Polska wersja tego dokumentu znajduje się tutaj

IMPORTANT NOTICE: This English translation is provided for reference. The only official version of this document is its original Polish version, available under the link above.

# Certification Practice Statement

Table of contents

Reservations

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

Trust services described in the Certification Practice Statement are provided by Signet Certification Center (hereinafter referred to as Signet CC) managed by Orange Polska S.A. based in Warsaw at Al. Jerozolimskie 160, postcode 02-326.

Document specification:

| | |
|---|---|
| **Document title** | Certification Practice Statement |
| **Document owner** | Signet Certification Center at Orange Polska S.A. |
| **Version** | 1.3 |

Approved by:

| Version | Approver |
|---|---|
| 1.3 | Network & Technology Managing Director |

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| 1.1 | 24.05.2011 | Deleting outdated provisions; modifications resulting from the auditor's recommendations |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 | 07.10.2013 | Changes resulting from Signet CC Public Key Infrastructure modification. Update of contact addresses. Editorial changes introduced into the document during approval process, taking into account the current internal regulations in force in the Orange Polska S.A. |
| 1.3 | 17.11.2017 | CPS review and updates made in due to entry into force of eIDAS Regulation and Polish Act on Trust Services and Electronic Identification of 5.09.2016 Adapting the document to the CA/Browser Forum requirements. |

# 1 Introduction

## 1.1 Document ID

| | |
|---|---|
| **Document name** | Certification Practice Statement of Signet Certification Center |
| **Version** | 1.3 |
| **OID** | 1.3.6.1.4.1.27154.1.1.1.1.1.3 |
| **Enforcement date** | 15.01.2018 |
| **Expiration date** | Until revoked |

## 1.2 Definitions and abbreviations

### 1.2.1 Definitions

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

**Act** - Polish Trust Services and Electronic Identification Act of 5.09.2016 (JoL. 2016, sec. 1579).

**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.

**Certificate Extension** - additional information provided in the certificate.

**Certificate for Electronic Signature** - an electronic attestation which links electronic signature validation data to a natural person and confirms at least the name or the pseudonym of that person.

**Certificate for Website Authentication** - an attestation that makes it possible to authenticate a website and links the website to the natural or legal person to whom the Certificate is issued.

**Certificate Policy** - detailed technical, organizational, and other solutions determining the methodology, scope, and protection of the certificate creation and use.

**Certification Authority (CA)** - a set of technical and organizational measures used to authenticate public keys (issuing and revoking Certificates, publishing Certificate validity information). The CA authenticates the relationship between the public key and the specific entity identified in the Certificate.

**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.

**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.

**Confidentiality** - property that the information is not made available or disclosed to unauthorized persons, entities or processes.

**eIDAS Regulation** - Regulation (EU) No 910/2014 of the European Parliament and of the Council of 23 July 2014 on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC (Off. J. of EU L 257 of 28.08.2014).

**Electronic Seal** - data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter's origin and integrity.

**Electronic Seal Creation Data** - unique data, which is used by the creator of the Electronic Seal to create an Electronic Seal.

**Electronic Signature** - data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign.

**Electronic Signature Creation Data** - unique data which is used by the signatory to create an Electronic Signature (Certificate private key).

**Information Security Incident / Incident /Security Incident** - a single event or series of unwanted or unexpected information security related events that are likely to disrupt business activities and endanger information security.

**Object Identifier (OID) / Identifiers**- n alphanumeric identifier registered according to the ISO/IEC 9834 standard, uniquely identifying a specific object or object class.

**Protected Information** - legally protected information such as: personal data, OPL company secrets and telecommunications secrets.

**Public Key Certificate / 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. trust service, website, server, or another device). In the case of data used to verify the Electronic Signature, they are assigned to the person signing the Electronic Signature and are identifiable.

**Registration Authority -** a set of technical and organizational measures applied to verify incoming applications, revoke, suspend or cancel the suspension of the Certificate before transferring them electronically to the appropriate Certification Authority and assigning the distinguished name to the Certificate Holders.

**Registration Inspector** trusted function in Signet CC, whose responsibility is defined in sec. 5.2.1 of the CPS. **Certification Practice Statement / CPS** - the rules and methodology adopted by the Certification Authorities (CAs) operated by Signet CC

**Registration Point** - Customer service point registering natural and legal persons applying for certificates, verifying such persons' identity in accordance to relevant Certificate Policies, storing the documentation related to the certificates, and transferring the certificate applications to the Registration Authorities.

**Relying Party -** a natural or legal person that relies upon an electronic identification or Trust Service.

**Repository** - a central database of Certificates and documents related to Signet CC functioning available at the website at the http://www.signet.pl/.

**Security Inspector -** trusted function in Signet CC, whose responsibility is defined in sec. 5.2.1 of the CPS.

**Supervisory Authority -** in accordance with the Act, the supervision of the Trust Service Providers is exercised by the Minister of Computerization.

**Trust Service -** an electronic service normally provided for remuneration which consists of:

a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or
b) the creation, verification and validation of certificates for website authentication; or
c) the preservation of electronic signatures, seals or certificates related to those services.

**Trust Service Provider** - a natural or a legal person who provides one or more Trust Services either as a qualified or as a non-qualified Trust Service Provider.

**Trust Service Recipient / Service Recipient / Certificate Holder / End User** - a natural person, legal person, or entity without the legal person status, which received a Certificate in accordance with a Certificate Policy.

### 1.2.2 Shortcuts

**Signet CC / System** - Signet Certification Center

**CRL** - Certificate Revocation List

**OSCP** - Online Certificate Status Protocol - for obtaining the revocation status of an X.509 digital certificate

**OPL** – Orange Polska S.A.

**SOC** - Orange Polska S.A. Security Operation Center, monitoring the security of systems / networks 24/7 and responding to emerging incidents and threats.

### 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 Signet CC and of all related Certification Authorities, Registration Authorities, and Trust Service Recipients.

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

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

The CC Signet Public Key Infrastructure System operates in accordance with the law in force in the Republic of Poland, in particular according to:

- eIDAS Regulation and The ACT,
- the provisions on the protection of personal data applicable in the territory of the Republic of Poland.

This CPS provides additional information on the principles of operation of Signet CC, which should be construed in connection with the Certificate Policies regulating the Certificate issuance by Signet CC, 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 Trust Service provided under such policy. This provides the 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 Trust Services offered by other providers.

Signet CC 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 Trust Services.

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

1) using the Electronic Signature for authentication, integrity, and non-repudiation
2) using the encryption mechanism to provide the confidentiality;
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 public key infrastructure basics is available from the Signet CC webpage at: http://www.signet.pl/.

## 1.4 Contact data

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

Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych
Centrum Certyfikacji Signet
ul. Piotra Skargi 56
03-516 Warszawa / POLAND
E-mail: kontakt@signet.pl

## 1.5 Standards

The CPS structure and its informational contents is based on the generally accepted guidelines published in the RFC 3647 document, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework".

## 1.6 Types of issued certificates

This CPS is applicable to the following Certificate types:

a) all types of Certificates issued to Service Recipients defined in the relevant Certificate Policies,

b) Certificates of Certification Authorities, including Root CA Certification Authority Certificates - 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

### 1.6.1 X.509 extensions used in the Certificates

Signet CC supports Certificates compliant with the standard X.509 version 3. Among other things, the standard defines Certificate Extensions.

#### 1.6.1.1 The Policy Identifier extension

Signet CC uses the "Policy Identifier" extension (according to X.509 standard: 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 Signet CC, the extension contains the name of the Certificate Policy and the URL of a file with the full text of the Policy.

#### 1.6.1.2 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 Signet CC certificates for public services :

1) Identifier class for the Signet Certification Center:

   1.3.6.1.4.1.27154.1.1

2) Identifier classes for the Signet Certification Center's Root CA Certification Authorities:

   1.3.6.1.4.1.27154.1.1.3 – for Signet Root CA (Public Root CA)

3) Identifier classes for the Signet Certification Center's Root CAs Certificate Policies:

   1.3.6.1.4.1.27154.1.1.3.10 – for Signet Root CA (Public Root CA)

4) 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 Signet CC - Public CA

The current list and register of Object Identifiers is contained in the document "Structure of CC Signet OID."

#### 1.6.1.3 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.

#### 1.6.1.4 Criticality of the Certificate extensions

Any Certificate extension must be marked as critical or non-critical.

Depending on an extension criticality:

- “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 standard: the keyUsage extension) is a critical extension in all Certificates issued by Signet CC.

### 1.7 Object Identifier hierarchy

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

Object Identifiers are assigned to:

1) each Root CA of Signet CC
2) each Certification Authority (CA)
3) each Certificate Policy
4) this CPS
5) private Certificate Extensions.

Registration Authorities have no OIDs assigned.

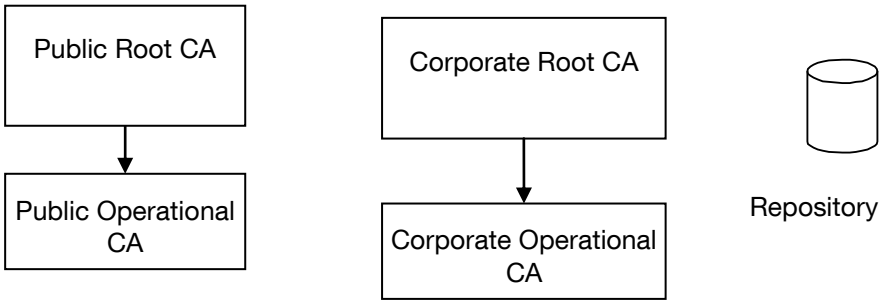
The identifiers are provided/stored as follows:

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
   - Identifiers of Root CAs
   - Identifier classed used in Signet CC,
3) In all internal registers of Signet CC
   - all Identifiers assigned by Signet CC.

## 1.8 Subject entities and scope of applicability of this CPS

### 1.8.1 Signet CC hierarchy and structure

Signet CC provides Trust Services through Certification Authorities (CA).
The diagram below presents the simplified hierarchy of Signet CC Certificate Authorities:




Signet CC Public Key Infrastructure providing Trust Services for external customers is separated from the infrastructure for internal OPL use.

This CPS is applicable to:

1) all Certification Authorities and Registration Authorities operated in the PKI hierarchy of Signet CC,
2) all Certificates issued in that hierarchy.

This CPS:

1) defines the minimal requirements necessary to ensure that the critical functions are performed at a proper level of trust disclosures basic information on how these requirements are implemented in Signet CC,
2) applies to all actors of the certification process, to the extent of generating, issuing, using, and managing all Certificates and cryptographic key pairs.

#### 1.8.1.1 The body responsible for establishing the Certificate Policies – Policy Approval Committee

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

Policy Approval Committee was set up by the Signet CC Business Owner decision, who accepts the statutes of the Committee and appoints its members.

The Policy Approval Committee is responsible for:

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

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

Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych
Centrum Certyfikacji Signet
Policy Approval Committee
ul. Piotra Skargi 56
03-516 Warszawa / POLAND

#### 1.8.1.2 Certification Authorities – Certificate issuing bodies

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

The Root Certification Authorities issue the highest-level Certificates and sign their own Certificates.

Operational Certification Authorities are subordinate to (certified by) appropriate Root CA.

#### 1.8.1.3 The superordinate Certification Authority – Root CA

Root CA — the superordinate Certification Authority, may issue Certificates only to its subordinate Certification Authorities and to itself (self-signed Certificate).

Root Certification Authorities have no Registration Authorities. No competencies of Root Certification Authorities in respect to registration of the subordinate CAs may be delegated to any other entity or institution.

#### 1.8.1.4 Operational Certificate Authorities – CAs

Operational 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 Service Recipients. In such case, the division of responsibility between Signet CC and such entity is regulated by the agreement. Signet CC is responsible to the Service Recipients for acts of such entities as for its own acts.

Final approval of Certificate application is always conducted by Signet CC Registration Inspector basing on check of the application itself and all required attachments and cannot be delegated to any third party.

A CA may issue Certificates both to Service Recipients and to other Certification Authorities.

#### 1.8.1.5 Certificates issued by Signet CC

The certificates issued by the Authorities operated by Signet CC contain the information provided by the Certificate Holders and guarantee that the data provided in the Certificate has been verified by Signet CC or by another entity acting in its name. The certificates enable identification of the Certificate Holder. The necessary identification information is possessed by Signet CC 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.

Certificates issued by Signet CC are not qualified certificates as defined by eIDAS Regulation.

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

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

### 1.8.2 Registration Points

The main task of the Registration Point is to register the 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 Signet CC operating documents and the relevant Certificate Policies.

### 1.8.3 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 Operator.

#### 1.8.3.1 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.

Access to CRLs, Policies and CPS is always free of charge.

Public access to Repository is read-only and is protected against unauthorized modification of content.

### 1.8.4 Applicability

This CPS is applicable to Trust Services provided by Signet CC to Trust Service Recipients.

The basic functional classes of Certificates managed by Signet CC 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 Electronic Signatures
- collection of the Certificate Holder's identification data
- protection of access to logical and physical resources.

### 1.8.5 Contact information

This CPS is managed by Signet CC.

Any comments on this CPS may be addressed to:

Orange Polska S.A.
Bezpieczeństwo Systemów Teleinformatycznych
Centrum Certyfikacji Signet
Policy Approval Committee
ul. Piotra Skargi 56
03-516 Warszawa / POLAND

## 2 General provisions

This section presents the obligations of Certification Authorities, Registration Authorities, Registration Points, and Service Recipients.

Service Recipients are informed through the Certificate Policy about their rights and obligations related to ensuring security, protection, and integrity of their private keys.

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 Trust Services offered by Signet CC 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 Trust Services offered by Signet CC (including the financial liability) are described in the relevant agreement and in the Certificate Policy.

### 2.3 Interpretation and enforcement of legal acts

The Trust Services are provided by Signet CC in compliance with the legal regulations in force in Poland.

### 2.4 Fees

Fees for the provision of Trust Services are established in the relevant contracts.

### 2.5 Repository and publications

#### 2.5.1 Information published by Certification Authorities

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

- Certificate Policies subject to this CPS: http://www.signet.pl/docs/index.html
- This CPS: <LINK>
- Certificates of Signet CC Certification Authorities: http://www.signet.pl/repository
- Certificate Revocation Lists (CRL): http://www.signet.pl/CRL/index.html

#### 2.5.2 Frequency of publications

The frequency of publications by Signet CC is as follows:

- Certificate Policy and this CPS — as per section 8.1, 8.1,
- Certificates of the Signet CC 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
- CRLs — 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 Signet CC
- auxiliary information — every time the information is updated.

At least once a year CPS, all Certificate Policies and other Signet CC key documents are reviewed for compliance against currently applicable law, standards and requirements and updated, if necessary.

### 2.5.3 Access control

The following information is available publicly:

- Certificate Policies and this CPS
- Certificates of Certification Authorities in the Signet CC hierarchy
- CRLs
- selected auxiliary information.

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

### 2.5.4 Test sites for software developers

Signet CC hosts test Web pages that allow Application Software Suppliers to test their software with End User Certificates that chain up to each publicly trusted Root Certificate. Signet CC hosts separate Web pages using Subscriber Certificates that are:

- valid (https://ssl-test.signet.pl)
- revoked (https://ssl-test.signet.pl:9443)
- expired (https://ssl-test.signet.pl:8443)

## 2.6 Auditing

Subject to sec. 2.6.3, the audit is conducted by an institution authorized to perform such activities and properly experienced in applications of the Public Key Infrastructure and cryptographic technologies, independent from Orange Polska S.A. and all other companies of Orange Polska group.

### 2.6.1 Audit frequency

The full audit of public Trust Services, verifying the compliance of Signet CC with the documented procedures and this CPS, is conducted annually.

### 2.6.2 Areas covered by the audit

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

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

### 2.6.3 Self-audits

Signet CC conducts internal self-audits on quarterly basis against a randomly selected sample of the greater of one certificate or at least three percent of the Certificates issued by it during the period

commencing immediately after the previous self-audit sample was taken. The compliance of the certificates and related documentation with CPS and the relevant Certificate Policy is checked.

Audits are conducted by the Registration Inspector under the supervision of the Security Inspector.

### 2.6.4 Actions undertaken to rectify deficiencies detected during the audit

In case of deficiencies, Signet CC shall promptly introduce the necessary corrective measures.

In the case of external audit, the scope and manner of deficiency rectification are communicated to the auditing institution and in the case of self-audit - to the Security Inspector.

## 2.7 Information protection

Processing of information in CC Signet is governed by applicable law, in particular the Act, the provisions on personal data protection and the internal normative documents of Orange Polska S.A. based on ISO/IEC 27001 "Information technology -- Security techniques -- Information security management systems -- Requirements" standard, comprising OPL's information security management system.

The access of operational personnel to information processed by Signet CC is limited to the minimum necessary to perform the official duties.

The information transferred to Signet CC in result of the practices and procedures defined in this CPS is subject to the personal data protection according to the legal regulations effective in Poland. "Orange Polska S.A. Privacy Policy".

Signet CC collects and process information supplied by certification Service Recipients only to the extent directly related to the issuance and management of User Certificates.

Signet CC does not copy or store Electronic Signature Creation Data nor Electronic Seal Creation Data (User private keys) or other data that could be used to restore them.

### 2.7.1 Types of information processed in CC Signet as Protected Information

### 2.7.2 The following information is treated as Protected Information

- the information provided in the Certificate application or collected through the application handling process, not disclosed (directly or indirectly) in the Public Key Certificate, in particular, personal data of Users,
- Information and data relating to the provision of Trust Services whose disclosure could be detrimental to the Trust Service Provider or the Trust Service Recipient, in particular Data for the Submission of Electronic Signature Creation Data or Electronic Seal Creation Data (protected information within the meaning of Article 15.1 of the Act).
- agreements with the Signet CC customers,
- Technical information (including internal records of systems), operational and procedural information whose disclosure could affect the security of the Services provided, non-publicized audit reports, safety tests and risk analysis,
- Access codes, passwords, and other secrets used to protect access.

### 2.7.3 Information types treated as non-classified

The following information is treated as non-classified:

- Certificate Policies
- Certification Practice Statement,
- Certification Authority Certificates,
- CRLs published in the Repository,

- Information about OPL's Trust Services infringements, and information about security breaches and loss of integrity that have a significant impact on the Trusted Services provided or personal data processed within it (Article 19 of the eIDAS Regulation)

### 2.7.4 Obligation to protect Confidential Information

All persons carrying out tasks related to the provision of the Trust Services are obliged to maintain the confidentiality of the Protected Information specified during the employment period and after the termination of the period, in accordance with applicable laws.

The obligation to protect the Confidentiality of information by external contractor employees performing tasks in favor of OPL is governed by the agreements concluded by OPL with those entities.

Persons responsible for keeping the rules of conduct and the Protected Information indicated above are liable in accordance with the law.

### 2.7.5 Disclosing the information on the Certificate revocation reason

Signet CC disclosures the information on the reasons of Certificate revocation or suspension in the form of the Certificate Revocation Lists (CRLs) and the OCSP service.

Revocation entries on a CRL or OCSP Response are not removed until after the Expiry Date of the revoked Certificate.

#### 2.7.5.1 OCSP Service

Information about the validity of certificates issued under the Policy is also available through OCSP at http://ocsp.signet.pl..

OCSP responses conform to RFC6960 and RFC5019. OCSP responses are signed by an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked. The OCSP signing Certificate contains an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960.

Signet CC supports an OCSP capability using the GET method.

If the OCSP responder receives a request for status of a certificate that has not been issued, then the responder responds with a "unknown" status.

Signet CC updates information provided via an Online Certificate Status Protocol immediately after every revocation operation, but no less frequently than every 24 hours. .

OCSP responses from this service have a maximum expiration time of ten days.

### 2.7.6 Providing information and data to authorized bodies

Except for Electronic Signature Creation Data or Electronic Seal Creation Data, Signet CC provides information only on request of:

- court or prosecutor - in the course of ongoing proceedings,
- minister responsible for computerization - in connection with his supervision of the activities of trust services,
- other authorities authorized by law - in connection with their ongoing proceeding.

### 2.7.7 Disclosure of Protected Information on request of the Certificate Holder

The Certificate Holder who is the subject of the Protected 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 electronically by the Certificate Holder in compliance with the relevant Certificate Policy
- written request submitted by the Certificate Holder.

This does not include Electronic Signature Creation Data (private keys) of the Certificate Holder, which shall remain under the exclusive control of the holder and never appear in Signet CC systems.

### 2.7.8 Other circumstances warranting disclosure of Protected Information

Unless otherwise specified in the Certification Policy, no other circumstances enable a disclosure of the Protected Information without the formal consent of the entity concerned.

## 2.8 Intellectual property rights

### 2.8.1 General provisions

Signet CC 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 Signet CC are property of their respective legal owners.

### 2.8.2 Copyrights

Proprietary rights to the CPS are owned exclusively by Orange Polska SA.

Proprietary rights to the Object Identifiers (OID) assigned for the purposes of the Signet CC infrastructure are owned exclusively by Orange Polska S.A.

# 3 Identification and authorization

The detailed method of identification and authorization of the Trust Service Recipient is specified in the relevant Agreement and Certificate Policy.

The most important elements of those processes are presented below.

## 3.1 Submission and handling of applications

Submission and handling of applications for issuance of a Certificate, including the implementation of identification and authentication tasks, shall be carried out in accordance with the relevant Certification Policy.

Applicants may be informed about the other types of Certificates available to them when submitting their application.

The application 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 it detailed provisions.

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 should explain to the Applicant the cause of rejection and allow him to improve, supplement, or re-submit the application, unless the relevant Certificate Policy 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 Signet CC allow a simplified registration procedure which does not require appearing in person in the Registration Point.

### 3.1.1 User 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.

Signet CC support using Certificates as a means of identification of the Certificate Holders.

### 3.1.3 Principles of interpretation of various name forms

In accordance with the relevant Certification Policy.

### 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

Signet CC 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 Electronic Signature appended to the Certificate request.

### 3.1.8 Authentication of institutions

In accordance with the relevant Certification Policy.

### 3.1.9 Authentication of identity of individual Certificate Holders

An individual certificate holder is authenticated in accordance with the relevant Certification Policy.

### 3.1.10 Authentication of server/device data disclosed in the Certificate

In accordance with the relevant Certification 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.

Existing Renewal Procedures for the Certificate are defined by the relevant Certificate Policy.

## 3.2 Renewal of a revoked Certificate

A revoked Certificate may not be renewed.

## 3.3 Request to revoke a Certificate

Existing Revoking Procedures for the Certificate are defined by the relevant Certificate Policy.

# 4 Functional requirements

This chapter defines the basic issues related to the procedure of initiating the certification process and other contacts with Signet CC. 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

In accordance with the relevant Certification Policy.

## 4.2 Issuing the Certificate

The Registration Point, Registration Authority, and Certification Authority 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, Signet CC 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

Signet CC 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 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 Root Certification Authorities, 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 Root CA, 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.

Detailed rules for keeping a security log are described in the Signet CC internal documents specifying the rules for performing the audit and archiving

The records of the security log also enable detection of any attempts to corrupt the protections in Signet CC and should be used in implementation of mechanisms preventing such corruption. The scope of retained information 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 Security Inspector.

### 4.5.1 Types of recorded events

The security log records the events listed below, related to the execution of automatic and manual procedures in system elements, 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 operating 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, a Certificate or a CRL. |
| Successful and unsuccessful attempts to create, modify, or delete the certificate holder information |
| Creating, archiving, and restoring backup copies |
| Changes to the configuration of operating systems and applications |
| Upgrades and updates of the software and hardware |
| Maintaining hardware that is part of the operating system and applications |
| Changes of the operating personnel |

### 4.5.2 Frequency of the event record processing

The Security Inspector supervise reviewing the event records in compliance with the security rules applicable for Orange Polska S.A.

The above tasks can be implemented automatically using the dedicated tools of the SIEM class (Security Information and Event Management).

### 4.5.3 Retention period of the event records

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 are 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

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

### 4.5.5 Procedures of making copies of event records

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

### 4.5.6 Notification of entities responsible for the event

The OPL SOC notifies the Security Inspector and System Administrator of any security-critical events occurring in the Signet CC systems components.

Notified persons take appropriate action to prevent emerging threats.

In case of any security breach or loss of integrity of the Trust Service provided, the CC Signet notifies immediately Supervisory Authority and, where applicable, other relevant entities - in accordance with OPL's security incident management procedure.

If, in the course of handling a security incident, it is found that a breach of security or loss of integrity adversely affects the natural or legal person or other subject for whom the Trust Service was provided, the CC Signet notifies immediately this person or subject, in accordance with applicable laws.

### 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 Signet CC system components to threats.

## 4.6 Data archiving

The following data must be archived:

a) all data related to the Signet CC system protection,

b) applications submitted by Certificate Holders and Certificate applications,

c) information about Certificate Holders, information about generated Certificates and CRLs,

d) information (such as password) necessary to access the keys used by the CAs and RAs,

e) exchange of information between the Signet CC authorities,

f) correspondence exchanged with the certificate holders.

### 4.6.1 Types of archived data

The following information must be archived:

a) system logs, according to sed. 4.5.1,

b) Certificate applications

c) Certificates and CRLs

d) private keys associated with the public keys disclosed in the encryption Certificates, if the relevant Certificate Policy stipulates so

e) full backup copies of the system components

f) all formal correspondence exchanges with Signet CC

### 4.6.2 Data archiving frequency

The data archiving frequency is the Signet CC policies for auditing and archiving.

### 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, or the Services provided by the Certification Authority concerned are subject to migration to another Authority.

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

### 4.6.4 Archive copy procedures

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

### 4.6.5 Requirements for time stamping of achieved data

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 internal documents adopted by Signet CC.

The integrity of the system logs of the Authorities is automatically verified by software used in Signet CC. The detected misstatements are handled in accordance with Signet CC rules.

## 4.7 Key distribution

The public keys of Root Certification Authorities are distributed through a self-signed Certificate (i.e. the Authority signs itself it own key).

Public keys of other Authorities are distributed through Certificates issued by their respective superordinate Authorities.

## 4.8 Key replacement

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

1) any impact upon the operations of the subordinate Trust Service Providers and Service Recipients must be minimized
2) the subordinate certification Trust Service Providers and 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 Root CA Certificate.

## 4.9 PKI compromise and disaster recovery

Signet CC has adopted and manages a detailed documentation covering:

- Signet CC business continuity plans and Signet CC basic system components recovery plans,
- procedures for data archiving and off-site storage.

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

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

### 4.9.1 Damage of computing resources, software, or data

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

### 4.9.2 Revocation of a CA key

The Signet CC Authorities have contingency plans in case of revocation of their keys due to compromise or other reasons. Those plans specify the activities 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 Signet CC security system. Those measures include changing all passwords, PIN codes, and room access codes, as well as a full internal audit of the system security.

### 4.9.4 Business continuity and disaster recovery plan

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

Signet CC has adopted and manages the business continuity plan and recovery plan by performing the following tasks:

1) identification of the internal resources necessary to implement the plan
2) identification of the persons authorized to decide about beginning of 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 components in case of unexpected events; setting the maximal downtime.

In order to ensure business continuity and disaster recovery, Signet CC 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 specifies 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 Signet CC and the building structure

Signet CC is located in Warsaw/Poland, in protected facilities accessible only to authorized persons. Signet CC has at least one backup location that is independent of the primary location, which can take over all functions in a short period of time.

The Signet CC PKI components are operated in a physically secure environment compliant with the legal requirements and OPL security standards.

Applied electronic security systems, building security and physical protection organization comply with the requirements of the Physical Security Policy of Orange Poland for such objects.

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

### 5.1.2 Physical access

Access to the Signet CC system components is exclusively authorized. The Signet CC rooms are equipped with access control systems based on personal identifiers and access code systems. The details of the access control system design constitute protected information.

### 5.1.3 Power supply and air conditioning

The working environment of Signet CC 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 Signet CC facilities are equipped with a redundant air conditioning system.

### 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 Signet CC are notified. They undertake actions envisaged in the building operating rules and report the incident to the competent utility company and to the Signet CC Security Inspector.

### 5.1.5 Fire protection

The fire protection system installed in the building complies with the relevant fire regulations and standards. The Signet CC server rooms are equipped with gas fire extinguishing system. In case of fire risk, OPL procedures are followed.

### 5.1.6 Information media

The media containing protected information that are not actually used in Signet CC, are stored in protected safes on site. Also, copies of the archive data and cryptographic materials of Signet CC in encrypted form and divided into parts, are stored in two external safes.

### 5.1.7 Destroying of unnecessary information media

Unnecessary paper documents, electronic documents and other information media containing protected information are destroyed in a safe manner in accordance with the rules applicable in the OPL:

- For data storage media in digital form - in accordance with the OPL standard for information erasure.
- in case of printed materials — through using a shredder located within Signet CC premises.

## 5.2 Checking the organizational protections

The following subsections present the trusted functions that can be performed by the Signet CC 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 Signet CC and of the 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 Signet CC:

- **Policy Approval Committee** - a body responsible for approving the Certificate Policies, Certification Practice Statement, and all other documents essential for the Signet CC operations
- **Security Inspector** - a person responsible for security of the Signet CC system components, and in particular for analyzing the logs of events occurring in the ICT system components used for providing the Trust Services by Signet CC.
- **Public Key Infrastructure Administrator (PKI Administrator)** - a person responsible for activating the CA keys, making any changes in the Signet CC hierarchy, submitting applications for issuing certificates to the subordinate authorities, and adding the approved Certificate Policies to the Signet CC 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 Signet CC system.
- **System Administrator** - a person responsible for the Signet CC system software and for making the system component copies under supervision of the Security Inspector and in compliance with the archiving rules and the operational procedures,
- **Repository Administrator** - a person responsible for all publicly available sites used by Signet CC 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 Signet CC archive, the whole Signet CC documentation, receiving documents to the archive, and issuing documents in compliance with the clauses and procedures in effect in OPL, as well as for the consistency and completeness of the archived documentation.

Some of the above mentioned functions may be performed by one person, unless the scope of responsibilities performed within a function may cause a conflict of interest (e.g., the Security Inspector function with the Administrator function). The Policy Approval Committee defines an up-to-date list of trusted functions and the detailed scope of their tasks.

Any task which involves creating, archiving, or recovering of a private key used by CA to Certificate and CRL signing, requires presence of at least two persons with sufficient authorization (e.g. the Security Inspector and the PKI Administrator).

The detailed principles and procedures are described in the relevant operational documents.

### 5.2.2 Identification and authentication of the entrusted functions

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

- entering into the list of persons entitled to access the Signet CC premises
- entering into the list of persons with physical access to the Signet CC system components and network
- making a decisions on the performance of the assigned function
- assignation of an account and password in the Signe CC system components
- 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 Signet CC system software or the operating system in compliance with the procedures adopted by Signet CC.

## 5.3 Checking the personnel

### 5.3.1 Qualifications and experience of the personnel

For each function in Signet CC, 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 trusted functions in Signet CC listed in sec, 5,2,1 are additionally subject to the procedure criminal record verification.

### 5.3.3 Preparation for the duties

Before assuming the duties, the Signet CC 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 ICT system
- duties entrusted or to be entrusted
- rules of handling Protected Information which will be accessed in official duties
- procedures to be followed in case of a failure or disaster affecting the CA systems.

### 5.3.4 Procedure in case of unauthorized actions

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

In case of any security breach or loss of integrity of the Trust Service provided, the CC Signet notifies immediately Supervisory Authority and, where applicable, other relevant entities - in accordance with applicable laws.

If, in the course of handling a security incident, it is found that a breach of security or loss of integrity adversely affects the natural or legal person or other subject for whom the Trust Service was provided, the CC Signet notifies immediately this person or subject, in accordance with applicable laws.

### 5.3.5 Documentation provided to the personnel

Employees performing trusted function have access to following documents:

- this CPS and relevant Certificate Policies
- system components documentation, to the extent necessary to perform the entrusted tasks
- a document with the scope of responsibilities associated with the function performed.

# 6 Technical security procedures

This section describes the procedures of creating and managing the cryptographic key pairs of Signet CC 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 cryptographic 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 Signet CC (Certification Authorities and Registration Authorities), which determine the security of the whole public key certification system.

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

Key generation procedure is conducted following detailed script, under the supervision of commission appointed by Policy Approval Committee. All procedure activities are logged in detail.

The detailed requirements and obligations related to generating and using the cryptographic key pairs of End Users are set forth in the Agreement and in the relevant Certificate Policies.

## 6.2 Protection of the private key

### 6.2.1 Hardware cryptographic module (HSM) standard

The hardware cryptographic modules (HSMs) used in the Signet CC CAs and RAs must comply with the industry standards: at least FIPS 140-2 Level 3 or Common Criteria EAL 4+, which define the level of logical and physical security.

### 6.2.2 Private key partitioning

The private keys of Certification Authorities are generated and 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 that are stored at separate locations.

### 6.2.3 Depositing the private keys

Copies of the private keys of the Signet CC Certification Authorities are deposited in the encrypted form and divided into parts at two secure, independent external sites, external to Signet CC server room . The principles of access to the deposited copies are strictly defined and controlled by Signet CC.

Private keys generated by RAs for End Users are not deposited.

### 6.2.4 Backups copies of the private keys

#### 6.2.4.1 Backup copies of Signet CC PKI entities private keys

The private keys of CAs and RAs are generated and stored in the secure environment of the hardware cryptographic module. Outside that environment, copies of the private keys are written onto electronic cards in the encrypted form and divided into parts 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 stored in separate locations, in compliance with the secret division scheme.

#### 6.2.4.2 Backup copies of End Users' private keys

End users may make backup copies of their private keys stored in operating system resources of computers, making 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 Electronic Signature should never be made.

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

Signet CC does not store copies of private keys generated for End Users, except as described below.

### 6.2.5 Archiving the private keys

Signet CC may archive private keys for decryption generated for End Users. The acceptability and principles of private key archiving depend on the specific Certificate Policy. The keys are securely stored in an encrypted form in a dedicated key achieve module. Relevant Certificate Policy precisely stipulates cases, in which key recovery is allowed. Unless stipulated otherwise by the 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 to the appropriate module. 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 Signet CC, 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 after restarting the cryptographic module containing the given key.

### 6.2.9 Private key destruction method

Private keys of Signet CC, 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, Signet CC 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 hardware cryptographic module requires the following: electronic cards issued to the module operators, passwords protecting access to such cards, and other mechanisms protecting the access to the applications controlling the hardware cryptographic module.

If a key pair is generated by Signet CC 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 cryptographic modules are stored in a separate, secure room and never leave Signet CC 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.

Access to passwords can only occur in the presence of the Security Inspector.

The activation data may be delivered to the Certificate 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 ICT system protections

### 6.5.1 Specific technical requirements for the ICT system protection

The Signet CC system components are protected in compliance with the ICT security standards adopted by Orange Polska S.A., with due consideration to the specifics of the provided Services.

Signet CC requires multifactor authentication for all accounts capable of directly causing certificate issuance.

Personal data are protected in accordance with the laws applicable in Poland and regulations in force in Orange Polska S.A.

### 6.5.2 Evaluation of the ICT system protection level

he protection level is evaluated in compliance with the guidelines of an external auditor and is based, among other things, on the guidelines provided in WebTrust™ standard.

## 6.6 Technical control cycle

Signet CC critical components are monitored continuously by dedicated units in Orange Polska (SOC OPL). In case of detection of anomalies, procedures are performed to inform the Administrators of Signet CC.

## 6.7 Controlling the network protections

The system components of Signet CC comply at least with the technical requirements stipulated by the legal regulations for Non-qualified Trust Service Providers.

The servers and workstations of the Signet CC are connected to a multi-segment internal LAN. The Certification Authorities are separated from the Internet by several 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.

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

All subnets from which any access to Signet CC 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 Signet CC network are monitored and logged in order to provide evidence in case of unauthorized activities.

## 6.8 Cryptographic module management engineering

Signet CC only accepts hardware cryptographic modules that meet the requirements of Section 6.2.1. Signet CC does not define additional requirements in this regard.

# 7 Certificate and CRL structure

The Certificate and CRL structure complies with the formats specified in the ITU-T X.509 v3 standard.

## 7.1 Certificate profile

The profile of the Certificates issued by Signet CC complies with the guidelines of the RFC 5280 document. Since Signet CC issues Certificates to various Holders who may use them in many areas of their operations, Signet CC 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

Signet CC supports the following basic fields of the certificate:

c) **version** - certificate format version; the value is always 2, meaning version 3 of the Certificate format, according to the X.509 standard.

d) **serialNumber** - an integer number, unique within the given Certification Authority, assigned to each Certificate issued by such authority.

e) **signature** I identifier (OID) of the algorithm used by the Certification Authority to digitally authenticate the Certificate.

f) **issuer** - a name identifying the Certification Authority which has issued and signed the Certificate. The field contains a distinguished name. The content of the Issuer field matches the Subject DN of the Issuing CA to support Name chaining as specified in RFC 5280, section 4.1.2.4

g) **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.

h) **subject** - distinguished name of the Trust 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,

i) **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 Signet CC is listed in the relevant Certificate Policy.

### 7.1.3 Private extension fields

The set of private extensions included in the Certificates issued by Signet CC 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 electronic confirmation of the Certificate.

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

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

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

Signet CC withdrew from using SHA-1 in the newly issued End User Certificates of Public Trust Services.

As a result of technological progress, individual Certificate policies may introduce stronger hash functions or cryptographic algorithms.

### 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

A 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 detailed structure of the CRL is defined by the relevant Certificate Policy.

### 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 Signet CC 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 Signet CC Policy Approval Committee.

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

- uniquely identifies the given CPS or Certificate Policy
- identifies the document version.

## 8.1 Change procedure

### 8.1.1 Initial publication

A new Certification Authority in the Signet CC 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. Signet CC 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:

- publish the Certificate Policy in the Repository
- 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 Signet CC, 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 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 Orange Polska S.A.

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

The current CPS is published in the Signet CC Repository.

A new or changed Certificate Policy is published in the Signet CC Repository indicated in the given Policy or in CPS. 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 Signet CC 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 Signet CC or of any Certification Authority in its hierarchy, Signet CC shall undertake all economically justified measures to minimize the negative impact of such decision upon the Trust Service Recipients.

In particular, Signet CC shall:

1) at least by 90 days before the liquidation:
   - publicly announce the liquidation by publishing an announcement on the Signet CC website at http://www.signet.pl,
   - notify in writing the authority, to which the application for accreditation has been made (if any),
   - notify all Certificate Holders with valid Signet CC 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
   - revoke, without request of the Holder, all Certificates issued by the liquidated Authority, including the infrastructure Certificates;
3) immediately after the closure of operations:
   - professionally destroy, in front of a commission, all copies of private keys of the liquidated infrastructure;
   - return the costs to the subscribers at their request, as per item 1.c above
   - 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,
   - destroy, in front of a commission, all remaining data and documents related to the liquidated operations.