.616.1.113527.2.5.1.6.14 |
| Certum Domain Validation CA SHA2 | 1.2.616.1.113527.2.5.1.3 |
| Certum Code Signing CA,<br>Certum Code Signing CA SHA2 | 1.2.616.1.113527.2.5.1.4,<br>2.23.140.1.4.1 |
| Certum Extended Validation Code Signing CA SHA2 | 1.2.616.1.113527.2.5.1.7<br>2.23.140.1.3 |
| Certum Class 1 CA,<br>Certum Class 1 CA SHA2 | 1.2.616.1.113527.2.5.1.5 |
| WoSign EV SSL CA<br>WoSign OV SSL CA<br>WoSign Code Signing CA<br>WoSign DV SSL CA | 1.2.616.1.113527.2.5.1.13.1<br>1.2.616.1.113527.2.5.1.12.2<br>1.2.616.1.113527.2.5.1.14.4<br>1.2.616.1.113527.2.5.1.15.3<br>2.23.140.1.2.1 |
| Yandex CA | 1.2.616.1.113527.2.5.1.10.2 |
| Certum Global Services CA SHA2 | 1.2.616.1.113527.2.5.1.9 |
| GIS CA | 1.2.616.1.113527.2.5.1.9.1.3 |
| nazwaSSL | 1.2.616.1.113527.2.5.1.9.2.3 |
| Shoper® SSL | 1.2.616.1.113527.2.5.1.9.3.3 |
| SpaceSSL CA | 1.2.616.1.113527.2.5.1.9.4.3 |
| www.lh.pl | 1.2.616.1.113527.2.5.1.9.5.3 |
| Certyfikat SSL | 1.2.616.1.113527.2.5.1.9.6.3 |
| 4fastssl.com | 1.2.616.1.113527.2.5.1.9.7.3 |
| TrustAsia DV SSL CA - C3 | 1.2.616.1.113527.2.5.1.9.8.3 |
| TrustAsia OV SSL CA - C3 | 1.2.616.1.113527.2.5.1.9.9.2 |
| TrustAsia EV SSL CA - C3 | 1.2.616.1.113527.2.5.1.9.10.1 |

[10] Certum Global Services CA and Certum Global Services CA SHA2 enter in the certificates issued to accredited certification authorities the **certification policy identifier** 2.5.29.32.0 (anyPolicy). In turn, all the certificates in the certification path between the certificate of an accredited authorities and the certificate of end-entities must bear the **certification policy identifier** established on the basis of the tree node identifiers of the value of 1.2.616.1.113527.2.2.9. An example of such a policy identifier is the policy value 1.2.616.1.113527.2.2.9.1. In special cases CERTUM may issue certificates for accredited certification authorities from main root CA under ctnDomena domain.

[11] According to the certification policy Certum Global Services CA and Certum Global Services CA SHA2 issues certificates to all other authorities that are not a certification authorities.

| | |
|---|---|
| TrustOcean Certification Authority | 1.2.616.1.113527.2.5.1.9.11.3,<br>1.2.616.1.113527.2.5.1.9.11.2 |
| GDCA TrustAUTH R4 DV SSL CA G2 | 1.2.616.1.113527.2.5.1.9.12.3 |
| GDCA TrustAUTH R4 OV SSL CA G2 | 1.2.616.1.113527.2.5.1.9.13.2 |
| GDCA TrustAUTH R4 EV SSL CA G2 | 1.2.616.1.113527.2.5.1.9.14.1 |
| GoGetSSL Domain Validation CA SHA2 | 1.2.616.1.113527.2.5.1.9.15.3 |
| GoGetSSL Business Validation CA SHA2 | 1.2.616.1.113527.2.5.1.9.16.2 |
| GoGetSSL Extended Validation CA SHA2 | 1.2.616.1.113527.2.5.1.9.17.1 |

*Certificates, issued to the intermediate certification authorities and certificates issued by* ***Certum CA*** *or* ***Certum Trusted Network CA*** *to other authorities and entities contain the extension* ***certificatePolicies****.*

The authorities do not include any other identifiers of certification policies in the issued certificates.

*The following authorities can issue certificates to other certification authorities:* ***Certum Level I CA, Certum Class 1 CA SHA2*** *(test certification authority) and* ***Certum Global Services CA*** *and* ***Certum Global Services CA SHA2*** *(commercial certification authorities). However, certificates issued to other CAs are subject to the exclusive control of CERTUM. Also, issuing of end user certificates by these authorities is exclusively under control of the CERTUM. None of these authorities to which have been issued certificates cannot act as Registration Authority, either themselves issue certificates to end users.*

The Primary Registration Authority and Registration Points fully cooperate with CERTUM. They represent CERTUM in contacts with subscribers and act within the rights delegated by the certification authorities, concerning customers' identification and registration. The functioning and the scope of duties of registration authorities depend on the credibility of a certificate issued to subscribers and related certification policy.

Intermediate certification authorities are adjusted to issuing certificates to:

- employees of CERTUM, the Primary Registration Authority operators and Registration Points operators,
- the certificate users who wish to ensure security and credibility for their electronic mail, stored data and service servers (e.g. web shops, information and software libraries),
- the hardware devices (physical and logical) owned by a private and a legal entities;
- the other certification authorities (applicable to **Certum Level I CA, Certum Class 1 CA SHA2, Certum Global Services CA** and **Certum Global Services CA SHA2** authorities).

## 1.3.2. Registration Authorities

The Primary Registration Authority receive, verify and approve or reject applications for registration, issuance, rekey, renewal, or revocation of the certificate. Verification of applications intends to authenticate (on the basis of the documents enclosed to the applications and authentication of the Applicant's ownership or control of the certified Distinguished Name) the requester, as well as the data included in the application. The Primary Registration Authority may submit requests – to an appropriate certification authority – for cancellation of a subscriber registration and a subscriber's certificate revocation. The level of precision of subscriber's identity identification results from the very subscriber's needs and it is imposed by the level of certificate the issuance of which the subscriber requests (see chapter 3). In the case of the simplest identification, the Primary Registration Authority checks the correctness of submitted

email address. The most precise identification may require the subscriber's attendance in person to the Registration Point and submission of suitable documents. This identification might be achieved either automatically or manually by the Primary Registration Authority operator.

The Primary Registration Authority functions on the basis of the authorization by an appropriate certification authority belonging to **certum** or **ctnDomena** domains; the authorization concerns the identification of the subscriber and the verification of the subscriber's right to use the Distinguished Name.

In the case of Registration Points managed by entities other than Asseco Data Systems S.A. (external Registration Points), a detailed scope of duties of the Points and their operators may be specified in an additional agreement between external Registration Points and such Points, this Certification Practice Statement and the procedures concerning operating of the Registration Points, which are an integral part of the agreement.

*Any organization (legal entity) might function as the Registration Point and might be accredited by CERTUM, provided that it submits an appropriate application to the Primary Registration Authority and fulfils other conditions stated in the Certification Practice Statement.*

The list of registration authorities currently accredited by the Primary Registration Authority is available in the repository at: http://www.certum.eu

The main difference between the Primary Registration Authority and the external Registration Points is that the Registration Point, unlike the Primary Registration Authority, cannot accredit other Registration Points and register new certification authorities. Moreover, Registration Points do not have the rights to verify the subscriber's right to use the Distinguished Name.

The Primary Registration Authority registers Registration Points, new certification authorities and subscribers (private and legal entities, devices). 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 the Primary Registration Authority. Additionally, the Primary Registration Authority approves of distinguished names of Registration Points.

*The Primary Registration Authority is located at the seat of CERTUM. Contact addresses with the PRA are listed in chapter 1.5.2*

## 1.3.3. Subscribers

Any private or legal entities and hardware devices they own could be the subscriber of CERTUM, provided that they fulfil the terms of the definition of a subscriber.

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

*CERTUM offers certificates of a different types and of a different levels of credibility. The subscribes should decide what type of certificate is the most suitable for their needs (see chapter 1.4).*

## 1.3.4. Relying Parties

A relying party, using CERTUM services can be any entity that decides on the acceptance certificate issued by CERTUM in reliance on the validity of the connection between subscriber's

identity and his/her/its public key (confirmed by one of the certification authorities subordinate to **CERTUM**.

The relying party is responsible for verification of the current status of subscriber's certificate. Such decision must be taken any time when the relying party wishes to use a certificate to verify an electronic signature, to identify the source or the author of a message, or to create a secret communication channel with the owner of a certificate. The relying party should use the information in a certificate (e.g. identifiers and qualifiers of certification policy) to state whether a given certificate was used in accordance with its declared purpose.

## 1.3.5. Other parties

As a part of the CERTUM there are also entities that provide complementary services for issuing and revoking certificates.

### 1.3.5.1. Certum Time-Stamping Authority

**Certum EV TSA SHA2**, operating within **ctnDomena** domain (Table 1.1) is a part of CERTUM infrastructure.

The time-stamping authority issues timestamp tokens in accordance with ETSI[12] recommendation. Each timestamp token contains the identifier of the policy, under which the token has been issued (identifier value is described in Table 1.4 and chapter 7.3). Timestamp tokens are signed only with a private key issued especially for time-stamping service.

Tab. 1.3 **Certum EV TSA SHA2** identifier, included in timestamp tokens

| Token name | Certification Policy Identifier | Compliance |
|---|---|---|
| Timestamp token | 1.2.616.1.113527.2.5.1.11 | RFC 3161 |
| | | ETSI TS 101 861,<br>Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates,<br>Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, |

Tokens, issued in accordance with policy described in Tab. 1.4, are used primarily in securing long-term electronic signatures[13] and global transactions.

**Certum EV TSA SHA2** employs solutions which guarantee synchronization with the international time source (Coordinated Universal Time – UTC), with the accuracy more than 1 second.

### 1.3.5.2. Certificate Validation Service

CERTUM, beside standard certificate status verification based on Certificate Revocation List (CRL), offers the online services – based on the Online Certificate Status Protocol (OCSP). This service is provided by a group of certificate status validation authorities with same name **Certum Validation Service**. Each certification authority within **certum** and **ctnDomena** domains has its

12 ETSI TS 101 861 *Time stamping profile*, August 2001

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

own, dedicated certificate status validation authority. All Certum's certificate status validation authorities operate using the authorized responder mode.

## 1.4. Certificate Usage

Certificates allow entities to prove its identity to other participants in electronic transactions. Certificates can be used to protect an electronic information exchange. Certificate applicability range states the scope of permitted certificate usage. This scope defines the character of certificate applicability (e.g. confidentiality, integrity or authentication).

Certificates issued by CERTUM can be used to process and secure information (including authentication) of various credibility levels. Information credibility level and information vulnerability to **breach**[14] should be evaluated by the subscriber. CERTUM certification authorities issue certificates in three classes with different levels of credibility. The levels are described in **Certification Policy of CERTUM's Certification Services**.

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

CERTUM is the member of CAB/Forum and provides its services in accordance with the requirements of the latest published version of:

- **Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates**,
- **Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates** and
- **Guidelines For The Issuance And Management Of Extended Validation Certificates**.

In the event of any inconsistency between this document and the CAB/Forum requirements, the requirements take precedence over this document.

In addition, from the date of 01/02/2017 all services related to the issuance, revocation and managing code signing certificates are provided in accordance with the **Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates**.

CERTUM also issues certificates in accordance with the **Certum Global Services CA** and **Certum Global Services CA SHA2** policy, which has defined sensitivity level that depends on the certain certificate type.

### 1.4.1. Certificate Types and Recommended Applicability

CERTUM issues the following basic types of certificates with different applicability ranges. They are:

1) **personal certificates** – that allow encryption and signing of electronic mail, and securing electronic documents (electronic mail based on S/MIME or PGP standard),

[14] See **Glossary**

2) **SSL and EV SSL certificates of server authentication confirmation** – they are used by global or extranet services operating in the shield of SSL/TLS/WTLS protocol,
3) **certificates used for authenticating subscribers** (individuals and legal entities, hardware devices) – used e.g. in SSL/TLS/WTLS protocol,
4) **certificates confirming certificate status** – they are issued to the servers functioning in accordance with OCSP protocol and issuing tokens of the current status of a verified certificate,
5) **certificates for encrypting** – applied to the security of files, folders and file systems,
6) **certificates for code signing** – applied by computer programmers to secure software from forgery,
7) **certification authorities certificates** – the usage is not restricted to the defined range; the range might result from the private key usage stated in a certificate (see the field **keyUsage**, chapter 7), or from its roles (e.g. a subscriber, a certification authority or other authority delivering PKI services); this type also comprises certification authorities operational certificates[15],
8) **timestamping authorities certificates** – they are issued to servers which as a response for subscriber's request issue timestamp tokens binding any data (documents, messages, electronic signature, etc.) with timestamp, which allow for alignment (unambiguous in particular cases) of data,

The certificates issued in accordance with any of the certification policies can be used with applications that meet at least the following requirements:

- they appropriately manage private and public keys, as well as their application and sending of them,
- certificates and the public keys associated with them are applied in compliance with their declared purpose that is confirmed by CERTUM,
- have built-in mechanisms of certificate status verification, certification path creation and validity control (signature validity and expiry date, etc),
- delivers appropriate information of certificate and application condition to a subscriber, etc

CERTUM offers its customers certificates in all types of applications described above. Groups of certificates are issued by the following intermediate certification authorities:

| Certificates | Cerification Authority |
|---|---|
| Test certificates | Certum Level I CA,<br>Certum Class 1 CA,<br>Certum Class 1 CA SHA 2, |
| Personal certificate with email address validation | Certum Level II CA,<br>Certum Domain Validation CA SHA2 |
| Personal certificates with DN data validation | Certum Level IV CA, |

[15] Operational certificates are universal certificates issued to certification authorities. These certificates enable certification authorities to operate and comprise the certificates applied to: verification of a signature in messages, data encryption, verification of signatures created on issued certificates and CRL's, key exchange, key agreement and non-repudiation services (see the certificate extension **keyUsage**).

| | |
|---|---|
| | Certum Digital Identification CA SHA2,<br>Certum Organization Validation CA SHA2 |
| SSL certificates with domain validation (DV) | Certum Level II CA,<br>Certum Domain Validation CA SHA2 |
| SSL certificates with organization validation (OV) | Certum Level IV CA,<br>Certum Organization Validation CA SHA2 |
| SSL Extended Validation certificates (EV) | Certum Extended Validation CA,<br>Certum Extended Validation CA SHA2 |
| Code Signing | Certum Code Signing CA,<br>Certum Code Signing CA SHA2 |
| Code Signing Extended Validation certificates | Certum Extended Validation Code Signing CA SHA2 |
| VPN and IPSec Client | Certum Level II CA,<br>Certum Level IV CA, |
| Certificates issued by affiliated CERTUM partners | Certum Global Services CA,<br>Certum Global Services CA SHA2 |

### 1.4.2. Prohibited Applications

It is forbidden to use the CERTUM certificates in a manner inconsistent with their declared purpose and in the applications that do not fulfil the minimal requirements specified in chapter 1.4.1

In addition, certificates of subscribers (except for certificates issued under the certification policy CERTUM Global Services CA and Certum Global Services CA SHA2) cannot be used as the certificates of the certification authorities. In other words, they cannot be used to verify the certificates of the certification authorities and certificates of other entities that provide certification services.

## 1.5. Certification Practice Statement management

Every version of the Certification Practice Statement is in force (has a **current** status) up to the moment of publication and approval of its new version (see chapter 9.10). A new version is developed by the **CERTUM employees** and with the status **requested for comment** supplied to approval questionnaire. Upon reception and inclusion of the remarks from the approval questionnaire, the new version of Certification Practice Statement is supplied for approval. During the CPS approval process, new version of the document has the status **under approval**. After completion of the approval procedure, a new version of the Certification Practice Statement is marked with the status **valid**.

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

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

Further rules and requirements concerning Certification Practice Statement management are described in chapter 9.10.

### 1.5.1. The organization responsible for administration of the document

Asseco Data Systems S.A.

Podolska Street 21

81-321 Gdynia, Poland

### 1.5.2. Contact

Asseco Data Systems S.A.

Podolska Street 21

81-321 Gdynia, Poland

Certum – Powszechne Centrum Certyfikacji

Bajeczna Street 13

71-838 Szczecin, Poland

### 1.5.3. The operators defining the validity of the principles set out in the document

CERTUM team, directly administers the present Certification Practice Statement, the Certification Policy and other documents concerning PKI services delivered by CERTUM. Above mentioned Team also test the compliance of the Certification Practice Statement and the Certification Policy. All inquiries and comments concerning the contents of the mentioned documents should be directed to the address given in the chapter. 1.5.2.

### 1.5.4. The CPS approval procedure

The comment period for any material amendments to the Certification Practice Statement incorporated on the basis of suggestions made on the stage of its acceptance questionnaire (method described in chapter 9.10) is ten (10) days starting on the date on which the amendments are published in the repository with the status **under approval**. After this period the Certification Practice Statement will become a governing document of the certification policy, respected by all subscribers of CERTUM, and the status of the version is changed into **valid**.

The decision to publish a new version of the Certificate Practice Statement shall be taken by Chief of CERTUM.

## 1.6. Definitions and abbreviations

Definitions and abbreviations used in this document can be found at the end of this document.

# 2. Responsibility for publishing and the repository

## 2.1. Repository

Repository is a collection of publicly available catalogues which is managed and controlled by CERTUM.

*For the purposes of CERTUM's non-qualified certificate services there is the only one common repository for subscribers of domains* ***certum*** *and* ***ctnDomena*** *and for all certificate authorities which operates within these domains.*

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

- ensure that all certificates published in the repository belong to the subscribers stated in a certificate and the subscribers approved of their certificates in accordance with the requirements specified in chapters and 4.4,
- make sure that certificates of the certification authorities, registration authorities and registration points belonging to **certum** domain and **ctnDomain**, and subscribers' certificates (upon their prior approval) are published and archived on time,
- publish and archive Certification Policy, Certification Practice Statement, templates of subscriber and relying party agreements,
- give access to the information concerning certificates status by publishing of CRL's, OCSP server or questions submitted by means of HTTP protocol,
- secure constant access to information in the repository for certification authorities, registration authorities, subscribers and relying parties,
- publish CRL's and other information swiftly and in accordance with the deadlines specified in this document,
- secure safe and controlled access to the information in the repository.

All subscribers, except for relying parties, have an unlimited access to the whole information in the repository. Limitations on relying parties' access usually concern subscribers' certificates.

## 2.2. Information Published by CERTUM

The whole information published by CERTUM is available in the repository at: http://www.certum.eu

The information consists of:

- the Certification Policy,
- the Certification Practice Statement,
- templates of agreements with subscribers,
- the certificates of subscribers, registration authorities and certification authorities ,

- Certificates Revocation Lists (CRLs); the CRLs are accessible at the so called CRL distribution points, whose addresses are set in each certificate issued by CERTUM; the basic point of CRLs distribution is the repository at: http://crl.certum.pl,
- records (as detailed as possible) of audits carried out by an authorized institution,
- supplementary information, e.g. announcements and notices.

Certificates belonging to certification authorities, registration authorities and subscribers are accessible on request submitted to the server (http://www.certum.pl) and – additionally they may also be published in directory services (ldap://directory.certum.pl) Besides periodical publication of the revoked certificates, the repository gives the on-line access to the up-to-date information regarding a certificate status, by means of WWW site (address http://www.certum.pl) or OCSP (address http://ocsp.certum.pl) service.

## 2.3. Frequency of Publication

CERTUM publications below are issued with the following frequency:

- the Certification Policy and the Certification Practice Statement – see chapter 9.12,
- certificates of the certification authorities functioning within CERTUM – upon every issuance of new certificates,
- the registration authorities certificates – upon every issuance of new certificates,
- subscribers' certificates – upon every issuance of new certificates, on subscribers' prior approval,
- the Certificate Revocation List – see chapter 4.9.7,
- the records of audits carried out by an authorized authority – every time CERTUM receives them,
- supplementary information – upon every updating of it.

## 2.4. Access to Publications

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

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

On discovering the breach of information integrity in the repository, CERTUM shall take appropriate actions intending to re-establish the information integrity, impose legal sanctions in relation to the abusers, notify the affected entities and compensate their loss.

# 3. Identification and Authentication

This chapter presents the general rules of subscribers' identity verification applied by CERTUM to certificate issuance. The rules are based on particular types of information that is included in certificates and they specify the means indispensable for assuring that the information is precise and credible at the time of issuing a certificate.

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

## 3.1. Names

### 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 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.500). 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.500 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 the subscriber, an alternative name of the subscriber is used in CERTUM certificates. The name can also contain the subscriber's electronic mail address that is in accordance with the recommendation RFC 822.

In the case of SSL certificates CERTUM employs an automated process that prevent the release of certificate with a wildcard character (*) which occurs in the first label position to the left of the top level domain.

For requests for internationalized domain names (IDNs) in certificates, CERTUM performs domain name owner verification to detect cases of homographic spoofing of IDNs. CERTUM employs a manual process to find the risk of a particular domain. A search failure result is flagged for manual review and the Registration Authority manually rejects the certificate request.

The names of directories where certificates, CRLs and the Certification Policy are retained, as well as the names of CRLs distribution points, comply with the recommendation RFC 1738 and names schemes applied by the protocol LDAP (see RFC 1778).

The whole information, submitted in subscriber's application for registration and included in the certificate is accessible for the public. The list of data included in a certificate is in accordance with the recommendation X.509 v.3 and is presented in chapter 7 (see also chapter 3.1.2).

### 3.1.2. Need for Names to be Meaningful

The names included in the subscriber's Distinguished Name have their meaning in Polish or other congress language.

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

The DN may consists of the following fields (descriptions of a field follows its abbreviated name that complies with the recommendation RFC 3280 and X.520):

- **field C** – international abbreviation of the country name (**PL** for Poland),
- **field ST** – the region/province where the subscriber lives or runs his/her business,
- **field L** – the city where the subscriber lives or has a seat,
- **field 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 E** – the subscriber's email address,
- **field UN** – router's or network device name,
- **field D** – subscriber's additional distinguished name.

According to the **Guidelines for the Issuance and Management of Extended Validation Certificates** requirements the additional attributes in the DN of EV SSL certificates are included.

Subscriber's DN must be confirmed by a registration authority operator and approved by a certification authority.

### 3.1.3. Anonymity of Subscribers

CERTUM does not issue certificates and other credentials to ensure the anonymity of the subscriber's data (e.g. name).

### 3.1.4. Rules for Interpreting Various Names Forms

The interpretation of the fields provided in the certificates issued by CERTUM is in compliance with the certificates profile described in chapter 7 of this CPS. In creating and interpreting of DNs, the recommendations specified in chapter 3.1.2 of this document are employed.

### 3.1.5. Names Uniqueness

The Subscriber's DN is suggested by the subscriber. If the DN is in accordance with general requirements stated in chapter 3.1.1 and 3.1.2 the submitted proposition is initially accepted.

To provide the uniqueness of issued certificates, CERTUM assigns a unique (within its domain) serial number for each issued certificate. Serial number, combined with subscriber's DN, precisely and uniquely distinguishes a specific subscriber.

### 3.1.6. Recognition, authentication and role of trademarks. Name Claim Dispute Resolution Procedure

Names that are not owned by a subscriber cannot be used in his/her/its applications. In the event of any question or doubt, the applicant is obliged to attach documents proving their ownership.

CERTUM checks if a subscriber is entitled to use the name placed in the application for registration but 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 registration does not possess a **valid certificate**[16] issued by any authority issuing certificates and affiliated by CERTUM.

Registration comprises a number of procedures which allow a certification authority – prior to issuing a certificate to a subscriber – to gather authenticated data concerning a given entity or identifying this entity.

Every subscriber is subjected to the registration process only once. After the verification of data supplied by a subscriber, the subscriber is included on the list of the authorized users of CERTUM services and supplied with a public key certificate.

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

- remotely fill in the registration form on WWW site of CERTUM or submit data required for issuing certificate (e.g. as an Order),
- generate RSA or DSA asymmetric key pair and supply a registration authority with the proof of the possession of a private key (see chapter 3.2.1); optionally, a subscriber can charge a certification authority with generating a key pair,
- suggest a distinguished name (**DN**, see chapter 3.1.1),
- optionally attend a registration authority and provide required documents (if it is required by a given certification policy on the basis of which a certificate is being issued),
- optionally (depending on the type of certificate being issued) make an agreement with Asseco Data Systems S.A. about delivery of services by CERTUM.

*Registration might require subscriber or a representative authorized by the subscriber to personally attend a registration authority. Nevertheless, CERTUM permits (for specified certificate types) sending applications for registration by mail, electronic mail, WWW sites, etc.; examination of the applications does not necessitate a physical contact with the requester.*

[16] See **Glossary**

### 3.2.1. Prove of Possession of Private Key

The basic proof of possession of private key is an electronic signature made on requests for registration, certification and modification of data and on requests for key/certificate renewal, submitted to the registration authority or certification authority.

The proof is considered as a Certificate Signing Request (CSR) in PKCS#10 format or as a Signed Public Key and Challenge (SPKAC).

### 3.2.2. Authentication of Legal Entity's Identity

CERTUM must confirms that the organization whose name is in the content of the certificate actually existed at the time of issuing the certificate.

The verification is performed based on the Qualified Independent/Government Information Sources e.g. publicly available records of companies/organizations registries.

CERTUM is required to request suitable documents from the subscriber, which without any doubts confirm the identity of the legal entity on whose behalf the application is submitted and the private entity that represent it (or submits the application).

The registration authority may collect the data required for identification by its own, e.g. through publicly available databases. Authentication of legal entity's identity has two purposes. The first purpose is to prove that at the time of application examination the legal entity stated in the application existed; the second purpose is to prove that a private entity applying for a certificate or receiving it is authorized by this legal entity to represent it. Submitted documents (or collected data) should prove:

- the name of subscriber,
- the legal existence of subscriber ,
- the address of subscriber
- the right of subscriber or certificate administrator to act on behalf of the institution or legal entity.
- the registration authority operator may verify the registration of the domain in publicly available WHOIS services.

There are two basic ways of legal entity's identity authentication. The first one requires the legal entity's authorized representative's personal attendance in the registration authority, or the registration authority representative's presence in person in the legal entity's seat (specified in the application). In the second case, the identity can be authenticated on-line by means of messages exchanged directly with the certification authority or its agent.

If the subject:countryName field is present, then CERTUM verify the country associated with the Subject using the ccTLD of the requested Domain Name.

Detailed requirements on the identification documents and their verification are specified on the https://www.certum.pl.

*The registration authority is committed to verify the correctness and truthfulness of all data provided in an application. In the case of EV SSL and EV Code Signing certificates additional procedure shall be applied according to* ***Guidelines for the Issuance and Management of Extended Validation Certificates*** *and* ***Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates*** *requirements.*

In the case of email certificates, the registration authority verifies an email address. The aim of this action is to receive by the subscriber an authentication data sent to the address which has previous placed in the certification request.

In the case of certificates issued for devices, authentication may be accomplished by verifying access to the domain placed in the certificate request. CERTUM may verify the subscriber's right to use the domain name by the procedure during which some verification element indicated by CERTUM is placed on destination server or when the Subscriber is required to be able to answer an e-mail sent by CERTUM to his/her/its address.

The process of authentication is recorded. The type of recorded information and actions depend on the credibility level of a certificate which is a subject of the application and it concerns:

- the identity of registration authority operator verifying the identity of subscriber,
- submission of the statement by the operator expressing that he/she verified the requester's identity in accordance with the requirements of the present Certification Practice Statement,
- day of the verification,
- operator's identifier and subject's identifier in the case of subject's attendance in person in the registration authority (provided the subject has been supplied with such identifier),

If the legal entity is not capable of effective authenticating of its application or upon certification authority request, an authorized representative of the entity must attend in person the registration authority to confirm the application.

In the case where the entity already possesses the certificates issued by CERTUM, which have been subjected to identity verification required by the specific sensitivity level, further identity verification may be based on previous documents and data.

## 3.2.3. Authentication of Private Entity's Identity

Authentication of private entity's identity has two purposes. The authentication must prove that (1) data provided in an application concern an existing private entity and (2) the requester is indeed the private entity stated in the application. Procedures and requirements for private entity identity authentication are the same as for legal entities. The only difference is that the existence of the legal entity and the right to act on its behalf verification is amended by verification of the right to use distinguished names other that name and surname. An email address verification is conducted in similar way as in section 3.2.2.

## 3.2.4. Non-verification data

CERTUM validates all information to be included within the subject DN of a certificate.

## 3.2.5. Validation of Authority

In the case where a certificate request contains the name of the organization (O), then this should be interpreted as the person who requests for a certificate is affiliated or authorized to act on behalf of the organization. This means that CERTUM verifies that the individual who requests for a certificate was an employee organization or its subcontractor at the time of issuance of the certificate and has the right to act on behalf of the organization; the scope of authorization and the period of validity may be regulated by separate legislation or the relying party in the course of verification a digital signature or decryption the received document and is outside the scope of liability of CERTUM; individual's identity and authorization may be checked

by CERTUM on the basis of available records or database, contact by phone or e-mail to the organization.

## 3.2.6. Authentication of Domain Name

For all SSL certificates, authentication of the Applicant's ownership or control of all requested Domain Name(s) is done using one of the following methods:

- by uploading file with the specified name to the directory /.well-known/pki-validation of the domain;
- by uploading specific metadata to the DNS text record of the domain;
- by direct confirmation with the contact listed by the Domain Name Registrar in the WHOIS record or Domain Authorization Document provided to CERTUM by the Domain Name Registrar or Domain Name Registrant directly – only if CERTUM authenticates the subscriber's identity and the authority of the subscriber representative under the chapter 3.2.2.;
- by successfully replying to a challenge response email sent to one or more of the following email addresses: webmaster@domain.com, postmaster@domain.com, admin@domain.com, administrator@domain.com, hostmaster@domain.com.

CERTUM only uses the WHOIS records linked to on the IANA root database and the ICANN approved registrars.

## 3.2.7. Criteria for Interoperation

CERTUM may provide or be subject to the interoperation services that allow respectively other certification service providers to be able to interoperate with the CERTUM by certifying that entities or allow CERTUM to be able to interoperate with other certification service providers Accreditation is carried out at the request of the company when it meets the following conditions:

- the accredited entity enabled to interoperate in this way will comply with the CP and the CPS as supplemented by additional policies when required. Both documents cannot be in conflict with this document;
- data communication network and the organizational structure of the accredited entity obtain a favorable opinion of the authorized CERTUM units or other auditor accepted by CERTUM;
- service or services provided by the accredited entity shall ensure interoperability with the corresponding services provided by CERTUM,
- the agreement shall constitute the business relationship between the accredited entity and CERTUM

Accredited entities shall receive certificates for the provision of adequate services. These certificates are issued by **Certum Global Services CA** and **Certum Global Services CA SHA2**. Such certificates may be revoked if an annual audit results – carried out by the authorized unit of CERTUM or other acceptable auditors – show a gross negligence accredited company and which are not remedied within the period specified by the auditor.

In supporting users who need certificates for code-signing kernel-mode binary files for Microsoft Windows, the certification authority Certum Trusted Network has been certified by the Microsoft Code Verification Root certification authority. Cross-certificate is available in the repository.

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

If a subscriber has an active certificate (one that is neither expired nor revoked)) she/he/it may request for a new certificate. The new certificate may be issued for a new key pair, generated by the subscriber or CERTUM (rekey) or the current key pair (recertification) CERTUM also permits the modification of the certificate due to changes in the information in an existing certificate and in the public key (more precisely – to the subscriber keys, see chapter 3.3.1.3 and 4.8).

Authentication of the identity of subscribers who apply for rekey, renewal or modification of certificates must be performed by a registration authority operator in the following cases:

- the application has been authenticated only by means of password,
- the data set in the certificate have been modified,
- on every request of the certification authority operator,
- when it concerns key certification resulting in a certificate issued for the first time to a given subscriber according to a new certification policy.

Subscribers submitting applications directly to the certification authority are authenticated by this authority on the basis of the electronic signature authenticity and the public key certificate associated with this signature or by other methods accepted by both parties and complying with this document.

## 3.3.1. Subscriber Identity Authentication in regular updating of key

### 3.3.1.1. Rekey

Rekey might be performed by the 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, validity period and the certification authority signature (see chapter 4.7)

If the subscriber is to send a complete and digitally signed application or provide the correct password, an update to the key issue of the new certificate may be automatic, provided that the new certificate is the same type as the certificate currently held by the subscriber and is issued according to the same certification policy.

It is possible to update the keys in automatic mode within 30 days from the date of the beginning of the period of validity of the certificate. The newly released certificate has the same expiration date as the previous certificate.

In other cases, verification of the identity of the subscriber requesting rekey is carried out on the basis of the valid documents submitted for modified (renewed) certificate.

### 3.3.1.2. Recertification

Subscribers or certification authorities use recertification if he/she/it already possess a certificate and the private key associated with it, and wishes to continue to use the same key pair. The new certificate, created as the result of renewal, consist in the same public key, the same subject name and other information originating from the previous certificate, but the validity

period, serial number and issuer signature varies from respective data in the previous certificate. (See chapter 4.6)

Recertification applies only to certificates which were not revoked and the information contained within the certificate are intact.

Recertification requests may be processed in automatic mode. It is possible to recertificate in automatic mode within 30 days from the date of the beginning of the period of validity of the certificate. The newly released certificate has the same expiration date as the previous certificate.

#### 3.3.1.3. Certificate Modification

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

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 the registration authority (see chapter 4.8).

Only valid certificates that have not been revoked and which subscriber's name and other attributes have not changed are subject to modification.

### 3.3.2. Subscriber Identity Authentication in Rekey after Revocation

If a subscriber upon a certificate revocation does not have an active (within a given certification policy) certificate and applies for renewal, the application must be confirmed by the registration authority or the certification authority operator. The subscriber's identification and authentication may be performed analogically to the case of initial registration (see chapter 3.2) or may be based of previously submitted documents.

Every subsequent application for certificate renewal, certificate modification or rekey is examined in the standard manner (see chapter 4.7)

## 3.4. Subscriber's Identity Authentication in Certificate Revocation

Applications for revocation can be submitted by e-mail directly to an appropriate certificate issuer or indirectly to a registration authority. It is possible to submit non-electronic application.

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

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

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

Authentication and identification of the subscriber in the registration authority is performed analogically to initial registration (see chapter 3.2) or rekey (see chapter 3.3.1.1). Authentication of the subscriber in the certification authority consists in verification of application authentication or identity of the requester.

Detailed procedure of revocation is disclosed in chapter 4.9.3.

# 4. Operational Requirements

Basic certification procedures are presented below. Every procedure starts with a subscriber's submitting a suitable application indirectly (upon prior confirmation of the application by a registration authority) or directly to certification authority. On the basis of the application, the certification authority takes an appropriate decision about the delivery/rejection of the requested service. Submitted applications should contain information necessary for correct identification of the subscriber.

CERTUM provides access to the following basic services: registration, certification, certificate renewal, rekey, certificate modification and revocation.

If the submitted application contains a public key, the key must be prepared in the way that – disregarding of applied certification policy – cryptographically binds the public key with other data listed in the application, particularly with the subscriber's identity data.

The application might contain, instead of the public key, subscriber's request to generate an asymmetric key pair on his/her/its behalf. It might be carried out in the certification authority or the registration authority. Upon generating, the keys are safely submitted to the subscriber.

## 4.1. Application Submission

Subscriber's applications are submitted directly to certification authority or indirectly by registration authority. Applications submitted directly might concern: certificate registration, certificate renewal, rekey and certificate revocation. Applications submitted indirectly concern: certificate registration and modification, although other applications connected with other certification services delivered by a certification authority are also permitted.

The registration authority operator has a double role: the role of subscriber and the role of person authorized to represent the certification authority. In the first case, the operator can submit the same applications as any other subscriber. In the second case, the operator can confirm application submitted by the subscribers and in well-founded cases create applications for revocation of certificates belonging to subscribers that violate the present Certification Practice Statement.

Applications are submitted by means of network protocols such as HTTP, S/MIME or TCP/IP, or in non-electronic form – e.g. Orders.

*CERTUM issues certificates solely on the basis of registration, modification, rekey, certificate renewal or certificate modification request.*

### 4.1.1. Who can submit applications

The requester of certificate can be any entity belonging to one of the following categories:

- an individual person, which is or will be the subject of certificate,
- an authorized representative of the legal person or institution, called an applicant,
- an authorized representative of the certification authority **certum** and **ctnDomena** domains or an authorized representative of the accredited external authority,
- an authorized representative of the Primary Registration Authority or the registration authority.

CERTUM does not issue certificates to entities that reside in countries where the law of Republic of Poland prohibit doing business.

In terms of **Guidelines for the Issuance and Management of Extended Validation Certificates** and **Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates**, the EV SSL and EV Code Signing certificates can only be issued to Private Organizations, Government Entities, Business Entities and Non-Commercial Entity subjects. CERTUM does not issue EV SSL and EV Code Signing certificates to the natural persons.

Before issuing the website authentication certificate, CERTUM compares the data from the certificate request with the internal database of the previously revoked certificates and rejected certificate requests. If the certificate was revoked or CERTUM rejected a given certificate request for users security reasons, the request for a new certificate may be rejected.

## 4.1.2. Application Processing and the relevant obligations

### 4.1.2.1. Subscribers certificates

All subscribers of certificates and all end users (including entities providing certification services except the issuance of certificates and revocation) should accept the commitments and guarantees defined in Terms of Use or Subscriber Agreement (see 9.6.3) and undergo the registration process that requires the implementation of the following:

- submission of an application which is completed and containing true and correct information;
- subscriber generates his/her/its key pair by himself/herself/itself. The generation may also be delegated to CERTUM
- in the case of self-generate a key pair subscriber should provide the public key to CERTUM directly or through the registration authority associated with CERTUM, and also prove possession of private key corresponding to public key submitted (see Chap. 3.2.1).

### 4.1.2.2. Certification Authority and Registration Authority certificates

The certification authorities and registration points, which provide services for, or under the authority of CERTUM and are not an organizational units of CERTUM must first enter into an agreement with CERTUM. The agreement, in addition to the rights and obligations of both parties, determine the identity of persons and their authorization to represent both parties during the execution of a contract. The person or persons authorized by the applicant should determine, before issuing a certificate, the distinguished name of the subject of certificate.

The keys and certificates of root certificates and sub-root certificates may be generated only during the Key Ceremony in which persons authorized by CERTUM must participate.

Based on the concluded agreement with the registration authority, certificates can be issued to eligible individuals and to their devices when necessary to provide services to the CERTUM.

### 4.1.2.3. Application for registration

An application for registration is submitted to the registration authority or directly to the certification authority by the subscriber and includes the following information:

- full name of the institution or the name and surname of the subscriber or certificate administrator,

- distinguished name whose structure depends on the subscriber's category (see chapter 3.1.2),
- identifiers: NIP (Tax Identification Number) or REGON (Business Entity Identification Number)/PESEL (Personal Identification Number),
- subscriber's postal address (state or province, postal code, city or town, building number and street, fax number),
- email address,
- the certificate type that the subscriber applies for,
- the identifier of certification policy on the basis of which the certificate is to be issued,
- the public key that is to be certified.

Depending on the content of the certificate and its class, some of the data mentioned above may be optional.

After authenticating the identity of the subscriber (see chap. 3.2.2, 3.2.3 and 3.2.5) and upon receipt of confirmation issued by the registration authority, the application is sent to the certification authority.

#### 4.1.2.4. Certificate renewal, rekey or modification application

An application of this type is submitted to the registration authority or directly to the certification authority by the subscriber. Applications are submitted to the registration authority in the following cases:

- directly upon certificate revocation,
- when the certificate which is supposed to be issued in accordance with a certification policy different than certificates currently owned by the subscriber,
- upon explicit demand of the registration authority operator.

If none of these conditions occurs, the subscriber might submit the application directly to the certification authority. Nevertheless, submission of the application to the registration authority is not prohibited.

The application for certificate modification, rekey or certificate renewal, must contain at least:

- the requester's (subscriber's) distinguished name,
- certificate type that the subscriber applies for,
- the identifier of certification policy on the basis of which the certificate is to be issued,
- the public key (previously used in the case of certificate renewal or modification or the new in the case of rekey) that is to be certified.

A part or whole of data contained in above application may be authenticated by application of an electronic signature, provided that the subscriber possesses a currently valid private key for the signature creation.

Upon authentication of the identity of subscriber (see chapters 3.2.2, 3.2.3 and 3.2.5) applying for registration and upon receipt of confirmation issued by the registration authority, the application is sent to the certification authority.

#### 4.1.2.5. Certificate Revocation Application

An application for certificate revocation is submitted by the subscriber to the registration authority or directly to the certification authority. Detailed requirements on the revocation request are presented in chapter 4.9.3.

In the moment of certificate revocation, registration authorities operators and subscribers are notified about this fact (e.g. by means of e-mail).

## 4.2. Application Processing

CERTUM accepts applications submitted individually and collectively. Applications might be submitted *on-line* and *off-line*.

*On-line* submission is performed by means of WWW pages of CERTUM server at: http://www.certum.eu. A subscriber, having visited a suitable site, fills in (in accordance with the instruction on that site) an appropriate application form and sends it to the certification authority. Applications for **Certum Level I CA** certificates are mostly processed automatically, whereas applications for certificates of other levels are processed manually – if the application requires the comparison of data included in the application with documents submitted to CERTUM or automatically if the comparison with CERTUM database is sufficient.

*Off-line* submission of the application requires subscriber's or an authorized representative's of a company attendance in person in the registration authority or the certification authority, representatives of the certification authority attendance in requester's / payer's seat or submission of trustworthy data or documents for issuing the certificate to CERTUM or its representative. Authorization of the documents or persons is carried out as described at https://www.certum.pl. For the requests provided *off-line*, CERTUM may prepare dedicated processes for certificate retrieval or generate the certificate and keys by itself (solely on the smart cards).

*Off-line* submissions concern also the collective applications. These applications are confirmed by the certification or registration authority operator and processed in groups.

### 4.2.1. Implementing identification and authentication function

The functions of identification and authentication of all required subscriber's data is performed by the Primary Registration Authority and Registration Points associated with CERTUM in accordance with the conditions set out in chapter 1.3.2.

### 4.2.2. Acceptance or rejection of the application

#### 4.2.2.1. Application Processing in Registration Authority

Every application submitted to the certification authority or submitted to the registration authority, is processed in the following way:

- the registration authority operator obtains subscriber's application (a paper version or an electronic version),
- the registration authority operator checks whether the subscriber has made a charge for processing an application for a certificate, provided that such payment is provided in the price list of CERTUM, in the absence of such a charge, the request is rejected.
- the operator verifies data listed in the application, e.g. subscriber's personal data (see the procedure described in chapter 3.2.2, 3.2.3 and 3.2.5) and checks the proof of private key possession if it exists (see chapter 3.2.1),

- for certificates issued prior to March 1, 2018, CERTUM MAY use the documents and data provided in Chapter 3.2 to verify certificate information provided that CERTUM obtained these data or documents no more than 39 months prior to issuing the certificate,
- for websites authentication certificates (except for Premium EV SSL certificates) issued on or after March 1, 2018, CERTUM MAY use the documents and data provided in Chapter 3.2 to verify certificate information provided that CERTUM obtained these data or documents no more than 825 days prior to issuing the certificate,
- for Premium EV SSL certificates CERTUM MAY use the documents and data provided in Chapter 3.2 to verify certificate information provided that CERTUM obtained these data or documents no more than 13 months prior to issuing the certificate,
- upon the positive verification, the operator confirms (signs) the request; if the original application contains incorrect data, it is rejected or corrected,
- basis on the confirmed request a certificate is issued,
- the registration authority may also verify other data that are not listed in an application and required by CERTUM to run a business.

#### 4.2.2.2. Certificate Issuance Denial

CERTUM can refuse certificate issuance 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.

Certificate issuance denial can occur:

- if the subscriber cannot prove his/her rights to the proposed DN,
- if the certificate request consists any new gTLDs which are not added to the widely used current Public Suffix List,
- if there is suspicion or certainty that the subscriber falsified the data or stated false data,
- if the subscriber in especially inconvenient manner engaged resources and processing means of CERTUM by submitting number of request clearly in excess of his/her/its needs,
- subscriber did not make a payment for issuing a certificate, provided that such payment is provided in the price list of CERTUM,
- from other reasons not specified above.

Applicants whose applications have been rejected may subsequently re-apply.

### 4.2.3. Certificate Issuance Awaiting

CERTUM makes efforts to ensure that on receiving application for certification, certificate modification or renewal (keys or certificate), the authority examines the application and issues a certificate within the period no longer than 7 days.

This period depends mainly on the type of certificate, completeness of submitted application and possible administration co-ordinations and explanations between CERTUM and the requester.

### 4.2.4. Certificate Authority Authorization Records Processing

CERTUM performs CAA (Certification Authority Authorization ) records checking when issuing subscribers' certificates. CERTUM accepts the following CAA records:

- `certum.pl`
- `certum.eu`
- `yandex.ru`

When the CAA record is set as `certum.pl` then it takes the following form:

- standard SSL certificate:

```
domain.name  IN CAA 0 issue "certum.pl"
```

- wildcard SSL certificate:

```
domain.name  IN CAA 0 issuewild "certum.pl"
```

## 4.3. Certificate Issuance

### 4.3.1. Processing

On receiving an appropriate application and processing it (see chapterchapter 4.2), a certification authority **issues a certificate**.

Every certificate is issued on-line. The issuance procedure is the following:

- any certification request is recorded and verified at the Primary Registration Point,
- only persons performing trusted roles have access to operational accounts of the Primary Registration Point. Using the accounts is protected by multi-level authentication and enables the processing of certificate application including the ability to submit an appropriately formatted certificate request to the issuing CA,
- a processed certificate applications is sent to certificate issuance server,
- if the application contains the request for generating of a key pair, the server charges hardware key generator complying with the requirements of at least FIPS 140 Level 3 with this task,
- quality of submitted or generated by a certification authority public keys is tested,
- if the procedures are successful, the server issues the certificate and charges hardware security module with signing the certificate; the certificate is stored in certification authority database,
- the certification authority prepares an answer containing the issued certificate (if it was issued) and makes it available to the subscriber.

### 4.3.2. Communication of information

CERTUM certification authority employs two basic methods concerning notifying a subscriber about certificate issuance. The first method uses mail or electronic mail and consists in sending (to the address provided by the subscriber) the information allowing the subscriber to obtain the certificate. This method is also used in the case of necessity of notifying all subscribers of given certification authority about the issuance of a new certificate to this authority or notifying some subscribers about the issuance of the new certificate (e.g. to a server) of the organization these subscribers work for.

The second method consists in issuance of a certificate and placement of the certificate (usually in the same place as a private key) on the electronic cryptographic card and submission of the certificate (by mail) to the subscriber's address (a PIN is sent in a separate letter).

# 4.4. Certificate Acceptance

## 4.4.1. Confirmation of acceptance certificate

On receiving certificate, a subscriber is committed to check its contents, particularly the correctness of the data and complementariness of a public key with the private key he/she/it possesses. If the certificate has any faults that cannot be accepted by the subscriber, the certificate should be immediately revoked (it is equal to lack of approval of the valid certificate expressed by the subscriber). Unless the subscriber revokes or notifies CERTUM within seven (7) days from receipt the certificate that he/she/it does not accept it, the certificate is deemed accepted.

Certificate acceptance is univocal to the subscriber's stating that prior to applying the certificate to any cryptographic operation, he/she/it thoroughly familiarized with certificate issuance procedures, described in this document.

*Accepting the certificate, the subscriber accepts the rules of Certification Practice Statement and Certification Policy and agrees to comply with the agreement made with Asseco Data Systems S.A.*

A relying party might check whether the certificate associated with a private key by means of which a document was signed, has been accepted by the document issuer (see chapter 4.9.9)

## 4.4.2. Publication of certificate

Each issued and accepted certificate is published in the repository of CERTUM.

## 4.4.3. Information for other parties

The registration authority, which has confirmed the subscriber's data and the applicant, on the basis of contract with CERTUM, may be informed about the new certificate.

# 4.5. Certificate and Key Usage

## 4.5.1. By the subscriber

Subscribers, including registration authorities' operators, must use private key and certificates:

- in accordance with their purpose stated in the present Certification Practice Statement and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage**),
- in accordance with the optional agreement between the subscriber and Asseco Data Systems S.A.,
- only within the validity period (not applicable to certificates for digital signature verification),
- only until the certificate revocation.

### 4.5.2. By the relying parties

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

- in accordance with their purpose stated in the present Certification Practice Statement and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage**),
- only upon their status verification (see chapter 4.9) and verification of the signature of the certification authority that issued the certificate,
- only until the key revocation.

## 4.6. Recertification

CERTUM provides the services of recertification of the same pair of cryptographic keys under the same user account.

## 4.7. Certification and rekey (key update)

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

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

Certification and rekey could also apply to certification authority certificates.

*CERTUM always informs subscribers (at least 7 days in advance) about forthcoming validity period expiry. This information is also submitted when it is related to certificates of certification authority.*

### 4.7.1. Certification and rekey circumstances.

Rekey request supplied by a subscriber can apply only to:

- a currently valid certificate and certificate not revoked before.

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

- does not have a current and valid private key for electronic signatures creation,
- requests an additional certificate of the same type or of different type, but only within the certification policy used for issuance of at least one certificate,
- does not have any valid certificate, issued within one of the certification policies defined in this Certification Practice Statement.

### 4.7.2. Who can request key update?

Certification or rekey is performed only on subscribers or applicant representative demand and must be preceded by subscription of a suitable request form.

### 4.7.3. Rekey and certification request processing

Rekey and certification request authorization is carried out in accordance with specifications of instructions published at http://www.certum.eu.

Rekey and certification requests are processed in accordance with chapter 4.2. and 4.3.

### 4.7.4. Information for subscriber

See chapter 4.3.2

### 4.7.5. Confirmation of acceptance of a new certificate

See chapter 4.4.1

### 4.7.6. Publication of a new certificate

See chapter 4.4.2

### 4.7.7. Information for other parties

See chapter 4.4.3

## 4.8. Certificate modification

### 4.8.1. Certificate modification circumstances

Modification of a certificate means replacement of a certificate being used (**currently valid**) with a new certificate in which – in contrast to the certificate being replaced – some of the data can be modified, including public key change.

The modification is treated in the same way as the issuance of a new certificate.

CERTUM can modify the certificate that has been renewed, or whose keys have already been updated. The original certificate may be revoked at the end of the process of modifying the certificate.

### 4.8.2. Who can request certificate modification

See chapter 4.1.1

### 4.8.3. Certificate modification request processing

See chapter 4.2

### 4.8.4. Information for subscriber

See chapter 4.3.2

### 4.8.5. Confirmation of acceptance of a modified certificate

See chapter 4.4.1

### 4.8.6. Publication of a modified certificate

See chapter 4.4.2

### 4.8.7. Information for other parties

See also chapter 4.4.3

## 4.9. Certificate revocation and suspension

Certificate revocation has a significant influence on a certificate and obligations of subscriber owning such certificate.

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

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

This chapter states conditions which need to be fulfilled or exist for certification authority to have reasons for certificate revocation.

*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 until it is physically destroyed.*

### 4.9.1. Circumstances for certificate revocation

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

CERTUM revokes subscriber's certificate if the following situation occurs:

- any information within the certificate has changed,
- subscriber notifies CERTUM that the original certificate request was not authorized,
- cryptographic standards are no longer valid, which can present risks to subscribers or Relying Parties(e.g. technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties
- CERTUM obtains evidence that certificate was misused,
- CERTUM is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name or IP address in the certificate is no longer legally permitted,
- 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[17];the subscriber decides to terminate the agreement with Asseco Data Systems S.A. (in such a case, revocation is strictly bounded with cancellation of

[17] 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.

registration of the subscriber in a certification authority); 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 indicated in the certificate,
- when the subscriber does not comply with accepted Certification Policy or the provisions of other documents referenced in this document, which requires subscriber to comply with them.[18],
- 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 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 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.

These circumstances may also decide to revoke EV SSL certificates

The certificate belonging to a certification authority may be revoked by its issuing authority. Such revocation may occur in the following situation:

- the certification authority 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 credibility of certificates issued by this authority,
- the certification authority has breached material obligation arising from this Certification Practice Statement.

Revocation request might be submitted (see chapter 3.4) by means of a registration authority (this requires the subscriber to contact the registration authority) or directly to a certification authority (request might be authenticated with a signature). In the former case, a request signed by the registration authority or a paper document is submitted to the certification authority, whereas in the latter one – the subscriber personally authenticates the revocation request and submits it directly to the certification authority.

Revocation request should contain information which allows indubitable authorization of a subscriber in a registration authority, in accordance with chapter 3.2.2 or 3.2.3.

---

[18] Primarily:

- Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,
- Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates,
- Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates oraz
- Guidelines For The Issuance And Management Of Extended Validation Certificates

## 4.9.2. Who can request certificate revocation?

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

- a subscriber who is the owner of a certificate,
- an authorized representative of a certification authority (in the case of CERTUM this role is reserved for the security inspector),
- a subscriber's requester / payer[19], for example his/her employer; the subscriber has to be immediately informed about such fact,
- a registration authority operator, which may request revocation on behalf of a subscriber or on its own, if it has information justifying certificate revocation.,
- Relying Parties, Application Software Suppliers, and other third parties may submit reports informing CERTUM of reasonable cause to revoke the certificate.

*Registration 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 (e.g. acts as a subscriber's requester / payer),
- submit notification to the subscriber about revocation or initiation of revocation process.

Every request might be submitted:

- directly to a certification authority as an electronic request with or without registration authority confirmation,
- directly or indirectly (by means of another registration authorities) to the main certification authority as a non-electronic request (paper document, fax, phone call, etc).

## 4.9.3. Procedure for certificate revocation

### 4.9.3.1. Procedure for end-user certificate revocation

Certificate revocation may be carried out in following manners:

- **the first method** is based on submission of electronic revocation request authorized by a password, to the certification authority; such revocation is proceeded by subscriber in an unassisted manner.
- **the second method** requires submission of electronic revocation request to a certification authority, confirmed with an electronic signature of a registration authority; this method applies to situations when (a) the subscriber has lost both his/her/its private key and its password or (b) revocation request has been submitted by the applicant, an authorized representative of a certification authority or a registration authority, provided that there are sufficient reasons to request such revocation,

[19] See **Glossary.**

- **the third method** involves submission of the non electronic request - via traditional registered mail - official revocation request letter, signed by the subscriber or the authorized person or the electronic request – via form available on the website certum.eu in the Technical Support.

In all the cases the certification authority – after successful verification of the request – **revokes** the certificate. Information about the revoked certificate is placed on **Certificate Revocation List** (see chapter 7.2), issued by the certification authority.

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

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

Certificate revocation procedure is carried out as follows:

- the certification authority, upon receiving certificate revocation request, authorizes it: if the request is made electronically, the certification authority verifies the correctness of the certificate being requested for revocation and (optionally) the correctness of the **token** attached to the request, issued by the registration authority; request made on paper (compare above – the third method of revocation) requires authorization of the requester; such confirmation may be obtained by phone call, by fax or may be submitted while the subscriber personally visits an authorized representative of the certification authority (or vice-versa),
- if the request is verified successfully, the certification authority places information about certificate revocation on Certificate Revocation List (CRL), along with information concerning the reasons for revocation (see chapter 7.2.2),
- the certification authority submits proof of the certificate revocation or decision about cancellation of the request, along with the reasons for the cancellation to the entity requesting certificate revocation,
- additionally, if the entity requesting certificate revocation is not a subscriber of the certificate, the certification authority must notify the subscriber about revocation of the certificate or initiation of revocation process.

*It is required that requests for revocation, submitted by an authorized representatives of a certification authority or by an applicant, have to be authorized by the entitled registration authority.*

If a certificate being revoked or a private key, corresponding to the certificate, were stored on an electronic cryptographic card, upon certificate revocation, the card may be physically destroyed or securely wiped out. This operation is to be carried out by the holder of the card – a private or legal entity (a representative of such an entity). The holder of the card should store it in a manner preventing it from being stolen or unauthorized usage until physical destruction or the private key erasure.

#### 4.9.3.2. Procedure for Certification Authority or Registration Authority certificate revocation

The certificate belonging to a certification authority or registration authority may be revoked by its issuing authority. Such entity is required to submit request revocation directly to CERTUM.

CERTUM may also submit Certification Authority's or Registration Authority's certificate revocation request. (see chapter 4.9.2)

## 4.9.4. Certificate revocation grace period

CERTUM guarantees maximum 24 hours grace period[20] for revocation request processing:

- submitted electronically (with the correct format) or by phone call,
- submitted in paper form (from the time of reception of the request by certification authority operator).

*Certificate revocation requests submitted by certification authorities to the issuer of the certificate are processed within 1 hour from reception of the requests, independently from the certification policy used for the certificate issuance. CERTUM is not obliged to revoke certificates issued within Certum Level I CA, Certum Class 1 CA and Certum Class 1 CA SHA2 CERTUM.*

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).

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

## 4.9.5. Time limit for processing of revocation request

Request for revocation of the certificate is processed by CERTUM without undue delay.

## 4.9.6. Certificate Revocation List checking

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

Certificate status verification may be based solely on CRL only in the cases if CRL issuance frequency periods, declared by CERTUM, do not bear the risk of serious damages or losses to relying party. In other cases, a relying party should contact (by phone, fax, etc) the authority issuing the certificate or employ *on-line* certificate status verification service (see chapter 4.9.10).

The URLs for CRL distribution points are available in the public repository at http://www.certum.eu

## 4.9.7. CRL issuance frequency

Every certification authority being a part of CERTUM issues separate Certificate Revocation List.

Every Certificate Revocation List is updated at least once a week[21] if no additional certificate has been revoked within this period. Notwithstanding, the new CRL is published in the repository after every certificate revocation.

---

[20] 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 4.9.9.).

[21] 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

Certificate Revocation Lists for the root CAs: **Certum CA**, **Certum Trusted Network CA**, **Certum Trusted Network CA 2** and **Certum Trusted Network CA EC** authorities are issued at least every year, provided that there is no revocation of the certificate of one of the authorities affiliated by **root CAs**.

## 4.9.8. The maximum delay in the publication of the CRL

Each CRL is published without undue delay as soon as it is created (usually this is done automatically within a few minutes).

## 4.9.9. On-line certificate status verification availability

CERTUM provides real-time certificate status verification service. This service is carried out on the basis of OCSP, described in RFC6960. Using OCSP, it is possible to acquire certificate status information without requiring CRL.

OCSP functions 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[22],
- **revoked** – meaning the certificate has been revoked,
- **unknown** – meaning the certificate has not been issued by any of the affiliated certification authorities.

OCSP service generates response based on a database. OCSP response is valid for 7 days. In order to maintain the proper performance of the system, the OCSP responses are cached for a predetermined time (usually not more than a few hours). To force the current OCSP response the *–nonce* switch should be used when querying the OCSP responder.

## 4.9.10. Requirements for on-line certificate status verification

Relying parties must check revocation information of a certificate on which they wishes to rely. Otherwise all CERTUM's warranties becomes void.

**For the status of subscriber certificates:**

CERTUM updates information provided via an OCSP every few minutes.

OCSP responses have a maximum expiration time of seven days.

**For the status of subordinate CA certificates:**

CERTUM updates information provided via an OCSP at least every twelve months and within maximum 24 hours after revoking a subordinate CA certificate.

## 4.9.11. Other forms of revocation advertisements availability

Not applicable.

issuance. Publication of the succeeding CRL can be also made before this date. In the case of CAs isuuing end-entity certificates, value of this field is set to 10 days.

[22] See **Glossary**.

### 4.9.12. Special requirements regarding key security violation

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

CERTUM immediately informs the relying parties, referring to the information collected in a repository managed by CERTUM.

### 4.9.13. Circumstances for certificate suspension

CERTUM does not support suspension.

### 4.9.14. Who can request certificate suspension

Not applicable.

### 4.9.15. Procedure of certificate suspension and unsuspension

### 4.9.16. Not applicable.Limitation on suspension grace period

Not applicable.

## 4.10. Certificate Status Verification Services

### 4.10.1. Operational characteristics

Certificate status information is available via CRL and OCSP responder. The serial number of a revoked certificate remains on the CRL until the end of the certificate's validity period.

### 4.10.2. Service Availability

Certificate status verification services are available in the regime 24/7 (continuously operating).

### 4.10.3. Optional features

The certificate status verification service on-line (OCSP) is not available for all types of certificates, and all relying parties.

*The URL address of OCSP service is usually placed in the certificates issued to subscribers. It means that the OCSP service is available for this certificate.*

The OCSP service is obligatory for all of the intermediate certification authorities certificates, SSL certificates and EV SSL certificates issued by CERTUM.

## 4.11. End of subscription

The termination of the use of certification services by the subscriber occurs in the following cases:

- when validity period of the certificate has expired and the subscriber has not taken action to update its key, or modification,
- when subscriber certificate was revoked and has not been replaced by another certificate

## 4.12. 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.

# 5. Technical, organizational and operational security controls

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

## 5.1. Physical security controls

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. Every entry and exit is recorded in the event journal (system logs). Computers registering subscriber's requests and issuing their confirmations 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.

### 5.1.1. Site location and construction

CERTUM is located in Asseco Data Systems S.A. seat, at the following addresses: Bajeczna Street 13, Szczecin, Poland and Krolowej Korony Polskiej Street 21, Szczecin, Poland. Addresses of registration authorities are available in the repository and by email at the following address: info@certum.pl.

### 5.1.2. Physical access

Physical access to the seat and CERTUM area is controlled and monitored by the integrated alarm system. Physical security of the seat and CERTUM area operate 24 hours a day.

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 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. 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 the approval of Chief of CERTUM.

Access to the operators and administrators area is enforced through the use of an smart card and access control system. 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.

Access to Primary Registration Authority has to be performed as described in this chapter. In the case of other registration authorities, there are no additional restrictions addressing

physical access. It is recommended that offices of registration authorities should be separated and rigged with equipment allowing safe storage of data and documents. Access to such areas should be monitored and limited to authorized individuals associated with the activity of the registration authority (registration authority operators, system administrators) and their customers.

### 5.1.3. 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.

The Primary Registration Authority is connected with emergency power source system of the building. Air conditioning is not required. In the case of other Registration Points, there are no restrictions addressing emergency power source and air conditioning.

### 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 CERTUM buildings. Reception personnel are notified of the hazards and is 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. seat complies with local standards and regulations for fire safety. Computer system area is also equipped with fire control system (neutral gas), activated automatically in the case of fire detection in monitored area.

### 5.1.6. 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 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.

### 5.1.7. Waste disposal

Paper and electronic media containing information possibly significant for CERTUM security after expiration of the retention period (see chapter 5.5.5 5.5) 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 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.

### 5.1.8. Offsite backup storage

Copies of passwords, PIN numbers and cryptographic cards are stored in safe-deposit box outside CERTUM seat.

Offsite storage affects also archives, current copies of information processed by the system and full installation version of CERTUM applications. It enables emergency recovery of most substantial CERTUM function within 48 hours (in CERTUM seat or in the emergency facility).

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.

## 5.2. Organizational security controls

This chapter presents a list of roles which can be defined for personnel, employed in CERTUM. This chapter also describes responsibilities and duties associated with each defined role.

### 5.2.1. Trusted roles

#### 5.2.1.1. Trusted roles in CERTUM

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

- **Chief of CERTUM** – responsible for correct management of CERTUM, determines directions of development of certification authority, responsible to manage 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; reviews event logs; supervises service tasks,
- **system operator** – handles standard system operations, including backup copies and transfer of current copies and archives to offsite locations,
- **registration inspector** – verifies subscribers' identity and correctness of submitted certification application; authorizes certification request,
- **system administrator** – installs hardware and software for operating system; initially configures the system and network resources; manages folders of CERTUM available to the public; creates WWW page and manages links,
- **audit inspector** – responsible for review, archive and management of event logs (in particular verification of their integrity) and performance of internal audit for compliance of a certification authority operations with this Certification Practice Statement; this responsibility extends also on all Registration Points, operating within CERTUM,

### 5.2.2. Numbers of persons required per task

CERTUM keys – for the needs of certificate and CRL signing – generating and recovering process is the operation requiring particular attention. It requires presence of persons, acting as:

- security inspector,

- hardware security module operator,
- shared secret holder,
- reporter (e.g auditor) – optional.,

### 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,
- assignation of an account and a password in CERTUM information system.

Every confirmation and assigned account:

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

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

### 5.2.4. The roles that cannot be combined

Described in chapter 5.2.1 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 presented 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

CERTUM personnel performing trusted roles must have documented preparation and experience, which guarantees to meet requirements of trainings and provide certainty that they are ready to perform its future obligations. In cases where a person employed for the operation of certification for the government should have a safety certificate issued by the security administrator Asseco Data Systems SA or by the Internal Security Agency (ABW).

Control of professional training each person who acts as trusted role is repeated at least once every 5 years.

### 5.3.1. Qualifications, experience and authority

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

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

### 5.3.2. Personnel verification procedures

Each person who is a new employee and performing trusted role is verified by CERTUM which maintains controls to perform background checks of such person to:

- confirm previous employment,
- check personal references,
- confirm the highest or most relevant educational degree,
- obtained and search criminal records,
- search records of National Debt Register (Krajowy Rejester Długów) in the jurisdiction where the person will be employed,
- check ID (PESEL)

In the case when the required information is not available (eg, due to the current law), CERTUM may use other techniques that will allow to obtain information similar to the foregoing.

CERTUM may reject a candidacy associated with the performance of the trusted role, or take action against a person already employed in that position if it is found that:

- CERTUM was misled by candidate or employee regarding the above data
- CERTUM received highly unfavorable or not very reliable references from former employers
- CERTUM received information about candidate's or employee's criminal past and that he/she was convicted under a final and valid court judgement;

In case of any of the above, further steps are carried out in accordance with safety procedures Asseco Data Systems SA 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 Practice Statement,

- regulations of Certification Policy,
- regulations of procedures and documentation related with acted role,
- procedures and security controls employed by a certification authority and a registration authority,
- system software of a certification authority and a registration authority,
- responsibilities arising from roles and tasks performed in the system,
- procedures executed upon system malfunction or disruption of certification authority operations.

### 5.3.4. Retraining Frequency and Requirements

Trainings described in chapter 5.3.3 have to be repeated or supplemented always in situation when significant modification to CERTUM or its registration authority operation is executed.

### 5.3.5. Job rotation

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

### 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.

### 5.3.7. Contract Personnel

Contract personnel or consultants may perform trusted roles, listed in the chapter. 5.2.1. In such cases, they are subject to the same requirements applicable to CERTUM employees.

Because the contract personnel is subjected to the same verification procedure as employees of CERTUM, then, if they do not provide required information or do not pass the exam (see chapter 5.3.2), they must be escorted by CERTUM or the registration authority employee each time when performing their task at CERTUM seat or its registration authority..

### 5.3.8. Documentation Supplied to Personnel

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

- Certification Policy,
- Certification Practice Statement,
- 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 and audit procedures

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

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

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

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

## 5.4.1. Types of events recorded

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

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

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

The above event logs are common for every component installed on a 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.

Detailed list of recorded events depends of the certification policy of certificates issued or confirmed by a specific certification authority or a registration authority. However, the following shall in any event be included:

- CERTUM CAs key lifecycle management events, including:
  - key generation, backup, storage, recovery, archival, and destruction; and
  - cryptographic device lifecycle management events.
- Subscriber certificate lifecycle management events, including:
  - certificate requests, renewal, and re-key requests, and revocation;

- all verification activities stipulated in these Requirements and CERTUM Certification Practice Statement;
- date, time, phone number used, persons spoken to, and end results of verification telephone calls;
- acceptance and rejection of certificate requests;
- issuance of Certificates; and
- generation of Certificate Revocation Lists and OCSP entries.

- Security events, including:
  - successful and unsuccessful CERTUM's system access attempts;
  - security system actions performed;
  - security profile changes;
  - system crashes, hardware failures, and other anomalies;
  - firewall and router activities; and
  - entries to and exits from CERTUM facility.

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

## 5.4.2. Frequency of event logs checking

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.

Event journals are retained for at least 7 years.

## 5.4.4. Protection of event logs

Once a week every entry in event logs is subjected to copy to a magnetic tape. After surpassing accepted for specific log number of entries, log contents are archived. Archives may be encrypted with Triple DES or AES algorithm. A key used to archive encryption is placed under the management of the security inspector.

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 persons (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 5.4.3).

## 5.4.5. Procedures for event logs backup

CERTUM security procedures require that the event logs and activity records – created when reviewing this journal by the security inspector, system administrator or an audit inspector – such as activities on the journals, collective statements, analysis, statistics, detected threats etc, should be subjected to monthly backup. These backups are retained in main and alternate site of CERTUM. Backup copies may be signed with a timestamp.

## 5.4.6. The data collection system for the audit (internal and external)

Applications, components and network software and operating systems used in the systems of CERTUM automatically generate the information about events. Information about these types of events are also entered manually by staff CERTUM.

## 5.4.7. Notification to event responsible entities

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

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

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

## 5.4.8. Vulnerability assessment

This Certification Practice Statement requires the certification authority issuing certificates (including subordinate authorities of **Certum Global Services CA** and **Certum Global Services CA SHA2**), the Primary Registration Authority and affiliated Registration Points (in the case of delegation of rights to registered subscribers) to perform 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.

CERTUM classifies and keeps records of all assets according to PN-ISO/IEC 27001:2014 standard. This Certification Practice Statement requires performing vulnerability assessment analysis of every internal procedures, applications and information system. Requirements for analysis may be also determined by an external institution, authorized to carry out CERTUM audit.

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.

In accordance with the 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 to archive all data and files related to the registration of information associated with the system security, all requests submitted by subscribers, all information about subscribers, issued certificates and CRLs, all keys, used by certification authorities, The Primary Registration Authority and Registration Points and whole correspondence of CERTUM with subscribers. Subjected to archival are also all documents and data used in identity verification process. Some of data (marital status, photo and description), not directly required in the authentication process, may be removed from the documents. Hard-copy documents are processed to electronic form and are also subjected to archival.

CERTUM manages two types of archives: archive available *on-line* (*on-line* archive) and available *off-line (off-line* archive).

Valid certificates (including inactive, issued no more than 15 years before the current date) are retained in the *on-line* archive of active certificate and may be used to perform some of external certification authority services, for example certificate validity verification, certificate publication for their owners (restoration of certificates) and authorized entities.

*On-line archive might also contain the certificates issued 25 years (and more) in the past. On-line archive may replace off-line archive.*

The *off-line* archive contains certificates (including revoked certificates) issued in the period of 15 to 25 years before a current date. Revoked certificate archive contains information about a certificate identifier, date of revocation, reason for revocation, whether and when the certificate was placed on CRL. The archive is used for dispute resolving, applying to old documents, electronically signed (in the past) by a subscriber.

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.

## 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 CERTUM's certification authorities, the Primary Registration Authority and Registration Points, and the repository,

- received requests and issued decisions in an electronic or paper form, submitted by or to the subscriber as a paper document, files or electronic messages,
- subscribers database,
- certificates database,
- issued Certificate Revocation Lists,
- history of a certification authority key, from its generation to erasure,
- history of the subscribers' keys, from their generation to erasure, if the keys are subjected to archive in certification authority databases,
- documents and data used in identity verification process.

## 5.5.2. Archive retention period

CERTUM retain all documentation (in paper and electronic form) relating to certificate requests and the verification thereof, and all certificates and revocation thereof, for at least seven years after any certificate based on that documentation ceases to be valid

After expiration of the declared retention period, archived data may be destroyed. In the case of key and certification erasure, an appropriate procedure is executed with particular attention.

## 5.5.3. Protection of archive

Access to the archive have only authorized persons performing trusted roles in CERTUM. Archive is stored in the system, which meets the requirements of CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements*. This system provides protection against unauthorized browsing the archives, modification, removal or tampering. The media on which the archives are stored for processing applications and archives must be maintained in the state to ensure the declared period of access to the archives (chapter 5.5.2).

## 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.

## 5.5.5. Requirements for time-stamping of the records

It is recommended that archived data should be signed with a timestamp, created by the authorized Timestamping Authority (TSA), having a certificate issued by the operational certification authority affiliated by **Certum CA**.

### 5.5.6. The archive data collection system

The archive data collection system is internal system of CERTUM. The exception to this rule are the archives kept by Registration Points associated with CERTUM. The data in external files must be kept primarily for the purpose of the audits carried out by CERTUM or entity designated by CERTUM.

### 5.5.7. Access procedures and archived information verification

Only those persons who performing trusted roles in CERTUM have access to the archive and access is possible only after successful authentication (ie authentication and confirmation of a person's access rights).

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

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

## 5.6. Key changeover

Procedure for key changeover applies to the keys of certification authorities affiliated by the CERTUM and it describes procedure for key update (rekey) for a certificate and CRL signing which replaces a currently used key.

Rekey procedure is based on issuance of special certificates by a certification authority, facilitating a subscriber who has old certification authority certificate, a secure exchange for a new certificate, and allowing new subscribers who have a new certificate, for a secure way to obtain the old certificate and verification of current data (see RFC 4210, and chapter 6.1.1.1)

Every key changeover is announced in advance by means of CERTUM WWW page, distribution on new keys in the application and broadcasted by electronic mail. Additionally, in the case of **CERTUM root certificates** key changeover, information about changeover might be published by means of mass media in the week preceding expiration of private key validity period.

Frequency of key changeover of a certification authority, affiliated by the CERTUM results from the validity period of corresponding certificates, shown in Tab. 6.1.

*From the moment of key changeover, the certification authority 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. Threat Management Incident Handling

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.

CERTUM Business Continuity Plan includes:

- The conditions for activating the plan.
- Emergency procedures.
- Fallback procedures.
- Resumption procedures.
- A maintenance schedule for the plan.
- Awareness and education requirements.
- The responsibilities of the individuals.
- Recovery time objective (RTO).
- Regular testing of contingency plans.
- CERTUM's plan to maintain or restore business operations in a timely manner following interruption to or failure of critical business processes.
- A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location.
- What constitutes an acceptable system outage and recovery time.
- How frequently backup copies of essential business information and software are taken.
- The distance of recovery facilities to the CERTUM's main site; and
- Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

### 5.7.2. Corruption of computing resources, software and/or data

All information about corruption of computing resources, software and/or data are communicated to the security inspector who assigns the performance of activities under the procedures developed.

These procedures are designed to analyze the intensity of an attack, investigate the incident, to minimize its effects and eliminating it in the future. If necessary, in the case of CERTUM private key compromise or other corruption events appropriate steps must be taken with the Disaster Recovery Plan including.

### 5.7.3. Key compromise or suspicion of entity affiliated by the CERTUM private key compromise

In the case of certification authorities or other entities 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 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,
- a certificate corresponding to the compromised key is placed on Certificate Revocation List, along with a suitable reason for revocation ,
- 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

These operations are carried out in accordance with the plan developed by the security incident response team which includes Chief of CERTUM, security inspector, security administrators and other appropriate CERTUM personnel appointed by Chief of CERTUM . A plan must be approved by the member of the Asseco Data Systems S.A. Board.

## 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 is created. The copy includes all submitted requests, issued, renewed and revoked certificates; latest copies are retained both in main seat and in emergency location outside CERTUM,
    - periodically, following the procedures disclosed in chapter 5.5.4, every server full backup copy is created. This copy includes all submitted requests, entries to event logs, issued, renewed and revoked certificates; copies are retained in secure location outside CERTUM facility,
    - CERTUM keys, split according to procedures for secret sharing, are held by trusted individuals in the places known only to themselves,
    - computer replacement is carried out in a manner allowing disk image restoration, on the basis of most recent data and keys (applies to singing server),
    - system recovery procedures after disaster are tested on every system component, at least once a year. These tests are a part of an internal audit.

- **Modification monitoring**. Installation of updated software version in the production system is possible only after carrying out intensive tests in a testing environment, performed in strict accordance with disclosed procedures. Every modification in the system requires CERTUM security inspector's acceptance. If the newly implemented components, installed in accordance with the above procedures, cause target system corruption, accepted system recovery plans allow swift restoration of the system to the state before corruption occurred.
- **Emergency system**. In the case of corruption restraining CERTUM functionality, within 24 hours an emergency facility will be activated, which should substitute most substantial function of a certification authority until the primary facility is restored to service. Due to regular backup copy and archive creation, unprocessed requests accumulation and hardware-software redundancy, in the case of corruption restraining CERTUM activity, it is possible to:
    - activate emergency facility allowing provision of CERTUM services,
    - process all accumulated and unprocessed revocation requests,
    - process in real-time requests submitted by subscribers until restoration and recovery of the prime facility.
- **Backup copy creation system**. CERTUM system utilizes application, creating backup copy from data, allowing system recovery at any moment and performance of an audit.
- **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 decision of CERTUM's certification authority to cease operation, and include obligations to notify in advance all subscribers of the authority that certified the certification authority subjected to termination (if such exists) about the termination, and transition of responsibilities – on the basis of regulations with other certification authorities – for service of its subscribers, database and other resources management.

### 5.8.1. Requirements associated with duty transition

Before a certification authority ceases its services, it is obligated to:

- notify the certification authority that issued its certificate about their intention to terminate services as the authorized certification authority; the notification should be made 90 days before the agreed date of the termination,
- notify (at least 90 days in advance) its subscribers who hold active (unexpired and unrevoked) certificates issued by this authority about decision to terminate its services,
- revoke all certificates which remain active (unexpired and unrevoked) in the declared moment of service termination, regardless of the fact that a subscriber has submitted or has not submitted a suitable request,
- notify all subscribers associated with the certification authority about service cessation,
- make commercially reasonable effort to minimize disruptions to interests of subscribers and legal entities engaged in an ongoing process of electronic signature (remaining in usage) verification with public keys certified with the digital ID, issued by the certification authority being terminated,
- pay compensations of issuance fees to the subscriber or the applicant; compensations should be proportional to remaining validity period of the certificate.

If the decision to terminate services applies only to the Registration Point, the Registration Point is obligated to:

- notify the certification authority or certification authorities they work with about their intention to terminate services as the authorized Registration Point; the notification should be made 90 days before the agreed date of the termination,
- provide certification authorities with subscribers documentation, including archive and data for the audit.

### 5.8.2. Certificate issuance by the successor of terminated certification authority

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

Issuing a replacement certificate, the successor of the terminated certification authority takes over the rights and obligations of the terminated certification authority related to the management of the certificates which remain in usage.

Archive of the intermediate certification authority ceasing its service has to be turned over to the root certification authority or to the institution which the suitable agreement was signed up with (in the case of termination of CERTUM root certification authorities).

# 6. Technical Security Controls

This chapter describes procedures for generation and management of a cryptographic key pair of CERTUM's certification authorities, the Primary Registration Authority, Registration Points and subscribers, including associated technical requirements. Information below that applies to **Certum Trusted Network CA** root certificates applies also to another root certificate from the same domain: **Certum Trusted Network CA 2** and **Certum Trusted Network CA EC**.

## 6.1. Key Pair Generation and Installation

### 6.1.1. Key Pair Generation

Procedures for 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 root certification authorities, influencing secure operation of the whole public key certification system.

CERTUM root certification authorities own at least one self-certificate. A private key corresponding to a public key contained in a self-certificate is used solely for signing of public keys of intermediate certification authorities and issuing of Certificate Revocation List and operational certificates of a certification authority, necessary for the operation of the authority issuing the certificates.

Key pairs owned by each CERTUM certification authority should allow:

- to sign certificates and CRLs;,
- to sign messages transmitted to subscribers, the Primary Registration Authority and Registration Points (the operational key),
- to negotiate of keys used for confidential information exchange between the authority and its environment (the operational key).

The private keys of CERTUM root certification authorities, CERTUM intermediate certification authorities and CERTUM non-repudiation authorities keys are generated within CERTUM seat, in the presence of selected group of trusted persons (comprising additionally security inspector and system administrator). The group is required only in the case of certificate and CRL signing key generation.

Additionally, when generating keys for CERTUM root certification authorities, CERTUM have a qualified auditor witness the Root CA key pair generation process. The auditor confirms that key ceremony was conducted in conformance with CERTUM's procedures and that appropriate controls was used to ensure the integrity and confidentiality of the key pair.

Key ceremony is conducted in a secure, shielded room protecting against electromagnetic radiation.

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 authorities key pair 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.

#### 6.1.1.1. CERTUM root certification authorities rekey procedure

The cryptographic keys of CERTUM root certification authorities have a limited lifetime period; if the period has expired, the keys should be updated.

A particular procedure is applied for update of key pair used for certificate and CRL signing. It is based on the issuance of special certificates by the one of CERTUM root certification authority. The certificates enable subscribers who have already installed an expired **root-self-certificate** 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 4210).

To achieve effect described above, **CERTUM** 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 **root-self-certificate** 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 root certification authority key pair – designated to certificate and CRL signing – update (rekey), is executed as follows:

- generation of a new, succeeding main key pair $\mathbf{GPK_{(i,CA)}=\{K^{-1}_{GPK(i,CA)}, K_{GPK(i,CA)}\}}$, where $\mathbf{K^{-1}_{GPK(i,CA)}}$ – private key, while $\mathbf{K_{GPK(i,CA)}}$ – public key, distribution of the private key (according to accepted threshold method),
- creation of a self-certificate, containing new public key of CERTUM root certification authority, signed with old private key $\mathbf{K^{-1}_{GPK(i-1,CA)}}$ (**self-certificate NewWithOld**),
- deactivation of old private key $\mathbf{K^{-1}_{GPK(i-1,CA)}}$ and activation of new private key $\mathbf{K^{1}_{GPK(i,CA)}}$ – within hardware security module a new private key for certificate and CRL signing is loaded,
- creation of a self-certificate, containing old public key of CERTUM root certification authority, signed with new private key $\mathbf{K^{1}_{GPK(i,CA)}}$ (**self-certificate OldWithNew**),
- creation of a self-certificate containing new public key of CERTUM root certification authority, signed with new private key $\mathbf{K^{1}_{GPK(i,CA)}}$ (**self-certificate NewWithNew**),
- 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 root certification 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 root certification authority (it should be achieved before the expiry date of the old self-certificate).

Beginning and expiration of the validity period of **self-certificate OldWithNew** should be the same as beginning and expiration date of the old self-certificate.

Validity period of **self-certificate NewWithOld** starts in the moment of a new key pair generation and expires in the moment when all the subscribers will obtain new self-certificates (certificate of the new public key) of CERTUM root certification authority. Its expiration date should not be later than the expiry date of the old self-certificate.

Validity period of **self-certificate NewWithNew** begins in the moment of a new key pair generation and expires at least 180 days after the next anticipated date of succeeding key pair generation. This requirement means that CERTUM root certification authority terminates usage of the private key for signing certificates and CRL at least 180 days before the expiry date of the self-certificate corresponding to this private key.

## 6.1.2. Private Key Delivery to Entity

Subscriber's key pair is generated by himself/herself/itself or may be generated centrally by a certification authority inside a token (e.g. an electronic identity card) In the case of keys generation by CERTUM keys are delivered (together with a token) to the subscriber personally or by means of registered mail; data for the card activation (including PIN/PUK) or key decryption (password) are submitted separately from the media containing the key pair; the issued cards are personalized and registered by the certification authority.

In the case of code signing certificates, subscribers are obliged to generate and protect their own private key in an external device. CERTUM recommends to subscribers that they use CERTUM's electronic cryptographic cards which are certified as conformant with FIPS 140 Level 2.

CERTUM recommends using electronic cryptographic cards for ID certificates to generate private keys on board and store them together with the certificate. Using an electronic cryptographic card warrants the security of private key.

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

## 6.1.3. Public Key Delivery to certification authority

Subscribers and the Primary Registration Authority operators submit their generated public keys as an electronic request whose format has to comply with protocols of PKCS#10 Certification Request Syntax[23] (CRS).

*Currently, CERTUM supports only requests submitted in the format PKCS#10 Certification Request Syntax (CRS) and Netscape SPKAC (Signed Public Key and Challenge).*

Requests submitted to a certification authority may, in particular cases, require confirmation issued by a registration authority (see chapter 3 and 4).

Submission of a public key is expendable in the case when a key pair is generated on demand by a certification authority, which simultaneously issues a certificate for the generated key pair.

## 6.1.4. Certification authority public key delivery to relying parties

Public keys of the certification authority issuing certificates to subscribers are distributed solely in a form of certificates complying with ITU-T X.509 v.3 recommendations. In the case of **Certum CA** , **Certum Trusted Network CA, Certum Trusted Network CA 2** and **Certum Trusted Network CA EC**, certificates have a form of a self-certificates.

CERTUM certification authorities distribute their certificates in two different methods:

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

- placement in the publicly available web repository of CERTUM at http://www.certum.eu,
- distribution together with a dedicated software (e.g. web browsers, email 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 self-certificates or certificates issued as a result of execution of the procedure described in chapter 6.1.1

## 6.1.5. Keys Sizes

Size of keys deployed in most of the CERTUM's certification authorities is 2048 bits excluding **Certum Trusted Network CA 2** which has 4096-bit keys and **Certum Trusted Network CA EC** authority key which has 521-bit in length but encrypted with ECDH_P521 algorithm The key length in certificates used by the Primary Registration Authority operators and subscribers are defined by the user (2048 bit or more).

## 6.1.6. Public Key Generation Parameters and Quality Checking

CERTUM fulfills minimal requirements, described in NIST SP 800-89 recommendation.

CERTUM generates keys in accordance with FIPS 186. If key pair is generated by subscriber, CERTUM always validates the quality of public keys presented by subscribers before the issuance of subscriber's certificate. CERTUM recognizes subscriber's "weak keys" and rejects them before certificate request submission. It is not allowed to accept keys which are not compliant with the Baseline Requirements Section 6.1.6.

Person who generate 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,
- immunity to known attacks (applies to RSA cryptographic algorithm).

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

Parameter quality checking, covering for example checks of primness of the prime numbers, should be obligatory in the case of centralized key generation and should be executed according to recommendations listed in NIST SP 800-89

## 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 does not have to be obligatorily verified by the subscribers' application managing the certificates.

Usage of every bit of **keyUsage** field must comply with the RFC 5280.

Certificates used for both signature creation and encryption may be issued solely to subscribers.

Private keys corresponding to root certificates are not used to sign certificates except in the following cases:

- self-signed certificates to represent the root CA itself,
- certificates for subordinate CAs and cross certificates,
- certificates for infrastructure purposes certificates (i.e. internal CERTUM operational device certificates), and
- certificates for OCSP response verification.

# 6.2. Private Key Protection

Every subscriber, CERTUM's certification authority operator and the Primary Registration Authority operator generates and stores 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 ).

CERTUM implements physical and logical safeguards to prevent unauthorized certificate issuance. Protection of CERTUM private key outside the validated system or device MUST consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the private key.

CERTUM encrypts its private key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

## 6.2.1. Standards for Cryptographic Modules

Hardware security modules employed by a certification authority and a registration authority comply with the requirements of FIPS 140-2 Level 3 or higher standard. In the case of subscriber's using hardware key protection, it is recommended to comply with FIPS 140-2 Level 2 or higher.

## 6.2.2. Private Key Multi-Person Control

Multi-person control of a private key applies to private keys of all certification authorities of CERTUM used for certificate and CRL signing, as well as other cryptographic operations, e.g. message encryption.

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**. Required number of secrets allowing private key restoration and accepted number of a shared secret are 3 of 5 for the root certificates and 2 of 3 for the intermediate certificates.

Shared secrets are stored on cryptographic cards, protected by a PIN number and transferred in an authenticated 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 responsibilities for its storage, and it should state conditions and requirements for shared secret retransmission to authorized personnel.

## 6.2.3. Private Key Escrow

See chapter 4.12

## 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

CERTUM does not retain copies of the Primary Registration Authority and Registration Points' operator's private keys. Copies of a subscriber's private keys are created solely on subscriber's demand and in accordance with the methods presented in chapter 4.12

## 6.2.5. Private Key Archival

Private keys of all CERTUM's certification authorities are archived only by CERTUM.

Private keys of certification authorities used for electronic signature creation are archived for at least 5 years after their usage termination in cryptographic operation. The same requirement applies to public key certificate corresponding to private key after its expiration or revocation.

Private keys of certification authorities used in key agreement operations have to be archived after expiry of the validity date of the associated certificate or upon its revocation for the period at least 5 years. Archived keys have to be available for 25 years; for the first 15 years they must be accessible *on-line*.

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

## 6.2.6. Private Key Entry into Cryptographic Module

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

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

Entry of a private key into the security module is a critical operation, therefore measures and procedures, preventing key revelation, modification or forgery are implemented during execution of the operation. The private keys of all intermediate CAs authorities remain under the sole control of CERTUM.

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

- if the key is provided in one piece than outside the module it is not available in plain form, i.e. upon key generation in the module and its export to another cryptographic device, the key is encrypted with a secret key; the secret key is stored in a manner

preventing unauthorized access to both parts of the secret (private key and secret key used for its encryption) simultaneously,

- if a key, or its password is stored as secret shares, then the very module is able to verify, on shares loading, a potential attack or forgery attempts.

Entry of a private key into hardware security module of each certification authorities 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.

A private key of The Primary Registration Authority's and Registration Points operator is always available in one instance (no copies), therefore there is no need to enter it into the memory of the cryptographic module.

## 6.2.7. Storing Private Key in Cryptographic Module

Hardware security modules employed by CERTUM's certification authorities comply with the requirements of FIPS 140-2 Level 3 or higher standard. Regardless of the form of the private key's storage, the key is not accessible from outside the 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 (a subscriber, a Registration Point, a certification authority, a 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 authorities, entered into the module after their generation, import in an encrypted form from another module or restoration from shared secrets by the authorized person, remain in the active state until their physical erasure from the module or removal from CERTUM services.

Signing private keys of the Primary Registration Authority operators, used for information signing, are activated after authentication of the operator (PIN number provision) and only for the time of a single cryptographic operation requiring usage of this key. Upon the completion of this operation the private key is automatically deactivated and has to be activated again before execution of another cryptographic operation. Other private keys, e.g. used for authentication of the Primary Registration Authority's applications or creation of encrypted network channel are automatically activated for a period of a single session, immediately after authentication of the operator. The completion of a session deactivates all previously activated private keys.

Activation of a subscriber's private key is carried out similarly to private keys of the Primary Registration Authority operators, regardless whether they are stored on an electronic card or in an encrypted form as a file.

## 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 or the Primary Registration Authority operator, private signing key deactivation is carried out immediately after creation of an electronic signature or session completion (e.g. application logout). If during execution of this cryptographic operation the private key was stored in the operational memory of the application, the application has to prevent unauthorized restoration of the private key.

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

Every private key deactivation is recorded in the event journal.

### 6.2.10. Method of Destroying Private Key

Erasure of private keys of subscriber or the Primary Registration Authority operators involve respectively their erasure from the media (disc, electronic card, operational memory, 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.

Destruction of certification authority private key means physical destruction of the electronic cards and/or other media used for storage of copies or archives of shared secrets. Every private key destruction is recorded in the event journal.

### 6.2.11. Cryptographic Module Rating

See chapter 6.2.1

## 6.3. Other Aspects of Key Pair Management

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

### 6.3.1. Public Key Archive

The purpose of public key archive is to create possibility of 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 timestamp service or certificate status verification service.

*Archive of public keys involves archive of the certificates containing these keys.*

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

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).

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

## 6.3.2. Usage Periods of Public and Private Keys

Usage period of public keys is defined by the value of the field **validity** of every public key certificate (see chapter 7.1). Validity period of a private key may be shorter, which results from the possibility to cease private key usage at any time.

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

Tab.6.1 Maximal usage periods of certification authorities certificates

| Owner and key type | | Main key usage | |
|---|---|---|---|
| | | RSA for certificate and CRL signing | RSA for token signing |
| Certum CA | public key | 25 years | – |
| | private key | 15 years | – |
| Certum Trusted Network CA EC | public key | 35 years | – |
| | private key | 25 years | – |
| Certum Trusted Network CA | public key | 25 years | – |
| | private key | 15 years | – |
| Certum Trusted Network CA 2 | public key | 35 years | -- |
| | private key | 25 years | -- |
| Certum Level I CA | public key | 15 years | – |
| | private key | 12 years | – |
| Certum Level II CA | public key | 15 years | – |
| | private key | 12 years | – |
| Certum Level III CA | public key | 15 years | – |
| | private key | 12 years | – |
| Certum Level IV CA | public key | 15 years | – |
| | private key | 12 years | – |

| | | | |
|---|---|---|---|
| Certum Domain Validation CA SHA2 | public key | 15 years | -- |
| | private key | 12 years | |
| Certum Organization Validation CA SHA2 | public key | 15 years | -- |
| | private key | 12 years | |
| Certum Digital Identification CA SHA2 | public key | 15 years | -- |
| | private key | 12 years | -- |
| Certum Extended Validation CA | public key | 15 years | – |
| | private key | 12 years | – |
| Certum Extended Validation CA SHA2 | public key | 15 years | -- |
| | private key | 12 years | |
| Certum Code Signing CA | public key | 15 years | -- |
| | private key | 12 years | |
| Certum Code Signing CA SHA2 | public key | 15 years | -- |
| | private key | 12 years | |
| Certum Extended Validation Code Signing CA SHA2 | public key | 14 years | -- |
| | private key | 11 years | |
| Certum Class 1 CA | public key | 15 years | – |
| | private key | 14 years | – |
| Certum Class 1 CA SHA2 | public key | 15 years | -- |
| | private key | 14 years | |
| Certum Global Services CA | public key | 15 years | – |
| | private key | 10 years | – |
| Certum Global Services CA SHA2 | public key | 15 years | -- |
| | private key | 10 years | |
| Certum EV TSA SHA2 | public key | – | 10 years |
| | private key | – | 10 years |

*Every user, including a certification authority, can terminate private key usage for electronic signature creation at any time, although the certificate remains currently valid. Notwithstanding, a certification authority is obligated to notify its subscribers of this situation (related for example to key changeover).*

*The rules mentioned above do not applies to the keys used for validation service, signed by intermediate roots.*

The maximum validity period of subscriber's certificates depends on the use of a given certificate:

- The maximum validity period for SMIME certificates is 1095 days
- The maximum validity period for code signing certificates is 1095 days.
- The maximum validity period for website authentication certificates is 730 days

# 6.4. •. Activation Data

Activation data are used for activation of a private key used by the Primary Registration Authority, CERTUM's certification authorities, Registration Points 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.

The Primary Registration Authority's operators and CERTUM's certification authority's operators, as well as other persons performing the roles described in chapter 5.2.1 should operate passwords immune for brute force attacks (also called exhaustive attacks). It is recommended to create a subscriber's password in a similar manner.

In the case of 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 w NIST SP 800-63 and FIPS 180-3.

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

## 6.4.2. Activation Data Protection

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

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

It is recommended that activation data used for private key activation should be protected by means of cryptographic controls and physical access controls. Activation data should be biometric data or should be remembered (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 may be subjected to archive.

## 6.5. Computer Security Controls

The tasks of the Primary Registration Authority and CERTUM's 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 described in the document CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements***Błąd! Nie można odnaleźć źródła odwołania.**, at least EAL3 according to ISO/IEC 15408-3:1999 *Information technology – Security techniques – Evaluation criteria for IT security – Part 3: Security assurance requirements*.

### 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's certification authorities and in their associated components (e.g. the Primary Registration Authority) 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,
- possibility of conducting security audit,
- computers are accessible only by personnel, performing trusted roles in CERTUM,
- enforcement of duty segregation, arising from the role performed in the system,
- identification and authentication of roles and personnel performing these roles,
- cryptographic protection of information exchange session and protection of databases,
- archive of history of operation carried out on the computer and data required by audits,
- a secure path allowing credible identification and authentication of roles and personnel performing these roles,
- key restoration methods (only in the case of hardware security modules) and application and operating system,
- monitoring and alerting means in the case of unauthorized computer resources access.

CERTUM enforces multi factor authentication on any account capable of directly causing Certificate issuance. .

### 6.5.2. Computer Security Rating

CERTUM computer system complies with requirements described in CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures – Part 1: System Security Requirements*.. The above has been confirmed by an independent auditor, performing functionality assessment of CERTUM on the basis of the criteria described in WebTrust Principles and Criteria for Certification Authorities.

## 6.6. Technical Security Life Cycle

### 6.6.1. System Development Controls

Applications used by CERTUM system are developed and implemented by Asseco Data Systems specialists.

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

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

### 6.6.2. Security Management Controls

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

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

### 6.6.3. Life Cycle Security Ratings

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

## 6.7. Network Security Controls

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

.

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.. Security controls are developed on the basis of firewall and traffic filtering on the routers and Proxy services.

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

*Detailed configuration of CERTUM network and its protection means is presented in technical infrastructure documentation. Such documentation has a "non-public" status and is available only to 70nauthoriz individuals.*

## 6.8. Time stamps as a security control

Requests 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 CERTUM's certification authority, the Primary Registration Authority and a subscriber, it is recommended to apply time stamps. Time stamps are created within CERTUM system in accordance with the recommendation RFC 3161 and Microsoft Authenticode™ technology. Timestamps are issued in accordance with Timestamping Authority Policy (document is available *on-line* in the repository).

# 7. Certificate, CRL, timestamp token and OCSP profile

Certificate profiles and Certificate Revocation List profile comply with the format described in ITU-T X.509 v.3 standard, the profile of OCSP token complies with the requirements of RFC 2560, while the profile of timestamp token complies with RFC 3161 (see also *ETSI Time stamping profile, TS 101 861 v1.2.1*). Information stated below describes the meaning of respective certificate fields, CRL, timestamp and OCSP token, applied standard and private extensions employed for the needs of CERTUM.

## 7.1. Certificate Profile

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

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

CERTUM supports the following certificate basic fields:

- **Version**: third version (X.509 v.3) of certificate format,
- **SerialNumber**: certificate serial number, unique within certification authority domain (CERTUM generates non-sequential certificate serial numbers (positive numbers greater than zero) that contain at least 64 bits of output from a CSPRNG);
- **SignatureAlgorithm**: identifier of the algorithm applied by a certification authority issuing certificates,
- **Issuer**: distinguished name (DN) of a certification authority,
- **Validity**: validity period, described by the beginning date (**notBefore**) and the ending date (**notAfter**) of the certificate validity period,
- **Subject**: distinguished name (DN) of the subscriber that is the subject of the certificate,
- **SubjectPublicKeyInfo**: value of a public key along with the identifier of the algorithm associated with the key,
- **Signature**: the sign generated and encoded according to RFC 5280.

In certificates issued by CERTUM values of the above fields are set in accordance with the rules described in Table 7.1.

Tab.7.1 Profile of the basic fields of certificates

| Field name | Value or value constraint | |
|---|---|---|
| Version | Version 3 | |
| Serial Number | Unique value for all certificate issued by certification authorities within CERTUM | |
| Signature Algorithm | sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)<br>sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)<br>sha384WithRSAEncryption (OID: 1.2.840.113549.1.1.12)<br>sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13) | |
| Issuer (Distinguished Name) | Common Name (CN) = | Proper root certificate name |
| | Organization (O) = | **Unizeto Sp. z o.o.** (within certum) or **Unizeto Technologies S.A.** (within ctnDomena) |
| | Organization Unit (OU) = | **Certum Certification Authority** (only within ctnDomena) |
| | Country © = | PL |
| Not before (validity period beginning date) | Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard. CERTUM clock is known as valid world Stratum I service | |
| Not after (validity period ending date) | Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard. CERTUM clock is known as valid world Stratum I service | |
| Subject (Distinguished Name) | Distinguished names comply with the X.501 requirements. Values of all attributes of these fields are optional, except for the following fields: emailAddress (in the case of individual's certificates), organizationName (in the case of non-Repudiation and CA certificates), subjectAltName (in the case of server certificates: contain all domain names or IP addresses), commonName (in the case of server certificates: contain a single IP address or a domain name that is one of the values contained in the certificate's subjectAltName extension), unstructured {Address or Name} (in the case of VPN certificates) which are mandatory. | |
| Subject Public Key Info | Encoded in accordance with RFC 5280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key). | |
| Signature | Certificate signature, generated and encoded in accordance with the requirements described in RFC 5280 | |

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

### 7.1.1. Version

All certificates belonging to CERTUM are issued in accordance with Version 3 (X.509 v.3).

### 7.1.2. Standard extensions fields

The extensions values are created in accordance with RFC 5280. 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. Requirements imposed on the extensions of EV SSL certificates are described in ***Guidelines for the issuance and Management of Extended Validation Certificates***.

CERTUM Root CA Certificates:

basicConstraints (critical) – cA True
keyUsage (critical) – keyCertSign, cRLSign
certificatePolicies – not present
extendedKeyUsage – not present
cRLDistributionPoints – not present
authorityInformationAccess – not present

CERTUM Subordinate CA Certificates:

basicConstraints (critical) – cA True
keyUsage (critical) – keyCertSign, cRLSign
certificatePolicies – anyPolicy
extendedKeyUsage – not present
cRLDistributionPoints – present
authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2

CERTUM subscriber certificates:

basicConstraints (critical) – cA False
keyUsage (critical) –

- digitalSignature (SMIME certificates, codesigning certificates, website authentication certificates)
- keyEncipherment (SMIME certificates)
- Non Repudiation (SMIME certificates)
- Key Encipherment (SMIME certificates, website authentication certificates)
- Data Encipherment (SMIME certificates)

certificatePolicies – see 1.3.1.2
extendedKeyUsage –

- serverAuth (website authentication certificates),
- clientAuth (website authentication certificates, SMIME certificates)
- codeSigning (codesigning certificates)
- Kernel Mode Code Signing (codesigning certificates)
- emailProtection (SMIME certificates)

cRLDistributionPoints – present
authorityInformationAccess – 1.3.6.1.5.5.7.48.1, 1.3.6.1.5.5.7.48.2

### 7.1.3. Electronic signature algorithm identifier

The field of **signatureAlgorithm** contains a cryptographic algorithm identifier describing the algorithm applied for an electronic signature created by a certification authority on the certificate. In the case of CERTUM, RSA algorithm, in combination with SHA-1, SHA-384, SHA-256 or SHA-512 cryptographic hash is used.

```
sha-1WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2)
                            us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 5}
sha256withRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2)
                            us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 11}
sha384WithRSAEncryption OBJECT IDENTIFIER ::= {iso(1) member-body(2)
                            us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 12}
sha512WithRSAEncryption  OBJECT IDENTIFIER  ::=  { iso(1) member-body(2)
                            us(840) rsadsi(113549) pkcs(1) pkcs-1(1)  13}
```

In the case of website authentication certificates, CERTUM applies only SHA-256 or higher algorithms.

### 7.1.4. Name forms

Certificates issued by CERTUM contain the name of the issuer and name of the subject, which are developed in accordance with the principles described in the chapter 3.1.1.

### 7.1.5. Name constraints

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

### 7.1.6. Certificate Policy Object Identifiers

Certification Policy contains information of the policyInformation type (identifier, electronic address) about a certification policy, applied by the issuing authority – this extension is not critical.

Certificates issued by certification authorities include both qualifiers, recommended by the RFC 5280.

### 7.1.7. Usage of Policy Constraints Extensions

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

### 7.1.8. Policy qualifier syntax and semantics

In most cases, certificates issued by CERTUM contain two qualifiers of certification policy, placed in the policyInformation extension. The first qualifier contains a reference to the Certification Practice Statement. The second qualifier – note address qualifi–r - contains a number of note and its content. Number of note describe the type of certificate issued under a policy of certification, and the content of note contains the commercial name of certificate (see Table 1.4).

### 7.1.9. Processing Semantics for Critical Certificate Extensions

The present 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 fie–d - **signatureAlgorithm** and **signatureValue** contain information about respectively: the identifier of the algorithm used for list signing, and electronic signature created on the certificate by a certification authority. The meaning of the last two fields is the same as for the certificates.

The field of **tbsCertList** is the sequence of mandatory and optional fields. Mandatory fields identify CRL issuer, while optional fields contain information about revoked certificates and CRL extensions.

Tab 7.2 The following fields are the contents of mandatory and optional fields of CRL:

| Name | Value | |
|---|---|---|
| Version (wersja) | Version 3 | |
| Signature Algorithm (algorytm podpisu) | sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)<br>sha256WithRSAEncryption (OID: 1.2.840.113549.1.1.11)<br>sha384WithRSAEncryption (OID: 1.2.840.113549.1.1.12)<br>sha512WithRSAEncryption (OID: 1.2.840.113549.1.1.13) | |
| Issuer (wystawca, nazwa DN) | Common Name (CN) = | Proper root name |
| | Organization (O) = | **Unizeto Sp. z o.o.** (within **certum** domain) or<br>**Unizeto Technologies S.A.** ( within **ctnDomena**) |
| | Organization Unit (OU) = | **Certum Certification Authority** (only for certificates within **ctnDomena**) |
| | Count©(C) = | PL |
| thisUpdate | CRL publication date, | |
| nextUpdate | the next CRL publication date, | |
| revokedCertificates: | The information consist of four sub-fields:<br>• userCertif–cate - serial number of a revoked certificate,<br>• revocatio–Date - date of the certificate revocation,<br>• crlEntryExten–ions - **e**xtended access to CRL (contains additional information about revoked certificates – optional),<br>• CRLReason (contains information about a reason for the revocation of a certificate – optional)<br>Information about fields mentioned above are described below: | |
| userCertificate | Serial number of a revoked certificate | |
| revocationDate | Date of the certificate revocation | |
| CRLReason | Returns the reason the certificate was revoked. Values of this field are set in accordance with the rules described in chapter 7.2.2 | |
| Extensions | Extended information about certificate. (See chapter 7.2.1) | |
| Signature | An identifier of the algorithm used by a certification authority to sign CRL in accordance with requirements described in RFC 5280. | |

### 7.2.1. Version Number

CERTUM supports both X.509 Version 1 and Version 2 CRLs. Version 1 CRLs is used by CERTUM certification authorities which are no longer issue certificates (Certum Level I, Certum Level II, Certum Level III and Certum Level IV). CRLs for intermediate certification authorities

that issue certificates (Certum Level I CA, Certum Level II CA, Certum Level III CA, Certum Level IV CA) are published in version 2.

### 7.2.2. Supported CRL entry extension

Among numerous extensions, the most important are the following ones: **authorityKeyIdentifier**.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). Function and meaning of extensions are the same as for certificate extensions (see chapter 7.1.2).

## 7.3. OCSP response token profile

The protocol of on-line certificate status verification (OCSP) is used by certification authorities and allows certificate status evaluation.

Certificate status verification service is provided by CERTUM on behalf of all affiliated certification authorities. OCSP server, which issues certificate status confirmations, employs a special key pair, developed solely for this purpose.

Certificate status verification server certificate has to contain in its body the extension of **extKeyUsage**, described in RFC 5280. This extension should be set as **critical**, and means that a certification authority issuing the certificate to the OCSP server, confirms with its signature delegation of the authorization to issue certificate status conformation (of this authority subscriber's certificates).

Certificate may also contain information about the means of contact with the server of certificate status verification authority. This information is included in the extension **AuthorityInfoAccessSyntax**.

In accordance with RFC 2560 (*X.509 Internet Public Key Infrastructure: Online Certificate Status Protocol – OCSP*, June 1999), CERTUM's certificate status verification may be issued in three modes:

- the **Local** mode, where certification authority issued the revised certificate and the certificate status verification shall be signed by the same private key of certification authority that was used to sign the verified certificate,
- the **Trusted Responder** mode, where requestors trust the public key certificate of the responder;
- the **Authorized Responder** mode, where certification authority provides a primary source of certificate status information.

When certification authority provides OCSP service in the Authorized Responder mode, **extendedKeyUsage** extension must be entered with the value: *id-kp-OCSPSigning*.

All certification authorities that provide OCSP services within the framework of CERTUM work in the **Authorized Responder** mode.

### 7.3.1. Version Number

Certificate status verification server operating within CERTUM issues certificate status tokens in accordance with the RFC 2560. The only allowable value of the version number is 0 (it is an equivalent of version 1).

### 7.3.2. OCSP extensions

The current version of CERTUM certificate status verification server does not include extensions **certHash** and **archiveCutOff** in its OCSP response. Notwithstanding, CERTUM declares that the certificate status good, received in OCSP response, means the certificate was issued by (any) certification authority and that it has not been revoked prior to its expiration date

In accordance with RFC 6960, CERTUM's certificate status verification server supports the following extensions:

- Nonce – binding a request and a response to prevent reply attacks. Nonce value is included in **requestExtension** of the **OCSPRequest** and repeated in the field **responseExtension** of the **OCSPResponse**.
- If the verified certificate is included on CRL, the response should contain identification data of the list. Information about CRL should contain CRL's URL address, its serial number and time of the list issuance. These information is provided in the field **singleExtensions** of the **SingleResponse**.
- If the verified certificate is included on CRL, the response should additionally contain three extensions of the CRL, described in chapter 7.2.2. This information are included in the field **singleExtensions** of **SingleResponse** structure.
- Types of responses accepted by a subscriber (i.e. his/her/its application) submitting a request to OCSP server. This extension describes the declared type of responses which can be interpreted by the application (**id-pkix-ocsp-basic** among others) and is supplied in the request as the extension **acceptableResponses**.

Every recipient of token issued by OCSP server has to be able to support the standard type of a response with the **id-pkix-ocsp-basic** identifier.

# 7.4. Other profiles

## 7.4.1. Timestamp token profile

**Certum EV TSA SHA2** electronically signs issued timestamp tokens with one or more private keys reserved solely for this purpose. According to RFC 3280 recommendation certificates of their complimentary public keys contain field constraining allowed key usage (**ExtKeyUsageSyntax**), marked as **critical**. This means the certificate may be used by the time-stamping authority solely for the purposes of signing timestamp tokens issued by this authority.

Tab. 7.3 shows the various requirements imposed on the Certum Time Stamping Authority:

| Policy name | Policy identifier | Compliance | Time source |
|---|---|---|---|
| Certum Time Stamping Authority | iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum-tsa(5) 1 11 | RFC 3161 | External Time Source STRATUM 1 + NTP |
| | | ETSI TS 101 861, Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates, Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates | |

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

Timestamp token, issued by **Certum EV TSA SHA2** contains information on timestamp (**TSTinfo** structure), located in **SignedData** structure (see RFC 2630), signed by timestamping authority and embedded in **ContentInfo** structure (see RFC 2630).

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

### 7.4.1.1. Version number

**Certum EV TSA SHA2** operating within CERTUM issues timestamp tokens in accordance with the RFC 3161 or ETSI TS 101 861. The only allowable value of the version number is 1 (it is an equivalent of v1 version).

### 7.4.1.2. Timestamp extensions

Timestamp tokens issued by **Certum EV TSA SHA2** do not contain any extensions.

# 8. Audit

Audits intend to control the consistency of the actions of CERTUM service unit or subjects delegated by the unit, with their declarations and procedures (including Certification Policy and Certification Practice Statement).

The audit mainly regards a data processing and key management procedures. It also concerns all certification authorities belonging to the certification path of primary certification authority **Certum CA** and **Certum Trusted Network CA**, the Primary Registration Authority, and other elements of public key infrastructure, e.g. OCSP server.

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). In both cases, an audit is carried out on request of and under supervision of a **security inspector** (see chapter 5.2.1). **Criteria**.

## 8.1. Audit Frequency

On a quarterly basis, CERTUM performs regular internal audits against a randomly selected sample of at least three percent of its website authentication and codesigning certificates issued since the last internal audit.

On a monthly basis, CERTUM performs regular internal audits against a randomly selected sample of at least five percent of all its certificates issued from sub-root CAs affiliated to CERTUM's Partners issued since the last internal audit.

CERTUM is annually audited for compliance to **AICPA/CICA WebTrust for Certification Authorities – Extended Validation Audit Criteria** and **AICPA/CICA WebTrust for Certification Authorities – SSL Baseline Requirements Audit Criteria**.

## 8.2. Identity/Qualifications of Auditor

An external audit is carried out by an authorized and independent from CERTUM domestic institution or the institution with a representation in Poland. Such an institution should:

- hire employees who possess appropriate technical knowledge (with supplied documents proving it) concerning public key infrastructure, information security techniques and devices, and security auditing,
- be a registered, well-known and respected organization or society.

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

## 8.3. Auditor's Relation to Audited Party

See chapter 8.2

## 8.4. Topics Covered by Audit

External and internal audits are carried out in accordance with the rules specified by American Institute of Certified Public Accountants/Canadian Institute of Chartered Accountants (AICPA/CICA) *Web Trust Principles and Criteria for Certification Authorities*.

The scope of Web Trust audit includes:

- physical security of CERTUM,
- procedures of subscribers' identity verification,
- certification services and procedures of the services delivery,
- security of software and network access,
- security of CERTUM personnel,
- system journals and system monitoring procedures,
- backup copy creation and their recovery,
- archive procedures,
- records of configuration parameters changes of CERTUM ,

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 **security inspector**. Within 14 days of the record submission, the inspector is committed to prepare an opinion concerning the deficiencies specified in the records. Information about deficiencies removal is submitted to the auditing organization.

## 8.6. Notifying of Audit Results

Audit records (as detailed as possible) and the auditor's general opinion are published in the repository upon every audit.

# 9. Other business and legal issues

## 9.1. Fees

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

http://www.certum.eu

CERTUM applies four models of charging for its services:

- **retail sale** – fees are charged separately for every service unit, e.g. every single certificate or a small package of certificates,
- **wholesale** – fees are charged for a package of certificates, a number of certificates sold once,
- **subscription sale** – fees are charged once a month; the extent of this charge depends on a type and number of service units and is particularly used in timestamp services and certificate status verification by means of OCSP protocol,
- **indirect sale** – fees are charged for every service unit from a customer who renders services established on the basis of CERTUM infrastructure, e.g. if a new commercial certification authority receives a certificate from CERTUM, CERTUM charges a fee for every certificate issued by this authority.

Fees can be paid by money transfer or direct payment in Asseco Data Systems S.A. branches on the basis of an invoice or an order.

### 9.1.1. Certificate Issuance or Renewal Fees

CERTUM charges a fee for issuance or renewal of a certificate.

Considering the dissimilarity of the procedures of certificate issuance and renewal, the charges paid on the basis of the above mentioned models can be divided into three components:(1) identification and authentication costs or costs of service in a registration authority, (2) the costs of certificate issuance and (3) the costs of personalization and electronic cryptographic card issuance. These components can be individual items in a price-list and be useful in cases of certificate renewal (identification costs, subscriber's authentication costs, and smart card issuance costs can be omitted).

### 9.1.2. Certificate Access Fees

Certificate access fees are only applicable to particular cases of relying parties. In charging fees, models of subscription sale and indirect sale are employed. In the latter case, fees are charged depending on the number of applications (e.g. points of sale) owned by a relying party.

Certificate access fees are not fixed by means of agreements with relying parties. The extent of these fees is dependant on the certificates credibility.

*CERTUM does not charge a fee for making the certificates of Certum Level I CA credibility level accessible to relying parties.*

### 9.1.3. Revocation and Status Information Access Fees

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

CERTUM can charge fees for certificate status verification service, rendered on the basis of OCSP protocol or other accessible devices from third parties. In charging fees, the model of retail sale or subscription is employed.

Without CERTUM written approval, the access to CRLs or the information about certificate status is prohibited for third parties delivering the services of certificate status verification. The access might be provided only upon a prior agreement with CERTUM. In this instance, the indirect sale model is employed (i.e. a fee is charged for every confirmation of the status of the certificate issued by a third party) for charging fees.

### 9.1.4. Other Fees

CERTUM can charge fees for other services (see 9.1.) The services might concern:

- generating keys to certification authorities or subscribers,
- testing of applications 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,
- auditing Registration Points or subsidiary certification authorities,
- trainings.

### 9.1.5. Fees Refund

CERTUM makes efforts to secure the highest level of its services. If a subscriber or a relying party are not satisfied with the services, they may request certificate revocation and fee refund within 30 days of the certificate issuance. Following that period, a subscriber is entitled to claim the certificate revocation and the fees refund only if CERTUM does not fulfil its obligations and duties specified in the present Certification Practice Statement.

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

## 9.2. Financial Liability

The liability of CERTUM service unit and the parties connected by the services rendered by this unit results from routine activities performed by these entities or from third parties' activities. The liability of every entity is stated in mutual agreements or arises from statements of will.

CERTUM is responsible for the events defined in chapter 9.9 of this Certification Practice Statement.

CERTUM is financially responsible to the subscribers of CERTUM's certification services and **the relying parties being the beneficiaries of the warranty**. These entities are hereinafter referred to as **the entities being the beneficiaries of the warranty**.

CERTUM does not take any responsibility for the actions of other third parties not specified in chapter 9.2 of this Certification Practice Statement.

CERTUM's financial responsibility applies to the entities being the beneficiaries of the warranty only if damages are the fault of CERTUM or of the parties that Asseco Data Systems S.A. made an agreement with in such a way that the fault is transferred to CERTUM.

The entity being the beneficiaries of the warranty must submit all claims to CERTUM within 30 days of the occurrence of the event that gave rise to the warranty claim.

CERTUM's financial responsibility applies to the entities being the beneficiaries of the warranty only if damages have occurred within the validity period of the certificate of the certificate.

If CERTUM confirms and agrees that damages have occurred, Asseco Data Systems SA undertakes with the entities being the beneficiaries of the warranty to pay the damages. The maximum amount an entities being the beneficiaries of the warranty is entitled to recover under the one warranty claim per specific type of certificate issued on the basis of given certification policy doesn't exceed the maximum payment limit for one covered incident defined in the Table 9.1. The maximum payment limit doesn't exceed the amount of damage.

The entities being the beneficiaries of the warranty, in relation to the one certificate within its validity period, are collectively eligible to receive a maximum amount of the financial liability up to aggregate maximum payment limit defined in the Table 9.1

In the event the damages sustained by the use or reliance on a CERTUM certificate exceed the financial liability for such certificate , payment of damages shall be apportioned first to the earliest warranty claims asserted by the entities being the beneficiaries of the warranty**.**

### 9.2.1. Scope of insurance

CERTUM maintains actual errors and omissions insurance coverage. Also, it is recommended to subscribers, and the relying parties to (especially legal persons) have a risk insurance policy, if they want to have a higher level of security than that guaranteed by CERTUM.

Certification authorities and other entities affiliated by CERTUM are obligated to maintain a commercially reasonable level of insurance coverage for errors and omissions.

### 9.2.2. Other assets

CERTUM and each authority or other entity affiliated by CERTUM have sufficient financial resources to maintain their operations and perform their duties, and their obligations and guarantees provided to subscribers and relying parties.

### 9.2.3. Extended Warranty Coverage

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

## 9.3. Confidentiality of business information

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 *Personal Data Protection Law of 29th of August, 1997* including its later changes and execution acts.

Asseco Data Systems S.A. ensures that third parties are given the access only to the information that are publicly accessible in a certificate. The other data provided in applications submitted to CERTUM shall never be voluntarily or deliberately revealed to a third party in any circumstances (besides court and national authorities request, based on force in law).

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

## 9.3.1. Scope of Confidential Information

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[24] are managed and governed by internal company regulations and in particularly concerns:

- information supplied by subscribers, besides the information that needs to be revealed for appropriate certification services; in other cases the revelation of received information requires a prior written approval of the information beholder or a legally valid court writ,
- information supplied by/to subscribers (e.g. the contents of agreements with subscribers and relying parties, accounts, applications for registration, issuance, renewal, revocation of certificates (except for information included in certificates or the repository, in accordance with the present Certification Practice Statement); 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),
- record of system transactions (the whole of the transactions, as well as **data for control inspection** of transaction, the so called system transactions logs),
- record of information about events (logs) connected with certification services, stored by CERTUM and the Primary Registration Authority,
- records of an internal and external control, if it might cause a threat to CERTUM security (in accordance with chapter 9.3.2 the majority of this information should be accessible for the public),
- emergency plans,
- information about steps taken in order to protect hardware devices and software, information about administering of certification services and planned registration rules.

*Asseco Data Systems S.A. is not obligated to keep secret in relation to a party of the agreement about the delivery of certification services. Persons responsible for keeping secret and obeying the rules concerning information practice bear criminal liability in accordance with the law regulations.*

## 9.3.2. Information Not Within the Scope of Confidential Information

The whole information indispensable for the process of appropriate functioning of certification services is not considered confidential and private. It particularly concerns the information included in a certificate by certificate issuing authorities, in accordance with the description in chapter 7.17. 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.

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

The following information is accessible for the public in the repository:

- Certification Policy and Certification Practice Statement,
- templates of agreements of CERTUM with subscribers,
- the price list of services,
- guides for users,
- the Primary Registration Authority's, Registration Points and CERTUM's certification authorities certificates,
- certificates belonging to subscribers (upon their prior approval),
- Certificates Revocation List,
- extracts from post-control reports (as detailed as possible) prepared by an authorized institution.

The extracts from post-control reports, published by CERTUM, concern:

- the scope of audits,
- a general assessment by an auditing institution,
- the extent of the implementation of the recommendations.

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. Responsibility to Protect Private Information

CERTUM receiving private information shall secure it from compromise and disclosure to third parties.

## 9.4. Privacy of Personal Information

### 9.4.1. Privacy Policy

Personal data submitted to CERTUM are stored and processed in accordance with the law in force, particularly with *Personal Data Protection Law of 29th of August, 1997* including its later changes and execution acts. CERTUM collects information as proportional to its intended use. Consent of subscriber or representative for the processing of personal data is contained in the Subscriber/Applicant Agreement, and is mandatory.

Personal data are used only in connection with the provision of certification services.

Personal data are protected in accordance with privacy policies contained in the security policy Asseco Data Systems SA

### 9.4.2. Information Treated as Private

Any information about Subscribers that is not publicly available through the content of the issued certificate, repository and online CRLs is treated as private

### 9.4.3. Information Not Deemed Private

All information made public in a certificate is deemed not private, unless specifically provided otherwise in the *Data Protection Law of 29th of August, 1997* including its later changes and execution acts.

### 9.4.4. Responsibility to Protect Private Information

CERTUM and registration authorities receiving private information shall secure it from compromise and disclosure to third parties. Regardless of the above, granting access to private information must be consistent with the requirements of the *Data Protection Law of 29th of August, 1997* including its later changes and execution acts.

### 9.4.5. Notice and Consent to Use Private Information

Unless where otherwise stated in this Certificate Practice Statement, the applicable privacy policy or by agreement, private information will not be used without the consent of the party to whom that information applies.

Reservations and permits shall not violate the provisions of the *Data Protection Law* act.

### 9.4.6. Other information disclosure circumstances

The present 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 accordance with the requirements of the *Act of 4 February 1994 On Copyright and Related Rights.*

Detailed rules for the protection of intellectual property rights of subscribers and the relying parties are described below:

*CERTUM has exclusive rights to any product or information being designed and implemented on the basis of or in compliance with the present Certification Practice Statement. Trademarks, brand names, symbols and emblems company which belong to CERTUM may not be used in any manner without the prior written permission of CERTUM.*

### 9.5.1. Property Rights in Certificates and Revocation Information

Certification authorities forming CERTUM Certification Authority retain all intellectual property rights in and to the certificates and revocation information that they issue. CERTUM shall grant permission to reproduce and distribute certificates without any reservations and charges. Using the information might be payable and limited if so required by provisions of agreements or this Certification Practice Statement.

### 9.5.2. Property Rights in the Certificate Practice Statement

CERTUM retains all intellectual property rights in and to this Certificate Practice Statement.

### 9.5.3. Property Rights in the Names and Trademarks

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


Fig. 9.1 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 Point operating on behalf of CERTUM. The approval of the use of CERTUM logo is automatically issued when a new Registration Point is registered by the Primary Registration Authority.

All subscribers retain all rights it has (if any) in any trademark, service mark, or trade name contained in any certificate application and distinguished name (DN) within any Certificate issued to such subscriber.

### 9.5.4. Property Rights in Keys

Every key pair associated with a public key certificate issued by CERTUM is the property of the subject of the certificate, described in the field subject of the certificate (see chapter 7.1 ) regardless of the physical medium within which the keys are stored and protected.

CERTUM root certification authorities certificates are the property of CERUM. CERUM licenses software and hardware manufacturers to reproduce such root certificates to place copies in trustworthy hardware devices or software.

Finally, Secret Shares (so called shadows) of private keys of CERTUM root certification authorities, CERTUM intermediate certification authorities and other entities operating within **certum** and **ctnDomena** domains are the property of CERTUM, and the CERTUM retains all intellectual property right in and to such Secret Shares.

## 9.6. General Provisions

This chapter describes obligations/guarantees and liability of CERTUM's certification authorities, the Primary Registration Authority, Registration Points, subscribers and relying parties. The obligations and liability are governed by mutual agreements made by the parties mentioned above.

### 9.6.1. Certification Authority Obligations

CERTUM ensures that:

- at the time of issuance, CERTUM implemented a procedure for verifying that the Subscriber either had the right to use, or had control of, the Domain Name(s) and IP address(es) listed in the certificate's subject field and subjectAltName extension,

- at the time of issuance, CERTUM implemented a procedure for verifying that that the Subscriber Representative is authorized to request the certificate on behalf of the Subscriber,
- at the time of issuance, CERTUM implemented a procedure for verifying the accuracy of all of the information contained in the certificate (with the exception of the subject:organizationalUnitName attribute,
- at the time of issuance, CERTUM implemented a procedure for reducing the likelihood that the information contained in the certificate's organizationalUnitName attribute would be misleading,
- when issuing the certificate, if the certificate contains subject identity information, CERTUM implemented a procedure to verify the identity of the subscriber,
- CERTUM will revoke the certificate for any of the reasons specified in this CPS.
- its commercial activity is based on reliable devices and software creating a system that fulfils requirements stated in CWA 14167-1 Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signa–ures - Part 1: System Security Requirements and FIPS PUB 140 norm *Security Requirements for Cryptographic Modules*,
- comply with:
  - Baseline Requirements Certificate Policy for the Issuance and Management of Publicly-Trusted Certificates,
  - Guidelines For The Issuance And Management Of Extended Validation Certificates,
  - Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates,
  - Minimum Requirements for the Issuance and Management of Publicly-Trusted Code Signing Certificates,
- its activity and services are provided in accordance with the law; in particular they do not violate copyrights and licensed third parties rights,
- its services are provided in accordance with broadly accepted norms:
  - certification ser–ices - with X.509, PKCS#10, PKCS#7, PKCS#12,
  - timestamp services – with the recommendation RFC 3161,
  - certificate status verification (OSCP) – with the recommendation RFC 2560,
- it complies with and exacts the procedures described in the present Certification Practice Statement, particularly concerning:
  - verification of the subscriber's identity, whom a certificate within CERTUM domain is issued to; procedures verifying subscriber's identity depend on the information included in a certificate and vary according to certificate fees, nature and identity of the subscriber of the certificate and applicability range in which the certificate is credible (see chapters3 3 and 44),
  - certificates which are revoked in the case of existing supposition or certainty that the certificate contents are not up-to-date or that a private key connected with the certificate was compromised (revealed, lost, etc.),
  - informing a subscriber and other entities interested in issuing and revoking the certificate,
  - publication of the lists of revoked certificates,

  - generating and using private keys only for the purposes defined in the present CPS and securing keys in a way not permitting the application of the keys not in accordance with their purposes,
  - personalization and issuance of electronic cryptographic cards where certificates and a key pairs are stored (in the cases when the card was generated by a certification authority),
  - periodical and punctual publication of the information indispensable for correct reception, management and revocation of certificates,
- issued certificates do not contain any falsified data, neither known nor coming from the people confirming the applications for certificate issuance or issuing certificates,
- issued certificates do not contain any mistakes resulting from negligence or procedure violence by the people confirming applications for certificate issuance or issuing certificates,
- subscribers' Distinguished Names (DN) listed in certificates are unique within **CERTUM** domain,
- it secures personal data protection in accordance with *Personal Data Protection Law of 29th August, 1997* including its later changes and accomplishing regulations,
- 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:

- register and issue certificates only to certification authorities whose certification practices guarantee security level no lower than guaranteed by CERTUM and whose CP and CPS are approved by CERTUM,
- make agreements with subscribers, certification authorities and Registration Points; certification services are delivered only on the basis of the agreements and always on request of a subscriber, a certification authority or a Registration Point,
- manage a list of registered Registration Points with which CERTUM has cooperation agreements and agreements about recommending the devices and software used by these authorities,
- manage a list of recommended software and devices used for generating asymmetric key pairs,
- carry out scheduled audits in CERTUM's certification authorities, the Primary Registration Authority and Registration Points belonging to or connected with CERTUM domain,
- charge independent auditors with intended audits of CERTUM domain, make all necessary documents and information accessible to auditors, comply with auditors' post-audit recommendations.

## 9.6.2. Registration Authority Obligations

The Primary Registration Authority and every Registration Point operating within CERTUM or bound by an agreement with CERTUM ensures that:

- its commercial activity is based on reliable devices and software, recommended by CERTUM,

- its activity and services are in accordance with the law and do not violate copyrights and licensed third parties rights,
- it makes reasonable efforts to secure that subscribers' identification data set in CERTUM database are correct, and this information is updated in the moment of the data confirmation,
- confirmed subscriber's information, later sent to a certification authority for including it to a certificate, is precise,
- it does not contribute intentionally to mistakes or inaccuracy in information contained in a certificate,
- its services are in accordance with broadly accepted norms (de jure and de facto): X.509, PKCS#10, PKCS#7, PKCS#12,
- its services are delivered on the basis of procedures which are adjusted to the recommendations of the present Certification Practice Statement; this concerns in particular:
  - procedures of subscribers' identity verification,
  - procedure of performance of the check to prove a private key possession[25], associated with a public key requested for certification,
  - procedures of reception, processing and confirmation or rejection of customers' requests for the issuance, renewal and revocation of the certificate,
  - procedures of requesting a certification authority, on the basis of already accepted subscriber's application, for the issuance, renewal and revocation, of the certificate; these procedures also state the circumstances in which a certification authority can apply for the above services itself,
  - procedures of the registration of other Registration Points that already made agreements with CERTUM (these procedures does not apply to the Primary Registration Authority),
  - procedures of archive of applications and information received from subscribers, issued decisions and information submitted to certification authorities,
  - procedures of generating keys for subscribers, provided that the agreement with a certification authority and a subscriber permits that,
  - procedures of personalization and issuance of electronic cryptographic cards which stores certificates and key pairs (if the Primary Registration Authority generated the key pair),
- it submits to scheduled external and internal audits, particularly to those carried out by CERTUM service unit or to the ones commissioned by this unit.

Beside above, the Primary Registration Authority and each Registration Point commits itself to:

- submit to CERTUM recommendations, particularly to those resulting from audits,
- to secure personal data protection in accordance with *Personal Data Protection Law of 29th August, 1997* including its later changes and accomplishing regulations,
- protect operators' private keys in accordance with the security requirements specified in Certification Practice Statement,

25 See **Glossary**

- not to use operators' private keys for purposes different from those stated in the present Certification Practice Statement, unless it is approved by CERTUM,
- obtain from reliable sources and thoroughly verify public key **active certificates**[26] and CRL's of CERTUM certification authorities.

## 9.6.3. Subscriber Obligations

By applying for registration to the registration authority and accepting of issued certificate (see chapter 4.3 and 4.4), a subscriber agrees to enter the certification system on the conditions stated in this CPS.

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

Irrespective of the character of an agreement, the end subscriber is committed to:

- approve the terms stated in an official or informal agreement between a subscriber and CERTUM; this approval should consist of a hand-written signature (official agreement) or an electronic statement of will (informal agreement) at the moment of approval of data to be included in requested certificate; the contents of the subscriber's statement of will are published in the repository,
- approve (see chapter 4.4) certificate issued to him/her/it; warranties and CERTUM liability connected with a particular certificate are valid from the date of the approval of a certificate,
- take precautions allowing to generate appropriately (by itself or by the Primary Registration Authority) and safely store a private key of a key pair (prevent it from loss, compromise, modification and unauthorized usage,
- state true data in applications submitted to the Primary Registration Authority or Registration Point and then stored in CERTUM service unit database and in public key certificates issued by this unit; a subscriber must be aware of the liability for the direct or indirect damages that are a consequence of falsifying of data,
- check or guarantee that every electronic signature made by means of a private key belonging to the end subscriber and associated with an approved public key certificate is the subscriber's signature, and acknowledge that this certificate was neither invalid (beyond the expiry date) nor revoked when the signature was made,
- get to know in general the notions concerning certificates, electronic signatures and public key infrastructure (PKI).

Subscriber is also committed to:

- comply with the rules of the present Certification Practice Statement and Certification Policy,
- submit or present copies of required documents confirming the information included in a submitted application and the identity of the requester or the entity acting on behalf of the subscriber,
- in the case of security violation (or security violation suspicion) of their private keys, notify the issuer of the certificate or any Registration Point affiliated by CERTUM,

[26] See **Glossary**.

- apply public key certificates 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 (see chapter 1.4 1.4),
- generate cryptographic keys, manage passwords, public and private keys, exchange information with the Primary Registration Authority and CERTUM's certification authorities only by means of the software recommended by CERTUM; the access to this software, media, and devices on which the keys or passwords are stored should be appropriately controlled,
- regard the loss or revelation of the password (revealing it to an unauthorized person) as the loss or revelation of the private key (revealing it to an unauthorized person),
- not to make his/her/its private keys accessible to other persons and, in the case of the code signing certificates, generate and store the private key only on external devices,
- not to use as a subscriber a private key, associated with the certificate issued by CERTUM, for signing any CRLs or certificates,
- submit the proof of a private key possession to the Primary Registration Authority or CERTUM's certification authority, or prove the possession of the key in another way,
- obtain public key certificates of CERTUM's certification authorities and other CERTUM service units.
- accept the fact that, if the certificate is identified as a source of suspect code or was used to sign malware / code and the certificate is revoked for that reason, CERTUM reserves the right to share information about the applicant, signed application, certificate, and surrounding circumstances with other CAs or industry groups, including the CA/Browser Forum.

## 9.6.4. Relying Party Obligations

The object of an agreement between relying party and:

- Asseco Data Systems S.A. may be the delivery of repository services, timestamp services and certificate status verification services (OCSP) by this authority ,
- subscriber is specification of the conditions that an electronic signature must fulfil to be considered valid by a relying party or the certification services regulations.

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

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

- approve the terms stated in this CPS, CP, Timestamping Authority Policy etc. Relying party approves above terms at the time of the first usage of any service delivered by CERTUM or the first approval of the subscriber's signature. Warranties and liabilities of subscriber's or CERTUM are valid from the date of the acceptance of the certificate issued to the subscriber,
- thoroughly verify[27] every electronic signature made on a certificate or document submitted to him/her/it. In order to verify the signature a relying party should:

[27] 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.

  - specify a certification path containing all certificates belonging to other certification authorities that make it possible to verify the signature on the certificate of a signature issuer,
  - check whether neither of certificates creating a certification path are placed on the list of revoked certificates; revocation of any certificate from certification path influences the earlier expiry of the validity date up to which the verified signature could have been created,
  - check if all certificates belonging to a certification path belong to certification authorities and if they are authorized to sign other certificates,
  - (optionally) specify the date and time of signing a document or a message. It is possible only when the document or message were signed (prior to signing them) with a timestamp issued by a timestamp authority, or a timestamp was associated with an electronic signature just after the creation of the electronic signature on the document; such a verification allows for delivering of non-repudiation services or resolve possible disputes,
  - using a defined certification path, verify credibility 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 credibility 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, e.g. in a signature policy (see chapter 1.41.4),
  - whose status was verified on the basis of the valid Certificate Revocation Lists or OCSP service, available at CERTUM,
- specify the conditions that a public certificate key and a electronic signature must fulfil in order to be deemed valid by this party; the conditions can be formulated e.g. as an appropriate certification policy, and published.

Every document with a defective or questionable electronic signature should be rejected or possibly subjected to other procedures that allow for stating its validity. Any person approving of such a document bears responsibility for any consequences following it, disregarding of broadly accepted features of an electronic signature, which describe it as an effective means of verification of the identity of a subscriber who makes a signature.

## 9.6.5. Obligations of Other Parties

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

## 9.7. Disclaimers of Warraties

Warranties of CERTUM are based on the general rules stated in the present Certification Practice Statement and it is in accordance with the superior legal acts in force in the Republic of Poland. Disclaimer of warranties should be specified in an agreements with subscribers and CERTUM.

## 9.8. Limitations of Liability

If damages are the fault of CERTUM or of the parties that Asseco Data Systems S.A. made agreement with in such a way that the fault is transferred to CERTUM, collective financial warranties of CERTUM in relation to all parties (including relying parties) cannot exceed (in a single case) the total amount of sums for credibility level specified in Table 9.1.

Table 9.1 Financial liability

| Certificate type | Collective CERTUM's liability limit in relation to a particular policy | CERTUM's liability limit per covered damage |
|---|---|---|
| All certificates issued by:<br>Certum Level I CA,<br>Certum Class 1 CA,<br>Certum Class 1 CA SHA2 | 0 EUR | 0 EUR |
| Personal certificate with email address validation | 6 000 EUR | 600 EUR |
| Personal certificates with DN data validation[28] | 60 000 EUR | 6 000 EUR |
| SSL certificates with domain validation only (DV) | 200 000 EUR | 600 EUR |
| SSL certificates with organization validation (OV) | 400 000 EUR | 15 000 EUR |
| Extended Validation SSL certificates (EV) | 1 000 000 EUR | 15 000 EUR |
| Code signing certificates | 60 000 EUR | 6 000 EUR |
| Extended Validation Code Signing certificates (EV) | 1 000 000 EUR | 15 000 EUR |
| Certificates issued by Certum Global Services CA | Specified in agreement | Specified in agreement |

Total collective CERTUM liability in relation to a particular entity or all entities (private and legal) or the devices owned by the entity / entities, resulting from the usage of a certificate of a particular type for creating of an electronic signature or for other cryptographic operations, is limited to amounts not exceeding the amounts stated in Table 9.1.

[28] Maximum liability value for dedicated agreement

# 9.9. Liability

## 9.9.1. Subscriber Liability

Subscriber liability results from the obligations and warranties stated in chapter 9.6.3. The liability conditions are governed by an agreement with Asseco Data Systems S.A.

## 9.9.2. Relying Party Liability

Relying party liability results from the obligations and warranties stated in chapter 9.6.4. The liability conditions may be governed by an agreement with CERTUM and a subscriber.

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

The parties should state the financial value of transaction that will be approved by them solely on the basis of the information set in a certificate, and familiarize with information specified in chapter 9.6.4 of this document.

# 9.10. Term and termination of Certification Practice Statement

## 9.10.1. Term

This CPS becomes effective from the moment of marked with the status valid and publication in the CERTUM repository. Appendices to this CPS become effective upon publication in the CERTUM repository.

## 9.10.2. Termination

Certification Practice Statement is in force (has a current status) up to the moment of marked with the status **valid** and publication and approval of its new version.

## 9.10.3. Effect of Termination and Survival

Upon termination of this CPS, subscribers and relying parties are nevertheless bound by its terms for all certificates issued for the remainder of the validity periods of such certificates.

# 9.11. Individual Notices and Communications with Participants

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

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

Some information and announcements must be supplied to parties in accordance with an established schedule or deviation from this schedule. This particularly concerns publishing of CRLs and new certificates belonging to the Primary Registration Authority and CERTUM's certification authorities, in the way rendering them available by all interested parties (including relying party) at any time. Information on each security breach of private key owned by any certification authority must be published, rendering them available by all interested parties.

# 9.12. Amendments to the Certification Practice Statement

This Certification Practice Statement is reviewed at least annually. Modification to Certification Practice Statement may be a result of observed errors, CPS update and suggestions from the affected parties.

However, CERTUM updates the Certification Practice Statement whenever when the following documents change and changes affect CERTUM's activities:

- Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates,
- Guidelines For The Issuance And Management Of Extended Validation Code Signing Certificates and

- Guidelines For The Issuance And Management Of Extended Validation Certificates.

### 9.12.1. Changes 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 Certification Practice Statement may be submitted by the following authorized entities:

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

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

Introduced modification may be generally divided into two categories:

- the one that does not require notification of subscribers, and
- the one that requires (usually in advance) notification of subscribers.

*Decision on acceptance of the changes in Certificate Practice Statement version or build number is made by Chief of CERTUM.*

### 9.12.2. Notification Mechanism and Period

After notification in advance, each and every item of the Certification Practice Statement may be subjected to amendment. Information about every significant modification in question by CERTUM is submitted to every affected party in the form of indication of a storage point of a new version of Certification Practice Statement with the status **requested for comments**. 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.

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

Comments on modifications suggested by CERTUM may be submitted by the affected parties within 10 working days of their announcement. If as a result of the submitted comments, CERTUM administered **significant modification** to the suggested changes, the changes have to be published once more and subjected to assessment. In other cases, a new version of

Certification Practice Statement receives the status **under approval** and is subjected to approval procedure (see chapter 1.5.4).

*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 certification service users, Chief of CERTUM may assign a new identifier (Object Identifier) for a modified document of Certification Practice Statement. Identifiers of the certification polices applied by authorities issuing certificates may also be subjected to modification. Such is the case upon implementation of changes to:

- extension of a certificate user group for areas associated with e.g. electronic payment system, information interchange within banking environment and between banks, etc.,
- introduction of new types of certificates,
- allowance within the system of the cross-certification between authorities issuing certificates,
- significant modification to content and interpretation of certificate and CRL fields, e.g. modification of fields meaning from non-critical to critical and vice-versa,

## 9.13. Disputes Resolution

The subject of disputes resolution can only be discrepancies or conflicts between the parties bound with one another by mutual official or informal agreements referring to the present Certification Practice Statement.

Disputes or complaints following the usage of certificate, timestamping or certificate status services delivered by CERTUM will be resolved by mediation on the basis of written information. Claims must be made in writing to the following address:

Asseco Data Systems SA
Podolska Street 21
81-321 Gdynia
Poland

Complaints will be dealt with the Asseco Data Systems SA Legal Department. They will be proceed in a written form within 21 days. In a case no solution will be found according dispute within 45 days from the start of the conciliation, the parties can hand over the dispute to appropriate court. The court, appropriate for case handling, will be the Public Court of the defendant.

In the instance of the occurrence of arguments or complaints following the usage of an issued certificate or services delivered by CERTUM, complainers commit themselves to notify CERTUM (by means of a registered letter) of the reason for the argument or complaint.

*CERTUM resolves only the disputes with its customers (subscribers, Registration Points, certification authorities,*

*relying parties, etc.) resulting from agreements already made.*

# 9.14. The Law

## 9.14.1. Resolution Survival

The resolutions of the present Certification Practice Statement are valid of the date of the approval by Chief of CERTUM 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 new resolutions do not significantly violate former resolutions, the agreements in force should be regarded as valid, unless the agreement parties or the court to which one of the parties appeals state differently.

If the agreement made on the grounds of the present Certification Practice Statement contains contents confidentiality clause or a clause concerning the confidentiality of the information that the parties possessed when the agreement was in force, copyrights clause or intellectual rights clause, these clauses are assumed in force also after the validity period expires, for a period that should be an integral part of this agreement or Certification Practice Statement.

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

## 9.14.2. Resolution Merger

The present Certification Practice Statement and agreements being made can contain references to other resolutions, provided that:

- this fact was stated as a clause in this document or in the agreement,
- the resolutions to which this document or the agreement refer are stated in writing.

# 9.15. Compliance with Applicable Law

CERTUM obeys the law in force in the Republic of Poland

# 9.16. Miscellaneous Provisions

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

## 9.16.1. Entire Agreement

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

## 9.16.2. Assignment

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

## 9.16.3. Resolution Severability

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

Resolution severability is particularly crucial in the agreements mentioned in chapter 9.6. If a severability clause is not included in an agreement, the whole agreement can be against the law even if this is not the parties' intention.

### 9.16.4. Enforcement

Any delay or lack in the exercise of any of the rights arising from this CPS shall not be construed as a permanent waiver of this rights.

### 9.16.5. Force Majeure

CERTUM is excused party from not performing its contractual obligations due to unforeseen events beyond its reasonable control and occurring without its fault or negligence This type of claim should be specified in an agreement between a subscriber and a relying party.

## 9.17. Other Provisions

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

# Appendix 1: Abbreviations

CA Certification Authority

CAA Certificate Authority Authorization

CMP Certificate Management Protocol

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

DN Distinguished Name

PRA Primary Registration Authority

CPS Certification Practice Statement

KRIO Krajowy Rejestr Identyfikatorów Obiektów (National Object Identifiers Registry)

OCSP On-line Certificate Status Protocol

CP Certification Policy

PKI Public Key Infrastructure

RA Registration Authority

PSE personal security environment

QGIS Qualified Government Information Source

QGTIS Qualified Government Tax Information Source

QIIS Qualified Independent Information Source

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

TSA Time Stamping Authority

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

# Appendix 2: Glossary

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

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

**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 entiti103nauthorizferral to entities providing on-line certificate status verification service. In both cases the distribution should be performed with the usage of appropriate means (e.g. LDAP, FTP, etc.).

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

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

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

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

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

**Certificates revocation** – procedures concerning revocation of a key pair (certificate revocation) in the case when an access to the key pair has to be restricted for the subscriber to prevent possible usage in encryption or signature creation. A revoked certificate is placed on Certificate Revocation List (CRL).

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

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

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

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

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

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

**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

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

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

**Domain Authorization Document –** a document that confirms the subscriber's rights to use a specific name appearing in the certificate. In the case of legal person names, these will be authorizations, powers of attorney, employment certificates. In the case of domain names, they will be valid invoices or statements received from the registrar of the given domain name.

**Electronic signature** – electronic data, which together with other data they are appended to or logically connected to, 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).

**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.

**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.

**Personal Identification Number (PIN) –** code securing cryptographic card105nauthorizeduthorised 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)** – authority providing services of identity verification and confirmation of the certificate requesters; they provide complex subscriber handling in the area of certification services. Primary Registration Authority's additional duty is to approve the Registration Point and is allowed to generate – on behalf of CERTUM's 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 key** – one of the keys from a subscriber's asymmetric key pair which may be accessible to the public. In the case of the asymmetric cryptography system, a public key defines verification transformation. In the case of asymmetric encryption, a public key defines encryption transformation.

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

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

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

**Registration Point** – authority providing services of subsribers' identity verification.

**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.

**Relying party being a beneficiary of the warranty –** the subscriber of CERTUM's certification services who has received information containing a certificate or an associated electronic signature verified with a public key included in the certificate and who has to decide whether to accept or reject the signature on the basis of the trust for the certificate.

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

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

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

**Share**d **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.

**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.

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

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

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

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

**Token** – element of data used for exchange between parties and containing information transformed by means of cryptographic techniques. Token may be signed by a registration authority operator and may be used for authentication of its holder in the contact with a certification authority.

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

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

**CERTUM** – Asseco Data Systems S.A.'s service unit, providing certification and qualified certification services (certification authority).

**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.

**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.

# Appendix 3: Minimum Required for Cryptographic Algorithm and Key Sizes

## 1. CERTUM Root Certificates

| L.p. | Cryptographic algorithm | Certificate issued on or before 31 Dec 2010 | Certificate issued after 31 Dec 2010 |
|---|---|---|---|
| 1. | Digest algorithm | MD5 (not recommended), SHA-1 | SHA-1[29], SHA-256, SHA-384 or SHA-512 |
| 2. | RSA | 1024 | 2048 |
| 3. | ECC | NIST P-256 | NIST P-256 |

## 2. CERTUM Subordinate Certificates

| L.p. | Cryptographic algorithm | Certificate issued on or before 31 Dec 2010 | Certificate issued after 31 Dec 2010 |
|---|---|---|---|
| 1. | Digest algorithm | SHA-1 | SHA-1[37], SHA-256, SHA-384 lub SHA-512 |
| 2. | RSA | 1024 | 2048 |
| 3. | ECC | NIST P-256 | NIST P-256 |

## 3. Subscriber Certificates

| L. p. | Cryptographic algorithm | Certificate issued on or before 31 Dec 2010 | Certificate issued after 31 Dec 2010 | Certificate issued after 01 January 2015 |
|---|---|---|---|---|
| 1. | Digest algorithm | SHA-1 | SHA-1[37], SHA-256, SHA-384 lub SHA-512 | SHA-256, SHA-384 lub SHA-512 |
| 2. | RSA | 1024 lub 2048 (Note: subscriber certificates containing a 1024 bit RSA key MUST expire on or before 31 Dec 2010) | 2048 | 2048 |
| 3. | ECC | NIST P-256 | NIST P-256 | NIST P-256 |

[29] SHA-1 should be used until SHA-256 is supported widely by browsers used by a majority of relying parties worldwide.

| Document modification history | | |
|---|---|---|
| V 1.0 | 15th of April, 2000 | Draft of the document for comments |
| V 1.33 | 12th of March, 2002 | Full version of the document. Document approved |
| V 2.0 | 15th of July, 2002 | New certificate types defined. Modifications to certification procedures, detailing certificate and CRL profile. chapters 3,4, 6.1, 2.6, 6.2-6.9 and 7 re-edited. Document approved. |
| V 2.1 | 1st of February, 2005 | New certificate types defined. Modification to chapters regarding renewal and recertification of cryptographic keys. Introduction of entries considering usage of new extensions in the certificate. Revision of number of punctuation errors and modification of the chapter addressing requester verification. Number of lesser modifications introduced to maintain integrity of this document. |
| V 2.2 | 9th of May, 2005 | Editorial changes. Change to the company legal form and name (Unizeto Sp. z o.o. changed to Unizeto Technologies S.A,) |
| V 2.3 | 26th of October, 2005 | Change of service name and logo from Unizeto CERTUM – Centrum Certyfikacji to CERTUM – Powszechne Centrum Certyfikacji. Correction of company information in certificate's profiles. |
| V 2.4 | 19th of May, 2006 | Removal of former legal status of the company. Transfer of the details of identification documents and procedures to dedicated document. Removal of certificate suspension information. Adding information on archival of the documents and data used in identity verification process. Editorial changes and removal of inconsequence with polish version of the document. |
| V 2.5 | 12th of May, 2008 | Editorial changes and adjusting Polish and English version of this document. |
| V 3.0 | 19th of October, 2009 | Amended in line with the RFC 3647 requirements and the requirements for the issuance of EV SSL certificates. Added appendices 3-6. |
| V 3.1 | 12th of August, 2010 | Updating the information about subscriber's verification. Updating the Appendix 3. |
| V 3.2 | 9th of February, 2011 | Updated information about certificates status checking, certificates validity times and some other minor changes. |
| V 3.3 | 7th of October, 2011 | Updated information about new subordinate certificate Certum Code Signing CA. Other minor changes to certificate offer. Added information about new root certificate Certum Trusted Network CA 2 |
| V 3.4 | 19th of April, 2012 | CERTUM logo update |
| V 3.5 | 29th of May, 2013 | The Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates incorporated by reference in the CP. Updated information relating to the suspension of certificates. |
| V 3.6 | 13th of September, 2013 | Add reference to Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.<br>Updated information about CRL issuance frequency. |
| V 3.7 | 31st of October 2014 | Added the new intermediate CAs. Added the new signature algorithms. Added information about automatic recertification and rekey. Removal of the suspension service. Removal of Appendix 3. |
| V 3.8 | 14th of April 2015 | Added information about CAA DNS resource records processing. |
| V 3.9 | 01th of July 2015 | Upgrade for the *Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates* |
| V 4.0 | 03th of November 2015 | Added the new CERTUM root certification authority Certum Trusted Network CA EC and the intermediate authorities Certum Digital Identification CA SHA2 and Certum Extended Validation Code Signing CA SHA2 |

| | | |
|---|---|---|
| V 4.1 | 01th April, 2016 | Transfer of ownership of Unizeto Technologies S.A. Asseco Data System S.A. Adding the information on obligation to maintain certification certificate issued by Unizeto Technologies S.A. Asseco Data System S.A |
| V 4.2 | 22 August 2016 | Added information about new time-stamping authority Certum EV TSA SHA2 |
| V 4.3 | 22 November 2016 | Added the new intermediate CAs. |
| V 4.4 | 01 February 2017 | Update the code signing certificates information. Updating the information on CA/Browser Forum requirements. |
| V 4.5 | 13 March 2017 | Modification of Authentication of Domain Name (point 3.2.6) by removing domain authentication method involving "uploading specific metadata to the main page on the domain" |
| V 4.6 | 21 April 2017 | Modification of Authentication of Domain Name (p–int 3.2.6) - updated information relating to uploading file with the specified name by adding the directory: /.well-known/pki-validation |
| V 4.7 | 01 August 2017 | Change of Asseco Data Systems S.A. address. Added the intermediate CA: WoSign DV SSL CA. Added new Certification policy identifiers. |
| V 4.8 | 11 August 2017 | Added new Certification policy identifiers |
| V 4.9 | 08 September 2017 | Implementation the mechanism to handle CAA records |
| V 5.0 | 30 November 2017 | The new sub-CAs added: TrustAsia DV SSL CA - C3, TrustAsia OV SSL CA - C3, TrustAsia EV SSL CA - C3, TrustOcean Certificate Authority |
| V 5.1 | 07 March 2018 | Adjusting CPS to the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v1.5.4 |