
# Certification Practice Statement: CERTUM's Certification Services

**Version 2.7**

**Effective date: 27th of April , 2009**

**Status: previous**

Unizeto Technologies S.A.
CERTUM – Powszechne Centrum Certyfikacji
Królowej Korony Polskiej Street 21
70-486 Szczecin, Poland
http://www.certum.pl

# Trademark and Copyright notices

# Content

1.Introduction ..... 1
1.1.Overview ..... 2
1.2.Document Name and its Identification ..... 3
1.3.Certification Practice Statement Parties ..... 4
1.3.1.Certification Authorities ..... 4
1.3.1.1.Certum CA Root Certification Authority ..... 4
1.3.1.2.Intermediate Certification Authorities ..... 5
1.3.2.Time-Stamping Authority ..... 6
1.3.3.Certificate Validation Service ..... 6
1.3.4.Registration Authorities ..... 6
1.3.5.Repository ..... 7
1.3.6.End Users ..... 8
1.3.6.1.Subscribers ..... 8
1.3.6.2.Relying Parties ..... 8
1.4.Certificate Applicability Range ..... 9
1.4.1.Certificate Types and Recommended Applicability ..... 10
1.4.2.Recommended Applications ..... 13
1.4.3.Prohibited Applications ..... 14
1.5.Contact ..... 14
2.General Provisions ..... 15
2.1.Obligations ..... 15
2.1.1.CERTUM and registration authority obligations ..... 15
2.1.2.Registration Authority Obligations ..... 17
2.1.3.End Subscriber Obligations ..... 18
2.1.4.Relying Party Obligations ..... 19
2.1.5.Repository Obligations ..... 21
2.2.Liability ..... 21
2.2.1.Intermediate Certification Authorities Liability ..... 22
2.2.2.Registration Authority Liability ..... 23
2.2.3.Subscriber Liability ..... 23
2.2.4.Relying Party Liability ..... 23
2.2.5.Repository Liability ..... 23
2.3.Financial Liability ..... 23
2.4.Governing Law and Dispute Resolution ..... 24
2.4.1.Governing Law ..... 24
2.4.2.Supplementary Resolutions ..... 24
2.4.2.1.Resolution Severability ..... 24
2.4.2.2.Resolution Survival ..... 24
2.4.2.3.Resolution Merger ..... 25
2.4.2.4.Resolution Notice ..... 25
2.4.3.Disputes Resolution ..... 25
2.5.Fees ..... 26
2.5.1.Certificate Issuance or Renewal Fees ..... 26
2.5.2.Certificate Access Fees ..... 26
2.5.3.Revocation and Status Information Access Fees ..... 27
2.5.4.Other Fees ..... 27

2.5.5.Fees Refund ..... 27
**2.6.Repository and Publication ..... 27**
2.6.1.Information Published by CERTUM ..... 27
2.6.2.Frequency of Publication ..... 28
2.6.3.Access to Publications ..... 28
**2.7.Audit ..... 29**
2.7.1.Audit Frequency ..... 29
2.7.2.Identity/Qualifications of Auditor ..... 29
2.7.3.Auditor's Relation to Audited Party ..... 29
2.7.4.Topics Covered by Audit ..... 29
2.7.5.Actions Taken as a Result of Deficiency ..... 30
2.7.6.Notifying of Audit Results ..... 30
**2.8.Information Security ..... 30**
2.8.1.Types of Information to be Kept Secret ..... 30
2.8.2.Types of Information Not Considered Confidential and Private ..... 31
2.8.3.Disclosure of Certificate Revocation Reason ..... 32
2.8.4.Release of Confidential Information upon Court Writs ..... 32
2.8.5.Release of Confidential Information for Scientific Purposes ..... 32
2.8.6.Release of Confidential Information upon Owner's Request ..... 32
2.8.7.Other Circumstances of Release ..... 32
**2.9.Intellectual Property Rights ..... 32**
2.9.1.Trade Mark ..... 33
**3.Identification and Authentication ..... 34**
**3.1.Initial Registration ..... 34**
3.1.1.Types of Names ..... 35
3.1.2.Need for Names to be Meaningful ..... 36
3.1.3.Rules for Interpreting Various Names Forms ..... 36
3.1.4.Names Uniqueness ..... 36
3.1.5.Name Claim Dispute Resolution Procedure ..... 37
3.1.6.Prove of Possession of Private Key ..... 37
3.1.7.Authentication of Legal Entity's Identity ..... 37
3.1.8.Authentication of Private Entity's Identity ..... 39
3.1.9.Devices Origin Authentication ..... 39
**3.2.Subscriber's Identity Authentication in Rekey, Certificate Renewal or Certificate Modification ..... 39**
3.2.1.Rekey ..... 39
3.2.2.Recertification ..... 40
3.2.3.Certificate Modification ..... 40
**3.3.Subscriber Identity Authentication in Rekey after Revocation ..... 40**
**3.4.Subscriber's Identity Authentication in Certificate Revocation ..... 40**
**4.Operational Requirements ..... 42**
**4.1.Application Submission ..... 42**
4.1.1.Registration Application ..... 42
4.1.2.Certificate renewal, rekey, certification or modification application ..... 43
4.1.3.Certificate Revocation or Suspension Application ..... 44
**4.2.Application Processing ..... 44**
4.2.1.Application Processing in Registration Authority ..... 45
4.2.2.Application Processing in Certification Authority ..... 45
**4.3.Certificate Issuance ..... 45**
4.3.1.Certificate Issuance Awaiting ..... 46

4.3.2.Certificate Issuance Denial ..... 47
**4.4.Certificate Acceptance ..... 47**
**4.5.Certificate and Key Usage ..... 48**
**4.6.Recertification ..... 48**
**4.7.Certification and rekey (key update) ..... 49**
**4.8.Certificate modification ..... 49**
**4.9.Certificate revocation and suspension ..... 50**
4.9.1.Circumstances for certificate revocation ..... 51
4.9.2.Who can request certificate revocation ..... 52
4.9.3.Procedure for certificate revocation ..... 52
4.9.4.Certificate revocation grace period ..... 54
4.9.5.Reasons for certificate suspension ..... 54
4.9.6.Who can request certificate suspension ..... 55
4.9.7.Procedure of certificate suspension and unsuspension ..... 55
4.9.8.Limitation on suspension grace period ..... 55
4.9.9.CRL issuance frequency ..... 55
4.9.10.Certificate Revocation List checking ..... 55
4.9.11.On-line certificate status verification availability ..... 56
4.9.12.Requirements for on-line certificate status verification ..... 56
4.9.13.Other forms of revocation advertisements availability ..... 56
4.9.14.Checking requirements for other forms of revocation advertisements ..... 57
4.9.15.Special requirements regarding key security violation ..... 57
4.9.16.Revocation or suspension of CA certificate ..... 57
**4.10.Events recording and audit procedures ..... 57**
4.10.1.Types of events recorded ..... 57
4.10.2.Frequency of event logs checking ..... 59
4.10.3.Event journals retention period. ..... 59
4.10.4.Protection of event logs ..... 59
4.10.5.Procedures for event logs backup ..... 59
4.10.6.Notification to event responsible entities ..... 60
4.10.7.Vulnerability assessment ..... 60
**4.11.Records archival ..... 60**
4.11.1.Types of data archived ..... 61
4.11.2.Frequency of data archive ..... 61
4.11.3.Archive retention period ..... 61
4.11.4.Backup procedures ..... 61
4.11.5.Requirements for time-stamping of the records ..... 62
4.11.6.Access procedures and archived information verification ..... 62
**4.12.Key changeover ..... 62**
**4.13.Key security violation and disaster recovery ..... 63**
4.13.1.Corruption of computing resources, software and/or data ..... 63
4.13.2.Key compromise or suspicion of certification authority private key compromise ..... 64
4.13.3.Security coherence after disaster ..... 65
**4.14.Certification authority termination or service transition ..... 65**
4.14.1.Requirements associated with duty transition ..... 65
4.14.2.Certificate issuance by the successor of terminated certification authority ..... 66
**5.Physical, organizational and personnel security controls ..... 67**

**5.1.Physical security controls ..... 67**
5.1.1.CERTUM physical security controls ..... 67
5.1.1.1.Site location and construction ..... 67
5.1.1.2.Physical access ..... 67
5.1.1.3.Power and air conditioning ..... 68
5.1.1.4.Water exposure ..... 68
5.1.1.5.Fire prevention ..... 68
5.1.1.6.Media storage ..... 68
5.1.1.7.Waste disposal ..... 68
5.1.1.8.Offsite backup storage ..... 68
5.1.2.Registration authority security controls ..... 69
5.1.2.1.Site location and construction ..... 69
5.1.2.2.Physical access ..... 69
5.1.2.3.Power and air conditioning ..... 69
5.1.2.4.Water exposure ..... 69
5.1.2.5.Fire prevention and protection ..... 69
5.1.2.6.Media storage ..... 69
5.1.2.7.Waste disposal ..... 69
5.1.2.8.Offsite archive storage ..... 70
5.1.3.Subscriber security ..... 70
**5.2.Organizational security controls ..... 70**
5.2.1.Trusted roles ..... 70
5.2.1.1.Trusted roles in CERTUM ..... 70
5.2.1.2.Trusted roles in registration authority ..... 71
5.2.1.3.Subscriber's trusted roles ..... 71
5.2.2.Numbers of persons required per task ..... 71
5.2.3.Identification and Authentication for Each Role ..... 72
**5.3.Personnel controls ..... 72**
5.3.1.Training requirements ..... 73
5.3.2.Retraining Frequency and Requirements ..... 73
5.3.3.Job rotation ..... 73
5.3.4.Sanctions for Unauthorized Actions ..... 73
5.3.5.Contract Personnel ..... 73
5.3.6.Documentation Supplied to Personnel ..... 74
**6.Technical Security Controls ..... 75**
**6.1.Key Pair Generation ..... 75**
6.1.1.Key pair generation ..... 75
6.1.1.1.Procedures of generation of Certum CA initial keys ..... 76
6.1.1.2.Certum CA rekey procedure ..... 76
6.1.1.3.Subordinate certification authority rekey procedure ..... 77
6.1.1.4.Certum CA and subordinate authorities certificate recertification procedure ..... 77
6.1.2.Private Key Delivery to Entity ..... 78
6.1.3.Public Key Delivery to certification authority ..... 78
6.1.4.Certification authority public key delivery to relying parties ..... 78
6.1.5.Keys Sizes ..... 78
6.1.6.Public Key Generation Parameters ..... 79
6.1.7.Public Key Quality Checking ..... 79
6.1.8.Hardware and/or Software Key Generation ..... 80
6.1.9.Key Usage Purposes ..... 80
**6.2.Private Key Protection ..... 81**
6.2.1.Standards for Cryptographic Modules ..... 81

6.2.2.Private Key Multi-Person Control ..... 82
6.2.2.1.Acceptance of secret shares by its holders ..... 82
6.2.2.2.Protection of secret shares ..... 82
6.2.2.3.Availability and erasure (transfer) of shared secret ..... 83
6.2.2.4.Responsibilities of shared secret holder ..... 83
6.2.3.Private Key Escrow ..... 83
6.2.4.Private Key Backup ..... 84
6.2.5.Private Key Archival ..... 84
6.2.6.Private Key Entry into Cryptographic Module ..... 84
6.2.7.Method of Activating Private Key ..... 85
6.2.8.Method of Deactivating Private Key ..... 86
6.2.9.Method of Destroying Private Key ..... 86
**6.3.Other Aspects of Key Pair Management ..... 86**
6.3.1.Public Key Archive ..... 86
6.3.2.Usage Periods of Public and Private Keys ..... 87
**6.4.Activation Data ..... 89**
6.4.1.Activation Data Generation and Installation ..... 89
6.4.2.Activation Data Protection ..... 90
6.4.3.Other Aspects of Activation Data ..... 90
**6.5.Computer Security Controls ..... 90**
6.5.1.Specific Computer Security Technical Requirements ..... 90
6.5.2.Computer Security Rating ..... 91
**6.6.Technical Controls ..... 91**
6.6.1.System Development Controls ..... 91
6.6.2.Security Management Controls ..... 91
6.6.3.Life Cycle Security Ratings ..... 92
**6.7.Network Security Controls ..... 92**
**6.8.Cryptographic Module Engineering Controls ..... 92**
**6.9.Time stamps as a security control ..... 92**
**7.Certificate, CRL, timestamp token and OCSP profile ..... 93**
**7.1.Certificate Profile ..... 93**
7.1.1.Contents of the certificate ..... 93
7.1.1.1.Basic fields ..... 93
7.1.1.2.Standard extensions fields ..... 94
7.1.2.Certificate Extensions and issued certificates types ..... 97
7.1.2.1.Intermediate CA Certificates ..... 97
7.1.2.2.Server authentication certificates ..... 97
7.1.2.3.Code Signing Certificates ..... 98
7.1.2.4.Private entities certificates ..... 99
7.1.2.5.Virtual Private Network (VPN) certificates ..... 100
7.1.2.6.Cross-certification and non-repudiation certificates ..... 101
7.1.3.Electronic signature algorithm identifier ..... 102
7.1.4.Electronic signature field ..... 102
**7.2.CRL profile ..... 102**
7.2.1.Supported CRL entry extension ..... 103
7.2.2.Revoked certificate and CRL ..... 104
**7.3.Timestamp token profile ..... 104**
**7.4.OCSP response token profile ..... 109**
7.4.1.Version number ..... 109
7.4.2.Certificate status information ..... 109
7.4.3.Supported standard extension ..... 110

7.4.4.Supported private extensions ..... 110
7.4.5.Certificate status verification token issuer statement ..... 111
**8.Certification Practice Statement management ..... 112**
**8.1.Changes introduction procedure ..... 112**
8.1.1.Items that can be changed without notification ..... 113
8.1.2.Items that require notification ..... 113
8.1.2.1.List of items ..... 113
8.1.2.2.Comment period ..... 113
8.1.2.3.Changes requiring new identifier ..... 113
**8.2.Publication ..... 114**
8.2.1.Items not published in CPS ..... 114
8.2.2.Publication of the new version of Certification Practice Statement ... 114
**8.3.CPS Approval Procedures ..... 115**
**Document History ..... 116**
**Appendix 1: Abbreviations ..... 117**
**Appendix 2: Glossary ..... 118**
**Literature ..... 123**

# 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 the certificates resulting from this certification. The nature, aim and role of Certification Practice Statement is particularly important from the point of view of a **subscriber**[2] and a **relying party**[3]**.**

**Certification Policy** describes general rules of certification practice of **CERTUM – Powszechne Centrum Certyfikacji** (further referred to as CERTUM), defines certification parties, their responsibilities and obligations, types of certificates, authentication procedures and applicability range. Certification Policy states what level of trust can be applied to a given type of a certificate issued by CERTUM. Certification Practice Statement – on the other hand – describes how CERTUM secures the level of trust guaranteed by the policy.

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

Certification Practice Statement describes a set of four main and several additional certification policies[4] applied by CERTUM to issuance of certificates to authorities and 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 Certification Practice Statement are in accordance with the recommendation of RFC 2527 *Certificate Policy and Certification Practice Statement Framework*. Certification Practice Statement was created, assuming that the reader is generally familiar with the notions concerning certificates, electronic signature and Public Key Infrastructure (PKI).

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

Unizeto Technologies S.A. is a legal successor of Unizeto Sp. z o.o. According to Polish Kodeks Spólek Handlowych (commercial partnership regulation - Dz.U. No 94, pos. 1037 inc. later changes) universal succession was executed, resulting in Unizeto Technologies S.A. inherited all the rights and obligations of Unizeto Sp. z o.o.

---

[1] 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 certificate of given level of trust – 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. Overview

Certification Practice Statement is a description and basis for functioning of CERTUM and **certification authorities, registration authorities, subscribers** and **relying parties** associated with it. 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 are provided within the framework of the separate certification domains (see Fig. 1.1) **certum** with a separate root certification authority **Certum CA** and **ctnDomena** (Certum Trusted Network (TCN)) with a separate root certification authority **Certum Trusted Network CA.** Root certification authorities are independent from the each other and **cckDomena** domain and issue the so called self-certificates[6] to itself.

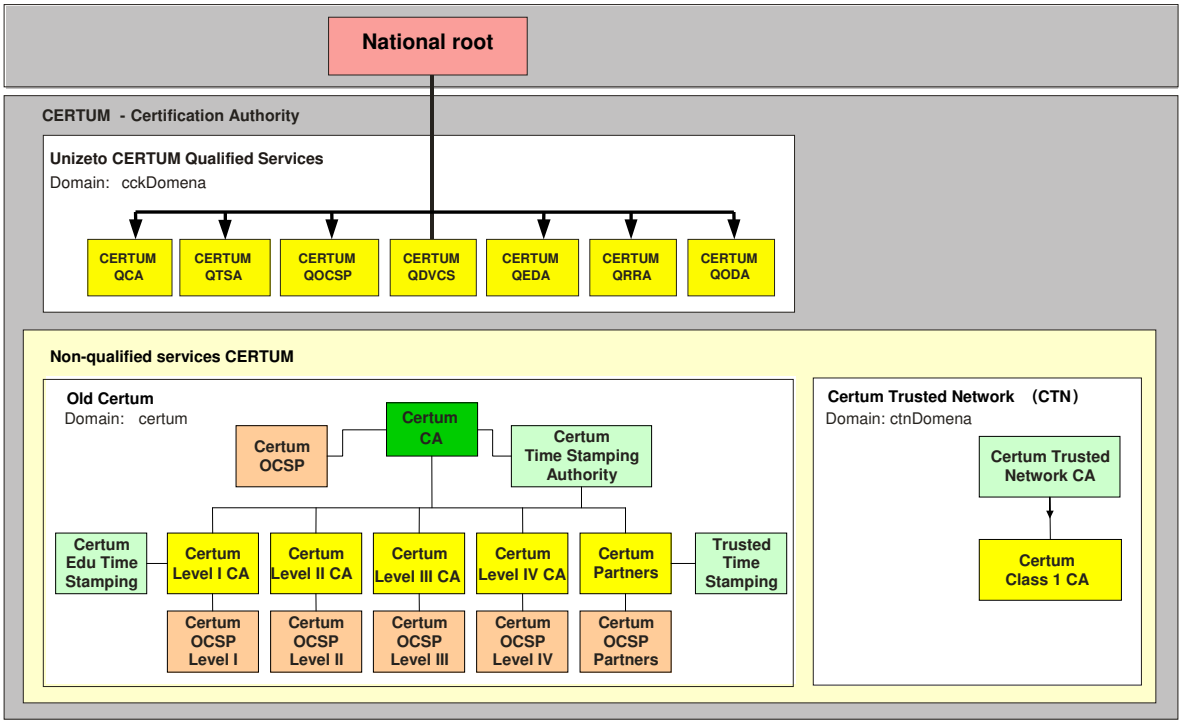


Fig.1.1 Authorities operating within CERTUM and other certification services of CERTUM Certification Authority

In terms of hierarchy, there are certification authorities subordinate to **Certum CA** root certification authority. These are: **Certum Level I** (CA will no longer issue certificates to this root), **Certum Level I (**CA will no longer issue certificates to this root), **Certum Level II (**CA will no longer issue certificates to this root), **Certum Level III (**CA will no longer issue certificates to this root), **Certum Level IV** (CA will no longer issue certificates to this root), **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** and **Certum Partners** issuing certificates with different credibility levels (see Chapter 1.4). Currently there is only one authority **Certum Class 1 CA** subordinates to **Certum Trusted Network CA** root certification authority.

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

[6] **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)

Certificates issued by CERTUM contain the identifiers[7] of certification policies, enabling relying parties to state if the application of a certificate being verified by the party is in accordance with the declared purpose of the certificate. The declared purpose might be specified on the basis of values set in **PolicyInformation** structure of the extension **certificatePolicies** (see Chapter 7.1.1.2) of every certificate issued by CERTUM.

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

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

Tab.1 Important document connected with Certification Practice Statement

| | Document name | Status | Availability |
|---|---|---|---|
| 1. | Certification Policy of CERTUM's Certification Services | public | http://www.certum.pl |
| 2. | Certification Policy of Time-Stamping Authority | public | http://www.certum.pl |
| 3. | CERTUM's Certification Services Regulation | public | http://www.certum.pl |
| 4. | Personnel book, range of duties and responsibilities | Non-public | Locally – only entitled persons and auditor |
| 5. | Registration authority book | Non-public | Locally – only entitled persons and auditor |
| 6. | Technical infrastructure book | Non-public | Locally – only entitled persons and auditor |
| 7. | Business continuity plan | Non-public | Locally – only entitled persons and auditor |
| 8. | Partnership Programme (Cross Root CA) | Non-public | Available on demand |
| 9. | Identity verification instruction | Non-public | Locally – only entitled persons and auditor |

Additional information and service are available by electronic mail 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 Policy of CERTUM's Certification Services**; the document is available:

- As an electronic version at the repository at: http://www.certum.pl or on request sent to: info@certum.pl,
- As a paper copy - on request sent to the address of CERTUM (see Chapter 1.5).

[7] 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)
```

The following registered object identifier is connected with the certification policy document (OID: 1.2.616.1.113527.2.2.0.1.2.7):

```
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(2) 7}
```

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

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 present Certification Practice Statement (described in Chapter 7.1.1.2 hereinafter) are included in certificates issued by CERTUM.

# 1.3. Certification Practice Statement Parties

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

- certification authorities **Certum CA**, **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA, Certum Partners** and any other authority established in accordance with the rules stated in the present Certification Practice Statement,
- Primary Registration Authority (PRA),
- Registration Authorities (RA),
- 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 the declared credibility levels of issued certificates are the reflection of certification authorities practices.

## 1.3.1. Certification Authorities

Certification authorities, forming a domains of certification authorities called **certum** and **ctnDomena**, are a part of CERTUM (see Fig. 1.1). **Certum CA** certification authority is a root certification authority of **certum** domain and **Certum Trusted Network CA** certification authority is a root certification authority of **ctnDomena** domain. All certification authorities in these domains are subordinated to their roots.

Currently, there are several certification authorities subordinate to **Certum CA**: **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** and **Certum Partners** and the only one that is subordinated to **Certum Trusted Network CA**: **Certum Class 1 CA**.

### 1.3.1.1. Certum CA Root Certification Authorities

**Certum CA** root certification authority can register and issue certificates only to certification authorities and authorities issuing electronic confirmation of non-repudiation that belong to **certum** domain, for the **Certum Trusted Network CA** is the **ctnDomena** domain.

Certum CA root certification authorites operate on the basis of the self-certificate issued by themselves. In such a self-certificate, the extension **certificatePolicies** is not placed, which should be interpreted as lack of limits to the set of **certification paths**[8], to which CA certificate can be attached.

***Certum CA*** or ***Certum Trusted Network CA*** *certification authority must be a* ***point of trust***[8] *for all subscribers of CERTUM. What follows is that every certification path must start with a certificate of* ***Certum CA*** *authority or* ***Certum Trusted Network CA*** *authority.*

Certum CA renders certification services to:

- itself (issues and renews self-certificates),
- **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA, Certum Level IV CA** and **Certum Partners** authorities and other certification authorities registered in certification domain **certum**,
- entities delivering services of on-line certificate status verification and other entities rendering services of non-repudiation (e.g. time-stamping service).

### 1.3.1.2. Intermediate Certification Authorities

Intermediate certification authorities **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA, Certum Level IV CA** and **Certum Partners** issue certificates to subscribers in compliance with the policies whose identifiers are stated in Table 1.2.

Table 1.2 The names of intermediate certification authorities and certification policy identifiers, included in certificates issued by these authorities

| 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 Partners | 1.2.616.1.113527.2.2.9 |
| Certum Class 1 CA | 1.2.616.1.113527.2.5.1.5 |

*The certificates, issued to* ***Certum Level I CA, Certum Level II CA, Certum Level III CA, Certum Level IV CA, Certum Partners and certificates issued by Certum CA*** *or* ***Certum Trusted Network CA*** *to other authorities and end-entities contain extension* ***certificatePolicies.***

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

[8] See **Glossary**

*Only two authorities can issue certificates to other certification authorities:* ***Certum Level I CA*** *(test certification authorities) and* ***Certum Partners*** *(commercial certification authorities).*

Primary Registration Authority and other registration authorities fully cooperate with CERTUM. Registration authorities represent CERTUM in contacts with subscribers and act within the rights delegated by 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 and registration authority operators,
- 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),
- hardware devices (physical and logical) owned by private and legal entities;
- entities delivering non-repudiation services (e.g. timestamp authorities or notary authorities) – applicable to **Certum Level I CA** and **Certum Partners** authorities,
- other certification authorities (applicable to **Certum Level I CA** and **Certum Partners** authorities).

## 1.3.2. Time-Stamping Authority

Certum Time-Stamping Authority, operating within certum domain (Fig. 1) is a part of CERTUM infrastructure.

Timestamping authority issues timestamp tokens in accordance with ETSI[9] recommendation. Each timestamp token contains identifier of the policy, under which the token has been issued (identifier value is described in Table 3 and Chapter 7.3). Timestamp tokens are signed only with private key issued especially for timestamping service.

Tab.3 **Certum Time-Stamping Authority** identifier**,** included in timestamp tokens

| Token name | Certification Policy Identifier |
|---|---|
| Timestamp token | 1.2.616.1.113527.2.2.5 |

Tokens, issued in accordance with policy described in Tab.3, are used primarily in securing long-term electronic signatures[10] and global transactions.

Certum Time-Stamping Authority employs solutions which guarantee synchronisation with international time source (Coordinated Universal Time - UTC) with the accuracy more than 1 second.

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

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

### 1.3.3. Certificate Validation Service

CERTUM beside standard certificate status verification based on Certificate Revocation List (CRL) offers online services – based on Online Certificate Status Protocol (OCSP). This service is provided by Certum Validation Service.

### 1.3.4. Registration Authorities

Registration authorities receive, verify and approve or reject applications for registration and issuance of a certificate, and rekey, renewal, or revocation of a certificate. Verification of applications intends to authenticate (on the basis of the documents enclosed to the applications) the requester, as well as the data included in the application. Registration authorities can submit applications – to an appropriate certification authority – for cancellation of a subscriber registration and the subscriber's certificate withdrawal.

The level of precision of subscriber's identity identification results from the very subscriber's needs and it is imposed by the level of a certificate the issuance of which the subscriber requests (see Chapter 3). In the case of the simplest identification, a registration authority checks the correctness of a submitted email address. The most precise identification may require the subscriber's attendance in person to a registration authority and submission of suitable documents. This identification might be achieved either automatically or manually by a registration authority operator.

Registration authorities function on the basis of the authorization by an appropriate certification authority belonging to **certum** domain; the authorization concerns the identification of the identity of a current or future subscriber and the verification of the proof of the possession of a private key. In case of RAs managed by entities other than Unizeto Technologies S.A. (external RAs), a detailed scope of duties of registration authorities and their operators may be specified in an additional agreement between Unizeto Technologies S.A. and such RA, this CPS and the procedures concerning operating of registration authorities, which are an integral part of this agreement.

*Any institution (legal entity) might function as a registration authority and might be accredited by CERTUM, provided that this institution submits an appropriate application to Primary Registration Authority and fulfils other conditions stated in Certification Practice Statement (see Chapter 2).*

The list of registration authorities currently accredited by Primary Registration Authority is available in the repository at:

http://www.certum.pl

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

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

The main difference between these types is that registration authorities, unlike Primary Registration Authority, cannot accredit other registration authorities and register new certification authorities. Moreover, registration authorities do not have the rights to confirm all requests of a subscriber. The rights might be limited only to some of all available types[11] of certificates. Therefore,

[11] Types of certificates are described in Charter 1.4

- **RAs** register end subscribers (private and legal entities) that request certificates of the credibility level up to Certum Level IV CA (including Level IV CA),
- **PRA** registers registration authorities, new certification authorities and end 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 subscribers registered in PRA; additionally, PRA approves of distinguished names (DNs) of current and future registration authorities.

*Primary Registration Authority is located at the seat of CERTUM. Contact addresses with PRA are listed in Chapter 1.5.*

## 1.3.5. Repository

Repository is a collection of publicly available catalogues containing certificates of:

- all certification authorities belonging to or connected with certum domain (e.g. new certification authorities certificates registered in PRA),
- end subscribers (private and legal entities, including CERTUM employees and the devices operated by them and indispensable for PKI services).

Additionally, in the repository there is information closely connected with the functioning of certificates, including Certificate Revocation List (CRL), a current and former version of Certification Policy and Certification Practice Statement, as well as other information modified in real time (e.g. list of recommended applications or registration authorities).

*In **certum** domain there is only one repository, common for all certification authorities functioning within or connected with the domain.*

The contents of the repository are available at:

http://www.certum.pl

## 1.3.6. End Users

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

### 1.3.6.1. 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 (see Chapter 1.3.6).

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

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

### 1.3.6.2. Relying Parties

A relying party, using CERTUM services can be any entity whose decision making is dependant on validity of the connection between subscriber's identity and his/her/its public key (confirmed by one of certification authorities subordinate to **Certum CA**).

A relying party is responsible for verification of the current status of a subscriber's certificate. Such a decision must be taken any time when a 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. A 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.

## 1.4. Certificate Applicability Range

Certificate applicability range states the scope of permitted certificate usage. This scope defines the character of certificate applicability (e.g. electronic signature, confidentiality or certification policy identifier).

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**[12] should be evaluated by a subscriber. In Certification Policy and the present Certification Practice Statement there are four sensitivity levels: Level I (testing level), Level II (basic level), Level III (intermediate level) and Level IV (high level). These levels correspond to certificate credibility levels (see Table 1.3)[13].

[12] See **Glossary**

[13] See also *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA*), Version 1.12, December 27, 2000

Tab.1.3 Sensitivity level of the information and the name of the policy

| Information Sensitivity Level | Certification Policy Name | Applicability Range |
|---|---|---|
| Level I (testing) | Certum Level I CA | The lowest credibility level of the identity of a certificate entity. Level I certificates should be applied to test the compatibility of CERTUM services with the services of other deliverers of PKI services, and to test certificate functionality in cooperation with applications being tested. These certificates can also be used for other purposes, as long as assurance of the credibility of a message being sent or received is not important. |
| Level II (basic) | Certum Level II CA | The level gives the basic security of information in the environment of slight risk of data breach[14] (risk with no substantial consequences). It concerns access to private information where the likelihood of unauthorized access is not very high. These certificates can be used to authenticate and control the integrity of the information that was signed, and to secure confidentiality of information, in particular electronic mail. |
| Level III (intermediate) | Certum Level III CA | The level applies to information security in the environment where the risk of information breach exists and the consequences of the breach are moderate. The certificates can be applied to financial transactions or transactions of a substantial level of fraud occurrence risk. They can also be used if the likelihood of unauthorized access to private information is substantial. |
| Level IV (high) | Certum Level IV CA | This level is appropriate in the cases of strong likelihood of data breach and if the consequences of security service failure are very serious. The certificates can be applied to transactions with unlimited financial value (unless it is stated differently in a certificate), or of the high level of fraud occurrence risk. |
| Level I (testing) | **Certum Class 1 CA** | The same as Certum Level I CA |

A relying party or the subscriber 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 also issues certificates in accordance with Certum Partners policy, which does not have a strictly defined sensitivity level, due to providing services to other certification authorities and issuing cross-certification certificates.

[14] See **Glossary**

### 1.4.1. Certificate Types and Recommended Applicability

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

1) **personal certificates** – allow for encryption and signing of electronic mail, and securing electronic documents (electronic mail based on S/MIME or PGP standard),
2) **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 a subscriber** (private 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,
9) **notary authorities certificates** – applied by DVCS (Data Validation and Certification Server), which certifies and confirms data.

Detailed commercial names and applications of the above mentioned types depend on credibility level and the name of certification policy that is employed to issue these certificates (see Table 1.4).

Tab. 1.4. Types of certificate and their applicability

| Certification policy | Commercial name of certificate type | Description and recommended applicability |
|---|---|---|
| Certum Level I CA | Private Email | Testing of electronic mail security, electronic signatures of electronic data, PGP |
| | Private WEB Server | Testing of data transmission security for WWW servers |

[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**).

| Certification policy | Commercial name of certificate type | Description and recommended applicability |
|---|---|---|
| | Private Microsoft Authenticode | Testing of software security against forgery, software distribution in global network in accordance with Microsoft Authenticode™ |
| | Private Java Code Signing | Testing of software security in accordance with Sun Microsystems® Java |
| | Private Software Publisher | Testing of software security in accordance with IETF RFC 2315 and IETF RFC 2633, UNIX® Code Signing (programmer's universal certificate) |
| | Private VPN | Testing of data transmission security – protocol IPsec. For network devices, servers and VPN channels |
| | Private Strong Internet | Testing of customer's authentication to network resources, service servers, workstation, authentication to Kerberos V (token based on X.509 certificates) |
| | Private SSL Server | Testing of security of data transmission between a service and a customer LDAP, NTP, POP3, SMTP etc. |
| | Private IPsec Client | Testing of client of encrypted transmission of data on the basis of IPsec protocol |
| | Private Data Encryption | Testing of data encryption for private entities; cryptographic file systems |
| | Private Microsoft VBS | Unavailable in public offer |
| | Private Netscape Object Signing | Unavailable in public offer |
| | Private WAP Server | Unavailable in public offer |
| | Private Time-Stamping | Unavailable in public offer |
| | Private Netscape Form Signing | Unavailable in public offer |
| | Private CA | Unavailable in public offer |
| | Private EDI | Unavailable in public offer |
| | Private Apple Code Signing | Unavailable in public offer |
| | Private Biometric Data | Unavailable in public offer |
| | Private Castanet Signing | Unavailable in public offer |
| | Private OCSP | Unavailable in public offer |
| | Private Notary Service | Unavailable in public offer |
| Certum Level II CA | Certum Silver | Electronic mail security, electronic signatures of electronic data, PGP |
| | Commercial Data Encryption | Data encryption; cryptographic file systems |
| | Commercial Strong Internet | Customer's authentication to network resources, service servers, workstation, authentication to Kerberos V (token based on X.509 certificates) |
| | Commercial IPsec Client | Client of encrypted transmission of data on the basis of IPsec protocol |
| | Commercial SSL Server | Unavailable in public offer |

| Certification policy | Commercial name of certificate type | Description and recommended applicability |
|---|---|---|
| | Commercial VPN | Unavailable in public offer |
| Certum Level III CA | Certum Gold | Electronic mail security, electronic signatures of electronic data, PGP |
| | Enterprise Web Server | Data transmission security for WWW systems |
| | Enterprise SSL Server | Security of data transmission between a service and a client of LDAP, NTP, POP3, SMTP, etc. |
| | Wildcard Domain | SSL/TLS security for web domains |
| | Microsoft Authenticode | Software security against forgery, software distribution in global network in accordance with Microsoft Authenticode™ |
| | Java Code Signing | Software security in accordance with Sun Microsystems® Java |
| | Software Publisher | Software security in accordance with IETF RFC 2315 and IETF RFC 2633, UNIX® Code Signing (programmer's universal certificate) |
| | Enterprise WAP Server | Unavailable in public offer |
| | Microsoft VBS | Unavailable in public offer |
| | Netscape Object Signing | Unavailable in public offer |
| | Enterprise VPN | Unavailable in public offer |
| | Netscape Form Signing | Unavailable in public offer |
| | Enterprise EDI | Unavailable in public offer |
| | Apple Code Signing | Unavailable in public offer |
| | Castanet Signing | Unavailable in public offer |
| Certum Level IV CA | Certum Platinum | Electronic mail security, electronic signatures of electronic documents, the use of microprocessor card is required |
| | Trusted WEB Server | Data transmission security for WWW servers, in particular electronic banking services and on-line transaction servers |
| | Trusted VPN | data transmission security – IPsec protocol for network devices, servers and VPN channels, in particular electronic banking routers |
| | Trusted Strong Internet | Unavailable in public offer |

| Certification policy | Commercial name of certificate type | Description and recommended applicability |
|---|---|---|
| | Trusted EDI | Unavailable in public offer |
| | Trusted Biometric Data | Unavailable in public offer |
| | Trusted IPsec Client | Unavailable in public offer |
| | Trusted Data Encryption | Unavailable in public offer |
| Certum Partners | Trusted Time Stamp | Timestamping of objects and electronic transmissions of a great value |
| | Trusted CA | Certificate services delivery |
| | Trusted OCSP | OCSP service confirming certificate status |
| | Trusted Notary Service | Electronic notary authority |
| Certum Class 1 CA | Private SSL Server | Testing of security of data transmission between a service and a customer LDAP, NTP, POP3, SMTP etc. |

## 1.4.2. Recommended Applications

Certificates issued in accordance with one of the four 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.

The list of recommended and approved (by CERTUM) applications is published in the repository at:

http://www.certum.pl

Applications are included in the list of recommended applications on the basis of written statements of producers and/or tests made by CERTUM. CERTUM requires from every subscriber to generate by himself/herself/itself encryption keys used for certification process by means of recommended devices. CERTUM leaves the choice of algorithm and the purpose of cryptographic keys to a subscriber. A certification authority can also generate keys on an integrated circuit card or in hardware security module (HSM) and deliver the card or HSM

containing these keys to a subscriber. In such a case, CERTUM applies cryptographic cards or modules fulfilling the requirements of FIPS PUB 140-1.

### 1.4.3. Prohibited Applications

It is prohibited to use CERTUM certificates not in accordance with their declared purpose and in the applications that do not fulfil the minimal requirements specified in Chapter 1.4.2.

The list of prohibited application (it might depend on certificate credibility level) which should not be used to handle certificates issued by CERTUM is published in the repository at:

http://www.certum.pl

The list of prohibited applications contains the applications that did not prove to be consistent with producers' statements in tests made by CERTUM.

## 1.5. Contact

PKI Services Development Team, directly administers the present Certification Practice Statement, Certification Policy and other documents concerning PKI services delivered by CERTUM. Above mentioned Team also test the compliance of Certification Practice Statement and Certification Policy. All inquiries and comments concerning the contents of the mentioned documents should be directed to:

Unizeto Technologies S.A.

CERTUM – Powszechne Centrum Certyfikacji

PL 70-486 Szczecin, Królowej Korony Polskiej St. 21

Email: info@certum.pl

Phone: +48 91 4801 340

# 2. General Provisions

This Chapter describes obligations/guarantees and liability of CERTUM, registration authorities, subscribers and relying parties. The obligations and liability are governed by mutual agreements made by the parties mentioned above (see Fig. 2.1).

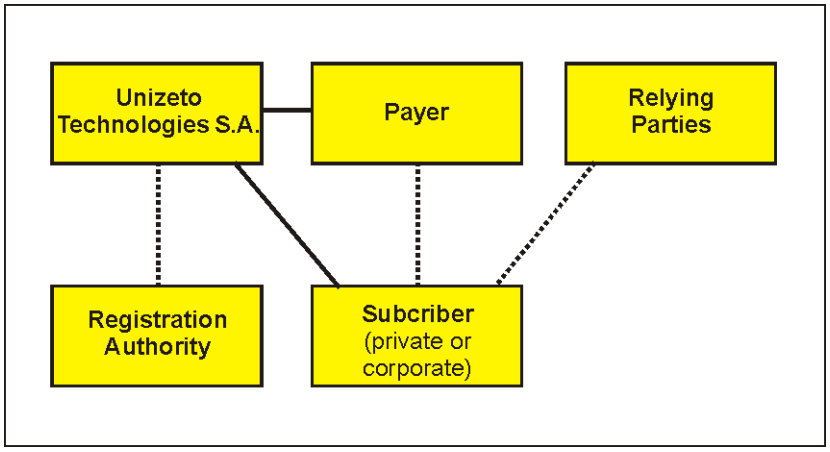


Fig. 2 Agreements between parties

CERTUM agreements with relying parties and subscribers describe types of services provided by CERTUM, mutual obligations and liabilities (including financial ones) of Unizeto Technologies S.A.

Agreements between CERTUM and registration authorities are made when this authority plays a role of an agent of any certification authority operating within **certum** domain. On the grounds of such an agreement, a registration authority can make agreements with subscribers on behalf of CERTUM. In well-founded cases, registration authorities can make separate agreements with subscribers for the services delivered by registration authorities and describing their mutual relations.

CERTUM can register and issue a certificate to any external entity that plays a role of a subordinate certification authority, provided that the registration and issuance are based on the agreement made between the two parties.

## 2.1. Obligations

### 2.1.1. CERTUM and registration authority obligations

CERTUM ensures that:

- 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 Signatures - Part 1: System Security Requirements and FIPS PUB 140 norm *Security Requirements for Cryptographic Modules*,
- its activity and services are in accordance with the law; in particular they do not violate copyrights and licensed third parties rights,
- its services are in accordance with broadly accepted norms:
    - certification services - 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,
  - notary services (DVCS) – with the recommendation RFC 3029,

- 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 Chapters 3 and 4),
  - 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, revoking or suspending the certificate,
  - publication of the lists of revoked or suspended 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 **only one** 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 authorities; certification services are delivered only on the basis of the agreements and always on request of a subscriber, a certification authority or a registration authority,
- manage a list of registered registration authorities 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 certification authorities and registration authorities belonging to or connected with **certum** domain and **ctnDomena** 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.

### 2.1.2. Registration Authority Obligations

Every registration authority operating within **certum** domain 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**[16], associated with a public key requested for certification,
    - procedures of reception, processing and confirmation or rejection of customers' requests for the issuance, renewal, revocation, suspension or unsuspension of the certificate,

[16] See **Glossary**

- procedures of requesting a certification authority, on the basis of already accepted subscriber's application, for the issuance, renewal, revocation, suspension or unsuspension of a 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 authorities that already made agreements with CERTUM (these procedures does not apply to 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 a 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, registration authority 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,
- 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**[17] and CRL's of CERTUM certification authorities.

## 2.1.3. End Subscriber Obligations

By applying for registration to a registration authority and signing confirmation of registration (see Chapter 4.3), 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 an 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,

[17] See **Glossary**.

- 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, by a registration authority or a certification 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 a registration authority or a certification authority 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 nor suspended when the signature was made,
- get to know in general the notions concerning certificates, electronic signatures and public key infrastructure (PKI).

End 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 authority affiliated by CERTUM,
- 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),
- generate cryptographic keys, manage passwords, public and private keys, exchange information with registration and 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,
- 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 a registration authority or certification authority, or prove the possession of the key in another way,
- obtain public key certificates of certification authorities and registration authorities and other CERTUM service units.

## 2.1.4. Relying Party Obligations

The object of an agreement between relying party and:

- Unizeto Technologies 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[18] every electronic signature made on a certificate or document submitted to him/her/it. In order to verify the signature a relying party should:
    - specify a **certification path**[19] 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 or suspended certificates; revocation or suspension of any certificate from certification path influences the earlier expiry of the validity date up to which the verified signature could have been created,
    - check if all certificates belonging to a certification path belong to certification authorities and if they are authorized to sign other certificates,
    - (optionally) specify the date and time of signing a document or a message. It is possible only when the document or message were signed (prior to signing them) with a timestamp issued by a timestamp authority, or a timestamp was associated with an electronic signature just after the creation of the electronic signature on the document; 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,

[18] 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.

[19] See **Glossary**

- 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 1.4),
    - 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.

## 2.1.5. Repository Obligations

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 2.1.3. and 4.4,
- make sure that certificates of certification authorities, registration authorities belonging to **certum** domain and **ctnDomena** domain 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. Liability

Liability of parties delivering services or using these services in the domain managed by CERTUM is governed by appropriate mutual agreements and regulations of this document. Contractual liability of parties results from the violation of the terms stated in an agreement or other documents connected with this agreement. In exceptional cases, if the agreement states so, a part of liability of one of the parties might be delegated to or taken by other parties. Such a situation may occur if a certification authority delegates its rights concerning the verification of subscriber's identity to any registration authority. The registration authority can take liability for its obligations, specified in Chapter 2.1.2.

*CERTUM bears liability for the consequences of the actions of* ***Certum CA, Certum Level I CA, Certum Level II CA, Certum Level III CA, Certum Level IV CA, Certum Partners, Certum Trusted Network CA and Certum Class 1 CA*** *certification authorities, Primary Registration Authority, the repository and – if agreements state so – other certification authorities and registration authorities.*

The record of parties' liability stated below neither eliminates nor substitutes for the liability stated in agreements between parties or resulting from separate law regulations.

## 2.2.1. Intermediate Certification Authorities Liability

CERTUM certification authorities bear liability in instances when direct or indirect damages incurred by a subscriber or a relying party:

- result from mistakes made by CERTUM, particularly concerning the discrepancy between the process of identity verification and declared procedures, inappropriate security of the private key of certification authorities or lack of access to rendered services (e.g. to CRLs),
- occurred as a result of the violation of other CERTUM warranties, specified in Chapters 2.1.1, 2.2.2 or 2.1.5.

If CERTUM made agreements with other registration authorities about services pertaining subscribers' identity verification, it bears the liability by virtue of the warranties stated in Chapter 2.1.2 only if in an agreement between CERTUM and a subscriber, the latter states that:

- the data and documents provided to a registration authority are true and precise,
- he/she/it agrees that approval of a certificate is tantamount to the fact that the certificate contains no mistakes that appeared as a result of negligence or violation of procedures by the persons accepting the applications for certificate issuance or issuing certificates.

*CERTUM does not make any agreements with the subscribers who do not make such a statement in the above mentioned case.*

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

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

- the damages arising from the installation and usage of applications and devices used for generating and managing cryptographic keys, encryption, creating of an electronic signature that are included in the unauthorized applications list (applicable to relying parties) or are not included in the authorized applications list (applicable to subscribers),
- the damages arising from inappropriate usage of issued certificates (term inappropriate understood as the use of a revoked, invalidated or suspended certificate, and not in accordance with the declared purpose of a certificate type, stated in the present Certification Practice Statement),
- in the instance of lack of approval of a certificate that was confirmed by a subscriber and its subsequent usage, the responsibility is taken by the subscriber and should be specified in an agreement between a subscriber and a relying party,
- storage of false data in CERTUM database and their publication in a public certificate key issued to the subscriber in case of subscriber's stating such false data.

*In case of corporate requests, responsibility for data to be included in the certificates, key distribution within the organisation and certificate management is imposed on the entity requesting issuance/renewal of the certificate. Certification authority reserves the rights to verify certificate management controls within such an organisation.*

## 2.2.2. Registration Authority Liability

Primary Registration Authority liability is automatically taken by CERTUM and is a result of warranties stated in Chapters 2.1.1, 2.2.2 and 2.1.5. The conditions of this liability are governed by agreements made by CERTUM with subscribers and relying parties.

Liability of other registration authorities functioning on behalf of and from authorization of CERTUM is specified on the basis of the agreements between these parties. The agreements specify the sanctions resulting from violation of warranties stated in Chapter 2.1.2 and regulate the liability of both parties in relation to subscribers and relying parties.

If a registration authority does not check the subscriber's issuing a statement containing what specified in Chapter 2.2.1, the whole liability resulting from the violation of warranties stated in Chapter 2.1.2 is delegated to a registration authority, unless an agreement between the registration authority and the subscriber states differently.

## 2.2.3. Subscriber Liability

Subscriber liability results from the obligations and warranties stated in Chapter 2.1.3. The liability conditions are governed by an agreement with CERTUM and with a registration authority.

## 2.2.4. Relying Party Liability

Relying party liability results from the obligations and warranties stated in Chapter 2.1.4. 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 2.1.4 of this document.

### 2.2.5. Repository Liability

The liability for functioning of the repository and results of its functioning is taken by CERTUM.

## 2.3. 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.

If damages are the fault of CERTUM or of the parties that Unizeto Technologies 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 2.1.

Table 2.1 Financial liability

| Certification Policy | Private Entity |
|---|---|
| Certum Level I | 0 PLN |
| Certum Level II | 400 PLN |
| Certum Level III | 20 000 PLN |
| Certum Level IV | 100 000 PLN |
| Certum Partners | Specified in agreement |
| Certum Trusted Network CA | 0 PLN |

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 credibility level for creating of an electronic signature or for other cryptographic operations, is limited to amounts not exceeding the amounts stated in Table 2.1.

## 2.4. Governing Law and Dispute Resolution

### 2.4.1. Governing Law

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

## 2.4.2. Supplementary Resolutions

### 2.4.2.1. Resolution Severability

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

Resolution severability is particularly crucial in the agreements mentioned in Chapter 2.1. 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.

### 2.4.2.2. Resolution Survival

The resolutions of the present Certification Practice Statement are valid of the date of the approval by PKI Services Development Team up to the invalidation or substitution of the resolutions. Modifications of the resolutions or introduction of new resolutions are carried out in accordance with the procedures presented in Chapter 8. If 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.

### 2.4.2.3. 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.

### 2.4.2.4. Resolution Notice

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

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

Some information and announcements must be supplied to parties in accordance with an established schedule or deviation from this schedule. This particularly concerns publishing of CRLs, new certificates belonging to registration authorities and 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.

### 2.4.3. 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. Complaint handling is reserved for Chairman of Unizeto Technologies S.A. Board. Complaints are proceeded within 10 days of their delivery.

If the complaint is not settled within 30 days of the commencement of conciliatory process, the parties can hand over the dispute to appropriate court. The court, appropriate for case handling, will be the Public Court of the defendant.

In the instance of the occurrence of arguments or complaints following the usage of an issued certificate or services delivered by CERTUM, 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 authorities, certification authorities, relying parties, etc.) resulting from agreements already made.*

## 2.5. Fees

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

http://www.certum.pl

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 Unizeto' branches on the basis of an invoice or an order.

## 2.5.1. Certificate Issuance or Renewal Fees

CERTUM charges a fee for issuance or renewal[20] 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 personalisation 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).

## 2.5.2. 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.*

## 2.5.3. 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.

## 2.5.4. Other Fees

CERTUM can charge fees for other services (see 2.5.) 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,

[20] See **Glossary**

- auditing registration authority or subsidiary authorities,
- trainings.

### 2.5.5. 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.

## 2.6. Repository and Publication

### 2.6.1. Information Published by CERTUM

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

http://www.certum.pl

The information consists of:

- Certification Policy,
- Certification Practice Statement,
- templates of agreements with subscribers,
- certificates belonging to **Certum CA** certification authority, **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA**, **Certum Partners** other certification authorities, registration authorities, subscribers,
- Certificates Revocation Lists (CRLs); CRLs are accessible at the so called CRL distribution points, whose addresses are set in every certificate issued by CERTUM; the basic point of CRLs distribution is 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 WWW server at:

http://www.certum.pl

Email certificates are also published in directory services at:

ldap://directory.certum.pl

Besides periodical publication of revoked certificates, the repository gives 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.

### 2.6.2. Frequency of Publication

CERTUM publications below are issued with the following frequency:

- Certification Policy and Certification Practice Statement – see Chapter 8,
- the certificates of certification authorities functioning within CERTUM – upon every issuance of new certificates,
- registration authorities certificates – upon every issuance of new certificates,
- subscribers' certificates – upon every issuance of new certificates, on subscribers' prior approval,
- Certificate Revocation List – see Chapters 4.9.4 and 4.9.9;
- records of audits carried out by an authorized authority – every time CERTUM receives them,
- supplementary information – upon every updating of it.

### 2.6.3. Access to Publications

The whole information published by CERTUM in its repository at http://www.certum.pl 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.

## 2.7. 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).

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

CERTUM audit may be carried out by internal units of Unizeto Technologies S.A. (internal audit) and organizational units independent from Unizeto Technologies S.A. (external audit). In both cases, an audit is carried out on request of and under supervision of a **security inspector** (see Chapter 5.2.1).

### 2.7.1. Audit Frequency

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

## 2.7.2. Identity/Qualifications of 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 Unizeto Technologies S.A. structure.

## 2.7.3. Auditor's Relation to Audited Party

See 2.7.2.

## 2.7.4. 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*, further referred to as Web Trust.

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.

## 2.7.5. 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.

*In deficiencies posing an immediate threat to the security of certification procedures of* ***Certum Level III*** *CA and* ***Certum Level IV CA*** *certification authorities, a security inspector might make a decision of a temporary suspension of their activities. All customers of CERTUM shall be notified of the suspension and an expected time of the resumption of the authorities activity. The notice shall be placed in the repository, sent by email and – in well-founded cases – published in the press.*

### 2.7.6. Notifying of Audit Results

Audit records (as detailed as possible) and the auditor's general opinion on the consistency of the functioning of CERTUM with the requirements stated in WebTrust and the security administrator's opinion are published in the repository upon every audit.

## 2.8. Information Security

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

Unizeto Technologies S.A. ensures that third parties are given the access only to the information that 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.*

### 2.8.1. Types of Information to be Kept Secret

Unizeto Technologies 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[21] 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),

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

- record of information about events (logs) connected with certification services, stored by CERTUM and registration authorities,
- records of an internal and external control, if it might cause a threat to CERTUM security (in accordance with Chapter 2.8.2, the majority of this information should be accessible for the public),
- emergency plans,
- information about steps taken in order to protect hardware devices and software, information about administering of certification services and planned registration rules.

*Unizeto Technologies 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.*

## 2.8.2. Types of Information Not Considered Confidential and Private

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

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

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

- Certification Policy and Certification Practice Statement,
- templates of agreements of CERTUM with subscribers,
- the price list of services,
- guides for users,
- registration authorities and 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.

### 2.8.3. Disclosure of Certificate Revocation Reason

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

### 2.8.4. Release of Confidential Information upon Court Writs

Confidential information might be released to law enforcement officials solely upon the fulfilling of all requirements set by the legal regulations in force in the Republic of Poland.

### 2.8.5. Release of Confidential Information for Scientific Purposes

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

### 2.8.6. Release of Confidential Information upon Owner's Request

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

### 2.8.7. Other Circumstances of Release

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

## 2.9. Intellectual Property Rights

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

Every key pair associated with a public key certificate issued by CERTUM is the property of the subject of the certificate, described in the field subject of the certificate (see Chapter 7.1).

*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.*

### 2.9.1. Trade Mark

Unizeto Technologies S.A. owns registered trade mark, consisting of graphic mark and inscription, which constitute the following logo:


Fig. 3.1 CERTUM Logo

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

CERTUM mark is an additional element of logo of every registration authority, operating on behalf of CERTUM. The approval of the use of CERTUM logo is automatically issued when a new registration authority is registered by certification authority.

# 3. Identification and Authentication

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

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

## 3.1. Initial Registration

Subscriber's registration takes place when a subscriber applying for registration does not possess a **valid certificate**[22] 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 a registration process only once. After the verification of data supplied by a subscriber, the subscriber is included on the list of 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 a registration form on WWW site of CERTUM or submit data required for certificate issue (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 3.1.6); optionally, a subscriber can charge a certification authority or registration 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 Unizeto Technologies 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.*

[22] See **Glossary**

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

The names of directories where certificates, CRLs and 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).

Table 3.1 shows minimal requirements imposed on subscribers' names within certification policies defined in Chapter 1.

Table 3.1. Requirements imposed on the name of a certificate subject.

| Certification policy | Requirements |
|---|---|
| Certum Level I CA | Non-empty value of the field subject or empty in the case when the field of the alternative name exists (SubjectAltName) and it is marked as non-critical[23]. |
| Certum Level II CA | Non-empty value of the field subject and optional field of the subject's alternative name (SubjectAltName) in the case when it is marked as non-critical |
| Certum Level III CA | Subject's DN in accordance with X.500 and optionally the alternative name in the case when it is marked as non-critical |
| Certum Level IV CA | Subject's DN in accordance with X.500 and optionally the alternative name in the case when it is marked as non-critical |
| Certum Partners | Subject's DN in accordance with X.500 and optionally the alternative name in the case when it is marked as non-critical |
| Certum Trusted Network CA | Non-empty value of the field subject or empty in the case when the field of the alternative name exists (SubjectAltName) and it is marked as non-critical |

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

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

## 3.1.2. Need for Names to be Meaningful

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

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

DN name 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.

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

## 3.1.3. Rules for Interpreting Various Names Forms

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

## 3.1.4. Names Uniqueness

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

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

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

## 3.1.5. Name Claim Dispute Resolution Procedure

Names that are not owned by a subscriber cannot be used in his/her/its applications. 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.*

## 3.1.6. Prove of Possession of Private Key

If an entity possesses a private key when applying for certificate issuance, certification authorities functioning within CERTUM and registration authorities (if a certificate issuer gave them authority concerning identity verification) need to make sure that the entity possesses a private key corresponding to the submitted public key.

The verification of private key possession is performed on the basis of the so called proof of possession (POP) of private key. This proof is the confirmation that a public key being subjected to the procedure composes a pair with a private key, exclusively owned by a subscriber.

The form of the proof depends on the type of a key pair being certified (a key pair for creation of an electronic signature, encryption and key agreement)

The basic proof is an electronic signature made (by subscriber's application):

- on requests for registration and modification of data and periodically on requests for key/certificate renewal or certificate revocation (in the case of loss of a private key or the secret of certificate revocation), submitted to a registration authority,
- on certification requests, certificate/key renewal and certificate revocation, submitted directly to a certification authority.

*The requirement of proof of private key possession presentation is not applicable if upon subscriber's request, a key pair is generated by a certification authority or a registration authority.*

Private keys should be generated inside a token (e.g. electronic cryptographic card). Any entity can possess a token at the very moment of generating and key import, or the token may be supplied to the entity after the key generation[24]. In the latter case, CERTUM must guarantee that the token and the key shall reach securely the entity for which they are intended. (see Chapter 6.1.2).

## 3.1.7. Authentication of Legal Entity's Identity

The registration authority 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 who represent it (or submits the application). 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

[24] It may be performed by the mans of a certification authority or registration authority.

it is authorized by this legal entity to represent it. Submitted documents (or collected data) should prove:

- identity of the subscriber or certificate administrator (in case of certificates issued for legal entities or devices),
- existence of the legal entity or institution,
- the right of the subscriber or the certificate administrator to act on behalf of the institution or legal entity.

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 a registration authority, or a 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 a certification authority or its agent.

Detailed requirements on the identification documents and their verification are specified in separate document – *Identity verification instruction*.

*A registration authority is committed to verify the correctness and truthfulness of all data provided in an application (see Table 3.2, Chapter 3.1.8).*

If the verification is successful, an authorized operator of a registration authority:

- assigns a distinguished name to the legal entity or approves the name suggested in the submitted application,
- issues a **token** confirming the truthfulness of data provided in the application being examined and sends the token to a certification authority,
- registers all the documents and certificates (or information of the public data source) used by the operator to verify the legal entity's identity and the identity of representative acting on behalf of the entity,
- (optionally) on behalf of a certification authority, makes an agreement with the legal entity about certification services delivery; the agreement may be made if the legal entity plays a role of a subscriber, a registration authority, a certification authority, or an entity rendering other certification services. The confirmation (token) is sent to a certification authority which checks if the token was issued by an authorized registration authority.

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 a registration authority operator verifying the identity of a 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 case of subject's attendance in person in the registration authority (provided the subject has been supplied with such identifier),

If a 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 a registration authority to confirm the application.

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

### 3.1.8. 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.

### 3.1.9. Devices Origin Authentication

In case of device certificates, the authentication is carried out the same as for the legal entities. Additionally, in case of certificates issued for networking devices, registration authority operator may – in doubtful cases – verify the registration of the domain in publicly available WHOIS services.

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

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 a password,
- the data set in the certificate have been modified,
- on every request of a 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 a certification authority are authenticated by this authority on the basis of 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.

### 3.2.1. Rekey

Rekey might be performed by a subscriber periodically, on the basis of parameters of a given certificate that is already owned by the subscriber. The result of rekey is a new certificate whose parameters are the same as the parameters of the certificate mentioned in the application, except for a new key, certificate serial number and validity period (see Chapter 4.7)

Verification of the identity of the subscriber requesting rekey is carried out on the basis of documents submitted for modified (renewed) certificate. Detailed requirements are specified in separate document – *Identity verification instruction.*

### 3.2.2. Recertification

A subscriber or certification authorities uses recertification if he/she/it already possesses a certificate and a 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 previous certificate. (see Chapter 4.6)

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

Each recertification request is processed in off-line mode, i.e. it requires manual acceptance by the certification authority operator.

*Currently CERTUM does not support recertification of the same key pair of the subscribers', due to security reasons. Such restriction does not apply certification authority key recertification (see Chapter 6.1.1.4)*

### 3.2.3. Certificate Modification

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

Modification might be necessary e.g. in the case of changing of position at work or the change of name, on the condition that these data were previously stated in the certificate or they should be added. If data that are verified in accordance with subscriber's authentication procedures on the basis of appropriate documents (e.g. certification of the position at work) have been modified, every application must be confirmed in a registration authority (see Chapter 4.8).

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. 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 a registration authority or certification authority operator. The subscriber's identification and authentication may be performed analogically to the case of initial registration (see Chapter 3.1) or may be based on 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 email 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.

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

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

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

Detailed procedure of revocation is disclosed in Chapter 4.9.3.

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

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

## 4.1. Application Submission

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

A registration authority operator has a double role: the role of a subscriber and the role of a person authorized to represent a 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.

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

### 4.1.1. Registration Application

An application for registration is submitted to a registration authority indirectly or directly to a certification authority and should contain 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),
- the subscriber's address or the address of his/her/its seat (province, postcode, city, commune, administrative district, street, house number, flat number, fax number),
- type of the certificate that is requested,
- the identifier of certification policy on the basis of which the certificate is to be issued,
- email address,
- a public key which is to be certified.

Depending on the certificate content and its sensitivity level, some of the above information may be optional.

Upon authentication of the identity of the subscriber (see Chapters 3.1.7, 3.1.8 and 3.1.9) applying for registration and upon reception of confirmation issued by a registration authority, the application is sent to a certification authority.

### 4.1.2. Certificate renewal, rekey, certification or modification application

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

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

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

An 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,
- a public key (previously used in the case of certificate renewal or modification or 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 a subscriber possesses a currently valid private key for signature creation.

Upon authentication of the identity of the subscriber (see Chapters 3.1.7, 3.1.8 and 3.1.9) applying for registration and upon reception of confirmation issued by a registration authority, the application is sent to a certification authority.

### 4.1.3. Certificate Revocation or Suspension Application

An application for certificate revocation is submitted to a registration authority or directly to a certification authority by a subscriber. Applications are submitted to a registration authority in the following cases:

- lack of a currently valid private key for an electronic signature creation,
- upon explicit demand of a certification authority operator.

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

Information included in electronic certificate revocation or suspension application:

- the requester's (subscriber's) distinguished name,
- list of certificates to be revoked or suspended, containing pairs: serial number, reason for revocation.

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

An application for revocation might be submitted by email along with authentication, as a written version (as a letter, by fax) or orally (telephone call). Detailed requirements on revocation request are presented in separate document – *Identity verification instruction*.

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

## 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: https://www.certum.pl. 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 a certification authority. Applications for Certum Level I 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 the CERTUM or automatically if the comparison with CERTUM database is sufficient.

*Off-line* submission of an application requires subscriber's or an authorized representative's of a company attendance in person in a registration authority or certification authority, representative's 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 in *Identity verification instruction*. 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 collective applications. These applications are confirmed by a certification or registration authority operator and processed in groups.

Every *on-line* certification application is sent to:

- **request confirmation box**, if an application requires the issuance of confirmation by a registration authority,
- **request box**, if an application does not require the issuance of confirmation by a registration authority.

Both boxes are fully controlled by a certification authority.

Applications processed on the basis of *off-line* request, upon successful verification by a registration or certification authority operator, are usually submitted to a **request box**.

### 4.2.1. Application Processing in Registration Authority

Every application submitted to a request confirmation box or submitted to a registration authority in a paper version, is processed in the following way:

- a registration authority operator obtains subscriber's application (a paper version or an electronic version from the request confirmation box),
- the operator verifies data listed in the application, e.g. subscriber's personal data (see the procedure described in Chapter 3.1.8) and checks the proof of private key possession if it exists (see Chapter 3.1.6),
- upon the positive verification, the operator confirms (signs) the request; if the original application contains wrong data, it is rejected,
- the confirmed application is submitted to a request box of a certification authority,
- a 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. Application Processing in Certification Authority

A certification authority retrieves applications out of a request query. The applications might contain confirmation issued by a registration authority. If a given application does not contain confirmation, a certification authority:

- binds the application with registered subscribers' database,
- verifies authentication of the application (electronic signature or authentication code),
- verifies formal correctness of the application (syntax and contents),
- checks if the subscriber is authorized to issue the type of request he/she/it has sent and its contents,
- records these procedures in database and system journals.

If the application contains confirmation, a certification authority checks whether the confirmation was issued by an authorized registration authority. If it is the case, further processing is carried out analogically to processing an application without confirmation. Additionally, if the application contains request for issuance of a signature verification certificate, the certification authority checks the proof of a private key possession submitted by the subscriber.

# 4.3. Certificate Issuance

On receiving an appropriate application and processing it (see Chapter 4.2), a certification authority **issues a certificate**. A certificate is considered valid (active or ready status) of the moment of the subscriber's approval (see Chapter 4.4). Validity periods of the issued certificate depend on the certificate type and the subscriber's category and they are in accordance with periods presented in Table 6.6.

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

- a processed application 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 2 with this task,
- quality of submitted or generated by a certification authority public keys is tested,
- if the procedures are successful, the server issues a certificate and charges hardware security module with signing the certificate; the certificate is stored in certification authority database,
- the certification authority prepares the answer containing the issued certificate (if it was issued) and sends it to the subscriber; the certificate is not published in the repository (even if the subscriber approved of that) until the reception of the subscriber's confirmation of approval of the certificate (see Chapter 4.4).

CERTUM certification authority employs two basic methods concerning notifying a subscriber about the 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 a given certification authority about the issuance of a new certificate to this authority or notifying some subscribers about the issuance of a 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).

Every issued and accepted certificate is published in CERTUM repository. Certificate publication is equal to notifying other relying parties that a certificate has been issued to a subscriber who as the owner of the certificate is entitled to be authorized as a relying party.

CERTUM publishes a certificate in the repository upon approval of the certificate by the subscriber (see Chapter 4.4)

## 4.3.1. Certificate Issuance Awaiting

A certification authority should make efforts to ensure that on receiving application for registration and certification, and certification or renewal (of keys or certificate), the authority examines the application and issues a certificate within the period stated in Table 4.1.

Table 4.1. Maximum awaiting period for certificate issuance

| Certificate Credibility Level | Expectation period |
|---|---|
| Certum Level I CA | 7 days |
| Certum Level II CA | 7 days |
| Certum Level III CA | 7 days |
| Certum Level IV CA | 7 days |
| Certum Class 1 CA | 7 days |

The periods depend mainly on completeness of a submitted application and possible administration co-ordinations and explanations between CERTUM and the requester.

### 4.3.2. 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:

- the subscriber cannot prove his/her rights to proposed **DN**,
- if there is suspicion or certainty that the subscriber falsified the data or stated false data,
- if the subscriber in especially inconvenient manner engaged resources and processing means of CERTUM by submitting number of request clearly in excess of his/her/its needs,
- from other reasons not specified above.

Information concerning the decision about certificate issuance denial and its reasons is sent to the requester. The requester can appeal to CERTUM within 14 days of the reception of the decision.

## 4.4. Certificate Acceptance

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

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

- usage of the PIN owing to which the certificate is installed by means of WWW site: (https://www.certum.pl) or,
- lack of certificate revocation in above mentioned period.

*If a certificate is not clearly rejected within 7 days of the reception of the certificate, the certificate is considered to be accepted.*

Every accepted certificate is published in CERTUM repository and accessible for the public.

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 Unizeto Technologies 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 4.9.11).

# 4.5. Certificate and Key Usage

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 Unizeto Technologies S.A.,
- only within the validity period (not applicable to certificates for digital signature verification),
- until the certificate revocation; when the certificate is suspended, the subscriber cannot use the private key, particularly for creating a signature.

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

- in accordance with their purpose stated in the present Certification Practice Statement and in compliance with the certificate contents (the fields **keyUsage** and **extendedKeyUsage**),
- only upon their status verification (see Chapter 4.9) and verification of the signature of the certification authority that issued the certificate,
- until the key revocation (applicable to public keys for key exchange, data encryption or key agreement); when the certificate is suspended, the relying party cannot use the public key.

# 4.6. Recertification

*CERTUM provides the services of recertification of the same pair of cryptographic keys solely to the certification authorities. If the recertification procedure turns successful, the certificate being the subject of the update is not revoked.*

# 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.

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.

*Certification or rekey is performed only on subscriber's demand and must be preceded by subscription of a suitable request form.*

Rekey and certification request authorization is carried out in accordance with specifications of *Identity verification instruction*.

Rekey and certification requests are processed in accordance with Chapter 4.2. and 4.3. As a result of the latter:

- the subscriber is notified of the new certificate issuance with the new serial number,
- the subscriber should submit an authorized certificate acceptance confirmation to a certification authority,
- a new certificate is published in the repository of a certification authority.

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.*

# 4.8. Certificate modification

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

Certificate modification:

- is performed only on subscriber's demand and must be preceded by submission of a suitable certificate modification request.

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

- email address,
- subscriber's postal address.

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

*If modification procedure is successful, a certificate being modified might be revoked and placed on Certificate Revocation List (CRL). As a reason for revocation,* ***affiliationChanged***[25] *term is provided, meaning that (1) the revoked certificate was replaced by another one, which contains modified data, i.e. subscriber's name and (2) informing relying parties that there is no reason to suspect that a private key related with the certificate was compromised.*

Modification procedure can be also applicable for certification authority certificates, although in such a case all customers of the certification authority should be informed about procedure execution.

# 4.9. Certificate revocation and suspension

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

*Certificate suspension is carried out only in closed corporate systems affiliated by CERTUM.*

During suspension period or 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 or suspension 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 or suspension. Although certificate suspension is a specific form of revocation, this CPS will distinguish both terms to emphasize the essential difference between them: certificate suspension can be cancelled while revocation – cannot.

Certificate suspension is temporary (usually lasts until explanation of reasons of the suspension). If a subscriber, for example, losses control over media which contains a key pair, secured by password or PIN, such a situation should be reported at once to a certification authority, along with certificate suspension request. In case of swift media restoration and assurance that the private key has not been compromised, the certificate may be (on subscriber's demand) unsuspended, restoring its valid status.

[25] This case incorporate by default the replacement of the certificate

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

## 4.9.1. Circumstances for certificate revocation

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

Certificate revocation may be performed if the following situation occurs:

- when any information within the certificate has changed,
- when a private key, associated with a public key contained in the certificate or media used for storing it has been, or there is a reason to strongly suspect it would be compromised[26]; certificate revocation procedure is in this case executed by a subscriber,
- the subscriber decides to terminate the agreement with Unizeto Technologies S.A. (in such a case, revocation is strictly bounded with cancellation of 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,
- by its issuer, CERTUM, for example when the subscriber does not comply with accepted Certification Policy or resolutions of other documents signed by a certification authority,
- if a certification authority terminates its services, all the certificates issued by this certification authority before expiration of declared period of service termination have to be revoked, along with the certificate of the certification authority ,
- the subscriber 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.

[26] 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.

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 3.1.8, or in a certification authority on the basis of request authorization.

## 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[27], 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.

*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

Certificate revocation may be carried out in following manners:

- **the first method** is based on submission of electronic revocation request, signed with a currently valid private key, or authorized by a password, to a certification authority;

[27] See **Glossary.**

such revocation may be initiated solely on subscriber's demand (any entity being the owner of certificate being revoked),

- **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 his/her/its private key or its password or his/her/its private key has been stolen or (b) revocation request has been submitted by the subscriber's sponsor, an authorized representative of a certification authority or a registration authority, provided that there are sufficient reasons to request such revocation,
- **the third method** involves submission of an authenticated non-electronic request (paper document, fax, phone call, etc) to Primary Certification Authority; authentication of a paper document (including fax) is described in *Identity verification instruction* document.

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

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

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

Certificate revocation procedure is carried out as follows:

- a 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 or suspension) 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 or information about certificate suspension (see Chapter 7.2.1),
- 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 a subscriber's sponsor, 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.

## 4.9.4. Certificate revocation grace period

CERTUM guarantees the following maximum grace period[28] 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)

as described in Table 4.2.

Tab. 4.2 Allowable grace period in certificate revocation request processing

| Certification Policy | Allowable grace period |
|---|---|
| Certum Level I CA | No obligation to revoke |
| Certum Level II CA | Within 48 hours |
| Certum Level III CA | Within 48 hours |
| Certum Level IV CA | Within 48 hours |
| Certum Class 1 CA | Within 48 hours |

*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.*

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 4.9.9).

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

Information about current status of a certificate is available through certificate status verification service (see Chapter 4.9.11), immediately after declared revocation grace period. This service may be requested for example by a relying party, verifying validity of an electronic signature on a document submitted by the subscriber.

[28] 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.).

## 4.9.5. Reasons for certificate suspension

Certificate suspension is applicable only for the certification authority certificates. Suspension may be carried out solely in case of certification policies modification, termination of providing certification services by CERTUM or justified suspicion related to certification authority key security.

## 4.9.6. Who can request certificate suspension

Due to availability of suspension services solely for the certificates of the certification authority, suspension request may be submitted only by the Security Inspector together with CERTUM Manger or Director suitable for certification services.

## 4.9.7. Procedure of certificate suspension and unsuspension

Certificate suspension requires formal request of the Security Inspector, confirmed by CERTUM Manager or Director suitable for certification services.

## 4.9.8. Limitation on suspension grace period

CERTUM guarantees the grace period in suspension request processing, as well as availability of certificate status verification to be the same as the in case of certificate revocation (see Chapter 4.9.4).

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

## 4.9.9. CRL issuance frequency

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

Every Certificate Revocation List is updated at least once a month[29] if no additional certificate has been revoked within this period. Notwithstanding, the new CRL is published in the repository after every certificate revocation. Certificate Revocation List for Certum CA authority is issued at least every 5 years, provided that there is no revocation of the certificate of one of the authorities affiliated by Certum CA.

In the case of revocation of the certificate of the authority affiliated by CERTUM this certificate is immediately published on Certificate Revocation List.

## 4.9.10. Certificate Revocation List checking

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

---

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

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 4.9.11).

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

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

If a certificate was revoked because of the following reasons:

```
affiliationChanged   – data modification
superseded           – amendment of the key
removeFromCRL[30]      – certificate removed from the CRL (unsuspended)
```

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

## 4.9.11. On-line certificate status verification availability

CERTUM provides real-time certificate status verification service. This service is carried out on the basis of OCSP, described in RFC 2560[31]. Using OCSP, it is possible to acquire more frequent and up-to-date information (in comparison to sole CRL usage) about a certificate status.

OCSP 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[32],
- **revoked** – meaning the certificate has been revoked,
- **unknown** – meaning the certificate has not been issued by any of the affiliated certification authorities.

*OCSP service is available to every subscriber and relaying party who accept service provision practices, described in this document..*

Certificate status is available in real-time (i.e. immediately after the certificate revocation) on the basis of CERTUM databases, and contains more current information than the information published in CRL .

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

A relying party is not obligated to verify certificate status *on-line* on the basis of mechanisms and services described in Chapter 4.9.11. Notwithstanding above, it is recommended to employ

[30] Reason for certificate removal from CRL (**removeFromCRL**) is disclosed only in **deltaCRL** lists (see *PKC Certificate and CLR profile*, published by Unizeto Sp. z o.o. Certification Authority, 22nd of Oct 2001).

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

[32] See **Glossary**.

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

### 4.9.13. Other forms of revocation advertisements availability

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

### 4.9.14. Checking requirements for other forms of revocation advertisements

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

### 4.9.15. Special requirements regarding key security violation

This Certification Practice Statement does not define any additional requirements regarding this area.

### 4.9.16. Revocation or suspension of CA certificate

The certificate belonging to a certification authority may be revoked or suspended 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.

## 4.10. 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.

### 4.10.1. Types of events recorded

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

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

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

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.

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

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

Recorded entries include:

- alerts generated by firewalls and IDS,
- operations associated with registration, certification, rekey and renewal procedures, revocation, suspension or other services provided by an authority issuing certificates,
- every modification to hardware or software structure,
- modification to the network and network connections,
- physical entries to secured areas and their violations,
- changes of passwords, PINs rights and personnel roles,
- successful and unsuccessful attempts to access CERTUM databases and server applications,

- key generation for a certification authority, as well as for other parties, for example registration authorities,
- every received request and issued decisions in an electronic form, submitted by subscribers or delivered to them as an electronic file or electronic mail; the requirement to record such activities is imposed not only on the certification authorities, but also on the registration authorities,
- history of creating backup copies and informative records archives, as well as databases.

A detailed list of recorded events depends of the level of credibility (the name of the certification policy) of certificates issued or confirmed by a specific certification authority or a registration authority.

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

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

## 4.10.2. 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.

## 4.10.3. Event journals retention period.

Records of registered events are stored in files on system disk until they surpass allowed capacities. In this time they are available *on-line*, on every authorized person's or process demand. Upon surpassing allowed capacities logs are stored in archives, and may be accessed only *off-line*.

Archived journals are retained for at least 5 years.

## 4.10.4. 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 authorised entities (i.e. auditors and personnel defined above) have the right to read log entries,
- only the security inspector may archive or erase files (after their archive) containing registered events,
- it is possible to detect every violation of integrity; it assures that the records do not contain gaps or forged entries,
- no entity has the right to modify the contents of the journal.

Additionally, procedures for event logs protection are implemented in a manner that even after the journal archival it is impossible to delete entries or erase the logs before surpassing an estimated period of logs retention (see Chapter 4.10.3).

### 4.10.5. 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.

### 4.10.6. Notification to event responsible entities

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

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

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

### 4.10.7. Vulnerability assessment

This Certification Practice Statement requires a certification authority issuing the certificates (including subordinate authorities of Certum Partners) and affiliated registration authorities (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.

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

## 4.11. Records archival

It is required that all data and files related to registration of information associated with the system security, requests submitted by subscribers, information about subscribers, issued certificates and CRLs, keys, used by certification and registration authorities, and whole correspondence within CERTUM and with the subscribers should be subjected to archive. Subjected to archival are also all the documents and data used in identity verification process. Some of the 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.*

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.

On the basis of the archives, backup copies are created and retained outside CERTUM seat.

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

## 4.11.1. Types of data archived

The following data are subjected to archive:

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

## 4.11.2. Frequency of data archive

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

- certificate database and subscriber's database are retained on CERTUM media, duplicated by the hardware matrix, for a period of three years (from the time of certificate issuance). For the following three years, archives are stored on magnetic apes or DVD disks, still available *on-line*. In the seventh year (six years after certificate issuance) all information regarding subscribers and their certificates is stored on DVD disk and may be available only *off-line*,

- CRL, electronic correspondence and requests submitted by subscribers, as well as issued decisions are subjected to archive in the same pattern and frequency as for the certificate and subscribers databases.

## 4.11.3. Archive retention period

Archived data (in paper and electronic form), described in Chapter 4.11.1, are retained for the period of minimum 25 years. After expiration of the declared retention period, archived data may be destroyed. In the case of key and certification erasure, an appropriate procedure is executed with particular attention.

## 4.11.4. 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.

Method for backup copy creation has significant importance for quickness and cost of the certification authority restoration upon malfunction or destruction of the system. CERTUM utilizes the following two methods:

- **hot reserve** – database backup copies are created every day and may be, if necessary, used for recovery of the lost data
- **weekly backup copies** – created in the primary facility and (if necessary) used for recovery of destroyed hardware and software configuration; backup copy should cover entire and current status of the CERTUM system; the facility should perform full restoration of CERTUM system functionality within 48 hour.

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

## 4.11.5. 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**.

### 4.11.6. Access procedures and archived information verification

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.

## 4.12. 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 2510, and Chapters 6.1.1.2 and 6.1.1.3).

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 CA** 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. 6.5.

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

## 4.13. Key security violation and disaster recovery

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

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

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

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

- corruption of a part of the network, used by CERTUM to provide its services – the corruption may imply obstruction for the customers and denial (unintended) of services.

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

- **Disaster Recovery Plan.** All subscribers and relying parties are informed, as soon as possible and in a manner most appropriate for the existing situation, about every significant malfunction or corruption, associated with any information system or network environment component. Disaster recovery plan includes number of procedures executed in the event any part of the system has been subjected to compromise (corruption, revelation, etc). The following actions are performed:
    - disk images of every server and workstation of CERTUM are created and archived; every backup copy is retained both in main seat and in emergency location outside CERTUM,
    - periodically, following the procedures disclosed in Chapter 4.11.4, 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 4.11.4, 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. Backup copies and archives are created from every data having significant importance on security and normal activity of CERTUM. Copies are created periodically and stored on magnetic tapes, while archives are stored on CD-ROM disks. Backup copies may be protected by a password, while CD-ROM disks are encrypted and may be additionally timestamped. Backup copies and their archives are retained outside primary facility.
- **Additional services**. To prevent the system from power cuts and to secure service continuity, emergency power sources (UPS) are employed. UPS devices are tested every six (6) months.

### 4.13.2. Key compromise or suspicion of certification authority private key compromise

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

- the certification authority generates a new key pair and a new certificate,
- all certificate users are immediately informed abut the compromise of the private key, by means of mass media system and electronic mail,
- a certificate 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.

### 4.13.3. Security coherence after disaster

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

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

# 4.14. Certification authority termination or service transition

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

## 4.14.1. 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 his/her/its sponsor; compensations should be proportional to remaining validity period of the certificate.

## 4.14.2. 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 certification authority ceasing its service has to be turned over to the prime certification authority – **Certum CA** (in the case of termination of services of **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** or **Certum Partners**) or to the **Certum Trusted Network CA** (in the case of termination of services of Certum Class 1 CA) or to the institution which the suitable agreement was signed up with (in the case of termination of services of **Certum CA** or **Certum Trusted Network CA**).

# 5. Physical, organizational and personnel security controls

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

## 5.1. Physical security controls

### 5.1.1. CERTUM physical security controls

Network computer system, operator's terminals and information resources of CERTUM are located in the dedicated area, physically protected against unauthorized access, destruction or disruption to its operation. These locations are monitored. Every entry and exit are recorded in the event journal (system logs). Power stability, as well as the temperature and humidity are monitored.

#### 5.1.1.1. Site location and construction

CERTUM is located in the Unizeto Technologies S.A. seat, at the following address: Królowej Korony Polskiej 21, Szczecin, Poland .

#### 5.1.1.2. Physical access

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

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

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 Unizeto Technologies S.A. Monitoring of the access rights is carried out on the basis of smart cards and access control system, whose terminals are mounted next to the area entry. Every entry and exit from the area is automatically recorded in the event journal. The presence of other individuals (e.g. auditors or service employees) requires presence of authorized personnel and authorization of CERTUM Manager.

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

### 5.1.1.3. Power and air conditioning

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

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

Each area is air-conditioned.

### 5.1.1.4. Water exposure

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

### 5.1.1.5. Fire prevention

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

### 5.1.1.6. Media storage

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

### 5.1.1.7. Waste disposal

Paper and electronic media containing information possibly significant for CERTUM security after expiration of the retention period (see Chapter 4.11) are destroyed in special shredding devices. In the case of cryptographic keys and PIN or PUK numbers, media used for their storage are shredded in DIN-3 class devices (this applies only to the media which do not allow definitive erasure of stored information and their re-usage).

### 5.1.1.8. Offsite backup storage

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

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

## 5.1.2. Registration authority security controls

Computers 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 bu authorized individuals.

### 5.1.2.1. Site location and construction

Registration authorities of CERTUM are located in the following sites:

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

### 5.1.2.2. Physical access

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

### 5.1.2.3. Power and air conditioning

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

### 5.1.2.4. Water exposure

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

### 5.1.2.5. Fire prevention and protection

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

### 5.1.2.6. Media storage

Media used for storage of archives and current information backup copies and paper documents are held in the safes located in the Primary Registration Authority area.

### 5.1.2.7. Waste disposal

Paper and electronic media, containing confidential or secret information are, upon expiration of the retention period (see Chapter 4.11.3), destroyed in special shredding devices.

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

#### 5.1.2.8. Offsite archive storage

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

It is recommended to store archives and current information processed by the computer system backup copy outside location of the registration authority.

### 5.1.3. Subscriber security

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

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

## 5.2. Organizational security controls

This Chapter presents a list of roles which can be defined for personnel, employed in CERTUM. 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:

- **PKI Services Development Team member** – determines direction of CERTUM development, implements and manages Certification Policy as well as Certification Practice Statement,
- **Certification Authority Manager** – responsible for correct management of CERTUM,
- **security inspector** – supervises implementing and handling information system security procedures; manages the administrators, initiates and supervises key and shared secret generation; assigns rights in the field of security and user's access privileges; reviews event logs; supervises service tasks,
- **system operator** – handles standard system operations, including backup copies and transfer of current copies and archives to offsite locations,
- **registration inspector** – verifies subscribers' identity and correctness of submitted certification application; authorizes certification request,

- **system administrator** – installs hardware and software for operating system; initially configures the system and network resources; manages folders of CERTUM available to the public; creates WWW page and manages links,
- **application programmer** – creates certification processes and WWW pages,
- **audit inspector** – responsible for review, archive and management of event logs (in particular verification of their integrity) and performance of internal audit for compliance of a certification authority operations with this Certification Practice Statement; this responsibility extends also on every registration authority, operating within CERTUM,

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

The 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.

#### 5.2.1.2. Trusted roles in registration authority

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

- **system administrator** – installs hardware and software of operating system; installs application software; configures system and applications; activates and configures security resources; creates operators' accounts and passwords; creates backup copies and archives information; reviews events journals (logs) and (together with registration authority operator) and by the order of the security inspector, erases excessive information;
- **registration inspector** – verifies subscriber's identity and correctness of provided request; authorizes requests and provides them to a certification authority; takes part in certificate generation, submitting information from a request to a certification authority; signs agreements with subscribers concerning services provided by the certification authority; archives (in paper form) requests and issued confirmation,
- **registration authority agent** – is responsible for efficient operation of a registration authority; his/her role is to provide financial support for the personnel, manage operators' and administrators' work, arbitrate disputes, make a decision arising from operations carried out by a registration authority,

#### 5.2.1.3. Subscriber's trusted roles

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

### 5.2.2. Numbers of persons required per task

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

- security inspector,
- hardware security module operator,
- shared secret holder,
- commentator,
- observers – (option) representatives of the auditor.

Any other operation and role, described within CERTUM, may be performed by a single person, assigned for such an operation or role.

### 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.

## 5.3. Personnel controls

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

- has graduated from at least the secondary school,
- has signed a work contract or other civil agreement describing his/her role in the system and corresponding responsibilities,
- has been subjected to required training on the range of obligations and tasks, associated with his/her position,
- has been trained in the field of personal data protection,
- has signed an agreement containing clause concerning sensitive (from the point of view of CERTUM security) information protection and confidentiality and privacy of subscriber's data,

- does not perform tasks which may lead to a conflict of interests between a certification authority and a registration authority acting on behalf of it.

## 5.3.1. Training requirements

Personnel performing roles and tasks arising from the employment in CERTUM or its registration authority have to complete following trainings:

- regulations of Certification Practice Statement,
- 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.

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

## 5.3.2. Retraining Frequency and Requirements

Trainings described in Chapter 5.3.1 have to be repeated or supplemented always in situation when significant modification to CERTUM or its registration authority operation is executed.

## 5.3.3. Job rotation

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

## 5.3.4. Sanctions for Unauthorized Actions

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

## 5.3.5. Contract Personnel

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

### 5.3.6. Documentation Supplied to Personnel

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

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

# 6. Technical Security Controls

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

## 6.1. Key Pair Generation

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

**Certum CA** certification authority owns 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 certification authorities **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA**, **Certum Partners** or other certification authorities established on the basis of this documentation (e.g. providing non-repudiation services) and issuing of Certificate Revocation List and operational certificates of a certification authority, necessary for the operation of the authority issuing the certificates. A similar purpose is intended for private keys being held by each authority: **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA**, **Certum Partners** and corresponding to public keys included in certificates issued by **Certum CA** for each of these authorities.

Key pairs owned by each certification authority should allow:

- certificate and CRL signing; a public key associated with a private key authenticated with a self-certificate (in the case of **Certum CA**) or certificate (in the case of **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA**, **Certum Partners**),
- signing messages, transmitted to subscribers and registration authorities (the operational key),
- negotiation of keys used for confidential information exchange between the authority and its environment (the operational key).

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

### 6.1.1. Key pair generation

**Certum CA** and **Certum Trusted Network CA** certification authority keys and **Certum Level I CA, Certum Level II CA, Certum Level III CA, Certum Level IV CA**, **Certum Class 1 CA** and **Certum Partners** and non-repudiation authorities keys are generated within CERTUM seat, in the presence of selected, trusted group of persons (comprising additionally security inspector and system administrator). The group is required only in the case of certificate and CRL signing key generation.

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.

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

Generally, every subscriber generates his/her/its key pair by himself/herself/itself. The generation may also be delegated to a certification authority (applicable only for keys generated on cryptographic cards).

*CERTUM may, on subscriber's demand or on certification authority operator's demand, generate a key pair and submit it securely to the subscriber. In such cases hardware security module complying with the regulations of at least FIPS 140-2 Level 2 (see Chapter 6.1.2) is employed.*

### 6.1.1.1. Procedures of generation of Certum CA and Certum Trusted Network CA initial keys

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

- secure generation of a main key pair for certificate and CRL signing – the main key pair has a form $\mathbf{GPK_{(1)}=\{K^{-1}_{GPK(1)}, K_{GPK(1)}\}}$, where $\mathbf{K^{-1}_{GPK(1)}}$ – private key, and $\mathbf{K_{GPK(1)}}$ – public key, distribution of private key (according to accepted threshold method),
- issuance of a public key ($\mathbf{K_{GPK(1)}}$) self-certificate.

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

### 6.1.1.2. Certum CA and Certum Trusted Network CA rekey procedure

**Certum CA** and **Certum Trusted Network CA** cryptographic keys have a limited lifetime period; if the period has expired, the keys should be updated.

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

To achieve effect described above, **Certum CA** or **Certum Trusted Network CA** deploys a procedure, owing to which new key pair generation will secure (authenticate) a new public key with the use of the former (previously used) private key and vice-versa (an old public key is secured with a new private key). It means that as a result of update of the self-certificate of

certification authority **Certum CA** or **Certum Trusted Network CA**, 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 CA** and **Certum Trusted Network CA** key pair – designated to certificate and CRL signing – update (rekey), is executed as follows:

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

### 6.1.1.3. Subordinate certification authority rekey procedure

Procedures for intermediate certification authority key update (rekey) of **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA**, **Certum Class 1 CA** and **Certum Partners** authorities are executed similarly as for **Certum CA** (see Chapter 6.1.1.2) except one step: **certificate NewWithNew** is issued by **Certum CA** authority.

### 6.1.1.4. Certum CA, Certum Trusted Network CA and subordinate authorities certificate recertification procedure

Certificates belonging to **Certum CA** and **Certum Trusted Network CA** authority and other authorities may be subjected to recertification. This operation is performed only upon occurrence of the situation presented in Chapter 3.2.2. Prior to issuance of a new certificate, the authority assess, whether the key size guarantees its further security during the period of extended certificate value.

## 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) and are delivered to the subscriber personally or by means of registered mail; data for the card activation (including PIN/PUK) are submitted separately from the media containing the key pair; the issued cards are personalized and registered by the certification authority.

*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 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[33] (CRS) supported by a certification authority, a registration authority and a subscriber.

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

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

CERTUM certification authorities distribute their certificates in two different methods:

- placement in the publicly available web repository of CERTUM at http://www.certum.pl,
- 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

Sizes of keys deployed in CERTUM by registration authority operators and subscribers are presented in Table 6.1.

Tab.6.1 Size of keys used

| Type of key owner | Prime key usage | | |
|---|---|---|---|
| | RSA for certificate and CRL signing | RSA for message signing and key exchange | Diffie-Hellman |
| Certum CA | 2048 bit | – | – |
| Certum Trusted Network CA | 2048 bit | – | – |
| Certum Level I | 1024 bit | – | – |
| Certum Level II | 1024 bit | – | – |
| Certum Level III | 1024 bit | – | – |
| Certum Level IV | 1024 bit | – | – |
| Certum Level I CA | 2048 bitów | – | – |
| Certum Level II CA | 2048 bitów | – | – |
| Certum Level III CA | 2048 bitów | – | – |
| Certum Level IV CA | 2048 bitów | – | – |
| Certum Class 1 CA | 2048 bitów | – | – |
| Certum Partners | 2048 bitów | – | – |
| Certum Notary Authority | 2048 bit | – | – |
| Certum Validation Service | 2048 bit | – | – |
| Certum Time-Stamping Authority | 2048 bit | – | – |
| Private and legal entities and their hardware | – | Defined by the users (2048 bit or more) | – |

## 6.1.6. Public Key Generation Parameters

This Certification Practice Statement does not imply any requirements in this field, although it is recommended that in the case of RSA and DSA key generation minimal requirements, described in *"Algorithms and Parameters for Secure Electronic Signatures"* [25], should be fulfilled.

## 6.1.7. Public Key Quality Checking

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

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

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 *"Algorithms and Parameters for Secure Electronic Signatures"* [25].

## 6.1.8. Hardware and/or Software Key Generation

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

In the case of key generation by a subscriber, a certification authority allows hardware and software key generation method (Chapter 6.2.1).

Tab.6.2 Subscriber's key generation method

| Certification Policy | Key generation method |
|---|---|
| Certum Level I CA | Hardware or software |
| Certum Level II CA | Hardware or software |
| Certum Level III CA | Hardware or software |
| Certum Level IV CA | Hardware or software |
| Certum Class 1 CA | Hardware or software |
| Certum Partners CA | Hardware Only |

## 6.1.9. Key Usage Purposes

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

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

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

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

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

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

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

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

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

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

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

In the case of certificates issued according to **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA** and **Certum Class 1 CA** policies, it is allowed to

use one key for both electronic signature creation operation (**digitalSignature** bit) and data encryption (**dataEncipherment** bit). Due to this, it is possible to use a certificate of this profile in applications based on Secure Multipurpose Internet Mail Extensions (S/MIME) protocol.

Certificates used for both signature creation and encryption may be issued solely to subscribers. Their issuance and management are subjected to requirements accepted for certificates intended solely for electronic signature verification, except for cases clearly described in this Certification Practice Statement.

# 6.2. Private Key Protection

Every subscriber, certification authority operator and certification authority 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).

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

Tab.6.3 Minimal requirements imposed on hardware security modules

| Certificate subject type | Employed security module |
|---|---|
| Certum CA certification authority | Hardware, complying with FIPS 140-2 Level 3 or higher |
| Certum Trusted Network CA certification | Hardware, complying with FIPS 140-2 Level 3 or higher |
| Certum Level I CA certification authority | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Certum Level II CA certification authority | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Certum Level III CA certification authority | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Certum Level IV CA certification authority | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Certum Partners certification authority | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Certum Time-Stamping Authority | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Certum Validation Service | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Certum Notary Authority | Hardware, complying with FIPS 140-2 Level 2 or higher |
| Private or legal entity or their devices | – |
| Registration Authority | Hardware, complying with FIPS 140-2 Level 2 or higher or ITSEC E3 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**. Accepted number of a shared secret and required number of secrets allowing private key restoration are disclosed in Table 6.4.

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

Tab.6.4 distribution of shared secrets

| Authority providing certification services | Number of shared secrets, required for private key restoration | Total number of distributed secrets |
|---|---|---|
| Certum CA | 3 | 5 |
| Certum Trusted Network CA | 3 | 5 |
| Certum Level I CA | 2 | 3 |
| Certum Level II CA | 2 | 3 |
| Certum Level III CA | 2 | 3 |
| Certum Level IV CA | 2 | 3 |
| Certum Class 1 CA | 2 | 3 |
| Certum Partners | 2 | 3 |
| Certum Time-Stamping Authority | 2 | 3 |
| Certum Validation Service | 2 | 3 |
| Certum Notary Authority | 2 | 3 |

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

### 6.2.2.1. Acceptance of secret shares by its holders

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

#### 6.2.2.2. Protection of secret shares

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

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

#### 6.2.2.3. Availability and erasure (transfer) of shared secret

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

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

#### 6.2.2.4. Responsibilities of shared secret holder

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

### 6.2.3. Private Key Escrow

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

Notwithstanding, copies of a subscriber's private key may be archived in a certification authority or by the subscriber and restored to usage. This operation may be carried out in two manners:

- a subscriber may generate a symmetric key, use it for private key encryption and submit to a certification authority the encrypted private key (symmetric key stored by the subscriber) or the symmetric key (encrypted private key is stored by the subscriber) in a safe manner,
- a subscriber submits, in a safe manner, a private key to a certification authority, which stores it in secure Electronic Vault.

If a subscriber wishes to retrieve a copy of the private key stored in the certification authority, he/she/it requests:

- in the first case – submission of either encrypted private key (decryption key possessed by the subscriber) or decryption key (encrypted private key copy possessed by the subscriber), while
- in second case – secure transmission of the archived private key.

## 6.2.4. Private Key Backup

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

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

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

CERTUM does not retain copies of registration authority operator's 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 6.2.3.

## 6.2.5. Private Key Archival

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*.

## 6.2.6. Private Key Entry into Cryptographic Module

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

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

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

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

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

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

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

Installation of a private key in the cryptographic module of a subscriber may require loading it from obtained media, e.g. a file protected with a password located on a floppy disc (this operation may be carried out only by the subscriber).

## 6.2.7. Method of Activating Private Key

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

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

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

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

### 6.2.8. Method of Deactivating Private Key

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

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

### 6.2.9. Method of Destroying Private Key

Erasure of private keys of subscriber or registration authority operators involve respectively their erasure from the media (floppy 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.

## 6.3. 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 2.6). 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.

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

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

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

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

Public keys are retained in the public key archive for the period of 25 years (see Chapter 4.11).

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.

Standard values of maximal usage period of certification authority certificates are described in Table 6.5, while subscriber's certificates are presented in Table 6.6.

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

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

Tab.6.5 Maximal usage periods of certification authority 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 | public key | 25 years | – |
| | private key | 15 years | – |
| Certum Level I CA | public key | 10 years | – |
| | private key | 9 years | – |
| Certum Level II CA | public key | 10 years | – |
| | private key | 9 years | – |
| Certum Level III CA | public key | 10 years | – |
| | private key | 8 years | – |

| | | | |
|---|---|---|---|
| Certum Level IV CA | public key | 10 years | – |
| | private key | 8 years | – |
| Certum Class 1 CA | public key | 15 years | – |
| | private key | 14 years | – |
| Certum Partners | public key | 10 years | – |
| | private key | 5 years | – |
| Certum Time-Stamping Authority | public key | – | 10 years |
| | private key | – | 10 years |
| Certum Validation Service | public key | – | 10 years |
| | private key | – | 10 years |
| Certum Notary Authority | 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).*

Tab.6.6 Maximal usage periods of the subscriber's certificates

| Key owner | Certification policy | Main key usage | | |
|---|---|---|---|---|
| | | RSA for message signing | RSA for key exchange | Diffie-Hellman |
| Private person and his/her/its device | Certum Level I CA | max. 3 months | max. 3 months | max. 3 months |
| | Certum Level II CA | 1 year | 1 year | 1 year |
| | Certum Level III CA | 2 years | 2 years | 2 years |
| | Certum Level IV CA | 2 years | 2 years | 2 years |
| | Certum Class 1 CA | max. 3 months | max. 3 months | max. 3 months |
| Legal entity and his/Her/its device | Certum Level I CA | max. 3 months | max. 3 months | max. 3 months |
| | Certum Level II CA | 1 year | 1 year | 1 year |
| | Certum Level III CA | 2 years | 2 years | 2 years |
| | Certum Level IV CA | 2 years | 2 years | 2 years |
| | Certum Class 1 CA | max. 3 months | max. 3 months | max. 3 months |
| | Certum Partners | – | 5 years | – |

# 6.4. Activation Data

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

### 6.4.1. Activation Data Generation and Installation

Activation data are used in two basic cases:

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

Registration authority and certification authority operators, as well as other persons performing the roles described in Chapter 5.2 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 FIPS-112.

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

### 6.4.2. Activation Data Protection

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

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

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

Tasks of registration authorities and certification authorities operating within CERTUM are carried out by means of credible hardware and software, being a part of the system which complies with the requirements described in the document *Information Technology Security Evaluation Criteria*[34] (ITSEC), at least level E3.

## 6.5.1. Specific Computer Security Technical Requirements

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

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

- mandatory authenticated registration on the level of operating system and application (in the case of significant importance, e.g. due to the role performed in the system),
- 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.

Assessment of computer security means is carried out in accordance with recommendations presented in ITSEC[35] and related to security level E4.

## 6.5.2. Computer Security Rating

CERTUM computer system complies with requirements described in Information Technology Security Evaluation Criteria (ITSEC). The above has been confirmed by an independent auditor, performing functionality assessment of CERTUM on the basis of the criteria described in WebTrust Principles and Criteria for Certification Authorities.

---

[34] Information System Security Controls Assesment Criteria

[35] *Information Technology Security Evaluation Criteria*

# 6.6. Technical Controls

## 6.6.1. System Development Controls

Applications used by CERTUM system are developed and implemented by Unizeto Sp. z o. o. specialists. Every application is developed and updated with Concurrent Versions System (CVS) usage. Within CVS, the system documentation is also created.

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

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

## 6.6.2. Security Management Controls

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

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

## 6.6.3. Life Cycle Security Ratings

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

# 6.7. Network Security Controls

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

Within the first subnetwork, the first segment contains WWW server and SMTP server (altogether – system repository) while the second segment comprises a designated, logically separated internal part maintaining proper certification process (it contains e.g. certification server and database server).

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

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

Network firewall's controls accept only messages submitted with the usage of http, https, 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 authorised individuals.*

# 6.8. Cryptographic Module Engineering Controls

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

# 6.9. Time stamps as a security control

Request created within CMP and CRS protocol (Chapter 6.1.3) do not require signing with trusted time. In the case of any other messages exchanged between a certification authority, a registration authority and a subscriber, it is recommended to apply time stamps.

Time stamps 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**).

### 7.1.1. Contents of the certificate

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

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

#### 7.1.1.1. Basic fields

CERTUM supports the following certificate basic fields:

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

In certificates issued by CERTUM values of the above fields are set in accordance with the rules described in Table 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 | md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4 ) or<br>sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) | |
| Issuer (Distinguished Name) | Common Name (CN) = | Certum {CA,CTNCA,Level{I,II,III,IV}, Class1, Partners} |
| | Organization (O) = | Unizeto Sp. z o.o. (older name)<br>Unizeto Technologies SA |
| | Country (C) = | 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 case of individual's certificates), organizationName (in case of non-Repudiation and CA certificates), commonName (in case of server certificates), unstructured {Address or Name} (in case of VPN certificates) which are mandatory. | |
| Subject Public Key Info | Encoded in accordance with RFC 3280, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key). | |
| Signature | Certificate signature, generated and encoded in accordance with the requirements described in RFC 3280. | |

### 7.1.1.2. Standard extensions fields

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

CERTUM supports the following fields of standard extensions:

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

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

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

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

- **CertificatePolicies** – information of the **PolicyInformation** type (identifier, electronic address) about a certification policy, applied by the issuing authority – **this extension is not critical**,

Tab.7.2 Policies identifiers and their description

| Policy identifier | Certificate policy description |
|---|---|
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-I(1)[36] | Identifies certification policy of the name of Certum Level I CA |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-II(2) | Identifies certification policy of the name of Certum Level II CA |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-III(3) | Identifies certification policy of the name of Certum Level III CA |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-IV(4) | Identifies certification policy of the name of Certum Level IV CA |
| iso(1) member-body(2) pl(616) | Identifies certification policy of the name of Certum Class 1 |

[36] CERTUM was assigned the object identifier of {iso(1) member-body(2) pl(616) organization(1) unizeto(113527) ccert(2) certum(2)}.

| Policy identifier | Certificate policy description |
|---|---|
| organization(1) id-unizeto(113527) id-ccert(2) id-ctnca(5) id-certum-class-1(1) | CA |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-tsa(5) | Identifies timestamping policy of the name of Certum Time-Stamping Authority. |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-dvcs(6) | Identifies notary policy of the name of Certum Notary Authority. |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-rfc-3125-signature(7) | Identifies electronic signature policy, complying with RFC 3125/RFC 3126 of the name of Certum Electronic Signature Policy. |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-dstamp(8) | Identifies service policy of the name of Certum Digital Stamp. |
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-partners(9) | Identifies certification authority policy of the name of Certum Partners. |

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

- **PolicyMapping – this field is not critical**; this field contains one or more pairs of OID, defining equivalency of the issuer policy with the subject policy,
- **IssuerAlternativeName**: alternative name of the certificate issuer – **this field is not critical**,
- **SubjectAlternativeName**: alternative name of the certificate subject – **this field is not critical**,
- **BasicContraints – this field is critical in the certification authority and may be not critical in the subscriber's certificate**. The extension allows definition whether the subject of the certificate is a certification authority (**cA** field) and what is the maximum (assuming certification authorities are ordered hierarchically) number of certification authorities on the certification path from the considered authority to the subscriber (**pathLength** field),
- **CRLDistributionPoints**: point of distribution of Certificate Revocation List – **this field in not critical**; the extension defines network addresses hosting current CLR, issued by the **cRLIssuer**,
- **SubjectDirectoryAttributes**: attributes concerning subject directory **– this field is not critical**; The extension contains additional attributes associated with the subscriber and supplementing information described in the field **subject** and **subjectAlternativeName**; this extension contains attributes not included within subject's Distinguished Name,
- **AuthorityInfoAccessSyntax**: access to certification authority information – **this field is not critical**; the field indicates the method of information and service provision by the issuer of the certificate,
- **BiometricSyntax**: information about biometric parameters of the subject of the certificate – **this field is not critical**; two types of biometric information are available:

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

## 7.1.2. Certificate Extensions and issued certificates types

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

### 7.1.2.1. Intermediate CA Certificates

A self-certificate of **Certum CA** and **Certum Trusted Network CA** certification authority and certificates of subordinate authorities, **Certum Level I CA**, **Certum Level II CA**, **Certum Level III CA**, **Certum Level IV CA, Certum Class 1 CA** and **Certum Partners** may contain extension described in Table 7.3.

Tab.7.3 Extensions of the CA certificates

| Extension | Value or Value constraint | Extension status |
|---|---|---|
| Basic Constraints | Subject type =CA<br>Path length constraints={none,1,2,...} | Critical |

### 7.1.2.2. Server authentication certificates

Certificates issued by certification authorities for server authentication (including certificates used for wireless communication and OFX servers) and network domain (including Wildcard) may contain extensions presented in Table 7.4

Tab.7.4 Server authentication certificate extensions

| Extension | Value or Value constraint | Extension status |
|---|---|---|
| Basic Constraints | Subject type = empty (end entity)<br>Path length constraint=none | Non-critical |
| Key Usage | Digital signature, bit 0<br>Key encipherment, bit 2 | Non-critical |
| Extended Key Usage | Server Authentication (serverAuth)<br>Client Authentication<br>Netscape SGC<br>Microsoft SGC | Non-critical |
| Certificate Template Name | (1.3.6.14.1.311.20.2):<br>Domain Controller | Non-critical |

| | | |
|---|---|---|
| Netscape Cert Type | SSL Server (bit 1) | Non-critical |
| Subject Alternative Name | OtherName: 1.3.6.1.4.1.311.25.1=Unique Domain Controller ID<br>DNS.1: Full DNS service name (FQDN)<br>DNS.2: Alternative service name (optionally) | Non-critical |
| CRL Distribution Points | URI: http://crl.certum.pl/class{1,2,3,4}.crl or http://crl.certum.pl/l{1,2,3,4}.crl or http://crl.certum.pl/c1.crl | Non-critical |
| Authority Info Access | OCSP: http://ocsp.certum.pl | Non-critical |
| Certificate Policies | Policies: 1.2.616.1.113527.2.2.{1,2,3,4}<br>CPS: http://www.certum.pl/CPS<br>Notice number: depends on certificate type<br>Organization: Unizeto Sp. z o.o. / Unizeto Technologies SA<br>Explicit text: depends on policy identifier (plain text) | Non-critical |

### 7.1.2.3. Code Signing Certificates

Certificates issued by certification authorities for the purposes of code signing (including form and cryptographic channel signing) may contain extensions specified in Table 7.5.

Tab.7.5 Code signing certificates extension

| Extension | Value or Value constraint | Extension status |
|---|---|---|
| Basic Constraints | Subject type = empty (end entity)<br>Path length constraint=none | Non-critical |
| Key Usage | digital signature, bit 0<br>non-repudiation, bit 1 | Non-critical |
| Extended Key Usage | Code Signing | Non-critical |
| Netscape Cert Type | Object Signing (bit 3) | Non-critical |
| Subject Alternative Name | URI: http://www.customer-site.somwhere.pl | Non-critical |
| CRL Distribution Points | URI: http://crl.certum.pl/class{1,2,3,4}.crl or http://crl.certum.pl/l{1,2,3,4}.crl or http://crl.certum.pl/c1.crl | Non-critical |
| Authority Info Access | OCSP: http://ocsp.certum.pl | Non-critical |
| Certificate Policies | Policies: 1.2.616.1.113527.2.2.{1,3}<br>CPS: http://www.certum.pl/CPS<br>Notice number: depends on certificate type<br>Organization: Unizeto Sp. z o.o.<br>Explicit text: depends on policy identifier (plain text) | Non-critical |

### 7.1.2.4. Private entities certificates

Certificates issued to private subscribers (including encryption file system (EFS) certificates, electronic data interchange (EDI) certificates, certificates qualified in the meaning of RFC 3039 standard, containing biometric data and strong authentication certificates, so called Strong Internet ID's) may contain extensions specified in Table 7.6.

Tab.7.6 Private entities certificates extension

| Extension | Value or Value constraint | Extension status |
|---|---|---|
| Basic Constraints | Subject type = empty (end entity)<br>Path length constraint=none | Non-critical |
| Key Usage | digital signature, bit 0<br>non-repudiation, bit 1<br>key encipherment, bit 2<br>dataEncipherment, bit 3 | Non-critical |
| Extended Key Usage | Encrypted File System<br>TLS Client Authentication<br>Email Protection<br>Smart Card Logon (1.3.6.1.4.1.311.20.2.2) | Non-critical |
| Certificate Template Name | (1.3.6.14.1.311.20.2):<br>Smart Card User<br>Smart Card Logon | Non-critical |
| Netscape Cert Type | SSL Client (bit 0)<br>S/MIME, bit 2 | Non-critical |
| Subject Alternative Name | OCSP: OtherName:<br>UPN:<br>http://ocsp.certum.plcustomer@somewhere.pl (OID: 1.3.6.1.4.1.311.20.2.3)<br>Email: customer@somewhere-in-world.com | Non-critical |
| CRL Distribution Points | URI: http://crl.certum.pl/class{1,2,3,4}.crl or http://crl.certum.pl/l{1,2,3,4}.crl or http://crl.certum.pl/c1.crl | Non-critical |
| Authority Info Access | OCSP: http://ocsp.certum.pl | Non-critical |
| Biometric Info | Biometric data:<br>Subscriber's photo, DNA, retinal scan, fingerprint (bit 0)<br>Hand-written signature (bit 1)<br>URI: biometric data location | Non-critical |
| Certificate Policies | Policies: 1.2.616.1.113527.2.2.{1,2,3,4}<br>CPS: http://www.certum.pl/CPS<br>Notice number: depends on certificate type<br>Organisation: Unizeto Sp. z o.o.<br>Explicit text: depends on policy identifier (plain text) | Non-critical |

### 7.1.2.5. Virtual Private Network (VPN) certificates

Certificates for creation of Virtual Private Network (VPN) may contain extensions specified in Table 7.7.

Tab.7.7 VPN certificates extension

| Extension | Value or Value constraint | Extension status |
|---|---|---|
| Basic Constraints | Subject type = empty (end entity)<br>Path length constraint=none | Non-critical |
| Key Usage | digital signature, bit 0<br>keyEncipherment, bit 2 | Non-critical |
| Extended Key Usage | IPsec Client<br>IPsec Tunnel<br>IPsec End System | Non-critical |
| Subject Alternative Name | DNS: full VPN router domain name (FQDN)<br>IP: VPN router IP address | Non-critical |
| CRL Distribution Points | URI: http://crl.certum.pl/class{1,2,3,4}.crl or http://crl.certum.pl/l{1,2,3,4}.crl or http://crl.certum.pl/c1.crl<br>URI: ldap://directory.certum.pl/C=PL,O=Unizeto Sp. z o.o.,CN=Certum Level I,II,III,IV},/?certificaterevocationlist | Non-critical |
| Authority Info Access | OCSP: http://ocsp.certum.pl | Non-critical |
| Certificate Policies | Policies: 1.2.616.1.113527.2.2.{1,2,3,4}<br>CPS: http://www.certum.pl/CPS<br>Notice number: depends on certificate type<br>Organisation: Unizeto Sp. z o.o.<br>Explicit text: depends on policy identifier (plain text) | Non-critical |

### 7.1.2.6. Cross-certification and non-repudiation certificates

Cross-certification and non-repudiation certificates may contain extension specified in Table 7.8.

Tab.7.8 Cross-certification and non-repudiation certificates extensions

| Extension | Value or Value constraint | Extension status |
|---|---|---|
| Basic Constraints | Subject type=CA<br>Path length constraint={none,1,2,...} | Non-critical |
| Key Usage | digital signature, bit 0<br>non-repudiation, bit 1 | Non-critical |
| Extended Key Usage | Validation Authority (OCSP)<br>Time-Stamp Authority (TSA)<br>Notary Authority (DVCS) | Non-critical |
| CRL Distribution Points | URI: http://crl.certum.pl/class{1,2,3,4}.crl or http://crl.certum.pl/l{1,2,3,4}.crl or http://crl.certum.pl/c1.crl | Non-critical |
| Subject Alternative Name | URI: http:// www.customer-service.somwhere<br>Client service location | Non-critical |
| Authority Info Access | OCSP: http://ocsp.certum.pl | Non-critical |
| Certificate Policies | Policies: 1.2.616.1.113527.2.2.{1,8}<br>CPS: http://www.certum.pl/CPS<br>Notice number: depends on certificate type<br>Organization: Unizeto Sp. z o.o.<br>Explicit text: depends on policy identifier (plain text) | Non-critical |

### 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 MD5, SHA-1, SHA-256 or SHA-512 cryptographic hash is used.

### 7.1.4. Electronic signature field

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

## 7.2. CRL profile

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

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

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

- **Version**: CRL format version,
- **Signature**: contains identifier of the algorithm used by a certification authority to sign CRL; CERTUM authorities sign **CRL** by means of **sha1WithRSAEncryption** algorithm,
- **Issuer**: name of the certification authority issuing CRL; every authority of CERTUM issues its own Certificate Revocation List; this requirement applies to the following authorities: **Certum CA, Certum Trusted Network CA, Certum Level I**, **Certum Level II, Certum Level III**, **Certum Level IV, Certum Level I CA**, **Certum Level II CA, Certum Level III CA**, **Certum Level IV CA, Certum Class 1 CA** and **Certum Partners**,
- **ThisUpdate**: CRL publication date,
- **NextUpdate**: announcement of the date of the next CRL publication; if the field is present, its value describes non-excessive date of the next CRL update (although the publication may be made prior to this date),
- **RevokedCertificates**: the list of revoked certificates (the field is empty in the case of lack of revoked certificates); the information consist of three sub-fields:

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

- **crlExtensions**: extended information about Certificate Revocation List (optional field). Among numerous extensions, the most important are the following ones: **AuthorityKeyIdentifier** (see also Chapter 7.1.1.2) allowing identification of a public key corresponding to a private key used for list signing, and **cRLNumber**, containing monotonically increased serial number of the lists issued by a certification authority (by means of this extension, a subscriber is able to define when a specific CRL replaced another list) .

## 7.2.1. Supported CRL entry extension

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

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

```
unspecified         – not specified;
keyCompromise       –      key revelation or compromise;
cACompromise        –      certification authority key revelation;
affiliationChanged  –      subscriber's data modification (affiliation);
superseded          –      certificate renewal;
cessationOfOperation – cessation of certificate usage;
certificateHold     –      suspension of certificate;
removeFromCRL       –      certificate removal from CRL;
privilegeWithdrawn – certificate was revoked due to change of the
                     certificate data, concerning subjects role; this
                     reason might also mean that the data used for
                     creating electronic signature were compromised
aaCompromise        – applies to attributes certificates; meaning is the
                     same as for withdrawal of privileges;
```

- **HoldInstructionCode**: code of the operation on certificate suspension. This field is **non-critical CRL entry extension** which defines a registered identifier of the

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

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

### 7.2.2. Revoked certificate and CRL

*Revoked certificates remain on Certificate Revocation Lists (issued by CERTUM) for the period of 25 years from the moment of their first appearance on the list. This rule applies also to revoked certificates of a certification authority: certificates have to be included in the succeeding Certificate Revocation Lists, published by the issuer of the revoked certificate (in the case of cessation of the issuer operation, the last published CRL should be transferred to the repository of another, for example supervising, authority issuing certificates (compare Chapter 4.14).*

*The rule described above does not apply to revoked certificates of Certum Level I CA and Certum Class 1 CA class. It is recommended that these certificates should be removed from the Certificate Revocation List at the moment of their expiration*

## 7.3. Timestamp token profile

**Certum Time-Stamping Authority (TSA)** 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 timestamping authority solely for the purposes of signing timestamp tokens issued by this authority.

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

Time-stamping authority certificate basic fields profile is described in table 7.9

Tab 7.9 TSA certificate basic fields profile

| Field name | Value or its constraint | |
|---|---|---|
| Version | Version 3 | |
| Serial Number | Unique value for each certificate issued by certification authority | |
| Signature Algorithm | sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5) | |
| Issuer (Distinguished Name) | Common Name (CN) = | Certum CA |
| | Organization (O) = | Unizeto Sp. z o.o. |

| | | |
|---|---|---|
| | Country (C) = | PL |
| Not before (validity period beginning date) | Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard (PPS). CERTUM clock is known as valid world Stratum I service | |
| Not after (validity period ending date) | Universal Time Coordinated based. CERTUM owns satellite clock controlled by Atomic Frequency Standard (PPS). CERTUM clock is known as valid world Stratum I service | |
| Subject (Distinguished Name) | Common Name (CN) = | Certum Time-Stamping Authority |
| | Organization (O) = | Unizeto Sp. z o.o. |
| | Country (C) = | PL |
| Subject Public Key Info | Encoded in accordance with RFC 3280, contains information about RSA public key (key identifier and value of the public key). | |
| Signature | Certificate signature, generated and encoded in accordance with the requirements described in RFC 3280. | |
| Basic Constraints | Subject type = empty (end entity)<br>Path length constraint=none | Non-critical |
| Key Usage | digital signature, bit 0<br>non-repudiation, bit 1 | Non-critical |
| Extended Key Usage | Time Stamping Authority (TSA) | Non-critical |
| Subject Alternative Name | URI: http://time.certum.pl<br>Client service location | Non-critical |

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

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

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

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

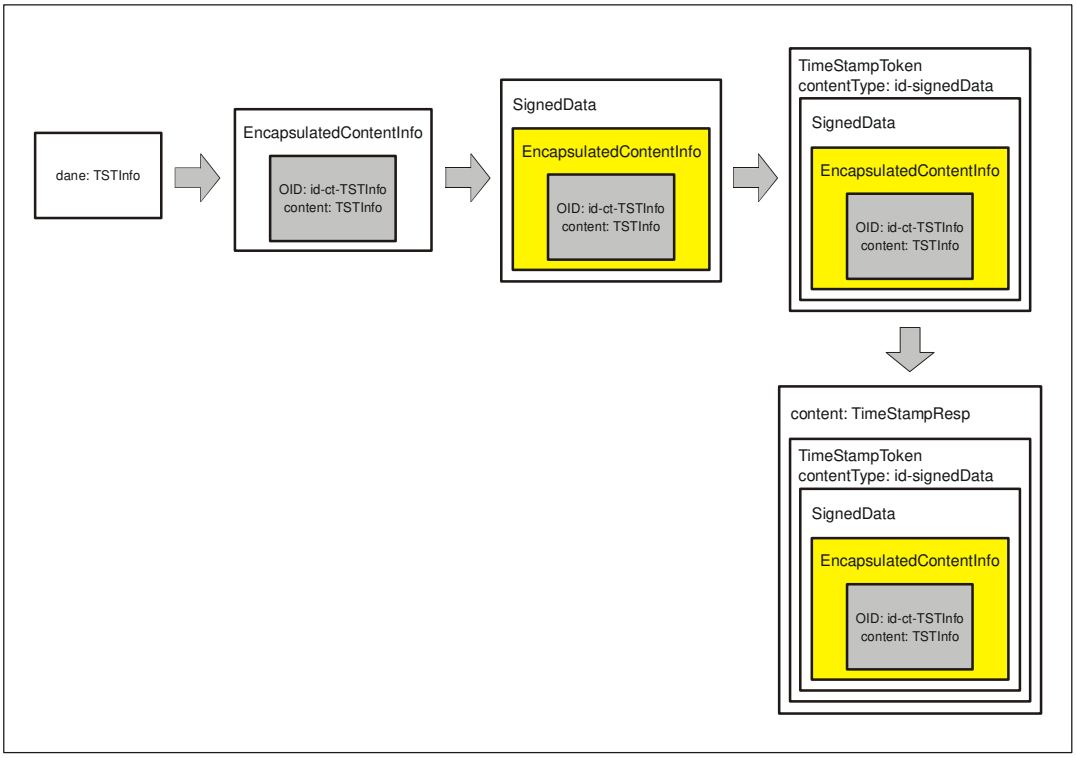


Fig. 4 Timestamp request response encapsulation

PKIStatusInfo structure has a following form:

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

Meaning of the fields:

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

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

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

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

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

```
PKIFailureInfo ::= BIT STRING (
    badAlg              (0),
      -- unknown or unsupported algorithm identifier
    badMessageCheck     (1),
      -- data integrity error (e.g. signature verification error)
```

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

Timestamp token general format complies with ContentInfo format:

```
TimeStampToken ::= ContentInfo
```

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

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

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

Timestamp informative content has the form:

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

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

- **policy** – must occur and specify the policy which is used for issuing timestamps by the timestamping authority; in case of **Certum Time-Stamping Authority** the policy identifier has the value:

| Policy identifier | Policy name |
|---|---|
| iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-tsa(5) | Certum Time-Stamping Authority<br>Identifies certification policy, used for issuing timestamp tokens |

- **messageImprint** contains information submitted by the requester, signed with the timestamp;

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

TimeStampToken structure is connected with the set of signed attributes. Timestamp token include at least the following attributes:

**1. Content type attribute**

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

**2. Message digest attribute**

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

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

**3. Signing certificate attribute**

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

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

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

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

IssuerSerial ::= SEQUENCE {
```

```
    Issuer          GeneralNames,
    SerialNumber    CertificateSerialNumber
}

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

# 7.4. OCSP response token 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 3280. 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** (see Chapter 7.1.1.2).

## 7.4.1. 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 v1 version).

## 7.4.2. Certificate status information

Information about certificate status is provided in the field **certStatus** of the structure **SingleResponse**. It may have one of the three accepted values, defined in Chapter 4.9.11. In the case of server response **good**, the entity requesting the certificate status should additionally check the extension **CertHash** contained within the response (see Chapter 7.4.4) to make sure that the verified certificate was published by this very issuer, and the extension **ArchiveCutoff**, whose value is the beginning date of the certificate status verification (the ending date is defined by the moment of certificate status verification, provided in the field **producedAt**). Positive result of those verifications allows so called **positive confirmation** of the certificate status.

## 7.4.3. Supported standard extension

In accordance with RFC 2569, 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 7.2.1. 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**.
- **Boundary date of archival** applies to the ending date of retention of information in CERTUM database, referring to certificate status (**ArchiveCutOff** extension). Placement of this information in a response of certificate status verification server means that server holds information about certificate revocation also in the situation of the certificate expiration. This information provides a proof whether an electronic signature associated with the certificate being verified was or was not valid in the moment of OCSP response issuance, even if the certificate has already expired. Because of information about certificate status being available *on-line* for the period of 15 years (see Chapter 6.2.5), the value of the boundary archive date is a difference of the values of date of certificate status conformation and the retention period of the revoked certificate information by OCSP server.

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.

## 7.4.4. Supported private extensions

If as a response to a request submitted to certificate status verification server, the subscriber receives confirmation containing status **good**, he/she/it is not able to state – having no further information – whether the certificate has or has not ever been issued or whether the moment of the response is within the validity period of the certificate. The latter problem may be resolved with placement of **boundary archive date** (**ArchiveCutOff**) extension within a response (see Chapter 7.4.3).

The former problem, described above, may be resolved by the implementation of the private extension **CertHash** within a response submitted by CERTUM certificate status verification server.

The **CertHash** extension is marked as **non-critical**. Describing data syntax and its identifier has the following form:

```
id-ccert-CertHash            OBJECT IDENTIFIER ::= { id-ccert-ext 4}
CertHash ::= SEQUENCE {
    hashAlgorithm   DigestAlgorithmIdentifier,
    hashedCert      OCTET STRING
}

id-unizeto                   OBJECT IDENTIFIER ::= { iso(1) member-body(2) pl(616)
                               organization(1) id-unizeto(113527)}
id-ccert-ext                 OBJECT IDENTIFIER ::= { id-unizeto ccert(2) 0}

DigestAlgorithmIdentifier ::= AlgorithmIdentifier
AlgorithmIdentifier ::= SEQUENCE {
    algorithm                OBJECT IDENTIFIER,
    parameters               ANY DEFINED BY algorithm OPTIONAL
}
```

The field **hashAlgorithm** defines the identifier of a strong cryptographic digest. It means the hash function should be one-way, immune to collision (e.g. SHA-1).

The field **hashedCert** contains a digest of a certificate whose current state is located in OCSP response. The size of this field depends of the applied hash function.

Another private extension, supported by CERTUM is **CertumDigitalStamp** extension, marked as **non-critical**. Describing data syntax and its identifier has the following form

```
CertumDigitalStamp::= SEQUENCE {
     type       CDStampType,
     issuerInfo GeneralNames,
     stampInfo  UTF8String (SIZE (128)),
     currency   Iso4217AlphaCurrencyCode,
     amount     INTEGER,
     exponent   INTEGER} -- value = amount * 10^exponent
```

This extension is employed by electronic fee stamps.

## 7.4.5. Certificate status verification token issuer statement

*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 for the last 15 years. If the certificate has been revoked during the last 15 years, OCSP server will return the response **revoked** and provide the date of revocation.*

# 8. Certification Practice Statement management

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

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

Decision on acceptance of the changes in Certificate Practice Statement version or build number is made by PKI Service Development Team.

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

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

## 8.1. Changes introduction procedure

Modification to Certification Practice Statement may be a result of observed errors, CPS update and suggestions from the affected parties. Modification proposals may be submitted by regular mail or electronic mail for the contract addresses of CERTUM. Suggestions propositions should describe modifications, their scope and justifications and means of contact the person requesting modification.

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

- 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,
- PKI Services Development Team,
- CERTUM subscribers,
- professionals from the area of information system security.

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

Introduced modification may be generally divided into two categories:

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

## 8.1.1. Items that can be changed without notification

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

## 8.1.2. Items that require notification

### 8.1.2.1. List of items

After notification in advance, each and every item of the Certification Practice Statement may be subjected to amendment. Information about every significant modification in question by the PKI Service Development Team is submitted to every affected party in the form of indication of a storage point of a new version of Certification Practice Statement with the status **requested for comment**. Suggested modification may by published in the CERTUM repository and transmitted by the means of electronic mail. Information about implemented modifications is also attached to the new CPS.

### 8.1.2.2. Comment period

Comments on modifications suggested by PKI Service Development Team may be submitted by the affected parties within 10 working days of their announcement. If as a result of the submitted comments, PKI Service Development Team administered **significant modification** to the suggested changes, the changes have to be published once more and subjected to assessment. In other cases, a new version of Certification Practice Statement receives the status **under approval** and is subjected to approval procedure (see Chapter 8.3).

*PKI Service Development Team may fully accept suggested changes accept with amendments or reject suggested changes after expiration of the allowable period for resubmission of published and posted acceptance questionnaire.*

### 8.1.2.3. Changes requiring new identifier

In the case of amendments which may have influence on extensive group of certification service users, PKI Service Development Team 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,
- implementation of the service of suspension and unsuspension of a certificate, within the CERTUM.

# 8.2. Publication

## 8.2.1. Items not published in CPS

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

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

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

## 8.2.2. Publication of the new version of Certification Practice Statement

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

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

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

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

## 8.3. CPS Approval Procedures

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

# Document History

| Document modification history | | |
|---|---|---|
| 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 2.6 | 1st of September, 2008 | Editorial changes. |
| V 2.7 | 27th of April, 2009 | Change information after new keys CA generation. |

# Appendix 1: Abbreviations

CA certification authority

CMP Certificate Management Protocol

CP Certification Policy

CPS Certification Practice Statement

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

DN Distinguished Name

KRIO Krajowy Rejestr Identyfikatorów Obiektów (National Object Identifiers Registry)

OCSP On-line Certificate Status Protocol

PKI Public Key Infrastructure

PRA Primary Registration Authority

PSE personal security environment

RA Registration Authority

RSA asymmetric cryptographic algorithm (name originates form first letters of its developers names: 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 entities or transferral to entities providing on-line certificate status verification service. In both cases the distribution should be performed with the usage of appropriate means (e.g. LDAP, FTP, etc.).

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

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

**Certificate Status Verification Authority** – trusted third party, providing relaying parties with the mechanisms for 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), Cert(2), ..., Cert(n-1)} the subject of the certificate Cert(x) is the issuer of the certificate Cert(x+1),
- the certificate Cert(1) is issued by a certification authority (**point of trust**) trusted by the verifier,
- Cert(n) is a certificate being verified.

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

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

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

**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.

**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 card against unauthorised usage

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

**Self-signed certificate** – any public key certificate, designed to verification of signature upon certificate, whose signature may be verified by public key included in the field **subjectKeyInfo**, whose content of the fields **issuer** and **subject** are the same, and whose **cA** field of **BasicConstraints** extension is set to true.

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

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

**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** – Unizeto Technologies 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.

# Literature

[1] ITU-T Recommendation X.509 – *Information Technology – Open Systems Interconnection – The Directory: Authentication Framework*, June 1997 (equivalent ISO/IEC 9594-8)

[2] ITU-T Recommendation X.520 – *Information Technology – Open Systems Interconnection – The Directory: Selected Attribute Types*, 1993

[3] *CARAT Guidelines – Guidelines for Constructing Policies Governing the Use of Identity-Based Public Key Certificates*, National Automated Clearing House Association (NACHA), The Internet Council CARAT Task Force, v.1.0, Draft September 21, 1998

[4] *VeriSign CPS – VeriSign Certification Practice Statement*, ver.2.0, August 31st, 2001, http://www.verisign.com

[5] *ARINC Digital Signature Service (ADSS) – Certification Practice Statement (CPS),* ver.2.0, August 6th, 1998

[6] ISO/IEC JTC 1/SC27 N691 *Guidelines on the Use and Management of Trusted Third Party Services*, August 1993

[7] RFC 822 D.Crocker – *Standard for the format of ARPA Internet text messages*, August 1982

[8] RFC 1738 T.Berners-Lee, L.Masinter, M.McCahill – *Uniform Resource Locators (URL),* December 1994

[9] RFC 1778 T.Howes, S.Kille, W.Yeong, C.Robbins *The String Representation of Standard Attribute Syntaxes*, March 1995

[10]RFC 2247 S.Kille, M.Wahl, A.Grimstad, R.Huber, S.Sataluri – *Using Domains in LDAP/X.500 Distinguished Names*, January 1998

[11]RFC 3280 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile*, 2002

[12]Steven Castell *Trusted Third Party Services – User Requirements for Trusted Third Party Services*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, July 29, 1993

[13]Steven Castell *Trusted Third Party Services - Functional model*, Report to the Commission of the European Communities for the Requirements for Trusted Third Party Services, December 13, 1993

[14]*Confidential and Private Information Protection Law of 22nd January, 1999,* Dziennik Ustaw Rzeczpospolitej Polskiej, No.11, Warszawa, 8th February, 1999 r.

[15]Simson Garfinkel, Gene Spafford *Practical Unix and Intenet security*, Ed. RM, Warszawa 1997

[16]S.Chkhani, W.Ford *Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, RFC 2527, March, 1999

[17]S. Chokhani, W. Ford, R. Sabett, C. Merrill, S. *Wu Internet X.509 Public Key Infrastructure – Certificate Policy and Certification Practices Framework*, PKIX Working Group, Internet Draft, July 12, 2001, < draft-ietf-pkix-ipki-new-rfc2527-00.txt >

[18]European Telecommunications Standards Institute *Policy requirements for certification authorities issuing qualified certificates*, ETSI TS 101 456 V1.1.1 (2000-12)

[19] *Digital Signature and Confidentiality, Certificate Policies for the Government of Canada Public Key Infrastructure* (Working Draft), v.2.0 August 1998

[20] RFC 3161 *Internet X.509 Public Key Infrastructure – Time Stamp Protocol (TSP), PKIX Working Group*, January 2001

[21] *PKI Assessment Guidelines - Guidelines to Help Assess and Facilitate Interoperable Trustworthy Public Key Infrastructures, PAG v0.30*, Public Draft for Comment, June 18th, 2001, Information Security Committee, Electronic Commerce Division, Section of Science & Technology Law, American Bar Association,

[22] *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000

[23] CWA 14167-1 *Security Requirements for Trustworthy Systems Managing Certificates for Electronic Signatures - Part 1: System Security Requirements*, CEN (European Committee for Standardization) November 2001,

[24] *Digital Signature Standard*, FIPS 186-2 NIST (Jan. 2000)

[25] *EESSI-SG Algorithms and Parameters for Secure Electronic Signatures*, October 19th 2001

[26] FIPS 112 *Password Usage*, May 30th 1985, http://csrs.nist.gov/fips/