

Certification Practice Statement

version 1.1

Table of contents

1	Preface.....	7
1.1	Change history.....	7
1.2	Definitions.....	7
1.3	Introduction.....	8
1.4	Contact data.....	9
1.5	Identification.....	9
1.6	Standards.....	9
1.7	Types of issued certificates.....	9
1.7.1	X.509 extensions used in the certificates.....	9
1.8	Hierarchy of X.500 object identifiers.....	10
1.9	Subject entities and scope of applicability of this CPS.....	11
1.9.1	CC Signet hierarchy and structure.....	11
1.9.2	Registration Points.....	12
1.9.3	Registration Authorities.....	12
1.9.4	Applicability.....	13
1.9.5	Contact.....	13
2	General provisions.....	14
2.1	Obligations.....	14
2.2	Responsibility.....	14
2.3	Interpretation and enforcement of legal acts.....	14
2.4	Fees.....	14
2.5	Repository and publications.....	14
2.5.1	Information published by Certification Authorities.....	14
2.5.2	Frequency of publications.....	14
2.5.3	Access control.....	15
2.6	Auditing.....	15
2.6.1	Audit frequency.....	15
2.6.2	Identity of the auditor.....	15
2.6.3	Relationships between the auditor and the audited entity.....	15
2.6.4	Areas covered by the audit.....	15
2.6.5	Actions undertaken to rectify deficiencies detected during the audit.....	15
2.7	Protection of information.....	15
2.7.1	Information types obligatorily classified as sensitive.....	16
2.7.2	Information types treated as non-classified.....	16
2.7.3	Disclosing the information on the certificate revocation reason.....	16
2.7.4	Disclosure of sensitive information in case of a court order.....	16
2.7.5	Disclosure of sensitive information on request of the certificate holder.....	16
2.7.6	Other circumstances warranting disclosure of sensitive information.....	16

2.8	Intellectual property rights	16
2.8.1	General provisions	16
2.8.2	Copyrights	16
3	Identification and authorization	17
3.1	Preliminary registration	17
3.1.1	Name types	19
3.1.2	The necessity to use meaningful names	19
3.1.3	Principles of interpretation of various name forms	19
3.1.4	Uniqueness of the name	19
3.1.5	The procedure of resolving disputes resulting from name-related complaints	19
3.1.6	Recognition, authentication, and role of trademarks	19
3.1.7	Proof of possession of the private key	19
3.1.8	Authentication of institutions	19
3.1.9	Authentication of identity of individual certificate holders	19
3.1.10	Authentication of server/device data disclosed in the certificate	20
3.1.11	Certificate renewal	20
3.2	Renewal of a revoked certificate	20
3.3	Request to revoke a certificate	20
4	Functional requirements	21
4.1	Certificate application	21
4.2	Issuing the certificate	21
4.2.1	Certificate issuance procedure	21
4.3	Acceptance of the certificate	21
4.4	Revocation and suspension of the certificate	21
4.5	Security audit procedures	21
4.5.1	Types of recorded events	22
4.5.2	Frequency of the event record processing	22
4.5.3	Retention period of the event records for the audit purposes	22
4.5.4	Protection of the event records for the audit purposes	23
4.5.5	Procedures of making copies of event records occurring during the audit	23
4.5.6	Notification of entities responsible for the event	23
4.5.7	Estimation of the vulnerability to threats	23
4.6	Data archiving	23
4.6.1	Types of archived data	23
4.6.2	Data archiving frequency	23
4.6.3	Archive retention period	23
4.6.4	Archive copy procedures	23
4.6.5	Requirements for time stamps	24
4.6.6	Procedures of accessing and verifying the archived information	24
4.7	Key distribution	24

4.8	Key replacement	24
4.9	Compromising, disaster recovery	24
4.9.1	Damage of computing resources, software, or data	24
4.9.2	Revocation of a CA key	24
4.9.3	Consistency of the security system after disaster recovery.....	24
4.9.4	Business continuity and disaster recovery plan	24
5	Checking the physical and organizational protections and the personnel	26
5.1	Checking the physical protections	26
5.1.1	Location of the Certification Center and the building structure.....	26
5.1.2	Physical access	26
5.1.3	Power supply and air conditioning	26
5.1.4	Protection against flooding.....	26
5.1.5	Fire protection	26
5.1.6	Information media	26
5.1.7	Destroying the information	26
5.2	Checking the organizational protections	27
5.2.1	Trusted functions	27
5.2.2	Identification and authentication of the entrusted functions.....	27
5.3	Checking the personnel	28
5.3.1	Qualifications, experience, and required security clearance	28
5.3.2	Verification procedure	28
5.3.3	Preparation for the duties.....	28
5.3.4	Procedure in case of unauthorized actions.....	28
5.3.5	Documentation provided to the personnel	28
6	Technical security procedures	29
6.1	Generating and using the key pairs	29
6.2	Protection of the private key	29
6.2.1	Cryptographic module standard.....	29
6.2.2	Private key partitioning.....	29
6.2.3	Depositing the private keys.....	29
6.2.4	Backups copies of the private keys	29
6.2.5	Archiving the private keys	29
6.2.6	Entering the private key to the cryptographic module	30
6.2.7	Private key activation method.....	30
6.2.8	Private key deactivation method	30
6.2.9	Private key destruction method	30
6.3	Other aspects of key management.....	30
6.3.1	Archiving the public keys	30
6.3.2	Periods of validity of public and private keys	30
6.4	Activation data	30

6.4.1	Generating and installing the activation data.....	30
6.4.2	Protection of the activation data	30
6.4.3	Other aspects of the activation data	31
6.5	Controlling the computer system protections.....	31
6.5.1	Specific technical requirements for the computer system protection	31
6.5.2	Evaluation of the computer system protection level	31
6.6	Technical control cycle.....	31
6.7	Controlling the network protections	31
6.8	Cryptographic module management engineering.....	31
7	Certificate and CRL structure	32
7.1	Certificate profile	32
7.1.1	Basic fields.....	32
7.1.2	Standard extension fields.....	32
7.1.3	Private extension fields	32
7.1.4	Type of the digital signature algorithm	32
7.1.5	The digital authentication field	33
7.2	CRL structure	33
7.2.1	Supported CRL extensions	33
8	Administration of the Certificate Policies and of this CPS	34
8.1	Change procedure	34
8.1.1	Initial publication	34
8.1.2	Changes.....	34
8.2	Publishing the CPS, Certificate Policies, and information about them	34
8.3	Certificate Policy approval procedure	34
9	Liquidation.....	35

Reservations

The information provided in this Certification Practice Statement are not a part of the certification service agreement between Telekomunikacja Polska S.A. and the recipient of certification services and do not affect the scope of rights and obligations of Telekomunikacja Polska S.A. towards such recipient. In particular, subject to the existing law, Telekomunikacja Polska S.A. shall not be responsible for any loss suffered by the certification service recipient in result of relying upon the information provided herein.

The certification services described herein are provided by the Signet Certification Center ("CC Signet") operated by Telekomunikacja Polska S.A. with its registered office address of 00-105 Warszawa, ul. Twarda 18 ("TP").

1 Preface

1.1 Change history

Change history		
Version	Date	Change description
1.0	09.03.2007	The first version
1.1	24.05.2011	Deleting outdated provisions; modifications resulting from the auditor's recommendations

1.2 Definitions

The following terms used herein shall have the meanings defined below:

Definitions	
Certificate, public key certificate	A digital certificate which assigns data used for digital signature verification of for another function (such as encryption, user/device authentication) to a specific person (natural or legal) or object (e.g. certification service provider's infrastructure element, website, server, or another device). The data used for digital signature verification is assigned to the person which appends the digital signature, enabling identification of such person (the definition is extended compared to Art. 3.10 of the Digital Signature Act of 18.09.2001 (JoL 130.1450, as amended) and in particular includes also the "attestation certificate" (Art. 3.11) and "qualified certificate" (Art. 3.12).
Object identifier (OID)	An alphanumeric identifier registered according to the ISO/IEC 9834 standard, uniquely identifying a specific object or object class.
Legally protected information	Information protected by the state law (such as classified information, communications secrets, company secrets, personal data).
Sensitive information	Information whose disclosure may affect the security of operations and image of CC Signet (e.g. company secrets, personal data).
Certification Practice Statement	The rules and methodology adopted by the certification authorities (CAs) operated by CC Signet (this document, hereinafter also referred to as this "CPS").
Certification service recipient	A natural person, legal person, or entity without the legal person status, which: <ul style="list-style-type: none"> a) has entered into a certification service agreement with a certification service provider, or b) is allowed, within the scope envisaged in the certificate policy, to act on the basis of a certificate or other data certified digitally by a certification service provider.
Certificate Policy	The detailed solutions, including technical and organizational solutions, defining the method, scope, and conditions of protection, creation, and use of a specific group of certificates issued by CC Signet.
Certificate holder (end user)	A natural person authorized to access the private key associated with the public key provided in the certificate.
Registration Point	A natural or legal person authorized by CC Signet or an internal organizational unit of CC Signet, responsible for direct contacts with the customers, in particular to the extent of registration of persons

	applying for certificates, verification of such persons' identity, storing the documentation related to the certificates, and transferring the certificate applications to the Registration Authorities.
Certificate extension	Additional information provided in the certificate.
Relying party	A certification service recipient belonging to the category defined in item (b) of the definition of the term "certification service recipient".
Certification path	An ordered sequence including CA certificates and the verified certificate, created so that each next certificate in the path can be verified as based on the previous certificate in the path, assuming the first certificate in the path as the trustworthy starting point.
Certification Authority (CA)	An internal organizational unit of CC Signet, responsible for authentication of public keys (issuing and revoking the certificates, publishing the certificate validity information). The CA authenticates the relationship between the public key and the specific entity identified in the certificate.
Company secret	Technical, technological, or organizational information of the company or other information of economic value, which has not been disclosed to the public and in respect to which the company has undertaken confidentiality measures.
Registration Authority (RA)	An internal organizational unit of CC Signet, responsible for verification of the received applications for issuing, revoking, suspending, or resuming a certificate before transferring them electronically to the competent CA, as well as for assigning distinguished names to certificate holders.
Applicant	A natural person, legal person, or entity without the legal person status, which applies under the registration process for issuing a public key certificate.

The table above does not define the terms used in the meaning strictly defined in Art. 3 of the Digital Signature Act of 18.09.2001 (JoL 130.1450, as amended).

1.3 Introduction

This Certification Practice Statement, hereinafter referred to as the "CPS", describes the public key certification process, the actors of the process, the areas of certificate applications, and the related procedures.

This CPS describes the basic principles of operation of the Signet Certification Center (CC Signet) and of all related Certification Authorities, Registration Authorities, and certification service recipients.

This CPS describes the procedures used by CC Signet in the certificate issuance process, as well as execution of the offered services. Also, this CPS describes all standard procedures followed by CC Signet while performing the certification services. The specific procedures required for specific Certificate Policies are described in the corresponding Policies.

The public key infrastructure of certification envisages only one Certification Practice Statement. The procedure of CPS amending and updating is described in Section 8.

This CPS provides additional information on the principles of operation of CC Signet, which should be construed in connection with the Certificate Policies regulating the certificate issuance by CC Signet, as well as with the relevant agreement.

The Certificate Policy defines, among other things, the detailed technical, organizational, and other solutions determining the methodology, scope, and protection of the certificate creation and use.

One of the main tasks of the Certificate Policy is to present the level of security of the certification service provided under such policy. This provides the certification service recipient with a basis for determining the level of trust in the issued certificates. Also, the Certificate Policy may enable the

provided services to be compared with services offered by other providers. CC Signet may issue certificates under multiple Certificate Policies, in compliance with the principles defined herein.

The agreement defines the obligations of parties thereto in respect of the provided certification services.

This CPS assumes that the reader has basic knowledge of the public key infrastructure (PKI), including such matters as:

1. using the digital signature for authentication, integrity, and non-repudiation
2. using the encryption mechanism to provide the confidentiality service
3. principles of asymmetric cryptography, public key certificates, and using cryptographic key pairs
4. tasks of the Certification Authority and Registration Authority.

Information on the PKI basics is available from the CC Signet webpage at: <http://www.signet.pl/>.

1.4 Contact data

For more information on the Signet CC services, please contact us at:

Telekomunikacja Polska S.A.
Centrum Certyfikacji Signet
ul. Czackiego 13/18
00-043 Warszawa
E-mail: kontakt@signet.pl

1.5 Identification

This CPS is identified as “ Signet Certification Center Certification Practice Statement”.

The OID identifier class assigned to the Certification Practice Statement:

1.3.6.1.4.1.27154.1.1.1.1.

The OID of this version of the Certification Practice Statement:

1.3.6.1.4.1.27154.1.1.1.1.1

1.6 Standards

The structure hereof is based on the generally accepted guidelines published in the RFC 2527 document, “Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework”. This CPS differs from the abovementioned document only to the extent necessary to properly describe the procedures used by CC Signet and to adapt the CPS to the legal regulations in force in Poland.

1.7 Types of issued certificates

This CPS is applicable to the following certificate types:

1. all types of certificates issued to certification service recipients defined in the relevant Certificate Policies approved by the Policy Approval Committee
2. certificates of Certification Authorities, issued by the RootCA Certification Authority, within the scope defined in the relevant Certificate Policies.

A list of all Certificate Policies with management processes compliant with this CPS is published in the Repository available at:

<http://www.signet.pl/repository>

1.7.1 X.509 extensions used in the certificates

CC Signet supports certificates compliant with the standard X.509 version 3. Among other things, the standard defines certificate extensions (see Definitions) which may be used to provide additional information in the certificate.

1.7.1.1 The “Policy Identifier” extension

CC Signet uses the “Policy Identifier” extension (according to X.509: the policyQualifiers field in the certificatesPolicies extension). The purpose of that extension is to provide such information as:

- scope and level of responsibility
- location of the essential data describing the given CA.

In the certificates issued by CC Signet, the extension contains the name of the Certificate Policy and the URL of a file with the full text of the policy.

1.7.1.2 Approved policy identifier classes

The following Policy Identifiers and Policy Identifier classes (i.e. the fixed public part and the beginning of the private part of the OID) have been approved for use in the CC Signet certificates:

- identifier class for the Signet Certification Center:
1.3.6.1.4.1.27154.1.1
- identifier class for the Signet Certification Center's RootCA Certification Authority:
1.3.6.1.4.1.27154.1.1.1
- identifier class for the Signet Certification Center's RootCA Certification Authority policies:
1.3.6.1.4.1.27154.1.1.1.10.
- identifier of the Signet Certification Center's RootCA policy (the certificates issued under this policy are self-signed and issued by RootCA for RootCA and for the Certification Authorities directly subordinate to it):
1.3.6.1.4.1.27154.1.1.1.10.1.
- identifier classes for the policies of authorities issuing certificates to end users:
1.3.6.1.4.1.27154.1.1.10.10. — for policies of the CC Signet PUBLIC CA
1.3.6.1.4.1.27154.1.1.20.10. — for policies of the TELEKOMUNIKACJA POLSKA CA.

1.7.1.3 Other extensions used in the certificates

The issued certificates may contain private extensions and extensions specific for a given service or customer group.

The information about all used extensions, their meaning, and their use is provided in the Certificate Policy applicable to the given certificate.

1.7.1.4 Criticality of the certificate extensions

Each certificate extension is assigned a criticality designation.

The following rules apply to the specific criticality designations:

- "critical extension" — the relying party is obliged to properly interpret the meaning of the extension and to reject the certificate if such interpretation is impossible
- "non-critical extension" — the relying party is not obliged to properly interpret the meaning of the extension nor to reject the certificate if such interpretation is impossible.

The extension defining the allowed key use (according to X.509: the keyUsage extension) is a critical extension in all certificates issued by CC Signet.

1.8 Hierarchy of X.500 object identifiers

Object identifiers, which uniquely identify the most important elements and documents of CC Signet, are assigned in compliance with the CC Signet procedures.

OIDs are assigned to:

1. Signet Certification Center RootCA
2. each Certification Authority (CA)
3. each Certificate Policy
4. this CPS
5. private certificate extensions.

Registration Authorities have no OIDs assigned.

The identifiers are provided/stored as follows:

1. In the relevant Certificate Policy — the Certificate Policy identifier is provided in the Certificate Policy itself
2. In this CPS:

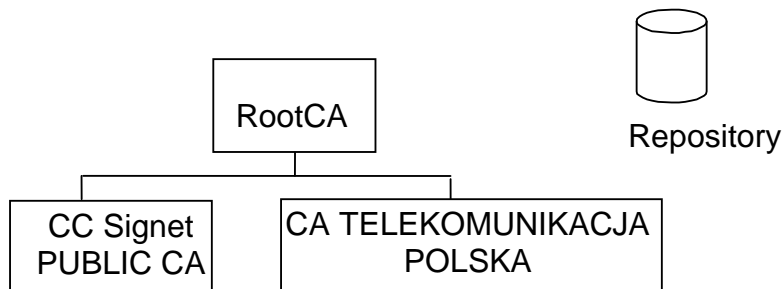
- the identifier of this CPS itself
 - the identifier of RootCA
 - all identifier classes used in CC Signet
3. In all internal registers of CC Signet
- all identifiers assigned by CC Signet.

1.9 Subject entities and scope of applicability of this CPS

1.9.1 CC Signet hierarchy and structure

CC Signet provides certification services through Certification Authorities (CA) and through services of Trusted Third Parties.

The diagram below presents the hierarchy of CC Signet authorities and bodies:



The CC Signet PUBLIC CA is a public certification authority providing services through the Internet to external customers. The TELEKOMUNIKACJA POLSKA CA provides certification services for internal purposes of Telekomunikacja Polska S.A.

This CPS is applicable to:

- all authorities operated in the PKI hierarchy of CC Signet
- all certificates issued in that hierarchy.

The practices described herein:

1. define the minimal requirements necessary to ensure that the critical functions are performed at a proper level of trust
2. apply to all actors of the certification process, to the extent of generating, issuing, using, and managing all certificates and cryptographic key pairs.

1.9.1.1 Policy Approval Committee as the body responsible for establishing the Certificate Policies

The certification Policy Approval Committee has been set up to approve the Certificate Policies in CC Signet and to ensure integrity of their structure.

The Policy Approval Committee is responsible for:

1. approving the Certificate Policies within CC Signet
2. managing this CPS
3. ensuring consistency of the Certificate Policies, this CPS, and other documents important for the CC Signet operations.

The CC Signet Policy Approval Committee can be contacted via e-mail at KZP@signet.pl and by traditional mail at:

Telekomunikacja Polska S.A.
Departament Zarządzania Bezpieczeństwem Systemów Teleinformatycznych
Centrum Certyfikacji Signet
Komitet Zatwierdzania Polityk
ul. Dzielna 52
01-029 Warszawa

1.9.1.2 Certificate issuing bodies

CC Signet includes certificate issuing bodies which constitute a hierarchy of Certification Authorities.

The RootCA certification authority issues the highest-level certificates and signs its own certificates.

The certification authorities CC Signet PUBLIC CA and TELEKOMUNIKACJA POLSKA CA (as well as CAs dedicated to other companies in the future) are subordinate to (certified by) RootCA.

1.9.1.3 RootCA — the superordinate certification authority

The superordinate certification authority, RootCA, may issue certificates only to its subordinate certification authorities and to itself (self-signed certificate).

RootCA has no Registration Authority. No competencies of RootCA in respect to registration of the subordinate CAs may be delegated to any other entity or institution.

1.9.1.4 Subordinate certification authorities

Subordinate certification authorities have their associated Registration Authorities. A CA may delegate to other entities or institutions some of its competencies in respect to registration of certification service recipients. In such case, the division of responsibility between CC Signet and such entity is regulated by the agreement. CC Signet is responsible to the certification service recipients for acts of such entities as for its own acts.

A CA may issue certificates both to certification service recipients and to other certification authorities.

1.9.1.5 Certificates issued within the CC Signet hierarchy

The certificates issued by the authorities operated by CC Signet contain the information provided by the certificate holders and guarantee that the data provided in the certificate has been verified by CC Signet or by another entity acting in its name. The certificates enable identification of the certificate holder. The necessary identification information is possessed by CC Signet or by the entity to which a certificate group has been issued. For example, a certificate issued to a company may contain the company name and the employee identification number. Such certificate is not a qualified certificate as defined by the Digital Signature Act of 18.09.2001 and a digital signature verified through such certificate does not have the legal consequences equivalent to a handwritten signature.

The scope and manner of verification of the registration data are defined in the relevant Certificate Policies.

CC Signet may include in the certificate a maximal value of a transaction verified with the certificate.

1.9.2 Registration Points

The main task of the Registration Point is to register the certification service recipients. The Registration Point is responsible for receiving the certificate application, authenticating the applicant by verification of his/her identity (if necessary in the given case), verifying the documents envisaged in the registration procedure, preliminarily accepting or rejecting the application, and transferring the preliminarily accepted applications to the competent Registration Authority. Those responsibilities are regulated by the relevant agreement and defined in the CC Signet operating documents and the relevant Certificate Policies.

1.9.3 Registration Authorities

Registration Authorities verify the received applications for issuing, revoking, suspending, or resuming a certificate and transfer them electronically to the competent Certification Authority. The verification process includes among other things checking the correctness and uniqueness of the distinguished names assigned to certificate holders.

The applications transferred to the CAs are authorized by Registration Authority Operators working in the Registration Authorities. The functions of Registration Authority Operators are defined by the CA in the relevant Certificate Policy, in particular to the extent of the rights and obligations of the Registration Authority Operators in the process of implementation of the given Certificate Policy.

Depending on the scope and method of verification of the application data, the Registration Authority may function automatically or with manual support of a Registration Authority, referred to as the Registration Authority Operator.

In functional terms, each Registration Authority is an integral part of the Certification Authority.

1.9.3.1 Repository

The Repository is a collection of publicly accessible databases containing certificates of all CAs and certificates issued to certificate holders (to the extent envisaged by the relevant Certificate Policy), as well as the following information related to the certificate functioning:

- Certificate Revocation Lists (CRL)
- current and previous versions of the Certificate Policies and of this CPS.

The principles of publishing the certificates and their revocation information are defined in the Certificate Policies.

Depending on the type of information downloaded from the Repository, the access may be implemented through one of the following protocols:

- HTTP
- HTTPS.

The access to the CRLs is always free of charge.

1.9.4 Applicability

This CPS is applicable to certification services provided by CC Signet to certification service recipients.

The basic functional classes of certificates managed by CC Signet may be applied to:

- remote identification and authentication of the certificate holders or workstations and servers managed by them
- ensuring integrity and confidentiality of information transmitted via electronic mail
- implementation of the services of non-repudiation of the origin, in particular for the purpose of verification of the e-mail sender identity, software authenticity, etc.
- implementation of digital signatures
- collection of the certificate holder's identification data
- protection of access to logical and physical resources.

The standard procedures presented herein, related to the certificate lifecycle management, apply to certification service recipients, but not to certificates issued for elements of the CC Signet PKI (and in particular to Certification Authorities and Registration Authorities).

1.9.5 Contact

This CPS is managed by CC Signet.

Any comments on this CPS may be addressed to:

Telekomunikacja Polska S.A.
Departament Zarządzania Bezpieczeństwem Systemów Teleinformatycznych
Centrum Certyfikacji Signet
Komitet Zatwierdzania Polityk
ul. Dzielna 52
01-029 Warszawa
E-mail: KZP@signet.pl

2 General provisions

This section presents the obligations of Certification Authorities, Registration Authorities, Registration Points, and certification service recipients.

The certification service recipients shall be:

1. informed through the Certificate Policy about their rights and obligations related to ensuring security, protection, and integrity of their private keys
2. obliged to accept an agreement which clearly defines their obligations, either before applying for a certificate in a specific functional class or during the registration process
3. informed about possible consequences of proved intentional activities aimed to interfere with the PKI.

Any information included in the certificates by reference to the relevant Certificate Policy constitutes an integral part of the definition of mutual obligations and responsibilities of the parties, as well as of the warranties.

2.1 Obligations

All obligations of the parties related to the use of certification services offered by CC Signet are described in the relevant agreement (if required for the given service) and in the Certificate Policy.

2.2 Responsibility

Any responsibilities of the parties related to the use of certification services offered by CC Signet (including the financial liability) are described in the relevant agreement and in the Certificate Policy.

2.3 Interpretation and enforcement of legal acts

The certification services are provided by Signet CC in compliance with the legal regulations in force in Poland.

2.4 Fees

The scope of paid certification services and their prices are set forth in the Price List available on the CC Signet webpage at <http://www.signet.pl/>.

2.5 Repository and publications

2.5.1 Information published by Certification Authorities

All information published by CC Signet is available from the Repository at the following addresses:

1. Certificate Policies subject to this CPS:
<http://www.signet.pl/docs/>
2. This CPS:
<http://www.signet.pl/docs/kpc.pdf>
3. Certificates of CC Signet Certification Authorities:
<http://www.signet.pl/repository/>
4. Certificate Revocation Lists (CRL):
<http://www.signet.pl/CRL>

2.5.2 Frequency of publications

The frequency of publications by CC Signet is as follows:

- Certificate Policy and this CPS — as per section 8
- certificates of the CC Signet Certification Authorities — every time the certificate is issued
- certificates of the holders — every time the certificate is issued, subject to the provisions of the relevant Certificate Policy
- Certificate Revocation Lists — as envisaged in the relevant Certificate Policy

- non-confidential fragments of reports from audits conducted by an authorized organization — every time such report is received by CC Signet
- auxiliary information — every time the information is updated.

2.5.3 Access control

The following information is available publicly:

- Certificate Policies and this CPS
- certificates of Certification Authorities in the CC Signet hierarchy
- Certificate Revocation Lists (CRL)
- selected auxiliary information.

To restrict the information write and modification functions to only authorized personnel or applications, an appropriate access control level is applied.

2.6 Auditing

2.6.1 Audit frequency

The full audit of public certification services, verifying the compliance of CC Signet with the documented procedures and this CPS, is conducted at least every three years.

2.6.2 Identity of the auditor

The audit is conducted by an independent institution authorized to perform such activities and properly experienced in applications of the Public Key Infrastructure and cryptographic technologies.

2.6.3 Relationships between the auditor and the audited entity

See 2.6.2.

2.6.4 Areas covered by the audit

The areas covered by the audit include, but are not limited to, the following:

- Security Policy
- physical security of CC Signet
- security of private keys of devices belonging to the CC Signet technical infrastructure
- security of the software and access infrastructure
- verification of the CC Signet operating personnel
- assessment of the used technologies
- administration of the Certification Authorities and Registration Authorities
- system logs and system monitoring procedures
- implementation of the data backup/restore procedures
- Certificate Policies and this CPS
- maintenance contracts.

2.6.5 Actions undertaken to rectify deficiencies detected during the audit

The internal and external audit reports are handed over to CC Signet.

In case of deficiencies, CC Signet shall promptly introduce the necessary corrective measures. The scope and manner of deficiency rectification shall be communicated to the auditing institution.

2.7 Protection of information

The access of the CC Signet personnel to sensitive information is limited to the minimum necessary to perform the official duties. The sensitive information constitutes a company secret and is subject to protection.

The information transferred to CC Signet in result of the practices and procedures defined in this CPS may be subject to the personal data protection according to the legal regulations effective in Poland.

CC Signet does not collect or process any information provided by the certification service recipients, beyond the scope directly required in connection with issuing and managing the users' certificates.

2.7.1 Information types obligatorily classified as sensitive

The following information is treated as sensitive:

1. the information provided in the certificate application or collected through the registration interview, not disclosed (directly or indirectly) in the public key certificate
2. private keys of the CC Signet technical infrastructure elements
3. private keys generated for certificate holders
4. agreements with the CC Signet customers
5. internal system records
6. operational and procedural documents whose disclosure could affect the security of the provided services.

2.7.2 Information types treated as non-classified

The following information is treated as non-classified:

1. Certificate Policies
2. Certification Practice Statement.

2.7.3 Disclosing the information on the certificate revocation reason

CC Signet discloses the information on the reasons of certificate revocation or suspension in the form of the Certificate Revocation Lists (CRL).

2.7.4 Disclosure of sensitive information in case of a court order

As a general rule, no sensitive document or information from the CC Signet systems may be disclosed to administrative agencies or courts unless both of the following conditions are satisfied:

- appropriate guarantees and rights are established
- the representative of the administrative agency or court is duly identified.

2.7.5 Disclosure of sensitive information on request of the certificate holder

The certificate holder who is the subject of the sensitive information is entitled to access such information and authorize any transfer of such information to a third party. The formal authorization may be effected through either of the following two methods:

- electronic document duly signed digitally by the certificate holder in compliance with the relevant Certificate Policy
- written request submitted by the certificate holder.

2.7.6 Other circumstances warranting disclosure of sensitive information

No other circumstances may warrant disclosure of the sensitive information without the formal consent of the information subject.

2.8 Intellectual property rights

2.8.1 General provisions

CC Signet guarantees that it is the owner or licensee of the hardware and software used to implement this CPS.

All trademarks, trade names, patents, logos, licenses, and other intellectual property used by CC Signet are property of their respective legal owners.

2.8.2 Copyrights

The copyright to this CPS belongs solely to CC Signet.

The copyrights to the Object Identifiers (OID) assigned for the purposes of the CC Signet infrastructure belong solely to CC Signet.

3 Identification and authorization

The detailed method of identification and authorization of the certification service recipient is specified in the relevant agreement and Certificate Policy.

The most important elements of those processes are presented below.

3.1 Preliminary registration

During the submission of the certificate application, the applicant is presented with the relevant Certificate Policy and additional introductory information, such as:

1. advice about the documents required during the application verification process
2. advice about the certificate holder's entitlement to generate own keys (if applicable).

If the certificate applied for is to be used to verify a digital signature of a natural person, the following information is also communicated:

1. explanation of the nature, meaning, and effects of the Certificate Policy, the agreement, and the CPS
2. advice regarding the legal consequences of appending digital signatures verified through the certificates issued under the given Certificate Policy
3. advice regarding the place and method of publication of the Certificate Policy and the CPS
4. advice regarding the obligations of the certification service recipients and of CC Signet under the agreement, including in particular the conditions and limitations of the certificate issuance and use
5. information about the system of voluntary registration of the qualified entities and its meaning.

Additionally, the applicant may be informed about other offered certificate types available to the applicant.

All such information may be presented to the applicant in advance, before starting the data verification under the registration process. Also, contact data for the purpose of answering any questions and doubts may be provided.

The preliminary registration process is conducted always when the applicant requests a new certificate, even if the same applicant already has a valid certificate issued under the same Certificate Policy. However, the above requirement does not apply to a certificate renewal if such service is envisaged by the relevant Certificate Policy and unless stipulated otherwise in its detailed provisions.

The purpose of the registration interview, which procedure precedes the transfer of the certificate application by the Registration Point to the Registration Authority, is to:

1. collect the necessary information from the applicant present in person or (in case of an organization) from the authorized representative
2. verify (by the authorized employee of the Registration Point) the applicant's entitlement to submit the application
3. perform the following tasks:
 - collecting the information to be disclosed in the certificate
 - verification of the identity
 - verification of trustworthiness of other collected information
 - signing the agreement
 - accepting the public key generated by the applicant (if applicable).

Upon conclusion of the interview, the applicant is provided with copies of all forms and other filled-up documents, of the information included in the certificate, of the agreement, and of all advices and remarks provided by the Registration Point operator.

The information necessary to issue the certificate must be provided by the applicant or (in case of an organization) by its authorized representative. Also, the contact information is collected. The information collected during the interview under the registration process typically include:

1. certificate type
2. full name of the certificate holder
3. name of the organization (and possibly of its organizational unit) — in case of certificates for representatives of legal persons and institutions
4. e-mail address

-
5. mailing address
 6. other information, such as phone number, fax number, office address
 7. other information necessary to perform the specific task of the given Registration Authority or connected with the specific purpose of the certificate, such as:
 - billing information
 - attributed to be included in the certificate
 - authentication mechanism for the purpose of identification of the authorized person in case of a certificate revocation request submitted by phone or remotely.

The above information may be collected on a paper form (certificate application form) to be processed later, included in the agreement, or entered directly through the Registration Point software. The Registration Point must strictly comply with the operational procedures which define the methods of verification of the accuracy and truthfulness of the submitted information. The specific Certificate Policy may stipulate some specific criteria of authenticating information which is critical for the intended purpose of the certificate, for example:

1. if the end user's permanent residence address is to be included in the certificate or is required by the given Certificate Policy, the Registration Point operator must follow the address verification procedures
2. appropriate documentation may be required to verify the organization's membership in a chamber of commerce.

The documents confirming the applicants identity must be produced in original or a copy authenticated by a notary.

The specific requirements for verification of the certificate holder's identity are provided in the relevant Certificate Policies.

If the certificate confirms the holder's position in an organization or is based on the holder's authority resulting from such position, documents certifying such position must be produced. The specific requirements for the position verification process (including the required documentation) are provided in the relevant Certificate Policies.

Typically, the position in an organization is documented by a certification application submitted on a letterhead of the organization. The application should specify the certificate type and should be signed by a legally authorized representative of the organization.

Before obtaining the applicant's signature on the agreement, the Registration Point operator must make sure that the applicant understands his/her rights, obligations, and privileges under the agreement. The agreement must be signed in presence of the Registration Point employee.

Having completed the registration interview, the Registration Point operator considers the application and either accepts it preliminarily or rejects it.

The preliminarily accepted application is transferred to the relevant Registration Authority.

The Registration Authority verifies the application.

If the application is accepted, it is converted to the electronic form (if necessary), signed digitally, and transferred to the relevant Certification Authority.

If the application is rejected, the applicant must be promptly notified. The Registration Authority operator is not obliged to reveal the cause of rejection, unless the relevant Certificate Policy or legal regulations stipulate otherwise.

If the key pair is generated by the applicant, the Registration Point operator must make sure that the applicant:

1. possesses the associated private key
2. is the person identified in the submitted application.

Certain Certificate Policies adopted by CC Signet allow a simplified registration procedure which does not require appearing in person in the Registration Point.

3.1.1 Name types

Each certificate holder is assigned a distinguished name, according to the X.500 standard. The Registration Authority approves the convention used for creating the distinguished names of the users. Various domains of Certificate Policies may use different conventions. The Registration Authority proposes and approves the distinguished names of the users.

3.1.2 The necessity to use meaningful names

It is not required that the distinguished name be based on names and abbreviations meaningful in the Polish language. The requirements for the contents of fields in a relatively distinguished name are set forth in the relevant Certificate Policy.

CC Signet support using certificates as a means of identification of the certificate holders. Anonymous certificates are not supported.

CC Signet allows using pseudonyms in the names.

3.1.3 Principles of interpretation of various name forms

The standard procedures of generating certain certificate types require entering the organization name and the department name as parts of the distinguished name. If the Certificate Policy does not require the institution or organizational-unit name attribute in the certificate, the distinguished name does not contain those attributes.

3.1.4 Uniqueness of the name

Distinguished names must be unique within the domain of the given Certification Authority. It means that the distinguished name must be assigned to only one, unequivocally identified certificate holder. One certificate holder may have multiple valid certificates issued by the same Certification Authority. One certificate holder may be assigned multiple different distinguished names.

3.1.5 The procedure of resolving disputes resulting from name-related complaints

CC Signet reserves the right to make all decisions regarding the syntax of the certificate holder's name and assignment of the resulting names.

3.1.6 Recognition, authentication, and role of trademarks

The rules of accepting and verifying the entitlement to use specific trademarks are defined in the relevant contract documents.

During the registration process, the certificate holder must submit a statement of entitlement to use a name which constitutes a trademark.

3.1.7 Proof of possession of the private key

The possession of the private key associated with the public key which is to be included in the certificate is proven by correct verification of the digital signature appended to the certificate request.

3.1.8 Authentication of institutions

Authentication of an institution requires an authorized representative of the institution to appear in person in the Registration Point.

The verification process is described in the relevant Certificate Policy.

3.1.9 Authentication of identity of individual certificate holders

An individual certificate holder is authenticated:

1. while appearing in person during the registration interview by the authorized worker of the Registration Point
2. in compliance with the identity verification process described in this CPS
3. in compliance with the procedures and requirements set forth in the relevant Certificate Policy.

3.1.10 Authentication of server/device data disclosed in the certificate

If required by the nature of the server/device data to be included in the certificate, such data is subject to authentication.

The authentication may be based on:

- a relevant certificate produced by the future holder
- verification in publicly available databases published in the Internet by an authorized entity.

The required verification process is presented in detail in the relevant Certificate Policy.

3.1.11 Certificate renewal

The certificate holder may request the certificate to be renewed if:

1. such renewal is envisaged in the relevant Certificate Policy
2. the request is submitted before expiration of the current certificate
3. the certificate content information provided in the registration data remains unchanged
4. the current certificate has not been revoked
5. the current keys are not registered as compromised keys.

If any of the above conditions is not satisfied, the certificate may not be renewed and the registration procedure must be repeated to obtain a new certificate.

The certificate renewal process is described in the relevant Certificate Policy. If the Certificate Policy envisages renewing the certificate online, in particular via e-mail, the renewal request must be digitally signed with the private key associated with the public key disclosed in the certificate to be renewed.

The Certificate Policy set forth the requirements for the format of such online request.

3.2 Renewal of a revoked certificate

A revoked certificate may not be renewed.

3.3 Request to revoke a certificate

The certificate revocation request must contain the information required by the Certificate Policy applicable to the certificate subject to revocation. In particular, such information may include the reason of certificate revocation and the likely date of private-key compromising (if this is the reason of revocation).

The certificate revocation procedures are described in detail in the relevant Certificate Policies.

4 Functional requirements

Presented below are the basic issues related to the procedure of initiating the certification process and other contacts with CC Signet. Each procedure starts from submitting a relevant application in the Registration Point. Depending on the application, the Certification Authority undertakes the appropriate action by performing or refusing the requested service.

4.1 Certificate application

The candidate certificate holder must contact the Registration Point and submit the relevant certificate application in person or electronically (depending on the type of requested certificate).

The Registration Point shall inform the applicant about the available certificate types, about the documents required to verify the identity, and about the mutual obligations under the Certificate Policy and the certification service agreement.

4.2 Issuing the certificate

The Registration Point, Registration Authority, and Certification Authority shall undertake appropriate actions to verify and process the certificate application. Such actions shall comply with the practices described herein and with any additional regulations indicated in the relevant Certificate Policy.

The applicant shall be fully responsible for the correctness of the information provided in the application. The Registration Point shall verify the truthfulness of the information provided in the application, in compliance with the requirements set forth in the relevant Certificate Policy and with the procedure applicable to the requested certificate.

After issuing the certificate, CC Signet shall not be responsible for monitoring, verifying, and confirming the accuracy of the information included in the certificate. Upon receipt of a credible notification that the information included in the certificate is inaccurate, the certificate shall be revoked and the certificate issuance procedure may be repeated.

4.2.1 Certificate issuance procedure

CC Signet shall issue the certificate after receiving the appropriate, authenticated application and after verifying the applicant's entitlement. Issuing the certificate finally confirms the correctness of the submitted certificate application.

The certificate issuance process may be different depending on the type of requested certificate.

The detailed principles of certificate issuance are set forth in the relevant Certificate Policies.

4.3 Acceptance of the certificate

The detailed acceptance procedure is set forth in the relevant Certificate Policy.

4.4 Revocation and suspension of the certificate

The principles of certificate revocation, suspension, and resumption, including the guaranteed time limits for information publishing and frequency of CRLs, are set forth in the relevant agreement and Certificate Policy.

4.5 Security audit procedures

The RootCA, Certification Authorities, and Registration Authorities shall maintain and archive the information records related to the operation of the Public Key Infrastructure to enable auditing (monitoring) such operation. The RootCA, CA, and RA software systems automatically collect information on the basic states in the certificate management process, i.e. certificate issuance, revocation, suspension, resumption, and expiration.

Each party connected in any way with the certification procedures is obliged to record the information and manage it adequately to such party's duties. The recorded information constitute the so-called

security log and must be retained to enable the parties to access the necessary information and to resolve any disputes.

The detailed principles of maintaining the security log are set forth the “Audit and Archiving Policy”, an internal document of CC Signet.

The records of the security log should also enable detection of any attempts to corrupt the protections in CC Signet and should help in implementation of mechanisms preventing such corruption. The scope of retained information about such events results from the current needs and actual threats to the system.

The person responsible for regularly auditing the compliance of the deployed mechanisms with this CPS and with the Certificate Policies is the CC Signet Security Inspector. Such person is also responsible for assessment of the effectiveness of the existing security procedures.

4.5.1 Types of recorded events

The minimal scope of audit data for the purpose of the security log includes:

1. all types of records generated during the registration, including those related to rejected applications
2. key generation requests, including those related to unsuccessful attempts
3. certificate generation requests, including those related to unsuccessful attempts
4. certificate issuance and CRL generation records
5. security-related system events.

The security log records the events listed below, related to the execution of automatic and manual procedures in the CC Signet systems, CA applications, and RA applications, as well as procedures executed by the operating personnel.

Types of recorded events
Successful and unsuccessful attempts to change the operating system parameters
Application starts and stops
Successful and unsuccessful attempts to log on to the system and applications
Successful and unsuccessful attempts to create, modify, or delete system accounts
Successful and unsuccessful attempts to create, modify, or delete authorized-user accounts
Successful and unsuccessful attempts to request, generate, sign, issue, or revoke a key or a certificate
Successful and unsuccessful attempts to create, modify, or delete the certificate holder information
Creating, archiving, and restoring backup copies
Changing the system configuration
Upgrades and updates of the software and hardware
Maintenance of the system hardware
Changes of the operating personnel

4.5.2 Frequency of the event record processing

The CC Signet Security Inspector shall review or supervise reviewing the event records at least once every workday and shall review the security log records and assess their correctness and completeness at least monthly, with due attention to the integrity of the records and to any irregularities.

4.5.3 Retention period of the event records for the audit purposes

The event logs shall be retained for at least 12 months and shall be available online for 3 months on each request of the authorized person or process. After that period, the logs may be archived and available only offline, in a manner enabling them to be viewed electronically. The archived records must be retained for the period of at least 1 year following liquidation of the Certification Authority the records pertain to, unless the then-current legal regulations stipulate otherwise.

4.5.4 Protection of the event records for the audit purposes

No separate protection of the event records for the audit purposes is envisaged.

4.5.5 Procedures of making copies of event records occurring during the audit

The procedures of making the required copies of event records are defined in the internal operational documents of CC Signet.

4.5.6 Notification of entities responsible for the event

The operating personnel shall notify the Security Inspector of any security-critical events occurring in the CC Signet systems.

4.5.7 Estimation of the vulnerability to threats

Periodic risk-assessment reviews are conducted across the PKI hierarchy to identify and assess vulnerability of the CC Signet systems to threats.

4.6 Data archiving

The following data must be archived: all data and files related to the system protection, applications submitted by certificate holders, certificate applications, information about certificate holders, information about generated certificates, CRLs, information (such as password) necessary to access the keys used by the CAs and RAs, exchange of information between the CC Signet authorities, and correspondence exchanged with the certificate holders.

4.6.1 Types of archived data

The following information must be archived by CC Signet:

1. audit logs
2. certificate applications
3. certificates and Certificate Revocation Lists (CRL)
4. private keys associated with the public keys disclosed in the encryption certificates, if the relevant Certificate Policy stipulates so
5. full backup copies of the critical systems
6. backup copies of e-mail logs
7. all formal correspondence exchanges with CC Signet

In addition to the abovementioned information archived electronically, CC Signet must archive:

- certification service agreements signed by authorized representatives of the parties.

Private keys of the CAs and RAs are not archived.

4.6.2 Data archiving frequency

The data archiving frequency is specified in the following internal operational documents of CC Signet: "Audit and Archiving Policy" and "Operating Procedures".

4.6.3 Archive retention period

The data archived electronically or in the paper form, as contemplated in 4.6.1 above, shall be retained for the period of at least 1 year following liquidation of the Certification Authority the data pertains to, unless the then-current legal regulations stipulate otherwise. Upon expiration of the archiving period, the data shall be destroyed. The information destroying process, in particular to the extent of cryptographic keys, must be conducted in compliance with the internal procedures ensuring an adequate security level.

All data must be retained at least for the period stipulated by the then-current legal regulations.

4.6.4 Archive copy procedures

CC Signet has in place procedures of making archive copies to enable full system recovery in case of a disaster.

4.6.5 Requirements for time stamps

The current regulations do not require the archived data to be affixed with time stamps and such stamps are not currently used.

4.6.6 Procedures of accessing and verifying the archived information

The procedures of accessing the archived information are specified in the following documents adopted by CC Signet: "Audit and Archiving Policy" and "Operating Procedures".

The Security Inspector shall test the archived data to check their integrity, in compliance with the adopted procedures. If a data damage or destruction is detected, it shall be promptly corrected on the basis of the original data (if still available) or its archive copy.

4.7 Key distribution

The public keys of RootCA are distributed through a self-signed certificate (i.e. the authority signs itself its own key).

Public keys of other authorities are distributed through certificates issued by their respective superordinate authorities.

4.8 Key replacement

CC Signet shall replace the keys of the authorities, observing the following requirements:

1. any impact upon the operations of the subordinate certification service providers and certification service recipients must be minimized
2. the subordinate certification service providers and certification service recipients must be notified by three months in advance about any planned replacement of the key and about the method of distribution of the new RootCA certificate.

4.9 Compromising, disaster recovery

CC Signet has adopted and manages a detailed documentation covering:

- Recovery and Business Continuity Plan
- base system configuration
- procedures for data archiving and off-site storage.

CC Signet shall make the abovementioned documentation available on request to the auditor conducting the security or compliance audit.

CC Signet shall properly train its personnel on the recovery and business continuity procedures and shall test those procedures at least yearly.

4.9.1 Damage of computing resources, software, or data

The CC Signet systems have the base configuration documentation, as well as backup and archiving plans to enable identification of any damages and recovery of the system.

4.9.2 Revocation of a CA key

The CC Signet authorities have contingency plans in case of revocation of their keys due to compromising or other reasons. Those plans envisage the steps to be undertaken in case of revocation of the key of any CA or RA.

4.9.3 Consistency of the security system after disaster recovery

When the system resumes operation after disaster recovery, appropriate measures shall be undertaken to ensure consistency of the CC Signet security system. Those measures include changing all passwords, PIN codes, and room access codes, as well as a full audit of the system security.

4.9.4 Business continuity and disaster recovery plan

The objective of the plan is to enable the CC Signet systems to be recovered as soon as possible in case of a serious interruption due to a natural disaster or an act of sabotage.

CC Signet has adopted and manages the “Business continuity and disaster recovery plan”. Such management includes the following activities:

1. identification of the internal resources necessary to implement the plan
2. identification of the persons authorized to initiate the disaster recovery action
3. identification of the components associated with the highest risk
4. identification of the criteria substantiating the disaster recovery action
5. implementation of the recommended precautions
6. consideration of possibly required additional precautions
7. designing the disaster recovery action and timeframes
8. establishing the priorities of the recovery action
9. managing the base hardware/software configuration catalog
10. managing the list of hardware and procedures necessary to recover the system in case of unexpected events; setting the maximal downtime.

In order to ensure business continuity and disaster recovery, CC Signet manages a dedicated set of hardware and software supporting the recovery of Certification Authorities and Registration Authorities.

5 Checking the physical and organizational protections and the personnel

This section presents the general requirements for supervision of the physical protections, organizational protections, and activities of the personnel used/performed during such tasks as key generation, entity authentication, certificate issuance, certificate revocation, auditing, and making backup copies.

5.1 Checking the physical protections

5.1.1 Location of the Certification Center and the building structure

CC Signet is located in Warsaw, in protected facilities accessible only to authorized persons.

The IT systems of CC Signet are operated in a physically secure environment compliant with high-level security standards.

The deployed security mechanisms protect the facilities against various types of attacks, including electromagnetic attacks. Also, the facilities are protected against electromagnetic emanations.

5.1.2 Physical access

The CC Signet rooms are equipped with access control systems based on personal identifiers and access code systems. The details of the access control system design constitute sensitive information.

5.1.3 Power supply and air conditioning

The working environment of CC Signet is powered by a dedicated power supply system. All critical components of the system are equipped with uninterruptible power supply (UPS) units to protect against unexpected downtime due to electricity failures.

The CC Signet facilities are equipped with an air conditioning system independent from the building systems.

5.1.4 Protection against flooding

The critical elements of the systems are installed in zones with a low level or risk of flooding due to a failure of the water and sewage infrastructure.

If a threat of flooding or actual flooding is detected, the building personnel and the responsible person in CC Signet are notified. They undertake actions envisaged in the building operating rules and report the incident to the competent utility company and to the CC Signet Security Inspector.

5.1.5 Fire protection

The fire protection system installed in the building complies with the relevant fire regulations and standards. The installed sprinkler system is activated automatically in case of a spreading fire. The critical computer systems are extinguished with gas-based systems.

5.1.6 Information media

The media containing sensitive information used in CC Signet are stored in protected safes on site. Also, copies of the archive data and cryptographic materials are stored in two external safes.

5.1.7 Destroying the information

Paper documents and magnetic and optical media containing sensitive information are destroyed:

1. in case of magnetic and optical media, through:
 - physical destruction of the resource
 - using an approved tool to erase or overwrite the contents
2. in case of printed materials — through using a shredder or another special destroying device.

5.2 Checking the organizational protections

The following subsections present the functions performed by the CC Signet employees in connection with the certification services, as well as their respective responsibilities.

5.2.1 Trusted functions

In order to ensure that no person acting singly can abuse his/her position to the detriment of CC Signet and of the certification service recipients, certain trusted functions have been distinguished which must be performed by different persons and division of responsibilities on individual positions has been established. The persons with those functions may perform only the strictly defined tasks within their respective scopes of duties.

The following trusted functions which may be performed by one or more persons have been identified in CC Signet:

- Policy Approval Committee — a body responsible for approving the Certificate Policies, Certification Practice Statement, and all other documents essential for the CC Signet operations
- Security Inspector — a person responsible for security of the CC Signet systems, and in particular for analyzing the logs of events occurring in the ICT systems used for providing the certification services by CC Signet
- Public Key Infrastructure Administrator — a person responsible for activating the CA keys, making any changes in the CC Signet hierarchy, submitting applications for issuing certificates to the subordinate authorities, and adding the approved Certificate Policies to the CC Signet system
- Registration Inspector — a person responsible for the activities of the Registration Authority operators, activation of the RA keys, and approving the prepared certificate applications
- Registration Authority Operator — a person responsible for conducting the procedures of registration of new customers and for entering their applications to the CC Signet system
- System Administrator — a person responsible for the CC Signet system software and for making the system copies under supervision of the Security Inspector and in compliance with the archiving policy and the operational procedures
- Repository Administrator — a person responsible for all publicly available sites used by CC Signet to publish the information directly connected to the public key infrastructure (such as certificates, CRLs, and policies)
- Archivist — a person responsible for operations of the CC Signet archive, the whole CC Signet documentation, receiving documents to the archive, and issuing documents in compliance with the clauses and procedures in effect in TP, as well as for the consistency and completeness of the archived documentation.

One person may perform more than one of the abovementioned functions, in compliance with the principles set forth in an internal document of CC Signet, approved by the Policy Approval Committee. Any task which involves creating a private key, archiving it, or importing it to the database requires presence of at least two persons with sufficient authorization (e.g. the Security Inspector and the CA Administrator).

Also, each operation of the hardware cryptographic module requires presence of at least two persons with sufficient authorization. The detailed principles and procedures are described in the relevant operational documents.

5.2.2 Identification and authentication of the entrusted functions

The CC Signet personnel shall be subject to the identification and authentication procedure in the following cases:

- entering into the list of persons entitled to access the CC Signet premises
- entering into the list of persons with physical access to the CC Signet system and network
- issuing a certificate entitling the person to perform the given entrusted function
- assigning an account and password in the CC Signet computer system
- issuing a certificate for the purpose of authentication to CA and RA applications
- issuing a PIN-protected electronic card used to control the access to the systems and applications.

Each of the abovementioned certificates and accounts:

- must be unique and issued/assigned directly to a specific person

- may not be shared with other persons
- must be limited only to the operations resulting from the function entrusted to the given person, performed through the CC Signet system software or the operating system in compliance with the procedures adopted by CC Signet.

5.3 Checking the personnel

5.3.1 Qualifications, experience, and required security clearance

For each function in CC Signet, requirements are defined for the person entrusted with that function. The recruitment process includes (among other things) verification of the skills and predispositions required for the given position.

5.3.2 Verification procedure

Certain functions in CC Signet are additionally subject to the procedure criminal record verification.

5.3.3 Preparation for the duties

Before assuming the duties, the CC Signet personnel must complete the training and formally confirm in writing, by signing a statement, the knowledge and full acceptance, to the extent necessary for the given role, of the following matters related to the certification center operations:

- the provisions of the Certificate Policies
- the provisions of the Certification Practice Statement
- the principles and mechanisms of protections used by the CA and RA
- software of the CA/RA computer system
- duties entrusted or to be entrusted
- procedures to be followed in case of a failure or disaster affecting the CA systems.

Each significant change of the CC Signet operations requires such statements to be updated.

5.3.4 Procedure in case of unauthorized actions

Any unauthorized action performed by the CC Signet personnel should be reported to the CC Signet management and to the persons responsible for compliance with the Security Policy, and in particular (but not only) to the Security Inspector.

5.3.5 Documentation provided to the personnel

The CC Signet personnel has access to:

1. hardware and software documentation, to the extent necessary to perform the entrusted tasks
2. this CPS and relevant Certificate Policies
3. a document defining the scope of duties and entitlements connected with the given role.

6 Technical security procedures

This section describes the procedures of creating and managing the cryptographic key pairs of CC Signet and of certificate holders. Also, it describes the technical measures protecting the data necessary to activate the system: PIN codes, passwords, and shared secrets.

6.1 Generating and using the key pairs

The key management procedures apply to secure generation, storage, and use of cryptographic keys. Particular attention is required to protect the private keys of CC Signet (Certification Authorities and Registration Authorities), which determine the security of the whole public key certification system.

The generated keys of CAs and RAs are stored and used in the secure environment of the hardware cryptographic module.

The detailed requirements and obligations related to generating and using the key pairs are set forth in the agreement and in the relevant Certificate Policies.

6.2 Protection of the private key

6.2.1 Cryptographic module standard

The hardware cryptographic modules used in the CC Signet CAs and RAs comply with the industry standards FIPS 140-1 Level 4 or ITSEC E3, which define the level of logical and physical security.

6.2.2 Private key partitioning

The private keys of Certification Authorities are used exclusively in the secure environment of the hardware module. Access to that module is protected by a multi-level access control system. The private keys of Certification Authorities leave the secure environment of the hardware module only in the encrypted form, divided into parts remaining under control of several different persons.

The keys of the Certification Authorities are stored in the hardware module.

6.2.3 Depositing the private keys

Copies of the private keys of the CC Signet Certification Authorities are deposited in the encrypted form at two secure, independent external sites. The principles of access to the deposited copies are strictly defined and controlled by CC Signet. Private keys generated by RAs for end users are not deposited.

6.2.4 Backups copies of the private keys

The private keys of CAs and RAs are stored in the secure environment of the hardware cryptographic module. Outside that environment, copies of the private keys are written in the encrypted form onto electronic cards and stored in a secure place. Copies of the keys can be activated only in the hardware module environment to which relevant secrets have been entered. The secrets are under control of several different persons, in compliance with the secret division scheme.

Backup copies of private keys stored in the operating system resources in the certificate holders' computers can be made by making a backup copy of the whole operating system. Also, such keys may be written to an encrypted file in the PKCS#12 format. In such case, the certificate holder should make a backup copy of such file. It is recommended to make backup copies of private keys used for decryption. Backup copies of private keys used for appending a digital signature should never be made.

It is not possible to make a backup copy of a private generated onto a cryptographic card.

6.2.5 Archiving the private keys

Only keys used for encrypting may be archived. The acceptability and principles of private key archiving depend on the specific Certificate Policy. Unless stipulated otherwise by the relevant Certificate Policy, private keys remain in the archive for at least five years after the archiving date.

6.2.6 Entering the private key to the cryptographic module

Entering the private key to the module involves entering the required parts of the key. A private key can be recovered in a module different than the module in which the key was originally generated only if a specific number of parts of the shared secret are collected and entered. Such parts are stored at multiple locations and accessible by several different persons, in compliance with the adopted secret division scheme.

The cryptographic modules storing the private keys allow the keys to be exported only in the encrypted form and divided into parts, in compliance with the adopted secret division scheme.

6.2.7 Private key activation method

Private keys of CC Signet, stored in the cryptographic modules, must be activated before use through a multilevel access-control and permission-verification mechanism based on electronic cards, access codes, and physical protections controlling the access to such cryptographic modules.

The method of activation of end users' private keys depends on the adopted method of key storage. As a minimum, the key is stored in an encrypted file protected by a password.

6.2.8 Private key deactivation method

Private keys of CAs are deactivated at the moment of finishing the operation of the application relying on the given key or at the moment of removing the electronic card controlling the access to the cryptographic module containing the given key.

6.2.9 Private key destruction method

Private keys of CC Signet, stored in hardware cryptographic modules, are destroyed through deleting them from the module memory and destroying all secrets protecting the archived copy of the key. After completing that procedure, CC Signet is unable to restore the key.

6.3 Other aspects of key management

6.3.1 Archiving the public keys

The public keys are archived by the Certification Authority which has certified the given key.

6.3.2 Periods of validity of public and private keys

Periods of validity of public and private keys are set forth in the relevant Certificate Policy.

6.4 Activation data

6.4.1 Generating and installing the activation data

Activation of a cryptographic module requires the following: electronic cards issued to the module operators, passwords protecting access to such cards, physical key to the cryptographic module, and other mechanisms protecting the access to the applications controlling the hardware cryptographic module.

If a key pair is generated by CC Signet for a certificate holder, an activation password may be generated during the registration process for the purpose of protection of the user's keys and the certificate during the shipment.

6.4.2 Protection of the activation data

The activation materials necessary to operate the hardware modules are stored in a separate, secure room and never leave CC Signet in a form enabling anybody to get access to a set of activation data sufficient to operate the modules. The activation data stored at external sites are divided into sets. The critical cryptographic material can be recovered in case of disaster using the combined sets, but not with a single set if it becomes compromised. The operators knowing the passwords to the electronic cards have access to the cards only in CC Signet and in presence of the Security Inspector.

The activation data may be delivered to the holder by registered mail or another secure channel independent from the channel through which the generated keys and the certificate are delivered.

6.4.3 Other aspects of the activation data

No other aspects of the activation data are contemplated herein.

6.5 Controlling the computer system protections

6.5.1 Specific technical requirements for the computer system protection

The CC Signet computer systems are protected in compliance with the ICT security standards adopted by Telekomunikacja Polska S.A., with due consideration to the specifics of the provided services.

6.5.2 Evaluation of the computer system protection level

The protection level is evaluated in compliance with the guidelines of an external auditor and is based, among other things, on the guidelines provided in the Information Security Evaluation Criteria (ITSEC).

6.6 Technical control cycle

No conditions for this area are stipulated herein.

6.7 Controlling the network protections

The IT systems in CC Signet comply at least with the technical requirements stipulated by the legal regulations for qualified providers of certification services.

The servers and workstations of the CC Signet computer systems are connected to a multi-segment internal LAN. The Certification Authorities are separated from the Registration Authorities and the Repository by two firewalls from different manufacturers. The Repository resides in a dedicated sub-network constituting a demilitarized zone (DMZ). The Registration Authorities and Certification Authorities have limited access to the DMZ. The DMZ includes also communication gateways for communication with end users and external service providers (e.g. providers of the card personalization services).

Access to the DMZ is protected by firewalls running in the high-availability configuration.

All sub-networks from which any access to CC Signet from the outside is possible are equipped with mechanisms detecting any attempts of unauthorized access and other forms of attack, as well as with mechanisms actively responding to such attempts.

All activities involving access to the CC Signet network are monitored and logged in order to provide evidence in case of unauthorized activities.

6.8 Cryptographic module management engineering

CC Signet has developed and deployed the Cryptographic Module Management Procedures which identify the threats and define the methods of elimination of such threats.

7 Certificate and CRL structure

The certificate and CRL structure complies with the formats specified in the standard ITU-T X.509 v3. A certificate is a sequence of three fields. The first field contains the certificate body, the second field identifies the type of the algorithm used to sign the certificate, and the third field contains digital authentication of the contents of the first two fields, appended by the certificate issuer.

7.1 Certificate profile

The profile of the certificates issued by CC Signet complies with the guidelines of the RFC 3280 document. Since CC Signet issues certificates to various holders who may use them in many areas of their operations, CC Signet may generate certificates with various profiles, defined in the relevant Certificate Policies. This CPS sets forth the minimal requirements for the information contents of the certificate.

7.1.1 Basic fields

CC Signet supports the following basic fields of the certificate:

1. **version** — certificate format version; the value is always 2, meaning version 3 of the certificate format, according to the X.509 standard.
2. **serialNumber** — an integer number, unique within the given Certification Authority, assigned to each certificate issued by such authority.
3. **signature** — identifier (OID) of the algorithm used by the Certification Authority to digitally authenticate the certificate; CC Signet uses the algorithm SHA-1 with RSA encryption (SHA1WithRSAEncryption).
4. **issuer** — a name identifying the Certification Authority which has issued and signed the certificate; the field contains a distinguished name.
5. **validity** — certificate validity period; the field specifies the begin and end of the certificate validity period as a sequence of two date-and-time values, given to an accuracy of one second.
6. **subject** — distinguished name of the certification service recipient, identifying the entity whose public key is provided in the public-key field of the certificate; the value is a non-empty, relatively distinguished name.
7. **subjectPublicKeyInfo** — public key of the certificate holder, with the OID of the algorithm to which the key is designated.

7.1.2 Standard extension fields

The function of each extension is defined by the standard value of the respective OID. The extension may be critical or non-critical, depending on the option selected by the certificate issuer.

The set of standard extensions used in certificates issued by CC Signet is listed in the relevant Certificate Policy.

7.1.3 Private extension fields

The set of private extensions included in the certificates issued by CC Signet depends on the Certificate Policy defined for addressing the non-standard needs of the PKI users.

7.1.4 Type of the digital signature algorithm

The signatureAlgorithm field contains the identifier of the cryptographic algorithm used by the issuer to digitally confirm the certificate.

For the purpose of digital authentication of the certificates, cryptographic algorithms are used always in combination with a hash function.

For the purpose of digital authentication, CC Signet supports the following:

1. hash functions:
 - SHA-1
 - MD5
2. cryptographic algorithms:
 - RSA

■ DSA.

Presently, all CC Signet authorities use the algorithm SHA-1 with RSA encryption (SHA1WithRSAEncryption).

7.1.5 The digital authentication field

The digital authentication field (signatureValue) contains the value of the hash function applied to all certificate body fields, encrypted with the private key of the certificate issuer (Certification Authority).

To verify the certificate authenticity, it is necessary to compute the hash function of the certificate body, decrypt the digital authentication field using the public key of the certificate issuer, and compare the result with the computed hash value. If the values are equal, the certificate authenticity is confirmed.

7.2 CRL structure

The Certificate Revocation List (CRL) contains three fields. The first field contains the certificate revocation information. The second and third field contains (respectively) the type of algorithm used to digitally authenticate the list and the digital authentication generated by the certificate issuer.

The first field is a sequence of mandatory and optional fields. The mandatory fields identify the CRL issuer and the optional fields identify the revoked certificates and contain the CRL extensions.

7.2.1 Supported CRL extensions

The function of each extension is defined by the standard value of the respective OID. The extension may be critical or non-critical, depending on the option selected by the certificate issuer.

The set of standard extensions used in CRLs generated by CC Signet depends on and is listed in the relevant Certificate Policy.

8 Administration of the Certificate Policies and of this CPS

The body responsible for administration of this CPS and of all Certificate Policies is the CC Signet Policy Approval Committee, functioning within the Telekomunikacja Polska S.A. organization.

This CPS and each Certificate Policy used in the CC Signet hierarchy has its OID which:

1. uniquely identifies the given CPS or Certificate Policy
2. identifies the document version.

8.1 Change procedure

8.1.1 Initial publication

A new Certification Authority in the CC Signet hierarchy may be established only with the approval of the Policy Approval Committee which formally approves the first Certificate Policy under which the new authority is to issue certificates. CC Signet shall assign OIDs for the new authority, the policy class supported by it, and the approved Certificate Policy, in compliance with the adopted rules of OID assignment.

When the Certificate Policy is approved by the Policy Approval Committee and assigned its OID, the Certification Authority shall:

1. publish the Certificate Policy in the Repository
2. instructs all its subordinate entities about their duties under such Policy.

8.1.2 Changes

This CPS may be amended or updated. The changes must guarantee that the CPS remains compliant with all still valid obligations of CC Signet, undertaken under the previous version of the CPS.

A policy may be changed in either of the two ways:

- issuing a new Certificate Policy
- modification or correction of the existing Certificate Policy, without changing the responsibilities, applicability, and trust level.

If a new policy is issued, it must be assigned a new OID. If a modification or correction is introduced, the version number in the corresponding OID is changed.

The changed CPS is introduced for implementation in compliance with the internal regulations of Telekomunikacja Polska S.A.

8.2 Publishing the CPS, Certificate Policies, and information about them

The current CPS is published in the CC Signet Repository.

A new or changed Certificate Policy is published in the CC Signet Repository indicated in the given policy. The superordinate authorities must communicate to their subordinate authorities any changes and planned publications of policies by two weeks in advance.

8.3 Certificate Policy approval procedure

Any new Certificate Policy to be used in the CC Signet hierarchy, as well as any change of an existing Certificate Policy, must be approved by the Policy Approval Committee.

9 Liquidation

In the event of liquidation of CC Signet or of any Certification Authority in its hierarchy, CC Signet shall undertake all economically justified measures to minimize the negative impact of such decision upon the certification service recipients.

In particular, CC Signet shall:

1. at least by 90 days before the liquidation:
 - a. publicly announce the liquidation by publishing an announcement on the CC Signet website at <http://www.signet.pl>
 - b. notify in writing the authority (if any) which has accredited the liquidated entity
 - c. notify all subscribers with valid certificates of the liquidated entity, using the contact data provided in the registration process, advising them about their entitlement to recover the costs pro rata temporis, at their request
2. before the liquidation
 - a. revoke, without request of the subscriber, all certificates issued by the liquidated authority, including the infrastructure certificates
3. immediately after the closure of operations:
 - a. professionally destroy, in front of a commission, all copies of private keys of the liquidated infrastructure
 - b. return the costs to the subscribers at their request, as per item 1.(c) above
 - c. in case of total liquidation, send the data subject to obligatory archiving (as per section 4.6 above) to the archive and publicly announce the contact data for the purposes related to the liquidated operations
 - d. destroy, in front of a commission, all remaining data and documents related to the liquidated operations.