Certification Practice Statement Unizeto CERTUM - CCP

Version 2.0

Effective date: 15th July, 2002

Status: previous

UNIZETO Sp. z o.o.
„Unizeto CERTUM Certification Authority”
Królowej Korony Polskiej Street 21
70-486 Szczecin
Poland
http://www.certum.pl

Trademark and Copyright notices

Contents

1.Introduction

Certification Practice Statement[1] of **Unizeto CERTUM – Centrum Certyfikacji Powszechne** (further referred to as **Certification Practice Statement** or **CPS**) 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 Practice Statement specifies general rules of certification practice stated in **Certification Policy** of **Unizeto CERTUM – Centrum Certyfikacji Powszechne** (further referred to as **Certification Policy** or **CP**). Certification Policy states what level of trust can be applied to a given type of a certificate issued by **Unizeto CERTUM – Centrum Certyfikacji Powszechne** (Public Certification Authority) - further referred to as **Unizeto CERTUM - CCP**. Certification Practice Statement describes how Unizeto CERTUM - CCP secures the level of trust guaranteed by the policy.

Certification Policy and Certification Practice Statement were defined by Unizeto CERTUM - CCP, 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 Policy specifies general rules applied by Unizeto CERTUM - CCP to the process of public key certification, defines the participants of the process, their duties and responsibility, types of certificates, the procedures of identity verification applied to certificate issuance, and applicability range. Specification of the rules mentioned above is presented in the present **Certification Practice Statement**.

Certification Practice Statement describes four certification policies applied by Unizeto CERTUM - CCP to issuance of certificates to authorities and certifications to end users . These policies represent four different levels of credibility[4] (**Certum Level I, Certum Level II, Certum Level III, Certum Level IV**) 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 are different.

Structure and contents of Certification Practice Statement are in accordance with the recommendation of RFC 2527 *Certificate Policy and Certification Practice Statement Framework*.

This Certification Practice Statement assumes that the reader is familiar with the notions concerning certificates, electronic signature, Public Key Infrastructure (**PKI**). If this is not the case, it is advisable for a future user and subscriber of Unizeto CERTUM - CCP services to be trained in public key techniques and rules concerning electronic data interchange. The topics of trainings, the dates and the materials are accessible in the repository of Unizeto CERTUM - CCP at:

---

[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] 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

http://www.certum.pl/repository

There are many additional documents connected with Certification Practice Statement. They are used in Unizeto CERTUM – Certification Authority and regulate its functioning (see Table 1.1). These documents have a different status. They are usually not available for the public because of the importance of the information they contain and the system security.

Tab.1.1 Important document connected with Certification Practice Statement

	Document name	Status	Availability
1.	Certification Policy Unizeto CERTUM - CCP	public	http://www.certum.pl/repository
2.	Certum CA system documentation	Non-public	Locally – only entitled persons and auditors
3.	Procedure for Unizeto CERTUM CA key generation	Non-public	Locally – only entitled persons and auditors
4.	Procedure for Unizeto CERTUM CA keys archive and destruction	Non-public	Locally – only entitled persons and auditors
5.	Media Book	Non-public	Locally – only entitled persons and auditors
6.	Database technical documentation	Non-public	Locally – only entitled persons and auditors
7.	Registration Authority Book	Non-public	Locally – only entitled persons and auditors
8.	Server Book	Non-public	Locally – only entitled persons and auditors
9.	Server Software Exchange Book	Non-public	Locally – only entitled persons and auditors
10.	Emergency Server Restoration and Backup Copy Creation Book	Non-public	Locally – only entitled persons and auditors
11.	Server Starting and Stopping Book	Non-public	Locally – only entitled persons and auditors

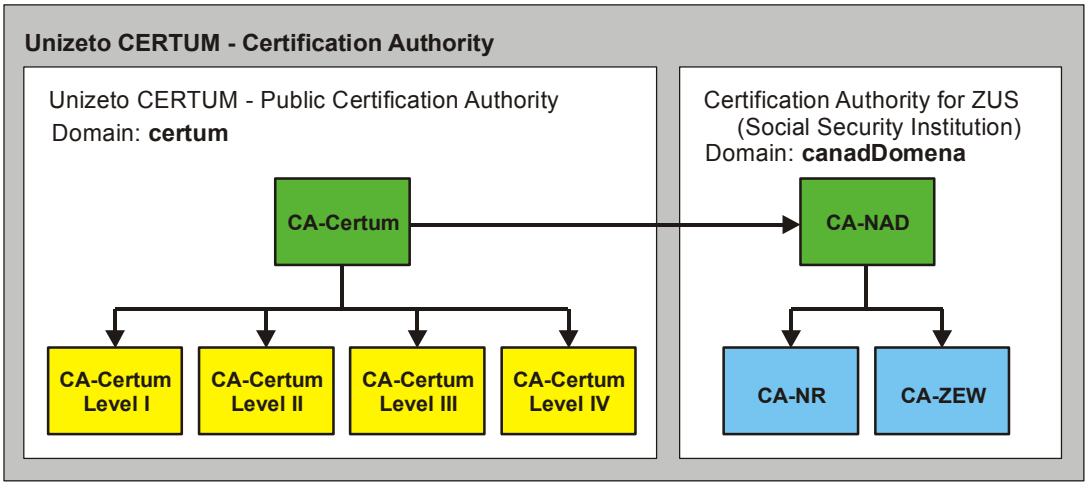
Additional information and service are available by electronic mail at: info@certum.pl.

1.1. Overview

Certification Practice Statement is a description and basis for functioning of Unizeto CERTUM - CCP 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.

Unizeto CERTUM – CCP is a part of Unizeto CERTUM – Certification Authority service unit and forms a separate certification domain **certum** within it (see Picture 1.1), with a separate primary certification authority **CA-Certum. CA-Certum** primary certification authority is independent from the **canadDomena** domain and issues the so called self-certificates[5] to itself.

[5] **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)



Pic.1.1 Hierarchical connections of certificate issuance authorities operating within Unizeto CERTUM – Certification Authority

In terms of hierarchy, there are four certification authorities subordinate to **CA-Certum** primary certification authority. These are: **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** and **CA-Certum Level IV**, all issuing certificates with different credibility levels (see Chapter 1.4).

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.

Certification Policy of Unizeto CERTUM – CCP permits the mechanism of cross-certification between **CA-Certum** and any of the certification authorities belonging to the **canadDomena** domain. Functional subordination of **CA-NAD** to the primary authority issuing certificates **CA-Certum** is also possible.

Currently, Unizeto CERTUM does not have any mutual certification agreements with any authorities issuing certificates. If this situation happens to change, the users will be informed about it by means of an appropriate version of Certification Policy and Certification Practice Statement.

Certificates issued by Unizeto CERTUM - CCP contain the identifiers[6] 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 **certificatesPolicies** (see Chapter 7.1.1.2) of every certificate issued by Unizeto CERTUM - CCP.

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

[6] Identifiers of Unizeto CERTUM CCP certification policies are constructed on the basis of the object identifier Unizeto Sp. z o.o. in Szczecin, 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)
```

1.2. Document Name and its Identification

The present document of Certification Practice Statement is given a proper name: **CPS of Unizeto CERTUM - CCP** or **Certification Policy of Unizeto CERTUM - CCP**. Any quotations of this document should employ one of two possible forms.

CPS of Unizeto CERTUM - CCP document is available:

As an electronic version at the repository at: http://www.certum.pl/repository or on request sent to: info@certum.pl,

As a paper copy - on request sent to the address of Unizeto CERTUM – CCP (see Chapter 1.5).

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

```
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) 3}
```

in which the last numeric value corresponds to the current version 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 are included in certificates issued by Unizeto CERTUM - CCP. The collection includes the certification policy identifiers described in Chapter 7.1.1.2.

1.3. Certification Practice Statement Parties

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

certification authorities **CA-Certum**, **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** and any other authority established in accordance with the rules stated in the present Certification Practice Statement,

Primary Registration Authority (PRA),

Local Registration Authorities (LRA),

repository,

on-line certificate status verification server (OCSP),

subscribers,

relying parties.

Unizeto CERTUM - CCP is an open service unit providing 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 procedures, certificate issuance procedures and information system security) is to convince the users of Unizeto CERTUM - CCP services that the declared credibility levels of issued certificates are the reflection of certification authorities practices.

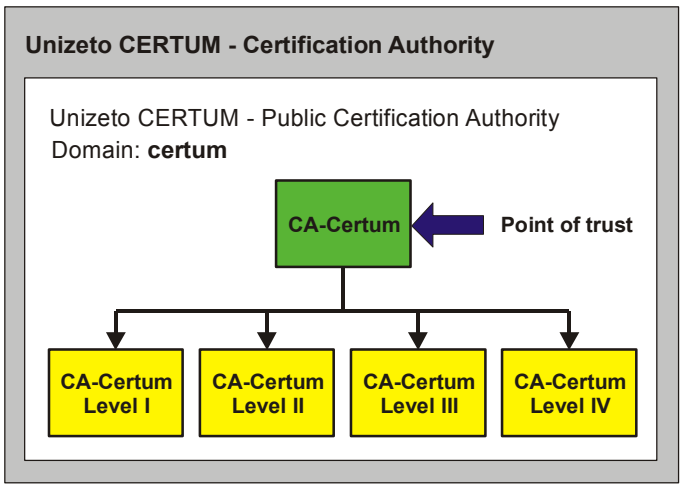
The regulations of Certification Practice Statement are in accordance with Certification Policy and the recommendations of PKI Sevices Development Team (see Chapter 8).

1.3.1. Certification Authorities

Certification authorities, forming a domain of certification authorities called **certum**, are a part of Unizeto CERTUM - CCP (see Picture 1.2).

CA-Certum certification authority is a primary certification authority of certum domain. All certification authorities in this domain are subordinate to CA-Certum certification authority.

Currently, there are four certification authorities subordinate to **CA-Certum**: **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**.



Pic.1.2 Structure of certification domain **certum** and its point of trust **CA-Certum**

1.3.1.1. CA-Certum Main Certification Authority

CA-Certum primary certification authority can register and issue certificates only to certification authorities and authorities issuing electronic confirmation of non-repudiation that belong to **certum** domain. Prior to starting an activity, every subordinate certification authority needs to submit an application to Main Certification Authority (MCA) for registration and public key certificate issuance (see the procedure described in *"Procedure of Registration and Certification of New Certification Authorities"*[7]).

CA-Certum authority operates on the basis of the self-certificate issued by itself. In such a self-certificate, the extension **certificatePolices** (see Chapter 7.1.1) is not placed, which should be interpreted as lack of limits to the set of **certification paths**[8], to which **CA-Certum** certificate can be attached.

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

CA-Certum certification authority renders certification services to:

itself (issues and renews self-certificates),

CA-Certum Level I, **CA-Certum Level II**, **CA-Certum Level III** and **CA-Certum Level IV** authorities and other certification authorities registered in certification domain **certum**,

[7] This procedure does not apply to four basic certification authorities: **CA-Certum Level I, CA-Certum Level II, CA-Certum Level III, CA-Certum Level IV** and to other entities providing non-repudiation services.

[8] See **Glossary**

entities delivering services of on-line certificate status verification and other entities rendering services of non-repudiation (e.g. timestamp service).

*The extension **certificatePolicies** is not placed in certificates issued to **CA-Certum Level I, CA-Certum Level II, CA-Certum Level III** and **CA-Certum Level IV** authorities and certificates of other authorities and entities, to which certificates are issued by **CA-Certum** authority.*

1.3.1.2. Subordinate Certification Authorities

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

Table 1.2 The names of certification authorities and the corresponding certification policies

Certification authority	Certification policy
CA-Certum Level I	Certum Level I
CA-Certum Level II	Certum Level II
CA-Certum Level III	Certum Level III
CA-Certum Level IV	Certum Level IV

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

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

Primary Registration Authority and local registration authorities cooperate with subordinate certification authorities. Registration authorities represent subordinate certification authorities 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.

Subordinate certification authorities are adjusted to issuing certificates to:

certificate users who wish to ensure security and credibility for their electronic mail and service servers (e.g. e-commerce, information and software libraries) by means of certificates,

entities delivering non-repudiation services (e.g. timestamp authorities or notary authorities),

suppliers of the services connected with mobile telecommunication,

network devices providing encrypted connections over VPN,

operators of registration authorities (Primary Registration Authority and local registration authorities),

employees of Unizeto CERTUM - CCP,

hardware devices (physical and logical) owned by private and legal entities; certification services for hardware devices allow possibility to create other services on the basis of a public key certificate, such as certificate status verification service (OCSP),

other certification authorities (applicable to **CA-Certum Level I** and **CA-Certum Level IV** authorities).

1.3.2. 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 requires the subscriber's attendance in person to a registration authority and submission of proofs of the subscriber's identity. 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. A detailed scope of duties of registration authorities and their operators is specified in an agreement with Unizeto CERTUM - CCP, the valid Statement and the procedures concerning operating of registration authorities, which are an integral part of this agreement.

Any institution (legal entity) might function as a local registration authority and might be accredited by Unizeto CERTUM - CCP, 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 local registration authorities currently accredited by Primary Registration Authority is available in the repository of Unizeto CERTUM - CCP at:

http://www.certum.pl/repository

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

local registration authorities, further referred to as LRA's,

Primary Registration Authority (PRA).

The main difference between these types is that local registration authorities, unlike Priamry Registration Authority, cannot accredit other local registration authorities and register new certification authorities. Moreover, local registration authorities do not have the rights to

confirm all requests of a subscriber. The rights might be limited only to some of all available types[9] of certificates. Therefore,

LRA's register end subscribers (private and legal entities) that request certificates of the credibility level up to Certum Level III (including Level III),

PRA registers local registration authorities (LRA's), 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 Unizeto CERTUM - CCP) imposed on the types of certificates issued to subscribers registered in PRA; additionally, PRA approves of distinguished names (DN's) of current and future registration authorities.

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

1.3.3. Repository

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

all certification authorities belonging to or connected with certum domain (e.g. new certification authorities certificates registered in PRA),

operators of LRA's and PRA,

end subscribers (private and legal entities, including Unizeto CERTUM - CCP employees and the devices owned by them and indispensable for PKI services) who approved of that.

Additionally, in the repository there is information closely connected with the functioning of certificates, that is:

Certificate Revocation List (CRL),

a current and former version of Certification Policy and Certification Practice Statement,

other information modified in real time.

*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/repository

1.3.4. 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.

[9] Types of certificates are described in Charter 1.4

1.3.4.1. Subscribers

Any private or legal entities and hardware devices they own are subscribers of Unizeto CERTUM - CA, provided that they fulfill the terms of the definition of a subscriber (see Chapter 1.3.4). In particular, registration authorities' operators, Unizeto CERTUM - CCP employees and the equipment elements indispensable for the security of Unizeto CERTUM - CCP infrastructure (e.g. firewalls, routers and authentication servers) are subscribers.

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

Unizeto CERTUM - CCP 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).

1.3.4.2. Relying Parties

A relying party, using Unizeto CERTUM - CCP 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 **CA-Certum**).

A relying party is responsible for whether or how to verify the current status of a subscriber's certificate. Such a decision must be taken anytime 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 is defined by two elements. The first one states the character of certificate applicability (e.g. electronic signature, confidentiality or certification policy identifier), whereas the second one is a list or a description of confirmed or prohibited applications.

Certificates issued by Unizeto CERTUM - CCP can be used to process and secure information (including authentication) of various credibility level. Information credibility level and information vulnerability to **breach**[10] 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), Level IV (high level). These levels correspond to certificate credibility levels (see Table 1.3)[11].

[10] See **Glossary**

[11] 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	The lowest credibility level of the identity of a certificate entity. Level I certificates should be applied to test the compatibility of Unizeto CERTUM - CCP 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	The level gives the basic security of information in the environment of slight risk of data breach[12] (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	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	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.

A relying party bears responsibility for stating the credibility level of a certificate that is applied to a given purpose. On considering various important risk factors, a relying party should state which of the certificates issued by Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP for issuance of an appropriate certificate that meets these requirements.

A subscriber must compare the requirements stated by a relying party with the applicability range (Table 1.3) and types of certificates (Table 1.4), issued by Unizeto CERTUM - CCP.

[12] See **Glossary**

1.4.1. Certificate Types and Recommended Applicability

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

1) **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[13],
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) **personal certificates** – allow for encryption and signing of electronic mail, and securing electronic documents (electronic mail based on S/MIME or PGP standard),
5) **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,
6) **timestamp 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,
7) **notary authorities certificates** – applied by DVCS (Data Validation and Certification Server), which certifies and confirms data,
8) **certificates for encrypting** – applied to the security of files, folders and file systems,
9) **certificates for code securing** – applied by computer programmers to secure software from forgery.

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	Private Email	Electronic mail security, electronic signatures of electronic data, PGP
	Private WEB Server	Data transmission security for WWW servers
	Private Microsoft Authenticode	Software security against forgery, software distribution in global network in accordance with Microsoft Authenticode™

[13] 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 VBS	Securing VB in Office 2000 against forgery, software security in accordance with Microsoft Visual Basic for Applications
	Private Netscape Object Signing	Plugin signing, Java applet and module signing in accordance with Netscape® technology
	Private Java Code Signing	Software security in accordance with Sun Microsystems® Java
	Private Software Publisher	Software security in accordance with IETF RFC 2315 and IETF RFC 2633, UNIX® Code Signing (programmer's universal certificate)
	Private VPN	Data transmission security – protocol Ipsec. For network devices, servers and VPN channels
	Private WAP Server	Wireless data transmission security – WTLS
	Private Time Stamp	Time stamping of objects and electronic transactions
	Private Netscape Form Signing	Form signing in accordance with Netscape®
	Private Strong Internet	Customer's authentication to network resources, service servers, workstation, authentication to Kerberos V (token based on X.509 certificates)
	Private CA	Testing certification authority
	Private EDI	Dedicated solutions and systems, e.g.. Netscape EXpert, Softshare EDI, etc.
	Private SSL Serwer	Security of data transmission between a service and a customer LDAP, NTP, POP3, SMTP etc.
	Private Apple Code Signing	Software security in accordance with Apple® technology for Macintosh
	Private Biometric Data	Security of financial transmission of data, mainly between a bank and its customer
	Private Castanet Signing	Encryption and signing of software distribution channels in accordance with Marimba® Castanet
	Private IPsec Client	Client of encrypted transmission of data on the basis of IPsec protocol
	Private Data Encryption	Data encryption for private entities; cryptographic file systems
	Private OCSP	Certificate status confirmation request issuance to OCSP servers
	Private Notary Service	Notary services, a certificate for Notary Authority
Certum Level II	Certum Silver	Electronic mail security, electronic signatures of electronic data, PGP
	Commercial VPN	Data transmission security – IPsec protocol for network devices, servers and VPN channels
	Commercial Strong Internet	Customer's authentication to network resources, service servers, workstation, authentication to Kerberos V (token based on X.509 certificates)
	Commercial SSL Server	Security of data transmission between a service and a client of LDAP, NTP, POP3, SMTP etc

Certification policy	Commercial name of certificate type	Description and recommended applicability
	Commercial IPsec Client	Client of encrypted transmission of data on the basis of IPsec protocol
	Commercial Data Encryption	Data encryption; cryptographic file systems
Certum Level III	Certum Gold	Electronic mail security, electronic signatures of electronic data, PGP
	Enterprise Web Server	Data transmission security for WWW systems
	Microsoft Authenticode	Software security against forgery, software distribution in global network in accordance with Microsoft Authenticode™
	Microsoft VIS	Securing VB in Office 2000 against forgery, software security in accordance with Microsoft Visual Basic for Applications
	Netscape Object Signing	Plugin signing, Java applet and module signing in accordance with Netscape® technology
	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 VPN	Data transmission security – protocol Ipsec. For network devices, servers and VPN channels
	Enterprise WAP Server	Wireless data transmission security – WTLS
	Netscape Form Signing	Form signing in accordance with Netscape®
	Enterprise EDI	Dedicated solutions and systems, e.g.. Netscape EXpert, Softshare EDI, etc.
	Enterprise SSL Server	Security of data transmission between a service and a client of LDAP, NTP, POP3, SMTP etc
	Apple Code Signing	Software security in accordance with Apple® technology for Macintosh
	Castanet Signing	Encryption and signing of software distribution channel in accordance with Marimba® Castanet
Certum Level IV	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 Time Stamp	Timestamping of objects and electronic transmissions of a great value
	Trusted Strong Internet	Customer's authentication to network resources, service server, workstation, authentication to Kerberos V (token based on X.509 certificates)
	Trusted CA	Certificate services delivery
	Trusted EDI	Dedicated solutions and systems, e.g.. Netscape EXpert, Softshare EDI, etc.
	Trusted Biometric Data	Client of electronic banking services

Certification policy	Commercial name of certificate type	Description and recommended applicability
	Trusted IPsec Client	Client of encrypted data transmission in accordance with IPsec protocol, applied to particularly important transmissions
	Trusted Data Encryption	Data encryption for private entities, cryptographic files systems, applied in electronic trade systems and banking
	Trusted OSP	OCSP service confirming certificate status
	Trusted Notary Service	Electronic notary authority

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 Unizeto CERTUM - CCP,

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 Unizeto CERTUM - CCP) applications is shown in Table 1.5. The updated version of this list is published in the repository at:

http://www.certum.pl/repository

Applications are included in the list of recommended applications on the basis of written statements of producers and/or tests made by Unizeto CERTUM - CCP. Unizeto CERTUM requires from every subscriber to generate by himself/herself/itself encryption keys used for certification process by means of recommended devices (see Table 1.5). Unizeto 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, Unizeto CERTUM applies cryptographic cards or modules fulfilling the requirements of FIPS PUB 140-1.

Table 1.5 The list of recommended applications

Name of application / version /producer	Certificate commercial name	Short description of application
All applications supporting public key certificates X.509	All certificates issued by CA Certum	Various applications

1.4.3. Prohibited Applications

It is prohibited to use Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP is shown in Table 1.6. The updated version of the list is published in the repository at:

http://www.certum.pl/repository

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

Table 1.6 The list of prohibited applications

Name of application/ version/ producer	Certificate commercial name	Short description of application
–	All certificates issued by CA Certum	No restrictions concerning existing applications

1.5. Contact

Contact data concern an entity managing the present Certification Practice Statement, the address where comments concerning the Statement and Certification Policy can be sent, and the address if the Team verifying the compliance of the Statement with Certification Policy.

1.5.1. Administration Organisation Data

PKI Services Development Team operating within Unizeto Sp. z o.o. structure, directly administers the present Certification Practice Statement, Certification Policy and other documents concerning PKI services delivered by Unizeto CERTUM - CCP. All inquiries and comments concerning the contents of the mentioned documents should be directed to **Unizeto CERTUM – PKI Service Development Team** at:

Unizeto Sp. z o.o.

70-486 Szczecin, Królowej Korony Polskiej St. 21

Unizeto CERTUM – PKI Service Development Team

E-mail: info@certum.pl

1.5.2. Contact Address

Persons who want to receive a copy of Certification Practice Statement, Certification Policy or other information concerning these documents, or inquire about the documents or the information, are requested to use the following addresses:

Unizeto Spółka z o.o.

70-486 Szczecin, Królowej Korony Polskiej St. 21

Unizeto CERTUM – PKI Service Development Team

E-mail: info@certum.pl

Telephone number (+48 91) 48 01 297

Fax number (+48 91) 48 01 220

1.5.3. Person Determining CPS Compatibility with the Policy

CPS compatibility with the Certification Policy is determined by PKI Services Development Team. The Team also approves certification practice statements of the certification authorities that were registered by Unizeto CERTUM– CA and to which certificates concerning certification cervices delivery were issued. Contact addresses of the Team are stated in 1.5.2.

1.6. Acronyms and Definitions

CA Certification Authority

CP Certification Policy

CPS Certification Practice Statement of Unizeto CERTUM – CCP

CRL Certificate Revocation List

DN Distinguished Name

KRIO National Registry of Object Identifiers (*pl. Krajowy Rejestr Identyfikatorów Obiektów*)

LRA local registration authority

OSCP On-line Certificate Status Protocol

PKI Public Key Infrastructure

PRA Primary Registration Authority

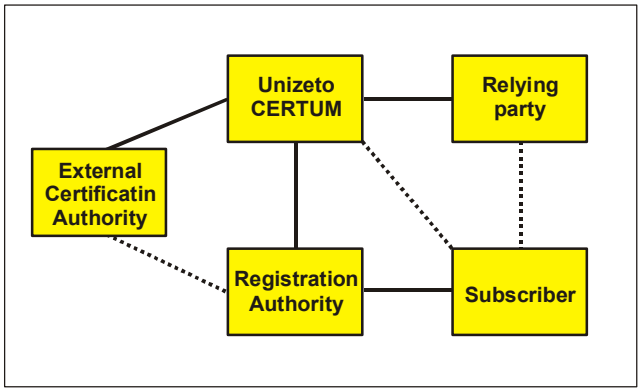
PSE Personal security environment – local secure media for private entity's key, public key (usually as an self-certificate);depending on certification policy the media can be a cryptographically encrypted file (e.g. in accordance with PKCS #12) or a tamper resistant token (e.g. electronic identity card)

RSA asymmetric cryptographic algorithm (its name originates from initials of its developer Rivest, Shamir, Adleman), in which one private transformation allows not only for signature creation but for message decryption as well, while one public transformation allows verification and encryption of the message

TTP trusted third party – an institution or its representative whom other entities trust as far as security and authentication actions are concerned, or whom authenticated entities and/or verifying entities trust (following PN 2000)

2. General Provisions

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



Picture 2.1 Agreements between parties

Unizeto CERTUM - CCP agreements with relying parties and subscribers describe types of services provided by Unizeto CERTUM - CCP, mutual obligations and liabilities (including financial ones of Unizeto Sp. z o.o.).

Agreements between Unizeto CERTUM and local 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 Unizeto CERTUM. In well-founded cases, registration authorities can make separate agreements with subscribers for the services delivered by registration authorities and describing their relations.

Unizeto CERTUM – Certification Authority 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.

Certification Practice Statement and Certification Policy are an integral part of agreements made by Unizeto CERTUM - CCP and subscribers, relying parties, external registration authorities or other entities that are deliverers of the service of public key infrastructure, e.g. timestamp, certificate status verification, etc.

Agreements between external certification authorities and local certification authorities should be made on the grounds of the same rules that govern relations between registration authorities and Unizeto CERTUM.

This Certification Practice Statement does not impose any restrictions concerning the contents of agreements between a relying party and a subscriber, provided that these agreements do not violate the parties' obligations and liability specified in the Statement.

2.1. Obligations

2.1.1. Unizeto CERTUM - CCP Obligations

Unizeto CERTUM - CCP 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,

its activity and services are in accordance with the law; 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 information identifying 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 this occurrence in cases when a subscriber is a subject of an certificate that is being issued, revoked or suspended,
- publication of the lists of revoked or suspended certificates in the sites stated in the present Statement,
- generating and using private keys only for the purposes defined in the present
- Statement; securing keys in a way not permitting the application of the keys not in accordance with their purposes,
- personalization and issuance of electronic identity cards where certificates and a key pair are stored (in the cases when the card was generated by a certification authority),
- periodical and punctual publication of the information indispensable for correct reception, management and revocation of certificates,

issued certificates do not contain any falsified data, neither known nor coming from the people confirming the applications for certificate issuance or issuing certificates,

issued certificates do not contain any mistakes resulting from negligence or procedure violence by the people confirming applications for certificate issuance or issuing certificates,

subscribers' Distinguished Names (DN) listed in certificates are unique within **certum** domain,

it secures personal data protection in accordance with *Personal Data Protection Law of 29th August, 1997, and Ministry of Home Affairs and Administration Decree of 3rd June 1998 concerning the stating of basic organizational and technical conditions used for devices and information systems applied to personal data processing*,

if a key pair is generated with the subscriber's authorization, the key pair is confidentially delivered to the subscriber and immediately after the delivery of the key to the subscriber, erased from the media used for delivery, unless the subscriber demands archive of the key pair.

Unizeto CERTUM - CCP commits itself to:

register and issue certificates only to certification authorities whose certification policy and certification practice statement are approved by PKI Services Development Team. The Team must point to at least one of the four certification policies (specified in Table 1.2 and Chapter 7.1.1.2) applied by a certification authority being registered,

make agreements with subscribers, relying parties, certification authorities and registration authorities; certification services are delivered only on the basis of the agreements and always on request of a subscriber, a relying party, a certification authority or a registration authority,

create and manage a list of registered registration authorities with which Unizeto CERTUM - CCP has cooperation agreements and agreements about recommending the devices and software used by these authorities,

create and manage a list of recommended software and devices used for generating asymmetric key pairs,

create and manage a list of recommended and prohibited applications that fulfil or do not fulfill the requirements stated in Chapter 1.4.2,

carry out scheduled audits in certification authorities and registration authorities belonging to or connected with **certum** domain,

charge independent auditors with intended audits of **certum** domain, make all necessary documents and information accessible to auditors, comply with auditors' post-audit recommendations.

2.1.2. Registration Authority Obligations

Every registration authority operating within certum domain or bound by an agreement with Unizeto CERTUM - CCP ensures that:

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

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 Unizeto CERTUM - CCP 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 or unintentionally 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**[14], 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,
- 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 Unizeto CERTUM - CCP (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; the keys cannot be stored by a registration authority, unless the agreement with the subscriber states differently,
- procedures of personalization and issuance of electronic identity 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 Unizeto CERTUM - CCP service unit or to the ones commissioned by this unit.

Beside above, registration authority commits itself to:

[14] See **Glossary**

submit to Unizeto CERTUM - CCP recommendations, particularly to those resulting from audits,

to secure personal data protection in accordance with *Personal Data Protection Law of 29th August, 1997,and Ministry of Home Affairs and Administration Decree of 3rd June 1998 concerning the stating of basic organizational and technical conditions used for devices and information systems applied to personal data processing*,

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 Unizeto CERTUM - CCP,

obtain from reliable sources and thoroughly verify public key **active certificates**[15] and CRL's of Unizeto CERTUM - CCP certification authorities.

2.1.3. End Subscriber Obligations

Certification Practice Statement and Certification Policy are an integral part of every agreement made by an end subscriber and Unizeto CERTUM - CCP. By applying for registration to a registration authority and signing confirmation of registration, a subscriber agrees to enter the certification system on the conditions stated in the documents mentioned above.

Depending on relations between Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP.

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 Unizeto CERTUM - CCP; this approval should consist of a hand-written signature (official agreement) and a statement of will (informal agreement) at the moment of approval of the issued certificate; the contents of the subscriber's statement of will are published in the repository,

approve every certificate issued to him/her/it; warranties and Unizeto CERTUM - CCP liability connected with a particular certificate are valid of the date of the approval of a certificate,

take precautions allowing an end subscriber 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); if subscribers generate the keys on their own, they should apply the devices and software recommended by Unizeto CERTUM - CCP,

state true data in applications submitted to a registration authority or a certification authority and then stored in Unizeto CERTUM - CCP 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,

acknowledge 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

[15] See **Glossary**.

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,

generate cryptographic keys, manage passwords, public and private keys, exchange information with registration and certification authorities only by means of the software recommended by Unizeto CERTUM - CCP; 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 unauthorized persons,

not to use as an end subscriber a private key, associated with the certificate issued by Unizeto CERTUM - CCP, for signing any CRL's 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,

not to reveal their passwords to unauthorized persons,

submit to a registration authority 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 Unizeto CERTUM - CCP,

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),

obtain public key certificates of certification authorities and registration authorities and other Unizeto CERTUM - CCP service units.

2.1.4. Relying Party Obligations

Certification Practice Statement and Certification Policy are an integral part of every agreement made by a relying party and Unizeto CERTUM - CCP or a subscriber. The object of such an agreement can be:

the delivery of repository services, timestamp services and certificate status verification services (OCSP) – in the case of agreements with Unizeto CERTUM - CCP,

specification of the conditions that an electronic signature must fulfill to be considered valid by a relying party – in the case of agreements with a subscriber.

Depending on relations between a relying party and Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP and a subscriber.

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

approve the terms stated in an official or informal agreement between a relying party and Unizeto CERTUM - CCP or a subscriber; this approval should consist in a handwritten signature (official agreements) or a statement of will (informal agreements) at the time of the first usage of any service delivered by Unizeto CERTUM - CCP or the first approval of the subscriber's signature; warranties and liabilities of subscriber's or Unizeto CERTUM - CCP are valid from the date of the agreement,

thoroughly verify[16] 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**[17] containing all certificates belonging to other certification authorities that make it possible to verify the signature on the certificate of a signature issuer,
- make sure that the chosen certification path is the best from the point of view of signature creating; it is possible that there is more than one path leading from a given certificate (by means of which the signature was made) to the certification authority that the verified signature relies on,
- check whether neither of certificates creating a certification path in the Unizeto CERTUM - CCP 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 originality on the document or the message,

carry out cryptographic operations accurately and correctly, using the software and devices whose security level complies with the sensitivity level of a certificate being processed and the credibility level of applied certificates,

consider an electronic signature to be invalid if by means of applied software and devices it is not possible to state if the electronic signature is valid or if the verification result is negative,

---

[16] 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 Unizeto CERTUM - PCA, and (2) a signed message (document) was not modified after signing it.

[17] See **Glossary**

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 OSCP service, available at Unizeto CERTUM - CCP,

specify the conditions that a public certificate key and a electronic signature must fulfill 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. A relying party is committed to familiarize /himself/herself/itself with CPS or CP (**guaranties** and **responsibility**).

2.1.5. Unizeto CERTUM - CCP Repository Obligations

The repository is managed and controlled by Unizeto CERTUM - CCP. Therefore, Unizeto CERTUM - CCP 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 4.3,

make sure that certificates of certification authorities, registration authorities belonging to certum 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 agreements and relying party agreements and lists of recommended and prohibited applications,

give access to the information concerning certificates status by publishing of CRL's, OCSP server or questions asked 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 Certification Policy,

secure safe and controlled access to the information in the repository.

All users, except for relying parties, have an unlimited access to the whole information in the repository. Limitations on relying parties' access usually concern subscribers' certificates and they are governed by agreements between Unizeto CERTUM - CCP and a relying party.

2.2. Liability

Liability of parties delivering services or using these services in the domain managed by Unizeto CERTUM - CCP is governed by appropriate mutual agreements. 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.

Unizeto CERTUM - CCP bears liability for the consequences of the actions of ***CA-Certum Level I, CA-Certum Level II, CA-Certum Level III, CA-Certum Level IV*** *certification authorities, Priamry 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. Unizeto CERTUM - CCP Certification Authorities Liability

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

occurred despite their obeying the rules stated in Certification Policy and Certification Practice Statement,

result from mistakes made by Unizeto CERTUM - CCP, 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 CRL's)

occurred as a result of the violation of other Unizeto CERTUM - CCP warranties, specified in Chapters 2.1.1, 2.1.5, 2.1.2.

If Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP 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.

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

Nevertheless, Unizeto CERTUM - CCP does not take any responsibility for the actions of third parties, subscribers and other parties not associated with Unizeto CERTUM - CCP. In particular, Unizeto CERTUM - CCP 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, 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 Unizeto CERTUM - CCP database and their publication in a public certificate key issued to the subscriber in case of subscriber's stating such false data.

2.2.2. Registration Authority Liability

Primary Registration Authority liability is automatically taken by Unizeto CERTUM - CCP and is a result of warranties stated in Chapters 2.1.1, 2.1.2, 2.15. The conditions of this liability are governed by agreements made by Unizeto CERTUM - CCP with subscribers and relying parties.

Liability of other registration authorities functioning on behalf of and from authorization of Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP 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 are governed by an agreement with Unizeto CERTUM - CCP and a subscriber.

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

In this agreement 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 make a statement saying that they are aware of legal consequences following the negligence of their obligations, specified in Chapter 2.1.4.

2.2.5. Repository Liability

The liability for functioning of the repository and results of its functioning is taken by Unizeto CERTUM - CCP (see Chapter 2.2.1)

2.3. Financial Liability

The liability of Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP or of the parties that Unizeto CERTUM - CCP made agreement with in such a way that the fault is transferred to Unizeto CERTUM - CCP, collective financial warranties of Unizeto CERTUM - CCP in relation to all parties (including relying parties) cannot exceed (in a single case) the total amount of sums for credibility level of certificates, persons and devices specified in Table 2.1.

Table 2.1 Maximal financial guarantees

Certification Policy	Entity			
	Private entity	Legal entity	Device	
			Private entity	Legal entity
Certum Level I	0 PLN	0 PLN	0 PLN	0
Certum Level II	400 PLN	400 PLN	400 PLN	400 PLN
Certum Level III	20 000 PLN	20 000 PLN	20 000 PLN	20 000 PLN
Certum Level IV	100 000 PLN	100 000 PLN	100 000 PLN	100 000 PLN

Total collective Unizeto CERTUM - CCP 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. Law Interpretation and Enforcement

2.4.1. Governing Law

Operating of Unizeto CERTUM - CCP 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 Certification Practice Statement 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, except for the cases specified in the agreement and in Chapter 4.1.4.

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 the Statement or in the agreement,

the resolutions to which the Statement 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 Statement 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 Unizeto CERTUM - CCP 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 CRL's, new certificates belonging to registration authorities and certification authorities, and supplying subscribers or relying parties (if the agreement states so) with the information about it, as well as informing about the breach of a private key owned by any certification authority.

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.

In the instance of the occurrence of arguments or complaints following the usage of an issued certificate or services delivered by Unizeto CERTUM - CCP, complainers commit themselves to notify Unizeto CERTUM - CCP (by means of a registered letter) of the reason for the argument or complaint. Complainers also commit themselves to allow a previously agreed amount of time for Unizeto CERTUM - CCP to resolve the problem, prior to resorting to other means of dispute resolution.

If the time limit is exceeded, a complainer can hand over the dispute to the agreed and independent mediator. The mediator's decision, approved by the parties, should be decisive and binding to the parties.

If the case of an unsatisfying outcome of the resolution, the dispute should be settled in court, in accordance with The Civil Code or other law regulations in force in the Republic of Poland.

Unizeto CERTUM - CCP resolves only the disputes with its customers (subscribers, registration authorities, certification authorities, relying parties, etc.) resulting from agreements already made. The rules mentioned above are an integral part of these agreements. Similar rules concerning dispute resolution should be also applied to the instances of agreements in which Unizeto CERTUM - CCP is not the party of the agreement.

2.5. Fees

Unizeto CERTUM - CCP charges fees for its services. The extent of fees and categories of chargeable services are published in a pricelist available in the repository at:

http://www.certum.pl/repository

Unizeto CERTUM - CCP 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 to a legal entity,

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 Unizeto CERTUM - CCP infrastructure, e.g. if a new commercial certification authority receives a certificate from Unizeto CERTUM - CCP, Unizeto CERTUM - CCP charges a fee for every certificate issued by this authority.

Fees can be paid by credit card or money transfer on the basis of an invoice or an order.

2.5.1. Certificate Issuance or Renewal Fees

Unizeto CERTUM - CCP charges a fee for issuance or renewal[18] of a certificate (see 2.5).

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 identity card (token) 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 token issuance costs can be omitted).

2.5.2. Certificate Access Fees

Certificate access fees are only applicable to 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 fixed by means of agreements with relying parties. The extent of these fees is dependant on the certificates credibility.

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

2.5.3. Revocation and Status Information Access Fees

Unizeto CERTUM - CCP does not charge a fee for certificate revocation, publishing certificates in CRL's and making CRL's published in the repository (or elsewhere) accessible to relying parties.

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

Without Unizeto CERTUM - CCP written approval, the access to CRL's 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 Unizeto CERTUM - CCP. In this instance, the direct 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

Unizeto CERTUM - CCP 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,

[18] See **Glossary**

sale of Certification Practice Statement, Certification Policy, handbooks, guides, etc, published in print,

trainings.

2.5.5. Fees Refund

Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP 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.

2.6. Repository and Publication

2.6.1. Information Published by Unizeto CERTUM - CCP

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

http://www.certum.pl/repository

The information consists of:

Certification Policy,

Certification Practice Statement,

templates of agreements with relying parties and subscribers,

Unizeto CERTUM - CCP statement concerning the confidentiality of received and processed information,

certificates belonging to **CA-Certum** certification authorities, **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**, other certification authorities, registration authorities, subscribers,

Certificates Revocation Lists (CRL's); CRL's are accessible at the so called CRL distribution points, whose addresses are set in every certificate issued by Unizeto CERTUM - CCP; the basic point of CRL's 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/search

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

Unizeto CERTUM - CCP publications below are issued with the following frequency:

Certification Policy and Certification Practice Statement – see Chapter 8,

the certificates of certification authorities functioning within Unizeto CERTUM - CCP – 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 Unizeto CERTUM - CCP receives them,

supplementary information – upon every updating of it.

2.6.3. Access to Unizeto CERTUM - CCP Publications

The whole information published by Unizeto CERTUM - CCP in its repository at http://www.certum .pl/repository is accessible for the public. This information can be accessed without limitations only upon a relying party's approval of the terms stated in an agreement made with Unizeto CERTUM - CCP.

Unizeto CERTUM - CCP service unit has implemented logical an 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, Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP service unit or subjects delegated by the unit, with their declarations and procedures (including Certification Policy and Certification Practice Statement).

Unizeto CERTUM - CCP 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 **CA-Certum**, registration authorities, and other elements of public key infrastructure, e.g. OCSP server.

Unizeto CERTUM - CCP audit may be carried out by internal units of Unizeto Sp. z o.o. (internal audit) and organizational units independent from Unizeto Sp. z o.o. (external audit). In both cases, an audit is carried out on request of and under supervision of a **security administrator** (see Chapter 5.2.1).

2.7.1. Audit Frequency

An external audit checking the consistency with procedural and legal regulations (particularly the consistency with Certification Practice Statement and Certification Policy) is carried out at least every two years, whereas an internal audit 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 Unizeto CERTUM - CCP 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.

A current external auditor of Unizeto CERTUM - CCP is Ernst&Young.

An internal audit is carried out by Office for Information Security and Management, operating within Unizeto Sp. z o.o. 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 Unizeto CERTUM - CCP,

procedures of subscribers' identity verification,

certification services and procedures of the services delivery,

security of software and network access,

security of Unizeto CERTUM - CCP personnel,

event journals and system monitoring procedures,

backup copy creation and their recovery,

archive procedures,

records of configuration parameters changes of Unizeto CERTUM - CCP,

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 Unizeto CERTUM - CCP **security administrator**. Within 14 days of the record submission, the administrator is committed to prepare a written opinion concerning the deficiencies specified in the records and specify actions, as well as their deadlines, to be taken to remove the deficiencies. Information about deficiencies removal is submitted to the auditing organization.

In deficiencies posing an immediate threat to the security of certification procedures of ***CA-Certum Level III*** *and* ***CA-Certum Level IV*** *certification authorities, a security administrator might make a decision of a temporary suspension of their activities. All customers of` Unizeto CERTUM – CC 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 e-mail 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 Unizeto CERTUM - CCP with the requirements stated in WebTrust and the security administrator's opinion are published in the repository upon every audit.

2.8. Information Confidentiality and Privacy

Unizeto CERTUM - CCP ensures that the whole information it possesses is gathered, stored and processed in accordance with the law in force, particularly with *Confidential and Private Information Protection Law of 22nd of January, 1999, execution acts accompanying it, and Personal Data Protection Law of 29th of August, 1997*.

Relations among a subscriber, a relying party and Unizeto CERTUM - CCP are based on trust. Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP shall never be voluntarily or deliberately revealed to a third party in any circumstances (besides on court writ).

Unizeto CERTUM - CCP can possess the access to subscribers' private keys only in the cases of:

1) keys generating and archive order, submitted by the subscriber,
2) submission of the locally generated key for archive in the databases of Unizeto CERTUM.

Key archive is carried out on customer's explicit request.

Certificates issued by Unizeto CERTUM - CCP authorize the transmission of information between a subscriber and a relying party who can have a status of *non-public information*.

2.8.1. Types of Information to be Kept Confidential and Private

Unizeto CERTUM - CCP, 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[19] 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,

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

renewal, revocation of certificates (except for information included in certificates or the repository, in accordance with the present Certification Practice Statement); a part of the information mentioned above can be made accessible solely upon approval of and in the scope specified by its owner (i.e. subscriber),

record of system transactions (the whole of the transactions, as well as **data for control inspection** of transaction, the so called system transactions logs),

record of information about events (logs) connected with certification services, stored by Unizeto CERTUM - CCP and registration authorities,

records of an internal and external control, if it might cause a threat to Unizeto CERTUM - CCP security (in accordance with Chapter 2.7, 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 CERTUM 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 Unizeto CERTUM - CCP with subscribers and relying parties,

the pricelist of services,

guides for users,

registration authorities and certification authorities certificates,

certificates belonging to subscribers (upon their prior approval),

Certificates Revocation List,

information about trainings carried out by Certum,

extracts from post-control reports (as detailed as possible) prepared by an authorized institution.

The extracts from post-control reports, published by Unizeto CERTUM - CCP, 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 Non-Public Information to Law Enforcement Officials

Non-public 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 Non-Public Information for Scientific Purposes

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

2.8.6. Release of Confidential/Private 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 CERTUM - CCP are intellectual property of their legal owners. Unizeto CERTUM - CCP commits itself to place appropriate remarks (required by the owners) in this respect.

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

Unizeto CERTUM - CCP 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.

3. Identification and Authentication

This Chapter presents general rules of subscribers' identity verification applied by Unizeto CERTUM - CCP 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 modification of the subscriber's data, and **on request** of Unizeto CERTUM - CCP 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**[20] issued by any authority issuing certificates and affiliated by Unizeto CERTUM PCA.

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 Unizeto CERTUM - CCP services and supplied with a public key certificate. Upon subscriber's request, the certificate is published in the repository.

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

remotely fill in a registration form on WWW site of Unizeto CERTUM - CCP,

generate RSA or DSA asymmetric key pair and supply a registration authority with the proof of the possession of a private key; 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),

fill in and submit and application for registration containing a public key and the proof of the possession of a corresponding private key,

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),

make an agreement with a registration authority agent about delivery of services by Unizeto CERTUM - CCP; the present Certification Practice Statement is an integral part of this agreement.

[20] See **Glossary**

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

3.1.1. Types of Names

Certificates issued by Unizeto CERTUM - CCP comply with the norm X.509 v3. 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 Unizeto CERTUM - CCP certificates are in accordance with Distinguished Names - DN's – (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). 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 Unizeto CERTUM - CCP 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, CRL's and Certification Policy are retained, as well as the names of CRL's 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 four certification policies defined in Chapter 1.

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

Certification policy	Requirements
Certum Level I	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 critical[21].
Certum Level II	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	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	Subject's DN in accordance with X.500 and optionally the alternative name in the case when it is marked as non-critical

The whole information, submitted in subscriber's application for registration and included in the certificate by an authority issuing certificates 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).

[21] 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 a subscriber.

For **private entities** (individuals or employees of companies), DN consists of the following, obligatory or non-obligatory fields (descriptions of a field follows its abbreviated name that complies with the recommendation RFC 2459 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[22] – the name of the institution where the subscriber works,

field OU[22] – the name of the organizational unit employing the subscriber

and five optional fields[23] (set upon subscriber's request and upon prior consultation of a certificate issuer):

field S – the subscriber's family name (possibly maiden name or married name),

field G – the subscriber's name/names,

field P – the subscriber's pseudonym that the subscriber uses in his/her environment or that he/she wishes to use without revealing his/her true name and family name,

field T – telephone number,

field F – fax number.

For **legal entities**, DN consists of the following non-obligatory fields (description of a field follows its abbreviated name that complies with the recommendation X.520)

field C – international abbreviation of the country name (PL for Poland)

field O – the name of the institution,

field OU – the name of the organisational unit of the institution,

field ST – the region/province where the institution functions,

field L – the city where the subscriber lives or has a seat

field CN – common name of the institution

and two optional fields[24] (set on legal entity's request and upon prior consultation with a certificate issuer)

---

[22] This argument is set in DN only if a private entity is the employee of the company.

[23] These fields should not have any influence on the uniqueness of the subscriber's DN.

[24] These fields should not have any influence on the uniqueness of the subscriber's DN.

field T – telephone number,

field F – fax number.

In the case of devices owned by private/legal entities, DN comprises (besides the elements of a private/legal entity' name) a non-obligatory field:

field SN – serial number or identifier of the device.

Subscriber's name must be confirmed by a registration authority operator and approved by a certification authority. Unizeto CERTUM - CCP ensures (within its domain) the uniqueness of DN's.

3.1.3. Rules for Interpreting Various Names Forms

The interpretation of the fields provided in certificates issued by Unizeto CERTUM - CCP is in compliance with certificates profile described in The Profile of Certificate and CRL's[25]. In creating and interpreting of DN's, the recommendations specified in Chapter 3.1.2 are employed.

3.1.4. Names Uniqueness

The identification of every subscriber of certificates issued by Unizeto CERTUM - CCP is performed on the basis of DN.

Unizeto CERTUM - CCP ensures the uniqueness of the DN assigned to a subscriber.

Subscriber's DN is suggested by the subscriber in his/her application. If the name is in accordance with general requirements stated in Chapter 3.1.1 and 3.1.2, a registration authority operator temporarily accepts the suggestion. If the registration authority operator has access to DN database[26], he/she additionally checks the uniqueness of a subscriber's name in Unizeto CERTUM - CCP domain. If the test proves successful, the DN is accepted. In the case of lack of access to Unizeto CERTUM - CCP database, a decision concerning approval or rejection of DN is taken by Main Certification Authority operator.

If a distinguished name suggested by a subscriber violates other entities' rights to this name (see Chapter 3.1.5), Unizeto CERTUM - CCP might add another attributes to DN (e.g. domain qualifier or serial number), which ensures the uniqueness of this name within Unizeto CERTUM - CCP domain. A subscriber is entitled to reject a suggested distinguished name in the course specified in Chapter 4.4.

The format of globally unique subscriber's name has a form:

certum.pl / issuer name / subscriber's name

in which **certum.pl** is the name of Unizeto CERTUM - CCP domain, issuer name is DN of one of certification authorities and subscriber's name is certificate subject DN. Values of the last two fields are retrieved from the certificate.

If any subscriber resigns form Unizeto CERTUM - CCP services, the request of attributing his/her/its DN to another subscriber must be rejected.

---

[25] *The Profile of Certificate and CRL's*, publication of Certification Authority, Unizeto Sp. z o.o.

[26] Priamry Registration Authority operator always has the access to DN database.

Unizeto CERTUM - CCP can register a subscriber with the distinguished name once used by another subscriber only on the basis of a written approval of the latter.

Within Unizeto CERTUM - CCP domain, the uniqueness of the names of directories within the repository is guaranteed. Applications basing on this property of the names of Certum 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. Unizeto CERTUM - CCP neither checks if a subscriber is entitled to use the name placed in the application for registration nor intends to 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, Unizeto CERTUM - CCP is entitled to reject or suspend a subscriber's application without taking liability in virtue of this suspension/rejection.

Unizeto CERTUM - CCP 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. Recognition, Authentication and Role of Trademarks

Unizeto CERTUM - CCP has its own registered trade mark consisting of a graphic mark and inscription, which constitute the following logo:

Pic. 3.1 Unizeto CERTUM logo

This mark and inscription constitute the logo of Unizeto CERTUM. The logo is a registered trademark of Unizeto CERTUM and cannot be used by any party without a written approval of Unizeto CERTUM.

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

3.1.7. Prove of Possession of Private Key

If an entity possesses a private key when applying for certificate issuance, certification authorities functioning within Unizeto CERTUM - CCP 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.

In the case of encryption keys, the proof is carried out indirectly. It consists of the issuance of a certificate that a subscriber requests and the encryption of the certificate by means of a public key contained within the certificate. The subscriber have to decrypt the certificate by means of a private key and send the certificate to a certification authority.

Verification of the private key possession, intended for key agreement, involves agreement of the secret by the certification authority and the subscriber and it usage by the certification authority for encryption of issued certificate. The subscriber has to decrypt the received certificate with possessed private key and submit it back to the 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 identity card) or, upon their generation outside the token, by means of hardware or software key generator, imported to the token. 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[27]. In the latter case, Unizeto CERTUM - CCP must guarantee that the token and the key shall reach securely the entity for which they are intended. (see Chapter 6.1.2).

3.1.8. Authentication of Legal Entity's Identity

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 and ran business; the second purpose is to prove that a private entity applying for a certificate or receiving it is authorized by this legal entity to represent it.

The procedures of legal entity's identity authentication are carried out if the entity:

acts as a subscriber and charges a certification authority with any certification service,

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

demands issuance of a certificate for a hardware device or application (software) owned by this entity,

acts as an entity applying for including it in the list of accredited registration authorities or certification authorities, subordinate to Unizeto CERTUM - CCP,

wishes to render other certification services, e.g. as a timestamp authority, OCSP.

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.

The first way is obligatory if a submitted application concerns the registration of and certificates issuance to a legal entity with credibility levels **Certum Level III** and **Certum Level IV**. This way also applies to cases if applications concern certification, certificate renewal and rekey or revocation of certificates of the same level.

A registration authority is committed to require that an requester submits appropriate documents confirming the identity of the applying institution and its representative.

For the sake of the present Certification Practice Statement, it is assumed that authorized representatives of institution, disregarding of the level of certificate they apply for, are committed to submit, upon a registration authority representative's request, the following documents:

the valid extract from the Country Court Registry or the authorized copy of the business evidence,

a document confirming allotted numbers: NIP (Tax Identification Number) or REGON (Business Entity Identification Number),

documents confirming the identity of the requester (identity card or passport) and authorization to represent the company.

The last requirement is important in the case of applying for certificates issued to certification authorities operators and institution employees.

The procedure of verification of legal entity's identity and its authorized representative's identity consists in (also see Table 3.2):

the verification of originality of documents submitted by a subscriber; the verification should be detailed, including the application of information included in the database of certificate issuer (on behalf of which a registration point operates) or other institutions associated with the issuer,

the verification of the application originality which consists in:

- checking the consistency of data set in the application with submitted documents,
- (optional) verifying the proof of possession of private key (if the application concerns a key pair for creating an electronic signature) and the appropriateness of the **distinguished name**,

the verification of information provided in the application with other sources of information (e.g. court register, General Statistics Office, inland revenue office, The Book of Companies) in order to confirm the existence of the legal entity stated in the application,

verification of authorization and identity of a legal entity's representative who supplies the application (including applications for accreditation as a registration authority or a certification authority) on behalf of this entity.

A registration authority is committed to verify the correctness and truthfulness of all data provided in an application (see Table 3.2, Chapter3.1.9).

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,

makes copies of all documents and certificates used by the operator to verify the legal entity's identity and the identity of its representative acting on behalf of the entity,

on behalf of a certification authority, makes an agreement with the legal entity about certification services delivery; the agreement is 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 (with a handwritten signature) 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),

the requester's statement (with a handwritten signature) about the truthfulness of data provided in the application; the statement might be signed upon sending it to the address of the requester (in the case when an requester is not required to attend in person the registration authority) or in the presence of a registration authority operator.

Unizeto CERTUM - CCP always rejects a subscriber's application for registration if it discovers that the legal entity has already been registered.

The second way of identity verification (on-line verification) is performed in the case of applications sent directly to a certification authority. It concerns:

applications for certification, which concerns additional certificates within the same certification policy,

applications for rekey and certificate renewal,

applications for certificate revocation,

applications for providing access to a certificate,

applications for certificate or CRL verification.

If a legal entity is not capable of effective authenticating of its application (e.g. does not possess a valid private key for signature creation or a key for message authentication), or upon certification authority request, an authorized representative of the entity must attend in person a registration authority to obtain confirmation of the application.

Authentication of a subscriber (institution) submitting applications directly to a certification authority is performed on the basis of information stored in Unizeto CERTUM - CCP database and consists of the following procedures:

authentication of the application is verified (e.g. an electronic signature made on the application),

if the application is signed electronically, the authenticity of the certificate, enclosed to the application and connected with a private key used for signature creation is verified,

the database of a certificate issuer is searched for a subscriber with the distinguished name stated in a certificate; the subscriber's certificate or message authentication key is compared with the certificate or authentication attached to the application,

entity's identifier included in the application or optionally in the certificate or database of certificate issuer is compared with the content of Unizeto CERTUM databases.

If the procedures are successful, it is assumed that the company's identity has been confirmed.

A detailed description of the functioning of a registration authority operator is disclosed in "Registration Authority Book". This document is "non-public" and available only to the personnel of registration authorities and particular notary offices in the Republic of Poland.

3.1.9. 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.

Authentication of private entities, similarly to legal entities, might be performed with or without the participation of a registration authority.

Authentication of private entities without the participation of registration authorities is carried out in the way depicted in Chapter 3.1.8. The authentication with the participation of a registration authority is performed on the basis of:

documents (identity card or passport) confirming the identity of a person applying for registration,

a document confirming allotted numbers: PESEL (Personal Identification Number) and NIP (Tax Identification Number),

and if the subscriber wishes to include the data of an institution (legal entity) he/she works for:

written authorization, with an the company's explicit approval of including its data in the private entity's certificate,

valid extract from the Country Court Registry or the authorized copy of the business evidence,

documents confirming allotted numbers: NIP (Tax Identification Number) or REGON (Business Entity Identification Number).

A subscriber might be represented by authorized third parties who must submit suitable authorizations issued by the subscriber.

The procedure of private entity's identity verification performed in the presence of a registration authority operator is similar to the procedure applied to legal entities and consists of:

verification of originality of documents submitted by a subscriber; the verification should be detailed, including the use of information included in the database of a certification authority (on behalf of which a registration point functions) or other institutions connected with it,

the verification of the originality of a submitted application; the verification comprises

- checking the consistency of data provided in the application with the submitted documents,
- (optional) verifying the proof of private key possession (if the application concerns a key pair for signature creation) and the appropriateness of the **DN**,

verification of information set in the application against other sources of information (e.g. Court Register, General Statistics Office, Inland Revenue Office, The Book of Companies) in order to confirm the existence of the legal entity stated in the application,

if the verification is successful, the operator performs actions specified in Chapter 3.1.8. Authentication process is recorded in the same way as it is described in Chapter 3.1.8.

The requirements imposed on the procedure of private entity's identity verification dependant on certificate credibility level are presented in Table 3.2.

Table 3.2. Requirements imposed on private entity's identity verification process

Certification policy	Requirements
Certum Level I	A. In the case of certificates for electronic mail: mail box authenticity is verified reply information containing certificate installation instruction to mail box address stated in the application. B. In the case of other testing certificates, there is a comparison of data that was received: by fax (recommended version), in a letter (option), in a registered letter (option), upon coming to a registration authority in person (option), by electronic mail with attachment: gif, tif, jpg, bmp (option) with the data submitted to a certification authority by a subscriber .

Certification policy	Requirements
Certum Level II	A. Registration authority operators compare subscriber's data received: By fax (recommended version), In a letter (option), In a registered letter (option), Upon attendance in person (option), By electronic mail with attachment: gif, tif, jpg, bmp (option), with the data submitted to a registration/certification authority by a subscriber B. In the case of individual customers, an operator confirms: Mail box address, Telephone or fax number C. In the case of collective orders, the following data are confirmed: Company credibility, Mail box address of a person responsible for certification process, Telephone or fax number, Address for correspondence.
Certum Level III	A. Registration authority operators verify customer's data received: In a registered letter (recommended version) Upon attendance in person in registration authority (option), with the data submitted by the subscriber to a registration authority by e-mail. A registered letter should contain copies of original documents confirmed by a handwritten, readable signature (optionally, with a seal of a person making a copy of the document) or confirmed by a notary. B. In the case of collective or individual orders., the subjects of checks are: Mail box address of a person responsible for certification process, Telephone or fax number, Address for corresppondence, A document confirming that a person applying for X.509 certificate is an employee or representative of the company (in the case of companies, not private entities).

Certification policy	Requirements
Certum Level IV	A. Operators verify subscriber's data received: Upon subscriber's attendance in person in registration authority (recommended version), In a registered letter containing data confirmed by a notary (option), with data submitted electronically by the subscriber to a certification authority. The letter should contain copies of the document confirmed by a notary. B. In the case of collective and individual orders, the subject of checks are: Mail box address of a person responsible for certification process , Telephone or fax number, Address for correspondence, Confirmation that a person applying for X.509 certificate is an employee or representative of the company (in the case of companies, not private entities). In the case of attendance in person, an operator makes copies of submitted documents and optionally puts a date and a handwritten signature. A person applying for a public key certificate can put a handwritten signature and a note: I submitted the documents personally on the copies.

A detailed description of the practice of a registration authority operator is presented in the document "Registration Authority Book". The document is non-public and is accessible only for registration authorities' personnel and particular notary offices in the Republic of Poland.

3.1.10. Devices Origin Authentication

In many instances a public key certificate is issued for hardware devices, e.g. router, firewall, server. In these cases it is assumed that every device must be owned by a private or legal entity (must have a sponsor). A sponsor is responsible for submission of the data associated with the device:

device identifier,

device public key,

attributes and authorizations of device (in the case when they should be listed in a certificate),

sponsor's contact data, allowing a registration authority or a certification authority for quick submission of information to the sponsor.

Verification of information being registered depends on credibility level of the certificate. There are two methods of authentication of device origin and integrity of submitted data:

verification of electronically signed application sent by a sponsor (the application must be signed with a private key associated with a certificate with equal or higher credibility level than the certificate being requested),

during sponsor's personally registering a device; sponsor's identity is confirmed in accordance with the requirements stated in Chapter 3.1.9.

3.1.11. Authorization and Other Attributes Authentication

Unizeto CERTUM registration authorities and certification authorities can confirm private entities' authorization to take actions on behalf of other entities, usually legal entities. Such authorizations are usually associated with a particular role in an institution, e.g. a president of a company can authorize any reliable person to sign money transfers on his/her behalf.

Authentication of authorizations is a part of registration or certification authority processing an application for a certificate for a legal entity or a device owned by a legal or private entity. In both cases, an issued certificate is a confirmation that a legal entity or a device are entitled to use a private key on behalf of a legal entity.

Authorization is delegated by a legal entity to either its employees or agents (account offices). Procedure of authorization authentication employed by Unizeto CERTUM - CCP comprises, apart from authorization authentication, the authentication of a private entity to whom these authorizations were delegated. This requirement can be omitted only if the entity is already Unizeto CERTUM - CCP subscriber. The authentication of private entity's identity is performed in the way described in Chapter 3.1.9.

Authorization authentication procedure comprises:

verification of authenticity of a submitted application,

checking the consistency of legal entity's data listed in the application against submitted documents,

(optional) verification of the proof of private key possession (if the application concerns a key pair for signature creation) and appropriateness of DN of a legal entity and a private entity who can act on behalf of this legal entity,

demanding that a document issued by at least one member of the board and confirming the authorization of the private entity must be submitted; the document must be certified by a notary,

contact with the private entity's direct superior and receiving the confirmation of the authorization delegated to this entity.

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,

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.

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 in accordance with the requirements stated in Table 3.3.

Table 3.3. Requirements concerning subscriber's identity verification for signing and encryption rekey

Certification policy	Requirements
Certum Level I	Subscriber can confirm his/her/its identity by authenticating directly with a certification authority, e.g. by means of TLS/SSL protocol. In this case the subscriber must possess a valid certificate and a private key associated with the public key included in the certificate.
Certum Level II	Authentication may be performed similarly to Certum Level I certificates, although the subscriber's identity must be verified in accordance with the procedure applied in initial registration (see Chapter 3.1.) at least every 5 years of the date of previous authentication performed in compliance with this procedure.
Certum Level III	Authentication may by performed similarly to Certum Level I certificates, although the subscriber's identity must be verified in accordance with the procedure applied in initial registration (see Chapter 3.1.) at least every 5 years of the date of previous authentication performed in compliance with this procedure.
Certum Level IV	Authentication may be performed similarly to Certum Level I certificates, although the subscriber's identity must be verified in accordance with the procedure applied in initial registration (see Chapter 3.1.) at least every 4 years of the date of previous authentication performed in compliance with this procedure.

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 validity period did not expire, 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 Unizeto CERTUM - CCP does not support recertification of the same key pair, due to security reasons. Such restriction does not apply certification authority key recerctification (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, but 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 operator. The subscriber's identification and authentication are performed analogically to the case of initial registration (see Chapter 3.1)

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

3.4. Subscriber's Identity Authentication in Certificate Revocation

Applications for revocation can be submitted by e-mail directly to an appropriate certificate issuer or indirectly to a registration authority. It s 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.

A subscriber who has lost an active private key (or it has been stolen) and secret of certificate revocation should follow the second method. Application for revocation must be certified by a registration authority. 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.). Authentication of a subscriber in a certification authority consists in verification of application authentication authenticity.

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.

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

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 demand to generate an asymmetric key 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 in accordance with the rule that keys cannot be activated by an unauthorized person.

4.1. Application Submission

Applications to one of certification authorities can be submitted by a subscriber or a registration authority operator.

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 or suspension. 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 can. In the second case, the operator can submit to a certification authority other subscribers' applications confirmed by the operator and in well-founded cases applications for revocation and suspension 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.

Unizeto CERTUM - CCP issues certificates solely on the basis of a application for registration, modification, rekey, certificate renewal or certificate modification submitted by a subscriber.

Applications might be submitted by different entities and might concern certificates whose application depends on the entities' needs:

private entity certificates – issued upon prior application submission,

private entity certificates – issued prior to application submission in the case when a certification authority or a registration authority generates a key pair and a certificate

and, by means of electronic identity card or other token, submits them to a private entity,

private entity certificates – issued upon an application submitted by a representative on behalf of the private entity,

private entity certificates – issued upon an application submitted by representatives or employees on behalf of the organization that delegated appropriate authorizations to them,

legal entity certificates – a legal entity is a certificate subject, provided that a private key is secured and might be used only by an authorized representative,

device certificates (applicable to e.g. servers) or certificates of applications owned by private entities (employees of organizations or their agents) authorized to use this device or application.

4.1.1. Registration Application

An application for registration is submitted to a registration authority indirectly or directly to a certification authority by a subscriber and contains at least the following information:

full name of the institution or the subscriber's family name and name(s),

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),

certificate type that is requested,

the identifier of certification policy on the basis of which the certificate is to be issued,

e-mail address,

a public key which is to be certified.

If a public key included in an application is a key for signature verification, the application must contain the proof of a private key possession.

Upon authentication of the identity of the subscriber (see Chapters 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 by the registration authority.

4.1.2. Certificate renewal, rekey 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,

lack of currently valid private key for an electronic signature creation,

upon explicit demand of a registration 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.

An application for certification, 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 new in the case of rekey) that is to be certified.

A part or whole of data contained in above application must be authenticated by application of an electronic signature, provided that a subscriber possesses a currently valid private key for signature creation. If a public key included in the application is a key verifying a signature, the application must include the proof of private key possession.

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 certificate revocation or suspension:

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 e-mail along with authentication, as a written version (as a letter, by fax) or orally (telephone call). In the last two cases, the certificate is suspended until the submitted request has been verified. Unizeto CERTUM - CCP does not suspend certificates in open systems .The suspension can be performed solely in closed corporate systems affiliated by Unizeto CERTUM - CCP.

In the moment of certificate suspension, registration authorities operators and the subscribers are notified about this fact.

4.2. Application Processing

Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP 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 concerning an agreement about certification services delivery (applicable to applications for registration), or automatically – if the comparison with Unizeto CERTUM - CCP database is sufficient.

Off-line submission of an application requires:

a subscriber's or an authorized representative's of a company attendance in person in a registration authority or certification authority, then filling in and making a handwritten signature on the application, signing an agreement about certification services delivery, and generating an identifier and a password by means of which the requester will be able to receive a certificate by means of WWW page (the last two actions concern only applications for registration) or generating PIN securing access to electronic card containing the keys and the certificate.

sending by mail the application and document copies (including these confirmed by a notary) necessary for the requester's identity verification; the verification is followed by generating of an identifier and a password, by means of which the requester will be able to obtain a certificate by means of WWW page (applicable to applications for registration) or generating a PIN securing access to electronic card containing the keys and the certificate; the identifier and the password or the card are sent back to the requester (the PIN submitted separately).

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 controlled by a certification authority. Moreover, if a certification authority operator decides that an application submitted to a request box requires that the subscriber must receive confirmation in a registration authority, this application is moved to a request confirmation box. The subscriber shall be notified about this fact by e-mail.

Off-line submitted applications, upon verification by a registration or certification authority operator, are always submitted to a **request box**.

4.2.1.1. 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 (the processing must be carried out in the presence of the requester if it is required by the certification policy) 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 Chapter3.1.8) and checks the proof of private key possession if it exists (see Chapter 3.1.9),

upon the 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 also verifies other data that are not listed in an application and required by Unizeto CERTUM - CCP to run a business.

4.2.1.2. Application Processing in Certification Authority

A certification authority retrieves applications out of a request box. 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 event 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 4.1.4.2), 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 4.3). 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 leas FIPS 140-1 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).

Upon certification authority request, the server can submit confirmation request of the certificate being processed. In such a case, the server;

sends the application to a request confirmation box;

sends the requester (by e-mail) information about the necessity of the application confirmation in one of indicated registration authorities .

Unizeto CERTUM - CCP 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 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 together with a private key) on the electronic identity card and submission of the certificate (by mail) to the subscriber's address (a PIN is sent in a separate letter). The issuance of the electronic identity card to the subscriber is recorded in certification authority database.

Detailed procedures of management of electronic identity cards are presented in the document "Registration Authority Book". The document is 'non-public' and accessible for authorized personnel and auditors.

Every issued certificate is published in Unizeto CERTUM - CCP 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.

Unizeto CERTUM - CCP publishes a certificate in the repository upon approval of the certificate by the subscriber (see Chapter 4.3)

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	7 days
Certum Level II	7 days
Certum Level III	7 days
Certum Level IV	7 days

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

4.3.2. Certificate Issuance Denial

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

Certificate issuance denial can occur:

if the subscriber's identifier (**DN**) coincides with other subscriber's identifier,

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 Unizeto 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 Unizeto CERTUM - CCP 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 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/install) or,

receive of a registered parcel (sent by Unizeto CERTUM) containing the certificate, or

lack of written denial, approved by a notary, of certificate acceptance upon the subscriber's receiving the certificate within 7 days of the reception of such certificate or PIN enabling the installation

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

Every accepted certificate is published in Unizeto CERTUM - CCP 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 read the agreement with Unizeto CERTUM - CCP that was made during registration procedure in a registration authority. In the case of electronic submission of the application, the subscriber automatically accepts future public key certificate at the moment of applying for this certificate.

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 CERTUM - CCP.

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.

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**, see Chapter 4.3),

in accordance with the agreement between the subscriber and Unizeto CERTUM - CCP,

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**, see Chapter 4.3),

in accordance with the agreement between the relying party and Unizeto CERTUM - CCP,

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

Unizeto CERTUM - CCP 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 revoked.

4.7. Certification and routine 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 request supplied by a subscriber can apply only to:

a currently valid certificate and certificate not revoked before,

the case if the subscriber has a current and valid private key for creating electronic signatures.

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 valid and not revoked 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 request does not have to be confirmed by Registration Authority – a subscriber can send it directly to a request box. Despite above, in situations when:

Registration Authority operator requests so,

subscriber does not have a current and valid private key for signing the request to be submitted,

the request has to be confirmed by Registration Authority. Personal attendance of subscriber in Registration Authority is necessary in this situation, and suitable identification and authorization procedures are to be executed (see in Chapter 3.1).

Key certification request has to be always confirmed in situations when:

Registration Authority operator requests so,

the subscriber does not have a current and valid private key for signing the request to be submitted,

the request was authorized by authorization key (secret),

it applies to the certification policy within which the subscriber does not have any valid certificate.

In other situations, key certificate request, after being signed by the subscriber, may be submitted directly to a certification authority.

Procedure for rekey request processing is equivalent to the procedure described in Chapter 4.1 and certification issuance procedure described in Chapter 4.2. As a result of processing of the latter:

the subscriber is notified of the new certificate issuance with the new serial number,

the subscriber is obligated to submit an authorized certificate acceptance confirmation to a certification authority,

a new certificate is published in the repository of a certification authority.

Unizeto CERTUM - CCP always informs subscribers (at least 7 days in advance) about forthcoming validity period expiry.

Certification and rekey procedure is also applicable to certificates of a certification authority, although in such a case all customers of the certification authority should be informed about procedure execution.

Unizeto CERTUM - CCP 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, except public key change.

Certificate modification:

is performed only on subscriber's demand and must follow submission of a suitable certificate modification request,

can be executed for certificate whose validity period has not expired and which has not been revoked.

Only following data can be modified:

public key en masse with modification of at least one of the following information,

subscriber's surname, i.e. due to marriage, divorce or law execution,

organizational unit or job position,

electronic mail address,

subscriber's roles or rights included in the certificate,

certificate extension or one of the extension content,

certificate identifiers, i.e. certificate policy identifiers,

types of transaction or their limit, which may be approved by the subscriber using a specific certificate.

Procedures of certificate modification requires authentication of request by a subscriber with his/her/its electronic signature. The subscriber has to possess a currently valid private key for creating an electronic signature. If the subscriber does not have such key, he/she/it has to undertake certification procedure described in Chapter 4.7.

Requests of certification modification have to be confirmed by a registration authority. It requires a subscriber to contact a registration authority and undergo identification and authentication procedures (Chapter 3.18).

The procedure of certificate modification request processing is alike the procedure described in Chapter 4.1 whereas the procedure of certificate issuance is the same as the procedure described in Chapter 4.2. As a result of processing of the latter:

a subscriber is notified of a new certificate issuance with a new serial number,

the subscriber is obligated to submit authorized certificate acceptance confirmation to a certification authority,

the new certificate is published in certification authority's repository.

If modification procedure is successful, a certificate being modified is revoked and placed on Certificate Revocation List (CRL). As a reason for revocation, ***affiliationChanged***[28] *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 practiced only in closed corporate systems affiliated by Unizeto CERTUM – PCA.

Durig 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

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

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, revocation – cannot (however, where it is not clearly specified the term "revocation" will also contain certificate suspension).

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.

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 is 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[29]; certificate revocation procedure is in this case executed by a subscriber,

the subscriber decides to terminate the agreement with Unizeto CERTUM - CCP (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,

the subscriber, the owner of a certified public key, requests revocation,

by its issuer, Unizeto CERTUM - CCP, for example when the subscriber does not comply with Certification Policy or resolutions of other documents signed by a certification authority,

[29] 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.

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 or ignores fees for services provided by a certification authority,

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 identity 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.

Additionally, a certification authority revokes suspended certificates which have not been activated or revoked for a month since the time of suspension.

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.

If subscriber's identity authentication is not successful, the certification authority rejects the revocation request and suspends certificate until the revocation request is closely examined.

4.9.2. Who can request certificate revocation

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

ea subscriber who is the owner of a certificate,

an authorized representative of a certification authority (in the case of Unizeto CERTUM - CCP this role is reserved for the security administrator),

a subscriber's sponsor[30], for example his/her employer; the subscriber has to be immediately informed about such fact,

a registration authority, 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.

[30] See **Glossary.**

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

create and manage a list of entities allowed to initiate such revocation,

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; 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) can be carried out in any registration authority, for example with a stamp and a hand-written signature of person known to Primary Registration Authority or by placing the pass phrase in the document, for which the answer is known only to the person requesting revocation; a request made by phone call is proceeded only after providing the correct pass phrase; after successful verification of the request primary registration authority prepares electronically confirmed revocation request and forwards it to a certification authority.

In the case of the first and the second method of revocation, a certification authority – after successful verification of the request – **revokes** the certificate, whereas in the third method the certificate is only **suspended**. 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 notifies the entity requesting certificate revocation about the revocation or decision about cancellation of the request, along with the reasons for the cancellation.

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 notifies, electronically or by regular mail, the entity requesting revocation about the revocation or decision about cancellation of the request, along with the reason for the cancellation,

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 identity card, upon certificate revocation, the card should be physically destroyed or securely wiped out. This operation is to be carried out by the holder of the ID 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

Unizeto CERTUM - CCP guarantees the following maximum grace period[31] for revocation request processing:

submitted electronically (with the correct format) or by phone call,

submitted in paper form,

as described in Table 4.2.

[31] 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.).

Tab. 4.2 Allowable grace period in certificate revocation request processing

Certification Policy	Allowable grace period
Certum Level I	No obligation to revoke
Certum Level II	Within 48 hours
Certum Level III	Within 48 hours
Certum Level IV	Within 48 hours

Certificate revocation requests submitted by certification authorities to the issuer of the certificate are processed within 30 minutes from reception of the requests, independently from the certification policy used for the certificate issuance.

Information concerning certificate revocation is stored in Unizeto CERTUM - CCP 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.

4.9.5. Reasons for certificate suspension

Certificate suspension may be performed in following situations:

on every demand of a subscriber, the owner of a certified public key, for example due to temporary absence of an employee in an organization (not exceeding one month),

if a certification authority receives revocation request and is not able to authenticate the identity of the institution requesting revocation (applies to requests submitted by electronic mail which were verified against private key possession),

data in paper document for revocation evoke reasonable suspicion,

revocation request was submitted by phone call,

notwithstanding above, the certification authority may immediately suspend the certificate if there are strong reasons to suspect that the certificate was issued not in accordance with regulations of this Certification Practice Statement; the certificate may remain suspended until the certification authority detects reasons to revoke the certificate,

other circumstances, requiring additional explanations from the subscriber.

Certificate suspension request may be submitted by means of a registration authority (it requires personal presence of the subscriber) or directly to a proper certification authority. In the first case, a request for suspension or paper document signed by the registration authority is submitted by the registration authority operator to the certification authority; in second case – the

subscriber signs the suspension request by himself/herself/itself and submits it electronically to the certification authority.

Certificate suspension request contains the same information as revocation request.

It is recommended that every suspension request (in electronic and paper form) should be submitted by means of a registration authority. Such a procedure allows more accurate identification of suspension reason and assessment of the risk arising from suspending the certificate (instead of its revocation).

4.9.6. Who can request certificate suspension

The following entities may request suspension of a subscriber's certificate:

the subscriber who is the owner of the certificate,

an authorized representative of a certification authority (in the case of Unizeto CERTUM - CCP this role is reserved for the security administrator) provided that , on the basis of received revocation request, it is not possible to verify the identity of the subscriber, or there are other reasons for certificate suspension,

the subscriber's sponsor[32], always in the situation when there are reasons to suspect the subscriber is using assigned resources in an inconvenient manner, for example flooding other persons with the large capacity information,

a registration authority which may request revocation on behalf of the subscriber or on its own, if it has information justifying certificate suspension.

Certificate suspension on the subscriber's demand requires careful checking whether the entity requesting suspension is indeed the subscriber of the certificate being suspended.

A subscriber, no matter whether he/she/it has been the initiator of the request or the request has been submitted by an authorized institution, has to be immediately notified of the certificate suspension.

Every request may 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 Primary Certification Authority as a non-electronic request (paper document, fax, phone call, etc).

4.9.7. Procedure of certificate suspension and unsuspension

Procedure of the certificate suspension is the same as the procedure of certificate revocation (see Chapter 4.9.3). Upon successful verification of a request, a certification authority changes the status of a certificate (i.e. the certificate is revoked and places it on Certificate Revocation List - as the reason for revocation **certificateHold** is provided – see Chapter.7.2.1).

The certification authority may cancel certificate suspension (by restoring it to the normal status) if the following conditions are fulfilled:

[32] See **Glossary**.

a subscriber requesting certificate unsuspension and a certification authority verify each other's identity,

the certification authority detects that the request has been submitted without proper authorization from the entity submitting the request, for example it has not been signed by the requester or verified by a registration authority,

the certification authority states that the reasons for certificate suspension are no longer applicable or they have not been not confirmed.

Certificate unsuspension is initiated only on subscriber's demand, after submission of an authorized unsuspension request. Such a request has to be preceded by provision of the proof that a private key corresponding to the certificate being unsuspended is secure and there has not been any, or there will not be any, attempts of its unauthorized usage.

Certificate unsuspension request may be submitted to a certification authority by fax, regular mail (after authorization by a registration authority) or supplied by the subscriber in person.

A certification authority reserves the right to reject subscriber's request for unsuspension if there are reasons to believe that the trustiness of the certification authority will be breached.

If unsuspension request is reasonable, the certification authority removes the certificate from Certificate Revocation List and it becomes fully usable (it regains its previous status).. If the suspension reasons turn valid or if the certificate remains suspended for more than a month, it is revoked, without the possibility to cancel the operation.

4.9.8. Limitation on suspension grace period

Unizeto CERTUM - CCP 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).

The above period does not include the time necessary to receive confirmation and to place the suspended certificate on Certificate Revocation List (see Chapter 4.9.9).

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 that is being a part of the Unizeto CERTUM - CCP issues separate Certificate Revocation List.

Every Certificate Revocation List is updated at least then once a month[33] if no additional certificate has been revoked within this period. Notwithstanding, the new CRL is published in the repository after every certificate revocation. If the reason for revocation is set to key compromise, the new CRL is issued immediately after processing the revocation request (see Chapter 4.9.4). Certificate Revocation List for CA-Certum authority is issued at least every 25

[33] 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 Unizeto CERTUM – CCP, value of this field is set to one month (except **CA-Certum**).

years, provided that there is no revocation of the certificate of one of the authorities affiliated by CA-Certum.

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

4.9.10. Certificate Revocation List checking availability

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

Certificate status verification may be based solely on CRL only in the cases if CRL issuance frequency periods, declared by Unizeto CERTUM - CCP, 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[34]     - 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

Unizeto CERTUM - CCP provides real-time certificate status verification service. This service is carried out on the basis of OCSP, described in RFC 2560[35]. 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 Unizeto 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[36],

revoked – meaning the certificate has been revoked,

---

[34] 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).

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

[36] See **Glossary**.

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 signed the agreement with Unizeto CERTUM - CCP about providing such services.

Certificate status is always provided in real-time (i.e. immediately after the certificate revocation) on the basis of Unizeto 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 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 Unizeto CERTUM - CCP, the appropriate information is placed immediately in CRL and obligatory 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 Unizeto 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 the material fact within the certificate issued for dubious authority is false,

the certification authority private key or its information system were revealed 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 Unizeto CERUM – PCA system and supervise Unizeto CERTUM - CCP users and personnel, all events occurring in the system are recorded.

It is required that every party – associated in any way with a subscriber's key certification procedures – 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 Unizeto CERTUM - CCP. Recorded events are subjected to backup procedures. Backup copies are retained outside Unizeto CERTUM - CCP localization.

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 (see Chapter 4.6.2).

Requirements, presented in Chapter 2.7, associated with guarantee of the system quality on the basis of a preaudit, governmental licences, contractual warranties or any other warranties, should not be mistaken with the term audit, described in this Chapter. Notwithstanding, they may have influence on the types of recorded events, if required due to party agreement.

In Unizeto CERTUM - CCP system, the security administrator is obligated to carry out a regular audit 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 Unizeto CERTUM - CCP security, is recorded in event logs and archived. Archives are encrypted and stored on unrewritable media type to prevent it from modification or forgery.

Unizeto CERTUM - CCP 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 journals 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 journal is automatically created. The previous event journal 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 Unizeto CERTUM - CCP 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 (see Table 4.3)[37].

Tab.4.3 List of events recorded in Unizeto CERUM – CCP system.

Recorded event	Place of origin		Certificate Policy name			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
SECURITY AUDIT						
Any modifications to audit parameters, i.e. frequency of event logging, types of event logged.	X	X	X	X	X	X
Every attempt to erase or modify event logging system.	X	X	X	X	X	X
Any event associated with electronic signature creation (electronic signature, cryptographic digest, authentication of entity or message, etc).	X	X	X	X	X	X

[37] Developed on the basis of *X.509 Certificate Policy for the Federal Bridge Certification Authority (FBCA)*, Version 1.12, December 27, 2000.

Recorded event	Place of origin		Certificate Policy name			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Retrieval of time stamp from trusted third party.	X	X	X	X	X	X
Commission and termination of event logging mechanisms.	X	X	X	X	X	X
Date and time of event journal archiving.	X	X	X	X	X	X
Event media used for storing event journals records capacity overloading.	X	X	X	X	X	X
Protection (electronic signature, access control) of current or archived event log from unauthorized modification, erasure or alteration.	X	X	X	X	X	X
Periodical event journal archival.	X	X	X	X	X	X
Every projected periodical and authorized review of current or archived event journal, including confirmation of event log integrity.	X	X	X	X	X	X
IDENTIFICATION AND AUTHENTICATION						
Successful and unsuccessful attempts to access any role in the system.	X		X	X	X	X
Modification to maximum amount of authentication attempts in the system.	X		X	X	X	X
Maximum amount of authentication attempts unsuccessful, while logging user into the system.	X		X	X	X	X
System administrator modifies authentication method, for example from password based to challenge/response token based.	X	X	X	X	X	X
LOCAL DATA ENTRIES						
Every data associated with security, entered into system (for example identity of the entity entering data, which should be accepted by this very entity).	X	X	X	X	X	X
REMOTE ENTRIES						
information associated with the security, broadcasted and received by the system.	X	X	X	X	X	X
OUTPUT AND EXPORT DATA						

Recorded event	Place of origin		Certificate Policy name			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Every successful or unsuccessful access requests to confidential or related with the security information.	X	X	X	X	X	X
KEY GENERATION						
Every key generation, for needs of a certification authority,a registration authority or a subscriber (entry to the event log is not obligatory in the case of one-time symmetric session key generation).	X	X	X	X	X	X
KEY LOADING AND STORAGE						
Loading of private key secrets into Hardware Security Module (HSM).	X	X	X	X	X	X
Certification authority, registration authority or a subscriber private key archival.	X	X	X	X	X	X
Every access to a private key stored in certification authority archives, on demand of the subject of the certificate, associated with this private key.	X	X	X	X	X	X
Every usage of any of the asymmetric key from a pair associated with a public key certificate, in cryptographic operations.	X	X	X	X	X	X
Every cancellation of key material, for example publicly available Diffie-Hellman key parameters.	X	X	X	X	X	X
Every erasure of certification authority or registration authority key.	X	X	X	X	X	X
Identity of an entity authorizing key management operations.	X	X	X	X	X	X
Identity of any entity having control over any key material (for example, key or keys secret, stored on removable media, for example cryptographic card).	X	X	X	X	X	X
Key, device and other media used for key storage management and administration.	X	X	X	X	X	X
Private key compromise.	X	X	X	X	X	X
ENTRIES ASSOCIATED WITH VALID PUBLIC KEY, THEIR ERASURE AND STORAGE						

Recorded event	Place of origin		Certificate Policy name			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Each modification associated with valid public keys, including amendment and erasure.	X	X	X	X	X	X
STORAGE OF CONFIDENTIAL KEYS						
Handwritten entries of usage of confidential keys, utilized in authentication procedures.	X	X	X	X	X	X
CONFIDENTIAL KEY AND PRIVATE KEY EXPORT						
Export of private keys and confidential keys (not applicable to one-time keys).	X	X	X	X	X	X
SUBSCRIBERS REGISTRATION						
Initial registration in the certification authority system.	X	X	X	X	X	X
Rejection of the initial subscriber registration due to identifiers duplication.	X	X	X	X	X	X
Creation and submission of authenticated subscriber registration request.	X	X	X	X	X	X
Subscriber's registration on the basis of authenticated registration request.	X	X	X	X	X	X
Record of unique subscriber's identification data.	X	X	X	X	X	X
Place of storage of the copies of subscriber's request and identification documents.	X	X	X	X	X	X
Identity data of the operator accepting subscriber's application (request).	X	X	X	X	X	X
Identity data of the certification authority being an addressee of authenticated request.	X	X	X	X	X	X
Identity data of the registration authority authorizing the request.	X	X	X	X	X	X
CERTIFICATE REGISTRATION						
Every certificate registration request, including rekey request and certificate renewal.	X	X	X	X	X	X

Recorded event	Place of origin		Certificate Policy name			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
In the case of request acceptance the records of issued certificate in case of request rejection – reason for rejection (for example, incorrect data, lack of system administrator acceptance).	X	X	X	X	X	X
Every event associated with certificate request acceptance.	X	X	X	X	X	X
Every event associated with certificate acceptance by the subject of a certificate.	X	X	X	X	X	X
CERTIFICATE ISSUANCE						
Every events associated with signing certificate and infrastructure certificate life cycle management.	X	X	X	X	X	X
Every event associated with signing key life cycle management.	X	X	X	X	X	X
Every event associated with subscriber's certificate life cycle management.	X	X	X	X	X	X
Every certificate issuance or publishing.	X	X	X	X	X	X
Every submission of issued certificate to a subscriber.	X	X	X	X	X	X
CERTIFICATE REVOCATION						
Every certificate revocation request.	X	X	X	X	X	X
Every issuance of a new CRL.	X	X	X	X	X	X
Every submission of information on the certificate revocation to the subscriber.	X	X	X	X	X	X
HARDWARE SECURITY MODULE LIFE CYCLE MANAGEMENT						
Delivery of a device by a manufacturer or vendor.	X	X	X	X	X	X
Insertion or removal of a device into/form the safe.	X	X	X	X	X	X
Installation and activation of a device as well as preparation for usage.	X	X	X	X	X	X
Removal of a device from service.	X	X	X	X	X	X
Preparation of aadevice for service or reparation.	X	X	X	X	X	X
Unit erasure and destruction.	X	X	X	X	X	X

Recorded event	Place of origin		Certificate Policy name			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
CHANGES OF CERTIFICATE STATUS						
Acceptation or rejection of certificate status modification request (including certificate suspension).	X	X	X	X	X	X
CHANGES OF INFORMATION SYSTEM CONFIGURATION						
Every change in information system configuration having influence on system security.	X	X	X	X	X	X
USER ACCOUNT MANAGEMENT						
Added or removed roles and user's accounts.	X	X	X	X	X	X
Modification of access rights resulting from roles or user's account.	X	X	X	X	X	X
CERTIFICATE PROFILE MANAGEMENT						
Every modification in certificate profile	X	X	X	X	X	X
Every event related to certificate status modification request, including accepted and rejected.	X	X	X	X	X	X
REVOCATION PROFILE MANAGEMENT						
Every modification to revocation profile management.	X	X	X	X	X	X
Every event related to certificate status modification request, including accepted and rejected.	X	X	X	X	X	X
CERTIFICATE REVOCATION LIST PROFILE MANAGEMENT						
Every modification to CRL profile.	X	X	X	X	X	X
CERTIFICATE POLICY AND CERTIFICATION PRACTICE STATEMENT MANAGEMENT						

Recorded event	Place of origin		Certificate Policy name			
	CA	RA	Certum Level I	Certum Level II	Certum Level III	Certum Level IV
Acceptance or rejection of changes in Certificate Policy or Certification Practice Statement.	X	X	X	X	X	X
CERTIFICATION AND REGISTRATION AUTHORITY REGISTRATION						
Acceptance or rejection of new certification or registration authority registration (journal entry includes contents of the request).	X	X	X	X	X	X
PHYSICAL ACCESS / LOCATION SECURITY CONTROLS						
Access of personnel to personnel locations.	X	X	X	X	X	X
Access to certification authority servers.	X	X	X	X	X	X
Known or suspected physical security violations	X	X	X	X	X	X
ANOMALIES						
Reasons of software errors.	X	X	X	X	X	X
Unsuccessful software integrity verification test.	X	X	X	X	X	X
Attack against the network (suspected or confirmed).	X	X	X	X	X	X
Damages to the hardware.	X	X	X	X	X	X
Power cut.	X	X	X	X	X	X
Malfunction of auxiliary power system (UPS).	X	X	X	X	X	X
Obvious and credential error to network service or network access violation.	X	X	X	X	X	X
Certificate Policy violation.	X	X	X	X	X	X
Certification Practice Statement violation.	X	X	X	X	X	X

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

Access to event journal entries (logs) is granted solely to security administrators, certification authority administrators and auditors (see Chapter 5.2).

4.10.2. Frequency of event journals processing.

Event journal entries should be reviewed in details at least once a month. Every event of significant importance should be explained and described in an event journal. Event journal 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 journal.

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 journals are stored in archives, and may be accessed only *off-line* on a designated workstation.

Archived journals are retained for at least 2 months.

4.10.4. Protection of event journals

Weekly every entries in event journals are subjected to backup on a magnetic tape. After surpassing accepted for specific journal number of entries, journal 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 administrator.

An event journal may be reviewed solely by the **security administrator**, **certification authority administrator** or an **auditor**. Access to the event journal is configured in such a way that:

only entities representing one of the above groups have the right to read journal entries,

only the security administrator 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 journal protection are implemented in a manner that even after the journal archival it is impossible to delete entries or erase the journal before surpassing an estimated period of journal retention (see Chapter 4.10.3).

4.10.5. Procedures for event journal backup

Unizeto CERTUM - CCP security procedures require that the event journal and activity records - created when reviewing this journal by the security administrator, system administrator or an auditor - such as activities on the journals, collective statements, analysis, statistics, detected threats etc, should be subjected to monthly backup. These backups are retained in auxiliary seat of Unizeto CERUM – PCA. Backup copies may be signed with a timestamp.

4.10.6. Notification to event responsible entities

Module for analysis of the event journal implemented in the system examines current events and automatically notifies about suspected or security violating activities. In the case of activities having influence on the system security, the security administrator and certification

authority 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, affiliated registration authorities (in the case of delegation of rights to registered subscribers) and the repository 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 Unizeto CERTUM - CCP audit.

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

An external institution carrying our security audit executes this activity according to guidelines described in PN ISO/IEC 13355 and ISO/IEC 17799.

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 CRL's, keys, used by certification and registration authorities, and whole correspondence within Unizeto CERTUM - CCP and with the subscribers should be subjected to archive.

Unizeto CERTUM - CCP 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 a 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 max. 25 years 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 identified, rate 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 Unizeto CERTUM - CCP location.

It is recommended to encrypt and timestamp the archive. A key used for archive encryption is managed by the certification authority 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 authority, a registration authority and the repository information system,

received requests and issued decisions in an electronic form, submitted by a subscriber 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 destruction,

history of the subscribers keys, from their generation to destruction, if the keys are subjected to archive in certification authority databases,

internal and external correspondence (paper and electronic) between Unizeto CERTUM - CCP, its subscribers and relying parties in the operation of certificate suspension and unsuspension.

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 Unizeto CERUM – PCA 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 CD-ROM disks, still available *on-line*. In the seventh year (six years after certificate issuance) all information regarding subscribers and their certificates is stored on CD-ROM disk and 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,

certification authority and registration authority keys are stored – after expiration of corresponding certificate – on unrewriTable media and encrypted with the key, controlled by the security administrator; archived keys are available only *off-line*.

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 time presented in Tab.4.4. After expiration of the declared retention period, archived data are destroyed. In the case of key and certification erasure, an appropriate procedure is executed with particular attention.

Tab.4.4 Minimal archive retention periods

Certificate Policy	Minimal retention period
Certum Level I	25 years
Certum Level II	25 years
Certum Level III	25 years
Certum Level IV	25 years

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 Unizeto CERTUM - CCP. 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 authority 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 Unizeto CERTUM – CCP,

event journals.

Method for backup copy creation has significant importance for quickness and cost of the certification authority restoration upon malfunction or destruction of the system. Unizeto CERTUM - CCP 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 copies are protection if there is no possibility to synchronize primary and auxiliary facility; backup copy should cover entire and current status of the Unizeto CERTUM - CCP system; the facility should perform full restoration of Unizeto CERTUM - CCP system function within 48 hour.

Detailed backup copy creation procedures and system recovery after malfunction are disclosed in "Backup Copy Creation and Emergency System Restoration Book". The document 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 Time Stamp Authority (TSA), having a certificate issued by the operational

certification authority affiliated by **CA-Certum**. Timestamp service is available at Unizeto CERTUM - CCP.

4.11.6. Access procedures and archived information verification

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

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 Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP WWW page and broadcasted by electronic mail, submitted to every subscriber of a certification authority, whose keys are subjected to changeover. Additionally, in the case of **CA-Certum** key changeover, information about changeover should 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 Unizeto CERTUM - CCP 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 Unizeto CERUM – PCA 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 Unizeto CERTUM - CCP, takes into consideration the following threats influencing availability and continuity of the provided services:

physical corruption to the computer system of Unizeto CERTUM - CCP, including network resources corruption – this threat addresses corruptions originating from emergency 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 Unizeto CERTUM - CCP interests. It primary addresses power cuts and damages of the network connections,

corruption of a part of the intranet, used by Unizeto CERTUM - CCP 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 Unizeto CERUM – PCA must include:

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. System continuity 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 Unizeto CERTUM - CCP are created and archived; every backup copy is retained in secure location outside Unizeto CERTUM - CCP,
- once a day, 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 in secure location outside Unizeto CERTUM - CCP facility,
- once a week, following the procedures disclosed in Chapter 4.11.4, every server backup copy is created. This copy includes all submitted requests, entries to event journals, issued, renewed and revoked certificates; copies are retained in secure location outside Unizeto CERTUM - CCP facility,
- Unizeto CERTUM - CCP 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 on a testing environment, performed in strict accordance with disclosed procedures. Every modification in the system requires Unizeto CERTUM - CCP security administrator'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 occured.

Emergency system. In the case of corruption restraining Unizeto CERTUM - CCP functionality, within 24 hours an emergency facility will be activated, which should substitute all significant function of a certification authority until the prime 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 preventing Unizeto CERTUM - CCP activity, it is possible to:

- activate emergency facility similar to Unizeto CERTUM - CCP prime facility activation,
- process all accumulated and unprocessed requests,
- process in real-time requests submitted by subscribers until restoration and recover of the prime facility.

Backup copy creation system. Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP. Copies are created daily, weekly and monthly and they are 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. Backup copies and their archives are retained outside processing system facility.

Additional services. To prevent the system from power cuts and to secure service continuity, emergency power sources (UPS) are employed. They provide at least 6 hours of continuous system operation from the moment of power cut. 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 Unizeto CERTUM - CCP) 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 administrator or certification authority administrator should:

change all previously used passwords,

remove and reset all the access rights to the system resources,

change 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 should be changed,

review network security policy of Unizeto CERUM – PCA and physical access to locations and the system components,

inform 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 if 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,

prepare an agreement (for example, with another certification authority, compare Chapter 4.11.2), guaranteeing protection of accumulated data,

pay compensations (not exceeding fees for issuance and storage of certificates) to the subscribers whose unexpired and unrevoked certificates are revoked before their expiration date.

4.14.2. Certificate issuance by the successor of terminated certification authority

To provide continuity of the certificate issuance services to subscribers, a terminated 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 – **CA-Certum** (in the case of termination of services of **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**) or to the institution which the agreement was signed up with (in the case of termination of services of **CA-Certum**).

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 Unizeto CERTUM - CCP for example in the time of key generation, entity authenticity verification, certificate issuance and publication, certificate revocation, audit and backup copy creation. Detailed description of the implemented security measures and controls is available at a confidential and not publicly available version of Certification Practice Statement.

5.1. Physical security controls

5.1.1. Unizeto CERTUM - CCP physical security controls

Network computer system, operator's terminals and information resources of Unizeto CERTUM - CCP 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

Unizeto CERTUM - CCP is located in the Unizeto Sp. z o.o. seat, at the following address: Szczecin, Królowej Korony Polskiej St. 21 .

5.1.1.2. Physical access

Physical access to the seat and Unizeto CERTUM - CCP area is controlled and monitored by the integrated alarm system. Manned reception operates 24 hours a day. Fire prevention system, flood prevention system, intrusion detection system and emergency power system are employed.

Manned reception operates 24 hours a day. Unizeto Sp z o.o. facility and Certification Authority are publicly available every working day between 8.00 and 16.00. In the remaining time (including non-working days), the facility is available only to persons authorized by the Management of Unizeto Sp. z o.o. and known by name and surname by the security officers.

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

Areas occupied by Unizeto CERTUM - CCP are divided into:

computer system area,

operators and administrators areas,

developers and programmers area.

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 security administrator, certification authority administrator and the system administrator.

Monitoring of the access rights is carried out on the basis of identity cards and appropriate readers, mounted next to the area entry. Every entry and exit from the area is automatically recorded in the event journal.

Access to the operators and administrators area is enforced through the use of an electronic card and their appropriate reader. 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 Unizeto CERTUM - CCP personnel and authorized individuals. Additionally, the latter are not allowed to occupy the area unescorted. The only exception concerns the individuals occupying Unizeto CERTUM positions who are classified as **trusted**.

The developers and programmers area is protected in a manner similar to the protection of the operators and administrators area. Unescorted individuals are allowed to occupy the area. Programmers and developers do not have an access to sensible information. If such access is necessary, it requires presence of the security officer in the developers and programmers area. Projects being implemented and their software are tested on the development version of Unizeto CERTUM - CCP and / or its model.

5.1.1.3. Power and air conditioning

The operators and administrators area, as well as the programmers and developers area, are air conditioned only during working time. From the moment of power cut, emergency power source (UPS) allows one (1) hour of undisturbed work.

Working environment in the computer system area is monitored continuously and independently from other areas. Emergency power source (UPS) allows six (6) hours of continuous work from the moment of power failure.

5.1.1.4. Water exposure

In the computer system area humidity and water detecting sensors are installed. This sensors are integrated with the security system of UNIZETO building. Reception personnel are notified of the hazards and is obligated to notify appropriate public services, Unizeto Sp. z o.o. security administrator and Unizeto CERTUM - CCP administrator.

5.1.1.5. Fire prevention

Fire prevention and protection system is installed in Unizeto Sp. z o.o. seat and complies with local standards and regulations for fire safety. Sprinkle system, activated automatically in the case of violently spreading fire, is installed.

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.

5.1.1.7. Waste disposal

Paper and electronic media containing information possibly significant for Unizeto CERTUM - CCP 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 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, for example cryptographic cards).

5.1.1.8. Offsite backup storage

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

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

5.1.2. Registration authority security controls

Computers registering subscriber's requests and issuing their confirmations should be 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.

Every registration authority has to posses hardware security module.

5.1.2.1. Site location and construction

Registration authorities of Unizeto CERTUM - CCP are located in the following sites:

Primary Registration Authority (PRA) is located in the operators and administrators area in Unizeto CERTUM - CCP (see Chapter 5.1.1.1),

addresses of other registration authorities are available by electronic mail 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 specially designated to provide their services. Access to such areas should be monitored and limited to authorized individuals associated with the activity of the registration authority (registration authority operators, administrators and agents) and registration authority customers.

5.1.2.3. Power and air conditioning

Registration authority location should be equipped with emergency power source system (UPS), allowing several minutes of continuous work of the system from the time of power cut. After UPS system exceeds its capacity power, generators of Unizeto CERTUM are automatically started to provide power for the computer system. Air conditioning is not required.

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 are held in the safes located in the certification 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 4.6), destroyed in special shredding devices.

In the case of cryptographic keys and PIN 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, for example cryptographic cards). 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

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

5.1.2.9. Emergency backup copy and archive storage

Archival data, emergency backup copies and other sensitive information is held in boxes of the safe, accessible solely to two authorized Unizeto CERTUM - CCP employees.

5.1.3. Subscriber security

Subscriber have to protect their system access password and Personal Identification Number (PIN). If selected password or PIN is complicated and hard to remember, it might be written down. In this situation, the subscriber has to remember about storage of the written password in secure location (the safe, accessible solely to the authorized personnel).

Certificate owners should not leave their workstation and its installed software unattended while it is in the unsecured cryptographic state, i.e. password or PIN has been entered or a private key was loaded into cryptographic area.

In the case of a private key (after encryption with a subscriber's password) storage on unsecured media, for example floppy disk, the media should be protected from unauthorized access, similarly to a subscriber's purse, credit card or software licence. One of the methods for protection may be a safe.

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 Unizeto CERTUM - CCP and in registration authorities and institutions being the subscribers of certificates. This Chapter also describes responsibilities and duties associated with each defined role.

5.2.1. Trusted roles

5.2.1.1. Trusted roles in Unizeto CERTUM - CCP

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

PKI Services Development Team – determines direction of Unizeto CERTUM development, implements and manages Certification Policy as well as Certification Practice Statement,

Unizeto CERTUM - CCP Operational Team – responsible for standard operation of Unizeto CERTUM - CCP,

Security administrator – initiates installation, configuration and management of software applications and hardware (including network resources) of Unizeto CERTUM - CCP; initiates and suspends services provided by Unizeto CERTUM - CCP; manages the administrators, initiates and supervises key and shared secret generation; assigns rights in the field of security and user's access privileges; assigns passwords for new users' accounts; reviews event journals; supervises service tasks; supervises internal and external audits; receives and answers post-audit reports; supervises post-audit deficiency removal,

Certification authority administrator – oversees certification authority operators; installs userware; configures the system and the network; activates and configures network protections; creates accounts for Unizeto CERTUM - CCP users; reviews system logs; verifies compliance of Certification Policy and Certification Practice Statement; generates shared secrets and keys; manages Certificate Revocation List; creates emergency backup copies; modifies server names and addresses,

Certification authority operator – retrieves subscribers' certificates; revokes, suspends and unsuspends subscribers' certificates; requests subscribers to certify their applications in registration authority; provides continuity of backup copy and archive of database and system logs creation; manages databases; has access to confidential information about subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies outside Unizeto CERTUM - CCP seat,

System administrator – installs hardware and software for operating system; initially configures the system and network resources,

Repository administrator – manages folders of Unizeto CERTUM - CCP available to the public, in particular creates and updates contents of repository folders, creates WWW page and manages links,

Auditor – responsible for review, archive and management of event journals (in particular verification of their integrity) and performance of internal audit, compliance of a certification authority with this Certification Practice Statement; this responsibility

extends also on every registration authority, operating within Unizeto CERTUM - CCP,

Technical support (service) – provides continuity of computer system and network operation; maintains and the restores system and network resources after malfunction

Described duties segregation prevents abuses associated with Unizeto CERTUM - CCP system usage. Every user is assigned only the rights arising form the role a given user has and related responsibility.

The presented roles may be combined, modified or denied trusted clause, provided it results in at least four distinct roles. The following roles may cover: common operations, carried out by the computer system of Unizeto CERTUM - CCP, management and audit of such operations and management of changes significant for Unizeto CERTUM - CCP system, i.e. its security policy, procedures or personnel.

Apportion of responsibility between described roles may be as follows:

Security administrator – initiates installation, configuration and software and hardware support (including network resources) of Unizeto CERTUM - CCP; initiates and suspends services provided by Unizeto CERTUM - CCP; supervises administrators; initiates and oversees key and shared secret generation; takes part in cryptographic module activation and loading of operators' keys (in their presence); assigns rights in the field of security and user's access privileges; assigns passwords to new users' accounts; performs system log audit weekly; supervises service tasks; supervises Unizeto CERTUM - CCP personnel;

Certification authority administrator – installs hardware and software of operating system; installs application software; configures system and network resources; activates and configures security resources; creates users' accounts in Unizeto CERTUM computer system; changes names and addresses of servers; generates shared secrets and keys; manages Certificate Revocation List; creates emergency recovery copies;

Certification authority operator – retrieves subscribers' certificates; revokes, suspends and unsuspends subscribers' certificates; provides continuity of backup copy and archive creation of databases and system logs; manages databases; has access to confidential information concerning subscribers but is not allowed to physically access any other system resources; transfers archive copies and current backup copies outside Unizeto CERTUM - CCP seat.

*The role of the **auditor** cannot be combined with any other role in Unizeto CERTUM - CCP system. No entity acting any role different than an auditor may take auditor's responsibilities.*

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

5.2.1.2. Trusted roles in registration authority

Unizeto CERTUM - CCP has to be make sure that the personnel of a registration authority recognize their responsibility, arising from identification and authorisation 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 software; 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 secret administrator, erases excessive information;

Secret administrator – supervises and transfers secrets (cryptographic keys and other protected data) to registration authority operators; takes part in cryptographic module activation and operators' keys loading (in their presence); transfers and activates operators' identity cards (if the cards are subjected to blockage); mediates between a registration authority and a certification authority;

Operator – verifies subscriber's identity and correctness of provided request; issues confirmation of requests and provides them to a certification authority; in the case of Primary Registration Authority (PRA) he/she generates keys and 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 which are subjected to erasure by the order of the secret administrator and in the administrator presence,

Point Of Registration 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, supervise registration authority audit. The agent can mediate between the secret administrator, a registration authority and the system administrator.

The secret administrator must stay in touch with individuals acting as the security administrator and the certification authority administrator within Unizeto CERTUM - CCP.

5.2.1.3. Subscriber's trusted roles

The subscriber may assign an individual (operator) operating application supporting electronic data interchange, e.g. with Unizeto CERTUM - CCP. The individual is personally responsible for signing, encrypting and submitting of a message. He/she can also collect data for electronically submitted messages, although this operation, due to practical reasons, may be carried out by the personnel with lower privileges.

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 at least two persons, acting as the security administrator and the system administrator. Certification authority key generation process may be also observed by shared secret holders who retain their part of the key in secure location.

Presence of the security administrator, certification authority administrator and an appropriate number of persons, being holders of a shared secret (including a private key for certificate and CRS signing) are required when loading certification authority cryptographic key into hardware security module. Loading of cryptographic keys into registration authority hardware security module requires presence of the secret administrator and a registration authority operator.

Any other operation and role, described within Unizeto CERTUM - CCP or connected with a subscriber, may be performed by a single person, assigned for such an operation or role.

5.2.3. Identification and Authentication for Each Role

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

placement on the list of persons allowed to access Unizeto CERTUM - CCP locations,

placement on the list of persons allowed to physically access system and network resources of Unizeto CERTUM - CCP,

issuance of confirmation authorizing to perform the assigned role,

assignation of an account and a password in Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP system software, operating system and controls.

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

5.3. Personnel controls

Unizeto CERTUM - CCP has to make 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 Polish nationality,

has signed an agreement describing his/her role in the system and his/her corresponding responsibilities,

has been subjected to advanced training on the range of obligations and tasks, associated with his/her position,

has been trained in the field of personal data protection and confidential and private information protection,

has signed an agreement containing clause concerning sensitive (from the point of view of Unizeto 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. Personnel background, qualification, experience and required confidentiality clauses

It is recommended that the personnel employed in Unizeto CERTUM - CCP or in a registration authority and performing trusted role should obtain a certificate of trustiness, issued by a security agent. The certificate is not required in the case of a person not performing a trusted role.

Performance of trusted role of a member of PKI Service Development Team, the security administrator, the certification authority administrator and secret administrator (within registration authority) authorizes the access to information classified as *non-public*[38].

Procedures for access to undisclosed information and personnel trustiness verification check procedures comply with *Confidential and Private Information Protection law of 22nd January, 1999*, particularly with Chapters 36 and 37, corresponding to the so called common procedures.

On secret administrator's request, persons performing trusted roles in a registration authority confirming requests for certificate issuance may be exempted from verification check. The exemption must be accepted by the security agent of Unizeto CERTUM - CCP.

5.3.2. Verification check procedures for roles not considered as trusted

This Certification Practice Statement does not state any requirements in this area.

5.3.3. Training requirements

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

regulations of Certification Practice Statement,

regulations of Certification Policy,

regulations of "*Registration Authority Book*",

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, corruption to a certification authority.

Upon completion of the training, participants sign a document confirming their familiarization with Certification Practice Statement, Certification Policy and acceptance of associated restrictions and obligations.

5.3.4. Retraining Frequency and Requirements

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

---

[38] Classification of information as *non-public* means that its unauthorized reveal may cause loss or disruption to the law-protected interests of a private person or an organization [11].

5.3.5. Job rotation

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

5.3.6. Sanctions for Unauthorized Actions

In the case of a discovery or suspicion of unauthorized access, the system administrator together with the security administrator (in the case of Unizeto CERTUM employees) or a registration authority administrator (in the case of registration authority employees) may suspend the perpetrator's access to Unizeto CERTUM or the registration authority system. Disciplinary actions for such accidents should be described in suitable regulations and should comply with law in force.

5.3.7. Contract Personnel

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

5.3.8. Documentation Supplied to Personnel

Unizeto CERTUM - CCP and the registration authority have to provide their personnel with access to the following documents:

Certification Policy,

Certification Practice Statement,

"Registration Authority Books",

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 and usage

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

CA-Certum 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 purposes of public keys of certification authorities **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** and **CA-Certum Level IV** signing, Certificate Revocation List issuing 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: **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** and corresponding to public keys included in certificates issued by **CA-Certum** for each of the 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 **CA-Certum**) or certificate (in the case of **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**),

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

CA-Certum certification authority keys and **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** and **CA-Certum Level IV** and other subordinate authorities keys are generated within Unizeto CERTUM - CCP seat, in the presence of selected, trusted group of persons (the security administrator and acertification authority administrator have to be members of this group). The group is required only in the case of certificate and CRL signing key generation. Operational key pair may be generated in the presence of the security administrator and the certification authority administrator.

Key pairs of certification authorities operating within Unizeto CERTUM - CCP are generated on designated, authenticated workstation and connected to hardware security module, complying with the requirements of FIPS 140-2 Level 3 or superior requirements.

Certification authorities key pair generation process is similar to the accepted procedure for key pair generation in Unizeto CERTUM - CCP. 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.

A detailed process of certification authority key pair generation is described in "Procedures for Unizeto CERTUM Certification Authority Key Pair Generation". This document is classified as "non-public" and is available solely for the security administrator and an auditor.

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 secret administrators) by means of authenticated software supplied by a certification authority and connected with certified hardware security module complying with at least FIPS 140-2 Level 2.

Generally, every subscriber generates his/her/its key pair by himself/herself/itself . The generation may also be requested from a certification authority.

Unizeto CERTUM – CCP 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 3 (see Chapter 6.1.2) is employed.

A detailed description of certification authority key pair generation is disclosed in "Registration Authority Book". This document is classified as "non-public" and is available only to personnel of Unizeto CERTUM.

6.1.1.1. Procedures of generation of CA-Certum initial keys

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

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 key pair generation 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. CA-Certum rekey procedure

CA-Certum 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 (self-certificate) signing. It is based on the issuance of special certificates by **CA-Certum**. The certificates enable subscribers who have already installed an expired self-certificate of **CA-Certum** 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, **CA-Certum** deploys a procedure, owing to which new key pair generation will secure (authenticate) a new public key with the use of the former (previously used) private key and vice-versa (an old public key is secured with a new private key). It means that as a result of update of the self-certificate of certification authority, **CA-Certum**, apart from a new self-certificate, two additional certificate 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 latter **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 a key pair for **CA-Certum** update (rekey), designated to certificate and CRL signing, 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 **CA-Certum**, 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 **CA-Certum**, signed with new private key $\mathbf{K^{1}_{GPK(1)}}$ (**self-certificate OldWithNew**),

creation of a self-certificate containing new public key of **CA-Certum**, 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 and, optionally, placement of the cryptographic digest of the new public key in reliable newspapers.

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), **CA-Certum** authority signs new subscriber's 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 **CA-Certum** (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 **CA-Certum**. 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 **CA-Certum** 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 certification authority key update (rekey) of **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** and **CA-Certum Level IV** authorities are executed similarly as for **CA-Certum** (see Chapter 6.1.1.3) except one step: **certificate NewWithNew** is issued by **CA-Certum** authority.

6.1.1.4. CA-Certum and subordinate authorities certificate renewal procedure

Certificates belonging to CA-Certum authority and other authorities may be subjected to renewal. 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

If the subscriber's key pair is generated centrally by a certification authority, the keys may be delivered to the subscriber in one of the following ways:

carried out with the usage of key agreement scheme, on the basis of Diffie-Hellman's key pair owned by the certification authority; the certification authority generates a session key (symmetric), encrypts the generated keys and submits them to the subscriber *on-line*,

keys are stored inside a token (e.g. an electronic identity card) or on a floppy disk (only **Certum Level I**, in such a case keys are encrypted and stored in PKCS#12 format) and are delivered to the subscriber personally or by means of registered mail; data for the card activation (including PIN) or key decryption (password) are submitted separately from the media containing the key pair; the issued cards are personalized and registered by the certification authority.

Unizeto CERTUM – CCP guarantees that in any moment after generation of a key pair on subscriber's demand the keys will not be used for creating an electronic signature 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[39] (CRS) supported by a certification authority, a registration authority and a subscriber.

Currently, Unizeto CERTUM - CCP certification authority 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).

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

Submission of a public key is expendable in the case when a key pair is generated on subscriber's demand or registration authority operator's 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 **CA-Certum** certification authority, certificates have a form of self-certificates.

Unizeto CERTUM - CCP certification authorities distribute their certificates in two different methods:

placement in the publicly available repository of Unizeto CERTUM - CCP; retrieval of the certificates requires the subscribers to visit web page available at http://www.certum.pl/repository,

distribution together with the software (web browsers, email clients, etc.),which allows usage of services offered by Unizeto CERTUM - CCP.

In the case of Unizeto CERTUM - CCP 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 6.1.1.2 and 6.1.1.3.

6.1.5. Key Sizes

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

Tab.6.1 Size of keys used

Key onwer	Prime key usage			
	RSA for certificate and CRL signing	RSA for message signing	RSA for key exchange	Diffie-Hellman
CA-Certum	2048 bit	–	–	–
CA-Certum Level I	1024 bit	–	–	–
CA-Certum Level II	1024 bit	–	–	–
CA-Certum Level III	1024 bit	–	–	–
CA-Certum Level IV	1024 bit	–	–	–
Registration authority operator	–	1024 bit	–	–
Private entities and their hardware	–	1024 bit	1024 bit	1024 bit
Legal entities and their hardware	–	1024 bit	1024 bit	1024 bit

6.1.6. Public Key Parameters Generation

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. Parameter Quality Checking

The creator of a key is responsible for checking parameter quality of the generated key He/she 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 exponents).

Parameter quality checking, covering for example checks of primeness 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

Allowable methods for key generation depend on applicable Certification Policy and presented in Table 6.2.

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

Registration authority operators' keys are generated by means of hardware security modules of lesser requirements (than described 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	Hardware or software
Certum Level II	Hardware or software
Certum Level III	Hardware or software
Certum Level IV	Hardware or software

6.1.9. Key Usage Purposes

Allowed key usage purposes are described in **KeyUsage** field (see Chapter 7.1.1.2) of standard extension of a certificate complying with X.509 v3. This field has 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, as well as 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**, **Certum Level II**, **Certum Level III** and **Certum Level IV** 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. If a certification authority (see Chapter 6.1.1) generates a key pair on authorized subscriber's demand, it has to deliver it securely to the subscriber and enforce the subscriber to protect 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 requirements

Tab.6.3 Minimal requirements imposed on hardware security modules

Certification Policy	Certification authority	Subscriber	Registration authority
Certum CA	FIPS 140-2 Level 3 or higher hardware	–	–
Certum Level I	FIPS 140-2 Level 2 or higher hardware	–	FIPS 140-2 Level 1, ITSEC E2 or higher hardware
Certum Level II	FIPS 140-2 Level 2 or higher hardware	FIPS 140-2 Level 1, ITSEC E2 or higher hardware	FIPS 140-2 Level 1, ITSEC E2 or higher hardware
Certum Level III	FIPS 140-2 Level 2 or higher hardware	FIPS 140-2 Level 1, ITSEC E2 or higher hardware	FIPS 140-2 Level 2, ITSEC E3 or higher hardware
Certum Level IV	FIPS 140-2 Level 2 or higher hardware	FIPS 140-2 Level 1, ITSEC E2 or higher hardware	FIPS 140-2 Level 2, ITSEC E3 or higher hardware

Electronic signature creation and data encryption comply with PKCS#7 requirements.

Private keys (as well as public keys) may have one of the following states (according to ISO/IEC 11770-1 standard):

waiting for activation (ready) – key has already been generated but is not available for usage (the present date is not yet the date of beginning of the certificate validity period),

active – key may be used in cryptographic operations (for example, for electronic signature creation), the present date is within the certificate validity period, key has not been was not revoked,

inactive – key in this state may be used solely for electronic signature verification or decryption operations (the subscriber is not allowed to use this private key to create electronic signature – validity of the key expired; in the case of a public key, the subscriber is not allowed to encrypt information); the present date is beyond the certificate validity period.

6.2.2. Private Key Multi-Person Control

Multi-person control of a private key applies to private keys of certification authorities **CA-Certum** and **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** used for certificate and CRL signing, as well as other cryptographic operations, e.g. message encryption.

Unizeto CERTUM - CCP 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

Issuing authority	Number of shared secrets, required for private key, used for certificate and CRL signing, restoration	Total number of distributed secrets
CA-Certum	3	5
CA Certum Level I	2	3
CA Certum Level II	2	3
CA Certum Level III	2	3
CA Certum Level IV	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 transmission 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 is confirmed by a hand-written signature on an appropriate form whose copy is retained in certification authority archives and by the secret holder.

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 legal entities (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 Unizeto CERTUM - CCP, according to instructions submitted by the share issuer. Before the shared secret holder attend 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 Unizeto CERTUM - CCP 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 Certification Practice Statement 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 Unizeto CERTUM - CCP 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 should request:

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 Unizeto CERTUM - CCP 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).

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 the cards or PIN.

Unizeto CERTUM - CCP does not retain copies of certification authority operator 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 not archived – they are destroyed immediately after termination of performance of cryptographic operation employing such keys or expiry of the associated public key certificate or its 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. Archived keys have to be available for 25 years; for the first 15 years they should 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:

keys are generated outside the cryptographic module; this situation occurs for example in the case of subscriber's key generation (on his/her demand) by a certification authority, their entry into a cryptographic card or any other hardware token prior to transfer of the media to subscriber; a similar operation of key entry into a cryptographic module may be carried out by a subscriber when the keys are delivered in an encrypted form and require local storage on a cryptographic card or a token,

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.

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

if the key is provided in one piece than outside the module it is not available in plain form, i.e. upon key generation in the module and its export to another cryptographic device, the key is encrypted with a secret key; the secret key is stored in a manner preventing unauthorized access to both parts of the secret (private key and secret key used for its encryption) simultaneously,

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

Entry of a private key into hardware security module of certification authorities **CA-Certum** or **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV** 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 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 by the subscriber) or directly from the hardware key generator (operation carried out by the operator of a certification or registration authority).

6.2.7. Method of Activating Private Key

Methods of activation of a private key, possessed by various users and subscribers of Unizeto CERTUM - CCP 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 **CA-Certum** or **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III**, **CA-Certum Level IV**, 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 Unizeto CERTUM - CCP services. Activation of private keys is always preceded by the security administrator's authentication. The authentication is carried out on the basis of an electronic identity card held by the security administrator. After insertion of the card into the cryptographic module and provision of the PIN number, the private key remains in the active state until removal of the card from the module.

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 connection 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. In the case of subscribers who represent legal entities (organizations, institutions, etc) activation should be carried out by a person possessing a suitable authorization of the certificate subscriber.

Every private key activation is recorded in the event journal.

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 logoff). 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.

If a private key is held by a subscriber that is a legal entity, the key may be deactivated solely by the authorized representative of this subscriber.

In the case of Unizeto CERTUM - CCP, deactivation of a private key is carried out by the security officer 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 the removal of the card from the module.

Every private key deactivation is recorded in the event journal.

6.2.9. Method of Destroying Private Key

Erasure of aprivate 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 corruption, preventing definite private key erasure from this card.

If a private key is owned by a subscriber that is a legal entity, the key may be destroyed solely by the authorised representative of the subscriber.

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.

A detailed description of private key destruction procedure is disclosed in documents "Media Book", "Procedure for Unizeto CERTUM - CCP key generation" and "Procedure for Unizeto CERTUM - CCP key archive and destruction". All the documents are classified as non-public and are available only for the personnel of a certification authority and the representative of an auditor.

6.3. Other Aspects of Key Pair Management

From the point of view of technology, it is possible to use the same key pair either for electronic signature creation or for information encryption. Notwithstanding, this Certification Practice Statement does not recommend this practice except for the situation described in Chapter 6.1.9. In the case of certificates issued within Certum Level IV policy this practice is prohibited.

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 . 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 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 Unizeto CERTUM - CCP, 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 administrator** 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 (compare Chapter 4.11).

Every archive of a e 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). It is also a validity period of a private key.

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.

Generally, beginning 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

Key owner	Main purpose of key usage			
	RSA for certificate and CRL signing	RSA for message signing	RSA for key exchange	Diffie-Hellman
CA-Certum	25 years	–	–	–
CA-Certum Level I	10 years	–	–	–
CA-Certum Level II	10 years	–	–	–
CA-Certum Level III	10 years	–	–	–
CA-Certum Level IV	10 years	–	–	–

Every user, including a certification authoritiy, can anytime terminate private key usage for electronic signature creation, 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 purpose		
		RSA for message signing	RSA for key exchange	Diffie-Hellman
Registration authority operator	Certum Level II	1 year	1 year	1 year
	Certum Level III	1 year	1 year	1 year
	Certum Level IV	2 years	2 years	2 years
Private persons and their hardware devices	Certum Level I	min. 3 months	min. 3 months	min. 3 months
	Certum Level II	1 year	1 year	1 year
	Certum Level III	1 year	1 year	1 year
	Certum Level IV	2 years	2 years	2 years
Legal entities and hardware devices of private person	Certum Level I	min. 3 months	min. 3 months	min. 3 months
	Certum Level II	1 year	1 year	1 year
	Certum Level III	1 year	1 year	1 year
	Certum Level IV	2 years	2 years	2 years

6.4. Activation Data

Activation data are used for activation of a private key operated by a registration authority, a certification authority or by a 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.

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 identity 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 (see [26]).

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-112. Shared secrets become activation data after their activation, i.e. providing the correct PIN number protecting the token.

6.4.2. Activation Data Protection

Activation data protection includes activation data control methods preventing from their revelation. Activation data protection control methods depend on the fact whether they are authentication phrases and whether control in 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 blockage. Stored activation data should never be retained together with the token.

6.4.3. Other Aspects of Activation Data

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

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

Activation data are subjected to archive.

6.5. Computer Security Controls

Tasks of registration authorities and certification authorities operating within Unizeto CERTUM - CCP 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 *"Procedure for Operation and Preservation of Unizeto CERTUM – CCP System Security"*.

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 Unizeto CERTUM - CCP system operation. Security means protecting computer systems are executed on the level of operating system, application and physical protections.

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

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,

the computer is accessible only to service personnel and authorized personnel, performing trusted roles in Unizeto CERTUM - CCP,

enforcement of duty segregation, arising from the role performed in the system,

identification and authentication of roles and personnel performing these roles,

prevention of reusage of an object by another processes after the object release by an authorised process,

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 compute resource access.

Assessment of computer security means is carried out in accordance with recommendations presented in ITSEC[40] and related to security level E4.

6.5.2. Computer Security Rating

Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP on the basis of the criteria described in WebTrust Principles and Criteria for Certification Authorities. This assessment is available in the repository of Unizeto CERTUM - CCP .

[40] *Information Technology Security Evaluation Criteria*

6.6. Technical Controls Life Cycle

6.6.1. System Development Controls

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

Every application, prior to entry into Unizeto CERTUM - CCP computer system, is electronically signed. It allows control of the version of current software and prevents unauthorized supplementation of the software or its forgery.

Similar rules apply to system hardware replacement. In particular:

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 in the way described in the document *"Procedure for Operation and Preservation of Unizeto CERTUM – CCP security"*.

6.6.2. Security Management Controls

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

Current configuration of Unizeto CERTUM - CCP system, as well as any modifications and updates to its system are recorded and controlled. System configuration is carried out in accordance with the recommendations described in the document *"Procedure for Operation and Preservation of Unizeto CERTUM – CCP security"*.

Controls applied to Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP 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 call (according to ITSEC) and by means of intrusion detection systems (IDS).

The first subnetwork contains WWW server and SMTP server (altogether – system repository) and a designated, logically separated internal part maintaining proper certification process (it contains e.g. certification server and database server). The second subnetwork performs the role of development and model system, used in development and test operations and tasks.

Unizeto CERTUM - CCP 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.

Means of protection of the network security accept only messages submitted with the usage of http, https, NTP, POP3 and SMTP protocols. Event records (logs) are recorded in the system journals and allow supervision of correctness of the usage of services provided by Unizeto CERTUM - CCP.

Detailed configuration of Unizeto CERTUM - CCP network and its protection means is presented in "Server Books".

6.8. Cryptographic Module Engineering Controls

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

6.9. Time stamps

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 Unizeto CERTUM - CCP system in accordance with the recommendation RFC 3161.

7. Certificate, CRL and OCSP profile

Certificate profiles and Certificate Revocation List profile comply with the format described in ITU-T X.509 v.3 standard, while the profile of OCSP complies with the requirements of RFC 2560. Information stated below describes the meaning of respective certificate fields, CRL and OCSP, applied standard and private extensions employed for the needs of Unizeto CERTUM - CCP.

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 issuing authority).

Extensions defined in a certificate according to the norm 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 standard allow definition of proprietary extensions, unique for implementation of the system.

7.1.1.1. Basic fields

Unizeto CERTUM - CCP 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 Unizeto 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 Unizeto CERTUM - CCP	
Signature Algorithm	md5WithRSAEncryption (OID: 1.2.840.113549.1.1.4) or sha1WithRSAEncryption (OID: 1.2.840.113549.1.1.5)	
Issuer (Distinguished Name)	Common Name (CN) =	Certum {CA,Level{I,II,III,IV}}
	Organization (O) =	Unizeto Sp. z o.o.
	Country (C) =	PL
Not before (validity period beginning date)	Universal Time Coordinated based. Unizeto CERTUM owns satellite clock controlled by Atomic Frequency Standard. Unizeto CERTUM clock is known as valid world Stratum I service	
Not after (validity period ending date)	Universal Time Coordinated based. Unizeto CERTUM owns satellite clock controlled by Atomic Frequency Standard. Unizeto 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 (most of the user's certificate), organizationName (for non-Repudiation and CA certificates), commonName (for server certificates), unstructured{Address or Name} (for VPN certificates) which are mandatory.	
Subject Public Key Info	Encoded in accordance with RFC 2459, may contain information about RSA, DSA or ECDSA public keys (key identifier, key size in bits and value of the public key); RSA key size is presented in Chapter 6.1.5	
Signature	Certificate signature, generated and encoded in accordance with the requirements described in RFC 2459.	

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.

Unizeto CERTUM - CCP supports the following fields of standard extensions:

AuthorityKeyIdentifier: identifier of a certification authority public key certificate associated with a private key, used for signing issued certificates – **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 key exchange, key for electronic signature, etc (see below):

```
digitalSignature    (0), -- key for electronic signature creation
```

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

ExtKeyUsage: definition (constraint) of the key usage – **this extension is not 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**. Unizeto CERTUM - CCP 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 - E-mail 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, 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
```

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

Tab.7.2 Policies identifiers and name

Policy identifier	Certificate policy name
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-I(1))[41]	Certum Level I Identifies certification policy of the name of Certum Level I
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-II(2))	Certum Level II Identifies certification policy of the name of Certum Level II
iso(1) member-body(2) pl(616)	Certum Level III

[41] Unizeto CERTUM – CCP 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 name
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
iso(1) member-body(2) pl(616) organization(1) id-unizeto(113527) id-ccert(2) id-certum(2) id-certum-level-IV(4))	Certum Level IV Identifies certification policy of the name of Certum Level IV

Certificates issued by certification authorities include both qualifiers, recommended by the RFC 2459.

PolicyMapping: policy mapping – **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: basic constrains – **this field is critical in the certification authority and is not critical in the subscriber's certificate**. The extension allows definition whether the subscriber 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 in elements within subject 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

Certificates issued by Unizeto CERTUM - CCP 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. CA Certificates

A self-certificate of **CA-Certum** certification authority and certificates of subordinate authorities, **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** and **CA-Certum Level IV** 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 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) 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 = end entity Path length constraint=none	Non-critical
Key Usage	Key encipherment, bit 2	Non-critical
Extended Key Usage	Server Authentication (serverAuth) Netscape SGC Microsoft SGC	Non-critical
Netscape Cert Type	SSL Server (bit 1)	Non-critical
Subject Alternative Name	DNS.1: Full DNS service name (FQDN) DNS.2: Alternative service name (optionally)	Non-critical
CRL Distribution Points	URI: http://crl.certum.pl/class{1,2,3,4}.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} CPS: http://www.certum.pl/CPS Notice number: 1 Organization: Unizeto Sp. z o.o. Explicit text: dependable upon 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 = end entity Path length constraint=none	Non-critical
Key Usage	digital signature, bit 0 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{1,3}.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} CPS: http://www.certum.pl/CPS Notice number: 2 Organization: Unizeto Sp. z o.o. Explicit text: dependable upon 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 = end entity Path length constraint=none	Non-critical
Key Usage	digital signature, bit 0 non-repudiation, bit 1 key encipherment, bit 2	Non-critical
Extended Key Usage	Encrypted File System TLS Client Authentication	Non-critical
Netscape Cert Type	SSL Client (bit 0)	Non-critical
Subject Alternative Name	Email: customer@somewhere-in-world.com	Non-critical
CRL Distribution Points	URI: http://crl.certum.pl/class{1,2,3,4}.crl	Non-critical
Authority Info Access	OCSP: http://ocsp.certum.pl	Non-critical
Biometric Info	Biometric data: Subscriber's photo, DNA, retinal scan, fingerprint (bit 0) Hand-written signature (bit 1)	Non-critical

Extension	Value or Value constraint	Extension status
	URI: biometric data location	
Certificate Policies	Policies: 1.2.616.1.113527.2.2.{1,3} CPS: http://www.certum.pl/CPS Notice number: 3 Organisation: Unizeto Sp. z o.o. Explicit text: dependable upon 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 = end entity Path length constraint=none	Non-critical
Extended Key Usage	IPsec Client IPsec Tunnel IPsec End System	Non-critical
Subject Alternative Name	DNS: full VPN router domain name (FQDN) IP: VPN router IP address	Non-critical
CRL Distribution Points	URI: http://crl.certum.pl/class{1,3}.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} CPS: http://www.certum.pl/CPS Notice number: 4 Organisation: Unizeto Sp. z o.o. Explicit text: dependable upon 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 Path length constraint={none,1,2,...}	Non-critical
Key Usage	digital signature, bit 0 non-repudiation, bit 1	Non-critical
Extended Key Usage	Validation Authority (OCSP) Time-Stamp Authority (TSA) Notary Authority (DVCS)	Non-critical
Subject Alternative Name	URI: http://www.customer-service.somwhere Subscriber's service location	Non-critical
Authority Info Access	OCSP: http://ocsp.certum.pl	Non-critical
Certificate Policies	Policies: 1.2.616.1.113527.2.2.{1,3} CPS: http://www.certum.pl/CPS Notice number: 5 Organization: Unizeto Sp. z o.o. Explicit text: dependable upon 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 Unizeto CERTUM - CCP, RSA algorithm, in combination with SHA-1 cryptographic hash is used.

7.1.4. Electronic signature field

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

7.2. CRL profile

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

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

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

Version: CRL format version,

Signature: contains identifier of the algorithm used by a certification authority to sign CRL; Unizeto CERTUM - CCP authorities sign **CRL** by means of **sha1WithRSAEncryption** algorithm,

Issuer: name of the certification authority issuing CRL; every authority of Unizeto CERTUM - CCP issues its own Certificate Revocation List; this requirement applies to the following authorities: **CA-Certum**, **CA-Certum Level I**, **CA-Certum Level II**, **CA-Certum Level III** and **CA-Certum Level IV**,

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 aboutrevoked 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 acertification 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 Unizeto CERTUM - CCP 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 or compromise;
affiliationChanged – subscriber's data modification (affiliation);
superseded – certificate renewal;
cessationOfOperation – cessation of certificate usage;
certificateHold – suspension of certificate;
removeFromCRL – certificate removal from CRL;
```

HoldInstructionCode: code of the operation of 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 Unizeto CERTUM - CCP 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 Unizeto CERTUM - CCP 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 Unizeto CERTUM – CCP) 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 mentioned above does not apply to revoked certificates of Certum Level I class. It is recommended that these certificates should be removed from the Certificate Revocation List at the moment of their expiration

7.3. OCSP confirmation response profile

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

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

OCSP server certificate has to contain in its body the extension of **extKeyUsage**, described in RFC 2459. This extension should be set as **non-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).

OCSP certificate may contain information about the means of contact with OCSP server. This information is included in the field of **AuthorityInfoAccessSyntax** extension (see Chapter 7.1.1.2).

7.3.1. Version number

OCSP server operating within Unizeto CERTUM - CCP issues certificate status confirmations in accordance with the RFC 2560. The only allowable value of the version number is 0 (it is an equivalent of v1 version).

7.3.2. Certificate status information

Information about certificate status is provided in the field **certStatus** of the structure **SingleResponse**. It may have one of the three main values, defined in Chapter 4.9.11. In the case of server response valid, the entity requesting the certificate status should additionally check the extension **CertHash** contained within the response (see Chapter 7.3.4) to make sure that the verified certificate was published by this very issuer, and the extension **ArchiveCutoff**, whose value is the begging date of the certificate status verification (the ending date is defined by the

moment of OCSP confirmation issuance, provided in the field **producedAt**). Positive result of those verifications allows so called **positive confirmation** of the certificate status.

7.3.3. Supported standard extension

In accordance with RFC 2569, Unizeto CERTUM - CCP OCSP server supports the following extensions:

Nonce – binding a request and a response to prevent reply attacks. Nonce 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 URL address, serial number and time of the list issuance. The information is provided in the field **singleExtensions** of the **SingleResponse**.

If the verified certficate 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 acceptable response (**id-pkix-ocsp-basic** among others) and is supplied in the request as the extension.

Boundary date of archival applies to the ending date of retention of information in Unizeto CERTUM - CCP database, referring to certificate status (**ArchiveCutOff** extension). Placement of this information in a response of OCSP server means OCSP 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 reliable in the moment of OCSP response issuance, even beyond the certificate expiration. Because of information about certificate status being available *on-line* for the period of 15 years (see Chapter 6.3.1), the value of the boundary archive date is a difference value of the date of certificate status conformation and the retention period of the revoked certificate information by OCSP server.

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

7.3.4. Supported private extensions

If as a response to a submitted request, the subscriber receives confirmation containing status **good**, he/she/itis 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 was created within the validity period of the certificate. The latter problem may be resolved with placement of **boundary archive date** (**ArchieveCutoff**) extension within a response (see Chapter 7.3.3).

The former problem, described above, may be resolved by the implementation of the private extension **CertHash** within a response submitted by Unizeto CERTUM - CCP OCSP 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) 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 value of 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.

7.3.5. OCSP issuer statement

*The current version of Unizeto CERTUM – CCP OCSP server does not implement extensions **CertHash** and **ArchiveCutOff** in its OCSP response. Notwithstanding, Unizeto declares that the certificate status valid, 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 and its reason, along with the information about CRL containing the certificate.*

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

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

Subscribers have to comply only with the currently applicable Certification Policy and Certification Practice Statement.

8.1. CPS Changes procedure

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

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

sponsor,

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 administrator, system administrator and Unizeto CERTUM - CCP personnel,

PKI Services Development Team,

Unizeto CERTUM - CCP subscribers,

professionals from the area of information system security.

After introduction of every modification, Certification Practice Statement or Certification Policy date of its issuance is updated and the identifier and serial number of the document is modified.

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 change without notification

The only items not requiring, according to Certification Practice Statement, notification in advance apply to amendments resulting from implementation of educational modifications or amendments to the contact information of the person responsible for CPS management. Implemented changes do not require approval procedure execution.

8.1.2. Items that can change with 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 ever modification in question by the PKI Service Development Team is submitted to each and every affected party in the form of new version of Certification Practice Statement with the status **requested for comment**. Suggested modification are published on the Unizeto CERTUM - CCP WWW site and transmitted by the means of electronic mail. New CPS is also attached the information about implemented modifications, rendering the new CPS significantly distinctive from the previous version.

8.1.2.2. Comment period

Comments on modifications suggested by PKI Service Development Team may be submitted by the affected parties within 30 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. If the condition is not met, 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 change, 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 CPS identifier

In the case of amendments which may have influence on extensive group of Policy 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.

Certification Practice Statement object identifier is subjected to modification 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,

introduction, in the case of a subscriber, of two separate types of certificates: for signing and for session key exchange,

implementation, of the service of suspension and unsuspension of a certificate , within the Unizeto CERTUM - CCP.

8.2. Publication and notification procedures

8.2.1. Items not published in CPS

Applied computer system security means are not available to the public. It also applies to authentication procedures and controls and the elements which may affect security protections or suggest possible target of attack. It particularly refers to:

employed hardware-software environment,

details of applied hardware configuration,

system emergency recovery plan,

location of Unizeto CERTUM - CCP key retention stores and PIN numbers protecting access to these keys,

list of individuals being shared secret holders,

implemented means of Unizeto CERTUM - CCP personnel protection,

network protections,

system logging procedures,

operator's terminals protections.

System documentation regarding elements not available to the public are available to the security administrator, the certification authority administrator and the representative of anauditing institution. Documents describing such elements may be accessed only in Unizeto CERTUM - CCP seat in a specially designated area. Every instance of confidential documentation access allowance is recorded in the event journal by the security administrator.

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/CPS

e-mail at the address: info@certum.pl

Three versions (is applicable) of Certification Practice Statement are always available at the repository and via the email: the currently applicable version, the previous version and the version under approval (see Chapter 8.3).

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

8.3. CPS Approval Procedures

If within 30 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 8.3), PKI Service Development Team does not receive significant remarks concerning this changes, a new version of Certification Practice Statement, with the status **under approval**, becomes a governing document of the certification policy, respected by all subscribers of Unizeto CERTUM - CCP, and the status of the version is changed into **valid**.

Subscribers who do not accept new, modified terms and regulations of Certification Practice Statement are obligated to a make suitable statement within 15 days of the date of the new version of Certification Practice Statement approval.

Appendix: 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 in performed in accordance with accepted Certification Policy 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 activity period – period between the starting and ending date of the certificate validity or the period between the starting date of the certificate validity period and the moment of its revocation or suspension.

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 the 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.).

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

Certificate Revocation List (CRL) – periodically (or immediately) issued list, signed electronically by an authority, allowing identification of the certificates subjected to revocation or suspension before expiration of validity period. CRL contains the name of the CRL issuer, date of publication, date of the next update, serial numbers of revoked or suspended certificates and dates and reasons for their revocation or suspension.

Certificate update – prior to expiration of a certificate, CA may update it (renew it), confirming validity of the same key pair for the succeeding period of validity (in accordance to the certification policy).

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 fulfills 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 formed as a set of the rules that are strictly obeyed by an issuing authority during provision of certificate services.

Cross-certificate – public key certificate issued to a certification authority, containing different name of the issuer and the subject; a public key of this certificate may be used solely for electronic signature verification. 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 – set consisting of hardware, software, microcode or their combination, performing cryptographic operations, including encryption and decryption, executed within the area of this cryptographic module.

Distinguished name (DN) – set of attributes forming a distinguished name of a legal entity and distinguishing it (i.e. the entity) from another entities of the same type, e.g. C=PL/S=zachodniopomorskie/OU=UNIZETO Sp z o.o., etc.

Electronic 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.

End entity – authorized entity using the certificate as a subscriber or a relying party (not applicable to e a certification authority).

Information system – entire infrastructure, organization, personnel and components used for assembly, processing, storage, transmission, publication, distribution and management of information.

Key state transformations – state of a key may be changed only when one of the following transformations occurs (according to ISO/IEC 11770-1):

generation – key generation process; key generation should be performed in accordance with accepted key generation procedures; the process may include test procedure, aimed at enforcement of key generation rules,

activation – results in key becoming valid and available for cryptographic operation performance,

deactivation – constraint of a key; the situation may occur due to expiry of the validity period of a key,

reactivation – allows further usage of the key in the state of unavailability for cryptographic operation,

destruction – results in termination of key life cycle; this notion means logical key destruction but may also apply to physical key destruction.

Object – object with controlled access, for example a file, an application, the area of the main memory, assembly 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.

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 affiliating the rest of t RA's and allowed to (except for standard operations) generate – on behalf of a registration authority – key pairs, successively subjected to certification process.

Private key – one of asymmetric keys belonging to a subscriber and 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 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 in his/her/its possession. Unizeto CERTUM - CCP 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 – message (see message) 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 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) – architecture, organization, techniques, practices and procedures that collectively support implementation and operation of certificate-based public key cryptography systems. PKI consists of hardware, software, database, network resources, security procedures and legal obligation elements of infrastructure, bonded together, which

collaborate to provide and implement certificate services, as well as other services, associated with the infrastructure (e.g. time stamp tokens).

Registration point – trusted legal entity, operating on the basis of CA authorization, performing registration of other legal entities and assigning distinguished names. A registration procedure within every registration domain requires that every registered value should be uniquely defined within such domain. The registration authority does not generate – on behalf of legal entities – key pairs which may be subjected to certification procedure (see distinguished name, certificate).

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.

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

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.

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 storage of the 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.

States of private key – private keys may have one of the three basic states (according to ISO/IEC 11770-1 standard):

waiting for activation (ready) – the key has been already generated but is not accessible for usage,

active – the key may be used in cryptographic operations (e.g. for creation of electronic signatures),

inactive – the key may be used solely for electronic signature verification or decryption.

Subscriber's sponsor – institution which on behalf of the subscriber supports financially certification services provided by the authority issuing certificates. The sponsor is the owner of the certificate.

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.

Token – element of data used for exchange between parties and containing s information transformed by means of cryptographic techniques. Token is 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 identity 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.

Unizeto CERTUM - Centrum Certyfikacji Powszechne (**Unizeto CERTUM - CCP**) – trusted institution (or hardware device under its control) being a part of trusted third party and capable of createing, signing and issuinge certificates (compare Registration Point, trusted third party).

Unizeto CERTUM - CCP Operational Team – personnel responsible for proper operation of Unizeto CERTUM - CCP. 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 Unizeto CERTUM - CCP.

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 – verification of certificate status, allowing validation whether the certificate is revoked or not. This problem may be solved by the sole 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.

Violation (e.g. data violation) – 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.

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 2459 R.Housley, W.Ford, W.Polk, D.Solo – *Internet X.509 Public Key Infrastrukture – Certyfikate and CRL Profile*, 1999

[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] [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/

Document history

Document modification history		
V 1.0	15th April 2000 r.	Draft of the document for discussion.
V 1.33	12th March 2002 r.	Entire version of the document. The document approved.
V 2.0	15th July 2002 r.	Definition of additional certificate types. Certification procedure modification, precision of certificate and CRL profile. Edition of Chapters 3, 4, 6.1, 2.6, 6.2-6.9 and 7. The document approved.