# Certificate Policy

## Disig, a.s.

Version 5.4

Valid from September 1, 2020

OID 1.3.158.35975946.0.0.0.1.1

# Table of Content

| | |
|---|---|
| Business Name | Disig, a. s. |
| Residence | Záhradnícka 151, 821 08 Bratislava, Slovakia |
| Registration | Business Register of the District Court Bratislava I, Insert No. |
| Telephone | + 421 2 208 50 140 |
| E-mail | disig@disig.sk |

# 1. INTRODUCTION

This document defines the Certificate Policy (hereinafter referred to as "CP") of company Disig, a.s., with its registered office at Záhradnícka 151, 821 08 Bratislava, National Trade Register number: 35975946, registered in the Commercial Register of District Court Bratislava I, Sa, insert no. 3794/B, as a Trusted Service Provider (hereinafter referred to as "Provider"). This CP applies to all root CAs and subordinate CAs operated by the Provider, which provides trusted services except qualified trusted services.

The Provider's website for the provided trusted services is available here:

https://eidas.disig.sk

## 1.1 Overview

This CP defines the creation and management of public key certificates, according to X.509 version 3 [1], in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [2]Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [3] (hereinafter "BR") and the requirements of Regulation (EU) No. 910/2014 of 23 July 2014 on electronic identification and trustworthy services for electronic transactions in the internal market and repealing Directive 1999/93/EC (hereinafter referred to as the "eIDAS Regulation") [4].

The Provider confirms that this CP takes account of all requirements of the current version of the document [3], which is published at http://www.cabforum.org. In the event of any inconsistency between these requirements and this CP, the requirements of the current version of the document [3] prevail.

This policy is structured in accordance with RFC 3647 [4].

## 1.2 Document Name and Identification

| | |
|---|---|
| Document Name: | Certificate Policy |
| Name abbreviation: | CP CA Disig |
| Version: | 5.4 |
| Approved on: | August 25, 2020 |
| Valid from: | September 1, 2020 |
| This document is assigned an object identifier (OID): | 1.3.158.35975946.0.0.0.1.1 |

Description of the object identifier (OID):

1. - ISO assigned OIDs

1.3. - ISO Identified Organization

1.3.158. - Identification number (Company ID - **IČO))**

1.3.158.35975946. - Disig, a. s.

1.3.158.35975946.0.0.0.1. - CA Disig

1.3.158.35975946.0.0.0.1.1 - CP CA Disig

### 1.2.1 Revisions

| Revision | Revision date | Description; Reviewer |
|---|---|---|
| 1.0 | March 25, 2006 | Firs version; Mišković |
| 1.5 | December 20, 2006 | Formal text editing - Formatting, correcting links, editing text in section 4 "Operational requirements"; Mišković |
| 2.0 | January 23, 2007 | CP expansion in relation to the new type of certificates issued for the contracted client.<br>Addition of section 7 "Certificate Profiles"; Mišković. |
| 2.1 | March 29, 2007 | Correcting text in chap. 2.8 and Chap. 4.9<br>Text editing related to a minor change in a partner's certificate; Mišković |
| 3.0 | March 19, 2008 | Overall revision of the CP for each type of certificate; Ďurišová, Mišković |
| 3.1 | June 24, 2008 | A new type of certificate adding.; Mišković |
| 3.2 | November 10, 2008 | Change certificate validity for domain user PKI VsZP<br>Termination of operation at Záhradnícka 153; Mišković |
| 3.3 | November 25, 2008 | Editing the wording:<br>section 3.1.9 - Domain ownership verification<br>section 4.1.1; 4.1.2, - validation of the Applicant's e-mail address; Mišković |
| 3.4 | Jun 2, 2009 | Modification regarding the requirement for the minimum length of the public key to be issued by CA Disig (section 5.1.3; 6.1.2);<br>Change the email address location in the certificate profile (section 3.1.2; 6.1.2); Mišković |
| 4.0 | October 10, 2009 | Editing in connection with Mozilla Foundation requirements when applying for a CA Disig certificate to the Mozilla Root Certificate Store; Mišković |
| 4.1 | May 11, 2010 | Inclusion of proposed audit corrective actions of 13.11.2009 (audit according ETSI TS 102042 V1.3.4);; Mišković |
| 4.2 | March 3, 2011 | Changing the validity of certificates; incorporating Mozilla Foundation's new security policy requirements and Microsoft code signing requirements; formal edits of tables and texts; Mišković |
| 4.3 | January 25, 2012 | Supplementing the possibility to issue certificate for subordinate CAs, adding signature algorithms, and regular annual review of content; Mišković |
| 4.4 | June 22, 2012 | Incorporating Requirements for the Baseline Requirements for Issuing and Managing Publicly-Trusted Certificates, v.1.0, issued by the CA / Browser Forum; Mišković |
| 4.5 | August 15, 2013 | Refining of CA Disig CA root CA Certificate Profile and other Certified Types of Certificates; Mišković |
| 5.4 | June 21, 2013 | Correction of the OID of the document - deleting the version of the document from the OID (section 1.2). Editing Profiles for subordinate CAs - certificatePolicies Identifier (section 7.1.2);<br>Enable issuing "wildcard" TLS/SSL certificates to be issued at the third level of the domain name (3.1.2); Mišković |
| 4.7 | February 2, 2015 | Z Inclusion of the requirements of the current version of the Baseline Requirements for the Issue and Management of Publicly-Trusted Certificates, v.1.2.3; Revision of the CP in connection with the amendment to the Electronic Signature Act, pursuant to Act no. 305/2013 Coll.; Mišković |

| | | |
|---|---|---|
| 4.8 | May 22, 2015 | Verification of CAA records (4.1.5); Mišković |
| 4.9 | October 10, 2016 | Changes made in connection with the eIDAS Regulation and in connection with the expiry of Act no. 215/2002 Coll. and the entry into force of Act no. 272/2016 Z. z .; Inclusion of Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates, to Version v.1.4.1; Mišković |
| 5.0 | September 25, 2017 | Conversion of CP to RFC 3647 format; Inclusion of eIDAS requirements and incorporation of the requirements of the current version of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.5.2; Mišković |
| 5.1 | May 23, 2018 | Entry into force of Regulation no. 2016/679 - GDPR; Modification of the wording of point 1.3.3; amendment of the wording of point 3.2.2.4 (new verification method); addition of clause 4.2.2 (gTLD); addition of item 4.9.11 (OCSP stapling); Mišković |
| 5.2 | May 17, 2019 | Modifying chapter 4.9 in accordance with the Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates, v.1.6.1; Modifying chapter 8.4 in accordance with the Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates, v.1.6.5; Clarification of the definition in chapter 1.3.1; Addition of chapter 3.1.4; Mišković |
| 5.3 | December 2, 2019 | Editing the certificate profile for electronic signature (3.1.4.1.); modification of the validity of issued certificates for signature / seal (7.1.4); Update links (1.6.3.); Shortcuts and minor text edits; Mišković |
| 5.4 | September 1, 2020 | Modification of the validity of TLS / SSL certificates in accordance with the requirements [3]. Specification of domain ownership verification methods in section 3.2.2.4; Changing the titles of chapters according to their titles in [3]; Mišković |

## 1.3 PKI Participants

### 1.3.1 Certification Authorities

Root CA is the top-level Certification Authority whose Root Certificate is distributed by Application Software Suppliers. Root CA issues Subordinate CA Certificates.

Subordinate CA is a Certification Authority whose Certificate is signed by the Root CA, or another Subordinate CA.

### 1.3.2 Registration Authorities

The Registration Authority ("RA") is an entity that under contract carries out certain selected activities in the provision of trusted services on behalf of the Provider.

The RA shall carry out its activities in accordance with the approved CP and the Certification Practice Statement (hereinafter "CPS") as amended.

Provider may establish following types of RA:

- Commercial RA - is intended to mediate selected trustworthy services of the Provider to the general public and is operated by a third party, on the basis of a written agreement with the Provider;
- Corporate RA - is intended to mediate selected trustworthy services exclusively for the own needs of a particular legal body, For the needs of its operated systems requiring the use of certificates and is operated, on the basis of a written contract with the Provider;

- Internal RA - is operated by the Provider and is intended to provide trusted services for all interested parties. This RA is not a separate legal body.

### 1.3.3 Subscribers

Subscriber is understood to be a natural person or a legal person that is entitled to request for certificate on behalf of an entity whose name appears as the subject in the certificate - Certificate holder.

The Certificate holder may be:

- A natural person;
- A natural person identified in association with a legal person;
- A legal person (that can be an Organization or a unit or a department identified in association with an Organization);
- A device or system operated by or on behalf of a natural or legal person.

When a subscriber is the subject, it will be held directly responsible if its obligations are not correctly fulfilled.

When the subscriber is acting on behalf of one or more distinct subjects to whom it is linked (e.g. the subscriber is a company requiring certificates for its employees to allow them to participate in electronic business on behalf of the company), responsibilities of the subscriber and of the subject are addressed in the General Terms of Service and Use of the Trusted Certificate Issuance and Verification Service " (the "General Terms") [5] published at the Provider's website (see Chapter 1).

This CP. defines the requirement that the Customer shall meet.

Formal Certificate holder means a natural person who undertakes to use a corresponding private key and a certificate in accordance with this CP.

The link between the subscriber and the subject is one of the following:

- To request a certificate for natural person the subscriber is:
  - The natural person itself;
  - A natural person mandated to represent the subject; or
  - Any entity with which the natural person is associated (such as the company employing the natural person or a non-profit legal person the natural person is member of).
- To request a certificate for legal person the subscriber is:
  - Any entity as allowed under the relevant legal system to represent the legal person; or
  - A legal representative of a legal person subscribing for its subsidiaries or units or departments.
- To request a certificate for a device or system operated by or on behalf of a natural or legal person the subscriber is:
  - The natural or legal person operating the device or system;

- Any entity as allowed under the relevant legal system to represent the legal person; or
- A legal representative of a legal person subscribing for its subsidiaries or units or departments.

### 1.3.4 Relying Parties

Relying parties are a natural or legal person who relies, in its proceedings, on the electronic identification or trusted services of the Provider.

### 1.3.5 Other Participants

Policy Management Authority - PMA is a component provided for the purpose:

- Supervising of the CP creation and updating including the evaluation of plans to implement any of the changes;
- Revision of Certificate Practice Statement (hereinafter "CPS") to ensure that the Provider practice meets the requirements written in the CPS;
- Reviewing of audits findings, to determine whether Provider adequately comply with approved CPS;
- Giving recommendations for Provider regarding corrective actions and other appropriate measures;
- Giving advice regarding the suitability of the certificates associated with the CP for specific management applications and managing activities of the certification authority and registration authority;
- Interpretation of the CPS and its instructions for RA and CA;
- Performing the internal audit of the Provider, by assigning this to an independent employee;
- Ensuring that the adopted and approved Certification Policy (CP) and Certificate Practice Statement (CPS) are implemented duly and properly implemented.

PMA represents the top component, which shall decide finally on all matters and aspects related to the Provider and its activities.

## 1.4 Certificate Usage

### 1.4.1 Appropriate Certificate Uses

Certificates issued under this CP are issued for purpose of identifying the public key holder from a cryptographic keys pair (public and private) which is used within the PKI infrastructure.

The cryptographic key pair (private and public) and the certificate issued by the Provider can generally be used primarily for:

- E-mail security (signing and / or encryption of e-mails);
- Signing of electronic documents with advanced electronic signature;

- Creating an electronic seal;
- TLS/SSL communication security (web site authentication);
- Security mechanisms of user workstations;
- Internal PKI processes (secure communication between PKI components etc.).

Provider issued following types of certificates to the Subscribers:

- Certificate for natural person or a natural person identified in association with a legal person (the "certificate for a natural person") - the cryptographic keys associated with this type of certificate are primarily intended for the security of electronic mail, the creation of an advanced electronic signature, authentication for access to different IS; The issued certificate will include, among other things, the Normalized Certificate Policy (NCP) identifier-organization (4) etsi (0) other-certificate-policies (2042) policy-identifiers (1) i.e. 0.4.0.2042.1.1 respectively if the key pair and the issued certificate are stored in a secure electronic signature device, the Extended Normalized Certificate Policy (NCP +) identifier (NCP +) in accordance with EN 319411-1 [5]
- Certificate for a legal body - the cryptographic keys associated with this type of certificate are intended for the creation of an advanced electronic seal by a legal body (the seal originator). The issued certificate will include, among other things, the Normalized Certificate Policy (NCP) identifier-organization (4) etsi (0) other-certificate-policies (2042) policy-identifiers (1) i.e. 0.4.0.2042.1.1 respectively if the key pair and the issued certificate are stored in a secure electronic seal device, the Extended Normalized Certificate Policy (NCP +) identifier (NCP +) in accordance with EN 319411-1 [5]
- Publicly-trusted TLS/SSL certificate (hereinafter "TLS/SSL certificate") - cryptographic keys associated with this type of certificate are designed for authentication of internet accessible servers; Publicly-Trusted Certificates are trusted by virtue of the fact that their corresponding Root Certificate is distributed in widely-available application software. The issued TLS/SSL certificate will include, inter alia, the following certification policy identifiers for organization validation:
  - (4) etsi (0) other-certificate-policies (2042) policy-identifiers (1) ovcp (7)
  - joint-iso-itu-t (2) international-organizations (23) ca-browser-forum (140) certified-polcies (1) baselinerequirements (2)
- The Provider issues management certificates for its needs (Certificate for Subordinate CA, Certificate for Time Stamp Service (TS) or certificate for OCSP Responders).

The trusted certificate issuing services listed in this section are provided by the following Certification Authorities of the Provider:

| Name: | CA Disig Root R2 |
|---|---|
| Certificate serial number: | 0092b888dbb08ac163 |
| Hash (sha1) | B561EBEAA4DEE4254B691A98A55747C234C7D971 |
| Hash (sha256) | E23D4A036D7B70E9F595B1422079D2B91EDFBB1FB651A0633EAA8A9DC5F80703 |
| Comment | It issues certificates only for subordinate certification authorities of the Provider. |

| Name | CA Disig R2I2 Certification Service |
|---|---|
| Certificate serial number | 081792523668f5c8500000000000000003 |
| Issuer | CA Disig Root R2 |
| Hash (sha1) | 19F2783DEDD8561A61C682932EE9D5B4D86B00CE |
| Hash (sha256) | C96F24C45113FD91AE2F9E40E106653BFA0FFBCFA07E209524C844E7C8DA4148 |
| Comment | It only issues TLS/SSL end-user certificates (see 3.1.4.3). |

| Name | CA Disig R2I3 Certification Service |
|---|---|
| Certificate serial number | 08a2395ba703affdac0000000000000004 |
| Issuer | CA Disig Root R2 |
| Hash (sha1) | 1432AC3C02C8C89D6179A40B2EFF6B5AD5DA5D7F |
| Hash (sha256) | 239FFA86D71033BA255914782057D87E8421AEDD5910B786928B6A1248C3E341 |
| Comment | It issues certificates for end users - natural persons (see 3.1.4.1) or legal persons (see 3.1.4.2). |

### 1.4.2 Prohibited Certificate Uses

Certificates issued under this CP are not EU Qualified Certificates according the eIDAS Regulation [6] and cannot be used where EU Qualified Certificates are required.

## 1.5 Policy administration

### 1.5.1 Organization Administering the Document

Table 1contains the data of the Provider who is responsible for the preparation, creation and maintenance of this document.

Table 1 Contact details of the Provider

| Provider | |
|---|---|
| Company | Disig, a. s. |
| Address | Záhradnícka 151, 821 08 Bratislava 2 |
| Company ID | 359 75 946 |
| Phone | +421 2 20850140 |
| e-mail | disig@disig.sk |
| Web site | http//www.disig.sk |

### 1.5.2 Contact Person

For creating policies, the Provider has a PMA that is fully responsible for its content and is ready to answer any questions regarding the Provider's policies (see 1.3.5).

Table 1 contains the contact details of the person responsible for the operation of the Certification Authorities of the Provider.

Table 2 Contact detail of the Certification Authority

| Certificate Authority CA Disig | |
|---|---|
| Address | Záhradnícka 151, 821 08 Bratislava 2 |
| E-mail | caoperator@disig.sk |
| Phone | +421 2 20850150, +421 2 20820157 |
| Web site | http//eidas.disig.sk |
| Incident reporting | tspnotify@disig.sk<br>see more at<br>https//eidas.disig.sk/pdf/incident_reporting.pdf |

### 1.5.3 Person Determining CPS Suitability for the policy

The person who is responsible for deciding on the compliance of the Provider's practices with this CP is the PMA (see 1.3.5).

### 1.5.4 CPS approval procedures

Even prior to the start of operation, the Provider should have approved its CP and CPS and shall meet all of its requirements. A person named by PMA approves the content of CP and CPS.

Upon approval by the PMA, the relevant document is published in accordance with the publication and notification policy.

The PMA has to inform its decisions in such a way that this information is well accessible to the Relying Parties.

## 1.6 Definitions and Acronyms

### 1.6.1 Definitions

Certificate for website authentication means 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;

Trust service means 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;

Certificate holder means the entity identified in the certificate as the holder of the private key belonging to the public key contained in the certificate;

Electronic signature means 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 seal means data in electronic form, which is attached to or logically associated with other data in electronic form to ensure the latter origin and integrity;

Key pair means a part of a PKI system that uses an asymmetric cryptography and consists of a public key and a private key;

Domain Contact means the Domain Name Registrant, technical contact, or administrative contract (or the equivalent under a ccTLD) as listed in the WHOIS record of the Base Domain Name or in a DNS SOA record.

Trust service provider means 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;

RA employee means an employee of the Provider or other legal entity that has a contract with the Provider for the provision of certification services;

Relying party means a natural or legal person that relies upon an electronic identification or a trust service;

**Publicly-Trusted Certificate** means a certificate that is trusted by virtue of the fact that its corresponding root certificate is distributed as a trust anchor in widely-available application software.

Subscriber means a natural person or legal entity to whom a certificate is issued and who is legally bound by a subscriber agreement or terms of use.

Advanced electronic seal means an electronic seal, which meets the requirements set out in Article 36 of eIDAS Regulation; [6];

Advanced electronic signature means an electronic signature, which meets the requirements set out in Article 26 of eIDAS Regulation; [6];

Contractor means a legal entity with whom Disig has entered into a written agreement to provide trusted services;

PKCS#10 means a format of messages sent to a Certification Authority to request certification of a public key;

PEM means file format for storing and sending cryptography keys, certificates, and other data as is formalized by the IETF in RFC 746;

SAN means an extension to X.509 that allows various values to be associated with a security certificate using a subjectAltName field.

TLS, SSL are cryptographic protocols designed to provide communications security over a computer network.

### 1.6.2 Acronyms

| | | |
|---|---|---|
| CA | - | Certification Authority |
| CAA | - | Certification Authority Authorization |
| CMA | - | Certificate Management Authority |
| CP | - | Certificate Policy |
| CPS | - | Certificate Practice Statement |
| CRL | - | Certification Revocation List |
| FQDN | - | Fully Qualified Domain Name |
| HSM | - | Hardware Security Module |
| IČO | - | Organization identification number |
| NBÚ | - | National Security Authority |
| OID | - | Object Identifier |
| PKI | | Public Key Infrastructure |
| PMA | - | Policy Management Authority |
| RA | - | Registration Authority |
| QSCD | - | Qualified Signature Creation Device |

### 1.6.3 References

1. Recommendation ITU-T X.509; Information technology - Open Systems Interconnection - The Directory: Public-key and attribute certificate frameworks.

2. RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile.

3. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates version 1.7.1. s.l. : https://cabforum.org/baseline-requirements-documents/.

4. RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure: Certificate Policy and Certification Practices Framework, Chokhani, et al, November 2003.

5. General terms and conditions of provision and use of a trusted services Disig, a.s.

6. Regulation (EU) No 910/2014 of the European Parrliament and of the Council of 23 July 2014 on on electronic identification and trust services for electronic transactions in the internal market and repealing Directive 1999/93/EC.

7. X.501 Information technology - Open Systems Interconnection - The Directory: Models. s.l. : ITU-T, 10/2012.

8. X.520 Information technology - Open Systems Interconnection - The Directory: Selected attribute types. s.l. : ITU-T, 10/2012.

9. RFC5322 "Internet Message Format".

10. Electronic Signatures and Infrastructures (ESI);Certificate Profiles;Part 2: Certificate profile for certificates issued to natural persons. ETSI EN 319 412-2.

11. Electronic Signatures and Infrastructures (ESI); Certificate Profiles;Part 3: Certificate profile for certificates issued to legal persons. ETSI EN 319 412-3.

12. Informácia o spracúvaní osobných údajov, Disig, a.s.

13. Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation and Act No. 18/2018 Z. z. on the Protection of Personal Data.

14. Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

**15. RFC 6960 „X.509 Interne**t Public Key Infrastructure Online Certificate Status Protocol - **OCSP“.**

16. X.500 Information technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services. 10/2012. s.l. : ITU-T.

17. Electronic Signatures and Infrastructures (ESI);Certificate Profiles;Part 1: Overview and common data structures. ETSI EN 319 412-1.

# 2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

## 2.1 Repositories

Repository shall be located in such a way that they are accessible to the Subscriber and the Relying Parties and in accordance with the overall safety requirements.

The Provider's repository will be its website. The exact URL is given in section 1. The Provider's Web Site is publicly accessible to the Subscribers, the Certificate Holder, the Relying Parties, and the public at all through the Internet.

The publicly available information provided at the Provider's website has a controlled access character.

## 2.2 Publication of information

The Provider shall provide on-line storage that is accessible to the Contractors, Subscribers and Relying Parties that will include at least the following information

- Certificates issued in accordance with this CP,
- current CRL as well as all CRLs issued since the beginning of the certificate issuance activity,
- certificates of root CAs and subordinate certification authorities that belong to its public key to which corresponding private keys are used when signing certificates and CRL
- current version of CP,
- information on the outcome of a regular audit of the performance of the trusted services provided

The Provider may not publish information on issued certificates if they are issued for the internal needs of the Contractors and their partner and it is contractually agreed not to disclose them.

## 2.3 Time or frequency of publication

The certificate shall be published as soon as it is issued. Information on the issued certificate shall be available at the Provider's website (see section 1). Issued Certificates for closed systems or for the internal purposes of Provider may not be publicly available.

The Certificate Revocation List (CRL) shall be published as specified in section 4.9.7. Information about the revoked certificate shall be available at the Provider's website (see section 1), which serves as its repository.

All information to be published in the repository shall be published as soon as possible.

## 2.4 Access controls on repositories

Provider shall protect any information stored in a repository that is not available for public. Provider shall make every effort to ensure the integrity, confidentiality and availability of data related to the provision of trusted services. It also has to take logical and security measures to prevent unauthorized access to the repository for people, who could change, damage, add, remove them or delete data stored in the repository in any way.

# 3. IDENTIFICATION AND AUTHENTICATION

## 3.1 Naming

### 3.1.1 Types of names

Each CA shall be able to create certificates that contain distinguished name according to X.500 (X.500 Distinguished Name, hereafter "Distinguished Name") [6], namely X.501 [7] or X.520 [8] respectively and names according to RFC5322 Internet Message Format [9].

Subscribers shall choose the distinguished name to be included in their certificate themselves.

### 3.1.2 Need for names to be meaningful

The term "meaningfulness" means that the name shall be in a commonly used form to determine the identity of the Subscriber (natural person, legal person, public authority, and website)

Used names shall reliably identify the persons to whom they are assigned.

### 3.1.3 Anonymity or pseudonym of subscribers

The use of pseudonyms and nicknames in certificates is allowed only if is clearly defined that certificate is issuing for a pseudonym by filling in word "PSEUDONYM" in CommonName field (e.g. CN = Alias - PSEUDONYM). This does not affect the provisions regarding the unambiguous identification of the Subscriber.

Provider shall not issue a certificate to an anonymous person.

Provider has the right to refuse to issue a certificate that contains data that violates the principle of meaningfulness.

### 3.1.4 Rules for interpreting various name forms

The interpretation of the individual names of the certificates issued by the Provider shall be in accordance with the certificate profiles described in section 7 of this CP.

The distinguished name used in the different types of certificates issued by the Provider may consist of items that are described in the following sections.

Distinguished name item shall not contain only meta data such as characters "." (ASCII 0x2E), "-" (ASCII 0x2D), or "" (ASCII 0x20) only, or others that should indicate that the value of an item is not filled, is incomplete, or no entry is required.

#### 3.1.4.1 Certificate for a natural person

Table 3 contains a list of fields that may be contained in the DN of certificate for a natural person with a minimum range of mandatory fields. The list of mandatory fields is based on ETSI EN 319412-2. [10]

If required by the Provider, this type of certificate may be extended to other fields as defined in RFC 5280, clause 4.1.2.6. [2]

Table 3 Fields in the certificate for a natural person

| Filed name | OID | Abb. | Description | Note |
|---|---|---|---|---|
| commonName | 2.5.4.3 | CN | Name in the form chosen by the Subscriber | Mandatory field |
| givenName | 2.5.4.42 | G | Given name as it appears in the document submitted for identification | Mandatory field (only if in CN field is not used a pseudonym or G and SN are not in CN) |
| Surname | 2.5.4.4 | SN | Surname as indicated in the document submitted for identification | |
| pseudonym | 2.5.4.65 | | Pseudonym chosen by Subscriber | Mandatory field (only if in CN field is used a pseudonym) |
| serialNumber | 2.5.4.5 | | An identifier that ensures the uniqueness of the subject's name | Mandatory field |
| organizationName | 2.5.4.10 | O | Organization name | Optional field |
| serialNumber resp. organizationIdentifier | 2.5.4.5 Or 2.5.4.97 | | Reference to the legal entity identification | Optional field |
| organizationUnitName | 2.5.4.11 | OU | Organization unit name | Optional field |
| localityName | 2.5.4.7 | L | Locality name | Optional field |
| countryName | 2.5.4.6 | C | Two-character abbreviation for country name SK for Slovak republic | Mandatory field |

Important note If the certificate is used to sign and encrypt e-mail, the request shall contain a valid e-mail address of the Subscriber.

### 3.1.4.2 Certificates for a legal person

Table 4 contains a list of fields that may be contained in the DN certificate for a legal person with a minimum range of mandatory items. The list of mandatory items is based on ETSI EN 319412-3 [11].

If required by the Provider, this type of certificate may be extended to other fields as defined in RFC 5280, clause 4.1.2.6. [2]

Table 4 Fields in the certificate for a legal person

| Filed name | OID | Abb. | Description | Note |
|---|---|---|---|---|
| commonName | 2.5.4.3 | CN | Commonly used name of a legal person. | Mandatory field |
| organizationName | 2.5.4.10 | O | The name of the organization under which the organization is officially registered | Mandatory field |
| serialNumber respectively organizationIdentifier | 2.5.4.5 respectively 2.5.4.97 | | Reference to legal person identification[1] | Mandatory field (if exists) |
| organizationUnitName | 2.5.4.11 | OU | Organization unit name in the organization | Optional field |
| localityName | 2.5.4.7 | L | Locality name | Optional field |
| countryName | 2.5.4.6 | C | Two-character abbreviation for country name SK for Slovak republic | Mandatory field |

Table 5 TLS/SSL certificate fields and their description contains a list of fields that can be contained in the DN of TLS/SSL certificates. As required by the Provider, the TLS/SSL certificate may be extended to other fields as defined in RFC 5280, clause 4.1.2.6 [2].

Each TLS/SSL certificate shall contain a "subjectAltName" extension containing at least one entry with the Fully-Qualified Domain Name for which the certificate is intended.

As a Fully-Qualified Domain Name will be accepted also name containing the asterisk (*) in the third and higher position in the Fully-Qualified Domain Name (e.g. *.disig.sk; *.mail.disig.sk etc.) and this type of TLS/SSL certificate will be referred to as a “wildcard " TLS/SSL certificate.

Fully-Qualified Domain Name cannot be contained in any other field except CommonName (CN) and Extension of SubjectAlternativeName.

[1] See ETSI EN 319412-1 part 5 [12]

Table 5 TLS/SSL certificate fields and their description

| Filed name | OID | Abb. | Description | Note |
|---|---|---|---|---|
| commonName | 2.5.4.3 | CN | Full Qualified Domain Name (FQDN) for which certificate is issued | Mandatory field |
| organizationName | 2.5.4.10 | O[1)] | The name of the organization under which the organization is officially registered | Mandatory field[1)] |
| organizationUnitName | 2.5.4.11 | OU | Organization unit name in the organization | Optional field |
| localityName | 2.5.4.7 | L[1)] | Locality name | Mandatory field[1)] |
| stateOrProvinceName | 2.5.4.8 | ST [2)] | State or Province Name is recommended not to use for Slovak domain | Optional field |
| countryName | 2.5.4.6 | C | Two-character abbreviation for country name<br>SK for Slovak republic | Mandatory field |

1) If organizationName is present, then localityName is required. If organizationName is absent, then the certificate shall not contain a localityName. In the former case, the additional policy ID 2.23.140.1.2.2 is also used in the certificate, which states that the certificate was issued in accordance with the CA / Browser Forum Essential Requirements, section 7.1.6.1 [3]. In the latter case, an additional policy identifier in the form 2.23.140.1.2.1 is used. The provider prefers the first option for TLS/SSL certificates, with the name of the organization and its registered office.

2) It shall be filled in if the organizationName field is completed and the localityName entry is not filled in.

Underscore characters ("_")(ASCII code 0x5F) must not be present in dNSName entries.

### 3.1.5 Uniqueness of names

The Provider is responsible for the uniqueness of the names throughout the Subscribers community.

### 3.1.6 Recognition, authentication, and role of trademarks

Any entity has no guarantee that its name in the certificate will include the brand name (trademark), and even at his express request.

The certificate may be used only brand names, which the ownership or lease applicant for a certificate supports with evidence. Provider does not carry other authentication of trademarks.

Provider has not issue a certificate containing the name deliberately, which the competent court arbiters that violates another trademark. Provider is not obliged to examine the trademark or to resolve disputes relating to trademarks.

## 3.2 Initial identity validation

This section includes identification and authentication policies for individual entities.

### 3.2.1 Method to prove possession of private key

The RA shall require that the Contractor or a natural person acting on behalf of the Contractor has confirmed that the Subscriber owns a private key corresponding to the public key found in the certificate request.

In the case of a Subscriber requesting a subsequent certificate that has been generated on new cryptographic keys, it is permissible for the Subscriber to validate the ownership of the new private key by sending his new certificate request to the RA in signed e-mail. When signing an e-mail with the request, the Subscriber shall use a private key to which the Provider has issued a certificate and is valid at the time of verification of the received e-mail.

In the case of the certificate request delivery electronically, from the Subscriber who has already owned an issued certificate by the Provider, which cannot be signed with a private key of such a certificate, the ownership of the private key shall be verified by contacting the Subscriber by the Provider and verifying that it is the originator of the request.

Provider does not generate key pairs for foreign entities. Exceptions may only be generating the keys and request directly in QSCD on RA.

No Provider folder in any case does not archive any private keys belonging to Subscriber - Aliens.

Provider or part of its, in any case, does not archiving the private key belonging to the applicant (a foreign entity).

### 3.2.2 Authentication of Organization and Domain Identity

#### 3.2.2.1 Authentication of Identity

Legal person (organization) established in the Slovak Republic is proving its identity by extract from the Companies Register of Slovak republic or other existing register of legal persons. RA will require the original or certified copy of the original, not the older than three months. Evidence shall include full company name, identifier (usually company ID - ICO), seat, name of person acting as a legal person and the way of the signing procedure of a legal person.

In the event that a legal person not located in the Slovak Republic, its identity is verified in the same manner as described above. Extract from the current register of legal entities shall be officially translated into Slovak language (except to organizations based in the Czech Republic).

If the legal entity cannot prove its identity by a statement from the commercial, register, this legal entity shall prove its existence in writing with a reference to law or other legal regulation. This applies only to non-commercial entities such as the community, the church, civic associations, foundations, public authorities, etc. In the case of issuing a certificate, the legal person shall prove the truth of the

identification data given in the certificate application by submitting to view the original document proving this fact.

#### 3.2.2.2 DBA/Tradename

If the Subject Identity Information is to include a DBA or tradename, the CA SHALL verify the Applicant's right to use the DBA/tradename using at least one of the following

1. Documentation provided by, or communication with, a government agency in the jurisdiction of the Applicant's legal creation, existence, or recognition;
2. A Reliable Data Source;
3. Communication with a government agency responsible for the management of such DBAs or tradenames; or
4. An Attestation Letter accompanied by documentary support;

#### 3.2.2.3 Verification of Country

If the subject countryName field is present, then the CA SHALL verify the country associated with the Subject using one of the following

a) Information provided by the domain registrar

b) One of the methods listed in section 3.2.2.1.

#### 3.2.2.4 Validation of Domain Authorization or Control

If a domain name (FQDN) is used, it is a prerequisite that the respective second and higher level domains belong, respectively are under the control of the Customer requesting a TLS/SSL certificate.

The Provider shall confirm that at the time of issue of the TLS/SSL certificate, has verified all FQDNs in the certificate.

Verification must be performed at the specified time before the TLS/SSL certificate is issued.

Verify that the Customer is the domain owner or has control over the domain whose FQDN is in the CN entry or will be listed under Subject Alternative Name (SAN), must be done in one of the following ways

- By sending a randomly generated value via email to an email address identified as a legitimate domain contact for that domain by the domain name registrar (e.g., for top-level domain **".sk"** it is whois.sk-nic.sk). The random value generated must be sent along with the TLS/SSL certificate's eligibility for the TLS/SSL certificate request in the e-mail message returned from the email address to which it was sent. Random value must be unique for each sent e-mail. If successful FQDN eligibility validation is performed in this way, the Provider can also issue other TLS/SSL certificates that end with the same FQDN. (This method is given in document [3] in section 3.2.2.4.2). (this method is given in document [3] in section 3.2.2.4.2). This method can also be used to validate the "wildcard" TLS/SSL certificate request (see chapter 3.2.2.4.2. in [3]).

- By phone, by calling the number identified as a legitimate contact for that domain by the Registrar for that domain (e.g., for ".sk" it is whois.sk-nic.sk) and by verifying the eligibility of the TLS/SSL certificate from the Customer. In the event that there is a person in the telephone contact other than the contact listed for the given domain, the CA must request a connection with the person who is the given contact. If there is an answering machine on the telephone contact, the CA will leave a randomly generated value and a verified ADN (Authorization Domain Name) on the answering machine. If successful FQDN eligibility validation is performed in this way, the Provider can also issue other TLS/SSL certificates that end with the same FQDN. (This method is given in document [3] in section 3.2.2.4.15). This method can also be used to validate the "wildcard" TLS/SSL certificate request (see chapter 3.2.2.4.15 in [3]).

Unless one of the methods described makes it possible reliably, detect that the Customer is under a legitimate control of the domain, the Provider must refuse to issue the TLS/SSL certificate for that request.

#### 3.2.2.5 Authentication for an IP Address

Provider does not issue TLS/SSL certificates if the commonName or subjectAlernativeName extension is an IP address.

#### 3.2.2.6 Wildcard Domain Validation

Before issuing a certificate with a wildcard character (*) in a CN or subjectAltName of type DNS-ID, the CA MUST establish and follow a documented procedure [^pubsuffix] that determines if the wildcard character occurs in the first label position to the left of a “registry-controlled” label or “public suffix”.

#### 3.2.2.7 Data Source Accuracy

Before using any data source as a trusted source, the Provider must verify the reliability, accuracy, resistance to change or counterfeiting of such resource. It may take into account, for example, the timeliness of the data, the frequency of updating the data source, the data provider, and the public availability, the low probability of the possibility of changing or falsifying the data.

#### 3.2.2.8 CAA Records

As part of the issuance process, the Provider must check the CAA record for each dNSName specified in the subjectAltName extension of the issued certificate in accordance with the procedure in RFC 6844 and the processing instructions provided in RFC 6844 for all records found.

### 3.2.3 Authentication of individual identity

The Provider shall guarantee that the identity of the Subscriber and its public key are appropriately linked. The Provider shall specify the Subscriber's identity authentication procedures in the applicable CPS. Provider shall record this process for each certificate in written or electronic form. The authentication documentation shall include at least

- Identity of the person who carries out the identification;

- Unique identification numbers of the identity cards authenticated the person - Subscriber (ID card, driving license etc.);
- Date and site of the identification.

The Provider shall perform authentication on the on the base of presentation of these data

- Full name and surname;
- Permanent residence (if it is listed in the document);
- Birth registration number (applicants who have it assigned);
- Date of birth (applicants without birth registration number).

Subscriber shall also provide another document containing at the minimum name and surname of the Subscriber and his / her personal details (birthdate, birth number). This is not the case if it is a service card.

The provider shall also record the following data from the documents

- Identity card number;
- Identity card issuer;
- Identity card expiration date, if exists.

The Provider shall accept the following documents when verifying the Subscriber's identity

- ID card;
- Passport;
- Driving license;
- Birth certificate;
- Service card;
- The card of the public health insurer;
- Firearm license.

In the case of the delivery of a birth certificate, a firearm license, a service card or a health insurance card, one of the following documents shall also be provided ID card or passport.

If a natural person represents another natural person, it shall also be proved by an officially authenticated power of attorney from the text of which it is clearly clear that the representative natural person was empowered by the person empowered to act on the matter on its behalf.

A part of the Authentication of the Subscriber is the obligation to provide the email address, which will be stored with its personal data in the IS of the Provider and which will be used explicitly for communication between the Provider and the Subscriber and will not be part of the issued certificate. The Provider will not verify that this email address really belongs to the Subscriber.

If a certificate is issued to a natural person designated for e-mail signing (Secure Email extension - OID 1.3.6.1.5.5.7.3.4), then the Provider shall verify the ownership of the e-mail account by the procedure given in section 4.1.2.

#### 3.2.3.1 Authentication of device or system identity

If the certificate is issued for a device or system Provider shall guarantee that the device identity or the system are properly interconnected with its public key.

For this reason, the device or system shall be assigned to a natural person acting on behalf of a legal entity (the Contractor) that manages them.

This natural person shall provide the following information to the Provider

- Device or system identification;
- Device or system public keys (included in the certificate request);
- Device or system authorization (if any should be included in the certificate);
- Contact details to enable the Provider to communicate with that natural person, if necessary.

Provider shall verify the accuracy of any information (the values of the distinguishing name fields) to be listed in the certificate.

Methods for performing data verification include

- Verifying the identity of a natural person in accordance with the requirements of section 3.2.3;
- Verifying the identity of the person to whom the component belongs, in accordance with the requirements of section 3.2.2;
- Verifying the eligibility of the data to be listed in each certificate field, with emphasis on the contents of the commonName field.

Note The typical value of this field shall be the Full Qualified Domain Name (FQDN).

In the case of the use of a FQDN, it is a condition that the respective domain of the second and higher level belongs respectively was under the control of the Contractor requesting a TLS/SSL certificate.

Verifying that the Contractor is the domain owner, respectively has control of the domain whose FQDN is in the CN entry or will be listed under Subject Alternative Name (SAN) field, shall be done as follows

- Relating to confirmation from the authorized Contractor Authority in the form of a domain ownership statement. Domain ownership declaration must clearly demonstrate that it originates from the Authorized Domain Contact. Provider shall verify that the domain ownership confirmation
  - contains a date that is the same or later than the date when the request was accepted;
  - WHOIS database data has not changed compared with the data submitted in the domain ownership declaration for the given FQDN during the previous issuing procedure.

The same validation rules shall apply to wildcard TLS/SSL certificates that contain the asterisk (*) at the third or higher leftmost level of the domain name.

The Provider shall ensure that the field subject organizationUnitName (OU) is thoroughly inspected so that it does not include the name of a legal entity, business name, trademark, address, location, or other text pointing to a particular natural or legal person without not verifying such information.

#### 3.2.3.2 Contractors identity authentication

Authentication of the identity of a natural person or component belongs to the Provider's Contractor shall be carried out in cooperation with the responsible persons of that Contractor.

#### 3.2.3.3 Documents submitted

##### 3.2.3.3.1 General

All documents submitted to the RA by applicants for service must be either originals or certified copies of the originals. It cannot be there any indication about add on data, changing data, cross out data etc. The documents, which have expiration data, must be valid.

If the RA personnel has doubts about the identity of a potential customer (i.e. the apparent discrepancy between the photograph in the presentation of a personal document and view customer differences between the two documents etc.), he or she may refuse the registration.

Expert translators must translate any documents in foreign languages (except Czech) into Slovak language.

At the request of a potential customer or any RA contentious cases about proving the identity during the procedure of identification will deal under point 2.4.

When submitting the documents to RA it is required to present either the originals of these documents or copies of originals (not necessarily certified) except for personal ID documents. Extract from the Commercial register respectively trade register obtained from the Internet is not sufficient as it is informational only and is not applicable to legal acts

##### 3.2.3.3.2 Natural person

Natural person shall submit two documents identifying his identity. The primary document is

- Slovak citizens - a valid identity card or passport;
- Foreigners - proof of identity (namely identity card), residence permit in the Slovak Republic or passport.

Secondary evidence may be

- Passport;
- Driving license;
- Health insurance card;

- Birth certificate;
- Personal license of professional soldier;
- Temporary residence permit (or resident) in the case of a foreigner;
- Firearms license issued by the police department;
- Service card.

It is required, that at least one of the submitted documents was a document, which includes a photograph of the natural person.

In the case of issuing or revocation certificate for Contractor, it suffices that the natural person will establish his identity with one of the following personal documents - an ID card or passport. The applicant for a certificate for Contractor shall meet other conditions for issuing of this type of certificate determined by the Contractor.

If natural person representing on the RA another person, must in addition show a power of attorney, from which it is clear that the representative was acting on behalf that natural person.

As an applicant for a certificate is the legal representative (usually the parent), shall also submit the child's birth certificate, adopt parent shall also submit a decision of a court or an extract from the registers. Sufficient proof is the identity card, in which the child is registered.

#### 3.2.3.3.3 Natural person - employee

If the Contractor is a legal entity requesting the issuance of a certificate to a natural person who is its employee and the name of that legal person is in the request provided, in addition to the documents listed in section 3.2.3.3.2 also shall submit a document according section 3.2.2. This requirement does not apply to a Contractor's employee where a different verification mechanism should be agreed.

#### 3.2.3.3.4 Legal person

In this case, the Contractor/Subscriber shall submit the certificate documents referred to in section 3.2.3. It shall also submit a documents according section 3.2.2.

#### 3.2.3.3.5 Component or system

See section 3.2.3.1.

### 3.2.3.4 Submitted documents check

RA staff shall check on the submitted documents the following

Personal documents of natural persons

a) Data consistency in the request and the data referred in personal documents, particularly the name, surname and residence;

b) The validity of the document

c) Legal age (i.e. age 18 years);

d) Consistency between the photograph and personal view of the proprietor of identity documents;

e) Consistency in documentation as to whether the data in one document is the same as in another.

Extracts from the Commercial Register or another register of legal persons

a) Validity of extract - there must be not older than 3 months;

b) Acting as a legal entity - i.e. whether it has/have natural(s) person(s), who submitted a statement power to act (sign) for the legal person;

c) The form of extract - original or official (notary / registry) a certified copy of an extract.

Consent to the issuance of the certificate

a) The authority to act for the company - the person signing the consent shall be authorized to represent the employer. Eligibility is checked by an extract from OR respectively another designated register. As the person signing is not registered in this extract, he/she must submit other evidence on which it can act as a company (usually a power of attorney).

b) Validity - as far as in the agreement is written the validity of consent, is also controlled.

Power of attorney

a) Verification of power of attorney (notary/registry);

b) Consistency of the data listed in the power of attorney, which defines the representative natural or legal person, with the data provided on the personal identification card of representative respectively with those set out in the extract or another register representing a legal person;

c) The scope of the power of attorney - that is whether the power of attorney authorized empowered physical or legal person to act as required on the RA on behalf of the physical or legal persons;

d) Any time limit or other conditions specified in power of attorney.

Statutory declaration

a) The authority to sign - the person signing the declaration shall be authorized to represent the legal person. Eligibility is checked by an extract from companies register respectively another register of legal persons. As the person signing is not registered in this extract, he/she must submit other evidence on which it can act in the name of company (usually a power of attorney).

### 3.2.4 Non-verified subscriber information

During the initial issue of the certificate, the information contained in the request relating to the organizationUnitName item is not verified, with the exception of the inspection in the meaning according of 3.2.3.1 and for the certificates that do not contain the emailProtection extension, the e-mail address specified in the request is not verified.

### 3.2.5 Validation of authority

See 3.2.3.

### 3.2.6 Criteria for Interoperation or Certification

Provider does not apply any interoperability criteria.

## 3.3 Identification and authentication for re-key requests

### 3.3.1 Identification and authentication for routine re-key

Before issuing of a subsequent certificate, a pair of certificate keys is changed - a new certificate will be created that will have the same obligatory distinguished name entries, a different public key (corresponding to a new, different private key), a different certificate serial number and may have a modified validity period.

The holder of a valid certificate may apply for a subsequent certificate only for the last 30 days of validity of the certificate to which the subsequent certificate will be issued.

Subscriber (natural or legal person) may request for subsequent certificate by one of the following ways

- It generates a new certificate request, with the same content (except Organizational Unit and City fields) as the previous certificate, which shall be sent by the signed email to the contact email address of the RA. Application email shall be signed with the use of private key associated with a valid certificate on the base of which the subsequent certificate will be issued. In the same e-mail message, he/she shall notify that his/her personal details, based on which he/she was identified and authenticated when the previous certificate was issued, have not been altered. If it is not possible to use a signed email when a certificate is renewed, it is also possible to send such an application with an unsigned email from the same email address as found in the request. The email must also contain a notification of unchanged personal data. In this case, the process of verifying the request has to be run by the RA. If an application for a subsequent certificate is sent by an unsigned e-mail from a different address as stated in the request sent, it can be accepted only if the RA has subsequently verified the request. If it is not possible to use a signed email when a certificate is renewed, it is also possible to send such an application with an unsigned email from the same email address as found in the request. The email must also contain a notification of unchanged personal data. In this case, the process of verifying the request has to be run by the RA. If an application for a subsequent certificate is sent by an unsigned e-mail from a different address as stated in the request sent, it can be accepted only if the RA has subsequently verified the request.
- It generates a new certificate request, sends it to the RA's email address, and personally visit the RA, where he/she is subject of the same identity verification procedures and requirements as were when the first certificate issuing.

- Creates a new certificate request and issues the certificate in an automated way through an interface accessible to the Provider's Web site. The Provider reserves the right to allow the issue of a subsequent certificate in this way only for the selected Contractor.
- The holder of a valid certificate issued for the contractual partner may also apply for a subsequent certificate through another mechanism agreed between the Contractor and the Provider.

For TLS/SSL certificates, subsequent certificates are not issued.

The provider issues all certificates with the exception of TLS / SSL certificates valid for a maximum of 60 months (5 years)

### 3.3.2 Identification and authentication for re-key after revocation

In the event that, after the Certificate is revoked, the Contractor/Subscriber wishes to have a new valid certificate issued by the Provider, he/she shall apply for a new certificate according to section 4.1. This operation is subject to the same authentication as given in section 3.2.

## 3.4 Identification and authentication for revocation request

The certificate revocation request must be authenticated, see section 4.9.3. In the case of a personal certificate, the certificate revocation request may be authenticated by using a private key belonging to the certificate, regardless of whether or not the private key has been compromised.

# 4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

The content of this section is a description of the operational life cycle of the certificate from the request for its issuance.

## 4.1 Certificate Application

### 4.1.1 Who can submit a certificate application

Provider can be requested to issue

- Certificate for electronic signature by
  - A natural person or a natural person authorized by the Contractor;
  - A natural person identified in association with a legal person;
- Certificate for electronic seal
  - A legal person (that can be an Organization or a unit or a department identified in association with an Organization);
- TLS/SSL certificate for Web site authentication
  - The natural or legal person operating the facility or, a system, who demonstrates the eligibility to apply for a certificate with FQDN in the certificate request and for all the FQDN to be listed in the SAN extension.

### 4.1.2 Enrollment process and responsibilities

#### 4.1.2.1 Preparation

The Contractor/Subscriber shall take the following steps to prepare for a visit to the Provider

- Familiarize yourself with the „Všeobecné podmienky poskytovania a používania dôveryhodnej služby vydávania a overovania certifikátov (General Terms and Conditions for Providing and Using a Trusted Certificate Issuance and Verification Service)" [11] and "Informáciou o spracúvaní osobných údajov (Information on Personal Data Processing)" [12], which shall be accessible in a durable communication channel (see https//eidas.disig.sk/sk/documents/);
- To get acquainted with this procedure, possibly with the principles and instructions for obtaining the certificate;
- To have ready the values of each certificate request field so that these values are consistent with this CP (see paragraph 3.1.4);;
- To have prepared a certificate request in form of PKCS #10 or SPKAC, which will be send in advance to the Provider (see paragraph 4.1.4);
- To have prepared the selected identity documents and other necessary documents, i.e. Extract from business register, Power of Attorney, etc.;
- To arrange a date of the visit.

### 4.1.3 Request generation

To issuing a certificate, for electronic signature or Electronic seal can be requested only using PKCS#10 or SPKAC request format. The Customer is required to generate a request for a certificate for electronic signature or a certificate for electronic seal on the computer, using the appropriate browser and the Provider's website (see URL in section 1) and store it on the appropriate media (HDD, USB disk, floppy disk, etc.).

A request for electronic signature for the cryptographic keys, which are intended to be used to sign and encrypt emails, must be forwarded to the appropriate RA by e-mail in advance and from the e-mail address given in the certificate request in the E-mail item. The email addresses of each Provider's RA are available at the Provider's website (see section 1).

When requesting a TLS/SSL Certificate the Customer shall generate a cryptographic key pair (private and public) using their software (typically Microsoft IIS or Apache / OpenSSL, for example) and shall create a new TLS/SSL certificate request and save it on suitable medium.

The customer requesting a subsequent certificate shall create a certificate request using the procedure described in the section 4.7.3.

When entering values into certificate request, the Customer must be aware that to the RA will have to demonstrate in a satisfactory manner the rightfulness of all the data that is listed in each item of the certificate request.

A request for an electronic signature certificate issued to a natural person who is an employee of a Customer may be generated in a different way than through the Provider's web site, for example via own web portal of the Customer etc. This method has to be agreed in advance with the Customer and the individual applicants must be informed about the method of generating and sending the request both from the Customer and from the Provider.

### 4.1.4 Sending a certificate request

A request for an electronic signature certificate issued to a natural person who is an employee of a Customer may be generated in a different way than through the Provider's web site, for example via own web portal of the Customer etc. This method has to be agreed in advance with the Customer and the individual applicants must be informed about the method of generating and sending the request both from the Customer and from the Provider.

## 4.2 Certificate application processing

### 4.2.1 Performing identification and authentication functions

Before issuing the certificate, the employee representing the Provider shall

- Inform the attender natural person about the General Conditions [5];
- Check the completeness and accuracy of the data in the accepted certificate request;

- Verify the identity of the Subscriber and insert his/her personal data into the IS of the Provider, obliging him to fill in all required items required by the Provider's system;
- Verify other documents to verifying any identifying information to be entered into the certificate.

In the case of the certificate for electronic signature or electronic seal where the cryptographic keys are not in the QSCD, the RA personnel shall verify the delivered request, which can be in the PKCS #10 or SPKAC format and then he can verify the Subscriber identity. The contents of the request fields and the obligation how to fill it see at section 3.1.4 (bold fields are required).

An RA employee must verify that the electronically submitted application for the certificate of a given Customer has been sent from the same e-mail address as found in the certificate request. In the event of discrepancies, it may refuse to issue a certificate. This does not apply if the issued certificate does not contain an extension „Secure Email (1.3.6.1.5.5.7.3.4)“.

In connection with the verification of the e-mail to be used for signing electronic messages ("Secure Email (1.3.6.1.5.5.7.3.4)" extension), the RA personnel must check the e-mail address containing in the request by replying to the email from which the request was sent. Verification will be accomplished by sending a message to the given email address that will contain secret unpredictable information (verification information). The Customer shall return the verification information as proof of the verification of the email address. If the email address verification is unsuccessful, the Provider will refuse to issue the certificate. Verification of an email address is not necessary if a subsequent certificate request is sent electronically by e-mail signed by a valid Holder's certificate issued by the Certification Authority of the Provider, and the e-mail address from which the request was sent is identical to the e-email address in the request.

An RA employee shall verify the identity and authenticity of the Customer within the meaning of the section 3.2.

The customer shall show to the RA in a satisfactory manner all the data he / she has entered into each item of the certificate request.

RA personnel shall insert a certificate request and other required data to the Provider's information system.

In the case of a request for a subsequent certificate, it is necessary to proceed according to section 4.7.

When issuing a certificate for a Customer that is solely designated for its internal needs, detailed procedures for obtaining a certificate of these types and procedures for registration with the RA for a given contractor are given in the relevant CPS document or in the internal documents of the Customer.

### 4.2.2 Approval or rejection of certificate applications

Any request meeting the requirements of this CP must be processed immediately if the issuing is performed in the presence of the Customer or at the latest at the time agreed with the Customer in the process of applying for the certificate.

In the event of any reasonable doubt as to the identity of the Customer, also in case of deficiencies in the documents, providing incomplete documents, the RA employee shall refuse the Customer's registration.

The application shall also be rejected if its format or Content does not meet the requirements set out in the section 3.1.4 and 4.1.3.

The Provider may not issue TLS/SSL Certificates for FQDN that contains the highest domain (gTLD) that is not listed and in the "Root Zone Database" maintained by the Internet Assigned Numbers Authority (IANA) (https//www.iana.org/ domains / root / db).

If to the public key included in the request was previously issued certificates by the Provider's system, issuing a new certificate for this request shall be for security reasons denied, as once a certified public key cannot be used in another certificate.

### 4.2.3 Time to process certificate issuance

In order to guarantee the binding of the Subscriber's verified identity to the public key to which the certificate is to be issued, the public key (contained in the certificate requests) shall be delivered to the CA through the RA. The customer either shall deliver the request to the RA personally or via an agreement with the appropriate RA may also send the request via e-mail. In the case of an e-mail certificate (Secure Email extension (1.3.6.1.5.5.7.3.4)), the request shall be sent to the RA in advance in advance in order for the Provider to be able to check the e-mail -mail account.

## 4.3 Certificate issuance

### 4.3.1 CA actions during certificate issuance

After sending the certificate from the RA to the CA, the CA system shall verify the received request in order to verify if

- Was sent by an authorized RA employee;
- Corresponds to the standard for PKCS # 10 or SPKAC respectively;
- No certificate has been issued in the past to the public key found in the submitted certificate request.

Issuing a certificate for a key pair generated directly on an RA must be securely linked to the procedure of that request generation.

If all certificate requirements are met, CA shall issue the certificate.

### 4.3.2 Notification to subscriber by the CA of issuance of certificate

Once the certificate has been issued, the Subscriber has to be notified of its issuing by sending an e-mail message to an e-mail address notified to the Provider in the authentication and identification process.

## 4.4 Certificate acceptance

### 4.4.1 Conduct constituting certificate acceptance

Certificates will be created and issued in the Provider system automated and on a continuous basis. The holder will be able to take the issued certificate immediately after its issuing.

After the certificate is issued, the RA personnel and the Subscriber shall sign the relevant documentation related to the issuance of the certificate.

### 4.4.2 Publication of the certificate by the CA

The issued certificate shall be published in the Provider's repository, which is available through the Provider's web site (see section 1) if the Subscriber has consented to the disclosure.

### 4.4.3 Notification of certificate issuance by the CA to other entities

The provider does not send notification about certificate issuing to other entities besides the Subscriber.

## 4.5 Key pair and certificate usage

This section describes responsibilities for using keys and certificates.

### 4.5.1 Subscriber private key and certificate usage

The Subscriber in relation to the private key and certificate shall

- Provide the Provider with the exact and complete information required by this CP when applying for a certificate;
- Use a key pair in accordance with the limitations that have been notified by the Provider;
- Continually protect his/her private keys in accordance with this CP, and in accordance with the provisions of the General Conditions [5];
- Use a private key only after obtaining a public key certificate with which they create unique pair;
- Immediately notify the Provider, if the certificate has not yet been expired, of suspecting that
  - His/her private key was lost, stolen or compromised;
  - Lost control about the private key because his/her active data (PIN, PUK) were compromised;
- Immediately to request the certificate to be revoked in the event that any information on the entity's certificate becomes invalid;
- Comply with any terms, conditions and limitations imposed on your private key and certificate i.e. to stop use of a private key after an expiration or revocation of a public key certificate.

Subscriber who will fail to comply with his obligations is not entitled to compensation for any damage.

### 4.5.2 Relying party public key and certificate usage

The relying party that rely on the certificate issued under this CP and in accordance with the General Terms and Conditions [5] shall

- Assess whether the use of the certificate is in accordance with its purpose and is appropriate for a particular purpose;
- Check that the use of the certificate is not inconsistent with the restrictions of the certificate, which are contained in the certificate itself, the General Conditions [5] or this CP;
- When working with the certificate, including its validation, use only the intended and appropriate hardware or software;
- Verify the validity of the certificate in question by checking that
  - The certificate was valid at the time the relying party had confidence that the signature / seal had been created;
  - Before the time stated in the previous point, the certificate was not revoked via checking current CRL and, if applicable, via the OCSP provided by the Provider - reference to the address of the CRL and, optionally, to the OCSP service is mentioned in certificate;
- Make any further verifications that may be required in the context of this CP or standards for a particular type of certificate or its use, and verify the other certificates in the certification path as described in the previous way e.g. „trust anchor “.

## 4.6 Certificate renewal

### 4.6.1 Circumstance for certificate renewal

Provider will not allow the certificate to be renewed (issued) to a public key to which certificate has already been issued by the same CA of the Provider.

### 4.6.2 Who may request renewal

No stipulation.

### 4.6.3 Processing certificate renewal requests

No stipulation.

### 4.6.4 Notification of new certificate issuance to subscriber

No stipulation.

### 4.6.5 Conduct constituting acceptance of a renewal certificate

No stipulation.

### 4.6.6 Publication of the renewal certificate by the CA

No stipulation.

### 4.6.7 Notification of certificate issuance by the CA to other entities

No stipulation.

## 4.7 Certificate re-key

Certificate re-key means generating a new key pair and applying for the issuance of a new certificate that certifies the new public key.

### 4.7.1 Circumstance for certificate re-key

This section describes the conditions for the issuance of a subsequent certificate after the validity expiration or certificate revocation of certificate issued by the Provider. The term "successive certificate" means the issue of a new certificate of the same kind and with the same content for an existing Customer / Subscriber whose personal data is introduced in the Provider's system.

A subsequent certificate may only be issued if the previous certificate has expired or has been revoked for reasons that it could not be used e.g. due to the private key compromise.

### 4.7.2 Who may request certification of a new public key

The issuance of a subsequent certificate can be requested by an existing Subscriber to whom has previously been a certificate issued by the Provider, who meets the identification, and authentication requirements - see section 3.

### 4.7.3 Processing certificate re-keying requests

The subsequent certificate shall be issued in the same way as the original certificate was issued. Issuing can utilize modified authentication methods described in section 3.

### 4.7.4 Notification of new certificate issuance to subscriber

Once a certificate has been issued, the Subscriber has to be notified of its issuing by sending an e-mail message to an e-mail address provided during the authentication and identification process.

### 4.7.5 Conduct constituting acceptance of a re-keyed certificate

In the case of issuance of certificate in the holder's personal presence at the RA, the method of taking over described in the section 4.4 shall be applied.

In the case of submitting a subsequent certificate request electronically, the certificate shall be delivered to the Subscriber on the e-mail address given in the certificate.

Upon receipt of the certificate, the Customer is obliged to pay for the provided service in accordance with the Provider's price list in a pre-agreed manner.

### 4.7.6 Publication of the re-keyed certificate by the CA

See section 4.4.2.

### 4.7.7 Notification of certificate issuance by the CA to other entities

See section 4.4.3.

## 4.8 Certificate modification

### 4.8.1 Circumstance for certificate modification

Issuing a new certificate due to changes of the certificate content to the original keys Provider does not support.

### 4.8.2 Who may request certificate modification

No stipulation.

### 4.8.3 Processing certificate modification requests

No stipulation.

### 4.8.4 Notification of new certificate issuance to subscriber

No stipulation.

### 4.8.5 Conduct constituting acceptance of modified certificate

No stipulation.

### 4.8.6 Publication of the modified certificate by the CA

No stipulation.

### 4.8.7 Notification of certificate issuance by the CA to other entities

No stipulation.

## 4.9 Certificate revocation and suspension

The certificate must be revoked when the relationship between the entity and its public key defined in the certificate is no longer considered valid.

### 4.9.1 Circumstances for revocation

#### 4.9.1.1 Reasons for Revoking a Subscriber/Subject Certificate

The Provider shall revoke a certificate within 24 hours if one or more of the following occurs

- The Subscriber/Subject requests in writing that the Provider revoke the certificate;
- The Subscriber/Subject notifies the Provider that the original certificate request was not authorized and does not retroactively grant authorization;

- The Provider obtains evidence that the Subscriber's/Subject's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise; or
- In case of TLS/SSL certificate
  - The Provider obtains evidence that the validation of domain authorization or control for any Fully-Qualified Domain Name in the certificate should not be relied upon.

The Provider should revoke a certificate within 24 hours and must revoke a certificate within 5 days if one or more of the following occurs

- The Certificate no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
- The Provider obtains evidence that the Certificate was misused;
- The Provider is made aware that a Subscriber has violated one or more of its material obligations under the Subscriber Agreement or Terms of Use;
- In case of TLS/SSL certificate
  - The Provider is made aware of any circumstance indicating that use of a Fully-Qualified Domain Name in the Certificate is no longer legally permitted (e.g. a court or arbitrator has revoked a Domain Name Registrant's right to use the Domain Name, a relevant licensing or services agreement between the Domain Name Registrant and the Applicant has terminated, or the Domain Name Registrant has failed to renew the Domain Name);
  - The Provider is made aware that a wildcard certificate has been used to authenticate a fraudulently misleading subordinate Fully-Qualified Domain Name;
  - The Provider's right to issue certificates under these CA/Browser forum requirements [3] expires or is revoked or terminated, unless the Provider has made arrangements to continue maintaining the CRL/OCSP Repository;
  - The Provider is made aware of a demonstrated or proven method that exposes the Subscriber's/Subject's Private Key to compromise, methods have been developed that can easily calculate it based on the Public Key (such as a Debian weak key, see http//wiki.debian.org/SSLkeys), or if there is clear evidence that the specific method used to generate the Private Key was flawed.
- The Provider is made aware of a material change in the information contained in the Certificate;
- The CA is made aware that the Certificate was not issued in accordance with these Requirements or the CA's Certificate Policy or Certification Practice Statement;
- The CA determines or is made aware that any of the information appearing in the Certificate is inaccurate;

- The Provider terminates the business for any reason and does not arrange that another CA will provide information on revoked certificates on its behalf;
- The circumstances that required the issue of the certificate (testing, application verification, etc.) ended;
- Loss of private key;
- Technical parameters or certificate format could lead to an unacceptable risk from the point of view of software vendors or relying parties (change of cryptographic algorithms for signing, length of cryptographic keys, etc.);
- Subscriber/Subject died in the case of a natural person or extinct in case of legal person and the Provider will be informed of this fact,
- Revocation is required by this CP and/or CPS.

Whenever the Provider becomes aware of any of the above circumstances, the certificate must be revoked and placed on the Certificate Revocation List ("CRL").

The revoked certificate must be present in all new CRLs, at least until the certificate expires.

Revoked certificate cannot be restored in any circumstances.

#### 4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Issuing CA SHALL revoke a Subordinate CA Certificate within seven (7) days if one or more of the following occurs

- The Subordinate CA requests revocation in writing;
- The Subordinate CA notifies the Issuing CA that the original certificate request was not authorized and does not retroactively grant authorization;
- The Issuing CA obtains evidence that the Subordinate CA's Private Key corresponding to the Public Key in the Certificate suffered a Key Compromise or no longer complies with the requirements of Sections 6.1.5 and 6.1.6;
- The Issuing CA obtains evidence that the Certificate was misused;
- The Issuing CA is made aware that the Certificate was not issued in accordance with or that Subordinate CA has not complied with this document or the applicable Certificate Policy or Certification Practice Statement;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA

has made arrangements to continue maintaining the CRL/OCSP Repository; or

- Revocation is required by this CP and/or CPS;
- In case of TLS/SSL certificate
  - The Provider's right to issue certificates under these CA/Browser forum requirements [3] expires or is revoked or terminated, unless the Provider has made arrangements to continue maintaining the CRL/OCSP Repository;

### 4.9.2 Who can request revocation

Subscriber (or a natural or legal person authorized by him / her) may ask for certificate to be revoked at any time, even without giving the reason for canceling the certificate.

RA shall revoke the Holder's certificate if he / she becomes aware of any of the circumstances listed in section 4.9.1.

Certificate revocation may also request

- Provider - the RA personnel shall document this fact in writing, including the reason for his/her proceedings,
- the court, by means of its judgment or interim measure (a copy of the relevant court decision must be attached to the certificate revocation documents),
- entity (natural or legal person) by virtue of inheritance (a copy of the documents showing the right of the entity to apply for the certificate to be revoked),
- In the case of an RA certificate, the revocation of the certificate, except for its Holder (the personnel of the RA), may also require the PMA if a serious circumstance (see section 4.9.1) is found for revoking the certificate.

### 4.9.3 Procedure for revocation request

If the Subscriber's authentication requirements are met, which requests the cancellation of the certificate (see section 3.2.3 or 3.2.3); the certificate revocation request can be submitted

- Personally, at the RA branch, through the "Certificate Revocation Request" form available to the RA. RA personnel may request a password to revoke the certificate if the person requesting the certificate revocation is not the Subscriber but the person authorized to do so by Subscriber;
- By e-mail - by sending an electronic mail message signed using a private key that forms a key pair with a certificate that is canceled. The content of the message must be a clear wish to revoke the certificate, expressed in the sentence "I hereby ask to cancel my certificate with the serial number XXXXXX";

- By e-mail - by sending an e-mail message (it does not need to be signed). The content of the message must be a clear wish to cancel the certificate, expressed in the phrase "I hereby request to cancel my certificate with the serial number XXXXXX". In this message you must also include a password for the cancellation of the certificate;
- By postal mail sent to the Provider's address or of the relevant RA together with a password to cancel the certificate;

An application for revocation of a certificate issued for the purposes of a contractual partner may be filed either directly with the Provider or only to the RA, which is mentioned in the relevant contract and acts on behalf of the Provider with the contractor.

The certificate that expired cannot be revoked.

Reporting and incident reporting procedures for possible compromise of a private key, misuse of a certificate or other type of fraud, unauthorized release or other matter related to a issued Certificate are listed in 1.5.2.

### 4.9.4 Revocation request grace period

A certificate revocation request in the event of compromising of a private key must holder submitted as soon as possible. You may personally request cancellation only during the working hours specified by each RA whose list and working time is published at the Provider's website (see section 1). Electronic request for revocation can be sent to chosen RA at any time.

### 4.9.5 Time within which CA must process the revocation request

Provider shall

- Within 24 hours after receiving a Certificate Problem Report, the Provider shall investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.
- After reviewing the facts and circumstances, the Provider shall work with the Subscriber/Subject and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the Provider will revoke the certificate.
- The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1.1.
- The date selected by the CA SHOULD consider the following criteria
  - The nature of the alleged problem (scope, context, severity, magnitude, risk of harm);
  - The consequences of revocation (direct and collateral impacts to Subscribers and Relying Parties);
  - The number of Certificate Problem Reports received about a particular Certificate or Subscriber;

- The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and
- Relevant legislation.

- Publish the current CRL and all previous CRLs at its website (see section 1),
- Publish all revoked certificate in the CRL. j. even those that have expired in the meantime,
- Archive all CRLs it has released.

The Provider must automatically inform the certificate Holder about revocation of his / her certificate by sending an email to the email address provided by the Holder during registration to the RA.

CRL shall be published in the repository as quickly as possible after issuing.

### 4.9.6 Revocation checking requirement for relying parties

When relying on the certificate the relying party is obliged to verify its validity under the General Conditions [5].

At the time between submitting a valid certificate revocation request and publishing, the canceled certificate to the CRL, the Customer / Certificate Holder bears all responsibility for any damages caused by the misuse of his / her certificate. After publishing the certificate in the CRL, it bears all responsibility for any damages caused by the use of the revoked certificate, the party that has relied on the revoked certificate.

Non-verification of certificate using the CRL is considered a gross violation of this CP.

### 4.9.7 CRL issuance frequency

The frequency of issue of the CRLs varies depending on whether it concerns a root CA a subordinate CA. Table 1 contains information on maximum CRL issuance frequency.

Table 6 CRL issuance frequency

| CRL issuer | Issuing frequency | nextUpdate vs. thisUpdate | Notes |
|---|---|---|---|
| Root CA | max 365 days | < 365 days | Whenever to 24 hours after revoking a subordinate CA |
| Subordinate CA | max 7 days | < 10 days | |

Subordinate CAs of the Provider issuing certificates to end users must issue CRLs

- At least every 24 hours, even if no certificate has been revoked for the last 24 hours and the nextUpdate shall have value of 24 hours.

Root CA issuing certificates to subordinate CAs must issue CRLs

- At least every 7 days with nextUpdate for 14 days;

- Always within 24 hours of revoking a CA subordinate certificate.

### 4.9.8 Maximum latency for CRLs

The maximum CRL latency period from its release to its publication in the repository may not exceed 90 seconds.

### 4.9.9 On-line revocation/status checking availability

The Provider may provide the OCSP service for selected certificate types. In the case of the OCSP service, the addresses of the OSCP responders units must be included in the Authority Information Access extension.

### 4.9.10 On-line revocation/status checking requirements

Third parties interested in using OCSP must send a request to the appropriate OCSP responder unit, which URI is published in the certificate. The request submitted must comply with the requirements of RFC 6960.

### 4.9.11 Other forms of revocation advertisements available

Verification of the status of the certificate can be done manually through lists of current CRLs as well as archives of all CRLs issued for each CA, which must be available at the Provider's website (see section 1). The RA must respond to a query about the status of a particular certificate if this request was made by telephone, fax, or email.

The RA shall send the current CRL by email to the agreed email address as soon as possible upon request.

### 4.9.12 Special requirements re-key compromise

No stipulation.

### 4.9.13 Circumstances for suspension

Provider does not provide such a service.

### 4.9.14 Who can request suspension

No stipulation.

### 4.9.15 Procedure for suspension request

No stipulation.

### 4.9.16 Limits on suspension period

No stipulation.

## 4.10 Certificate status services

### 4.10.1 Operational characteristics

The CRL must be available at the Provider's website (see section 1) and shall be accessible through the HTTP protocol on port 80.

The OCSP shall be available at the URL specified in the issued certificate and the applicant for certificate status must send a request in the sense of the 4.9.10.

### 4.10.2 Service availability

The distribution points on which CRLs are published must be available in 24/7/365 mode.

OCSP must be available in 24/7/365 mode.

### 4.10.3 Optional features

No stipulation.

## 4.11 End of subscription

The Provider's service to the Holder of the certificate will be terminated upon expiration of the contract under which the certificate was issued.

Either party based on the agreement even before its expiry may terminate the agreement. The cancellation of the contract shall result in the immediate revocation of the certificate issued based on the contract.

## 4.12 Key escrow and recovery

### 4.12.1 Key escrow and recovery policy and practices

The Provider does not provide its Holders with any storage service or recovery of private keys.

### 4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

# 5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

The security of the Provider must be based on a set of security measures in the area of Physical, Object, Personnel and Operational Security. These security measures must be designed, documented and applied based on security rules and approved by the Provider's management.

Security measures shall be available to staff concerned.

Provider shall

- Take full responsibility for the compliance of its activities with the procedures defined in the security policy, including their fulfilling by his registration authorities;
- Define the responsibility of registration authorities and to oblige them to comply with established safety measures;
- Have a list of all their assets with their classification from the point of view of the risk assessment carried out.

The Security Policy of the Provider and the Summary of Security Assets shall be reviewed at regular intervals and always when the significant changes are made to ensure their continuity, suitability, sufficiency and effectiveness.

The Provider's management shall approve any changes that may affect the level of security provided.

The setting up of the Provider's systems shall be regularly reviewed for changes that threaten the Provider's security policy.

## 5.1 Physical security controls

### 5.1.1 Site location and construction

Technological facilities in which the Provider's basic infrastructure is located shall be located in protected areas accessible only to authorized persons and separated from other areas by appropriate security features (security doors, grilles, fixed walls, etc.). Provider equipment should consist only of equipment reserved for certification authority functions and should not serve any purpose that does not apply to this function.

### 5.1.2 Physical access

Access Control Mechanisms for Provider's Protected Areas e. g. the areas of the highest security zone shall be secured in such a way that these spaces are protected by a security alarm and are only accessible to persons holding a security token and listed in the list of authorized persons to enter the Provider's protected areas. Provider equipment must be permanently protected from unauthorized access, even from unauthorized physical access.

### 5.1.3 Power and air conditioning

The spaces in which the Provider's equipment is located shall be adequately supplied with electricity and air-conditioned to provide a reliable operating environment.

### 5.1.4 Water exposures

The spaces in which the Provider's equipment is located shall be located so that they cannot be endangered by water from any source. If this is not entirely possible, measures must be taken to minimize the risk of water hazard to the premises.

### 5.1.5 Fire prevention and protection

The spaces in which the Provider's equipment is located shall be reliably protected from direct fire sources, heat that could cause fire in the premises.

### 5.1.6 Media storage

Media must be stored in rooms that are protected against accidental, unintentional damage (water, fire, and electromagnetism). Media containing security audit, archive, or backed up information should be stored in a site separate from CMA.

### 5.1.7 Waste disposal

With the waste arising from the operation of the Provider shall be handled in such a way that no environmental pollution is involved.

### 5.1.8 Off-site backup

In the event of irreversible damage to the main site spaces where the Provider's infrastructure is located, it is necessary to have at least copies Provider's most important assets backed up outside this principal location.

## 5.2 Procedural controls

### 5.2.1 Trusted roles

Within CAs shall be defined as trustworthy roles responsible for individual aspects of trusted activities such as, for example, system administrator, security manager, internal auditor, policy maker, etc., which form the basis of trust in the whole PKI.

At the same time, responsibilities for individual roles shall be defined.

Persons selected to hold roles that require credibility must be accountable and trusted.

All persons in trusted rolls must have no conflict of interest to ensure the impartiality of the services provided by the Provider.

### 5.2.2 Number of Individual Required per Task

For each task, the number of individuals assigned to perform each task must be identified (rule K of N).

### 5.2.3 Identification and authentication for each role

Each role must have a defined way of identifying and authenticating when accessing the IS of the Provider.

### 5.2.4 Roles requiring separation of duties

Each role must have set criteria that take into account the need for separation of functions in terms of the role itself i.e. there must be roles that cannot be performed by the same individuals.

## 5.3 Personnel controls

Provider staff shall be formally appointed to the trusted role by executive management responsible for security.

### 5.3.1 Qualifications, experience, and clearance requirements

Employees in trusted roles must meet the qualification requirements, professional experience requirements, and have security clearance at the specified level or shall be in the process of requesting a security clearance respectively. Requirements for each role are described in separate sheets used to recruit new staff.

Persons in managerial positions shall

- Have appropriate training or experience in the field of trusted services provided by the Provider;
- Be familiar with security measures for safety roles;
- Have experience of information security and risk assessment to the extent necessary for the performance of managerial functions.

### 5.3.2 Background check procedures

Employee can only be included in a trusted role of the Provider if he/she has a security clearance of the specified level i.e. at least to the "Confidential" classification level or is in the process of requesting such a review respectively.

### 5.3.3 Training Requirements and Procedures

Some special training requirements may be specified for certain trustworthy roles of the Provider, which should be completed before or during the assignment. Topics should include the functioning of CMA software and hardware, operating and security procedures, the provisions of this CP, CPS, and so on.

### 5.3.4 Retraining frequency and requirements

For roles where the requirements for passing the prescribed training are set, it is possible to determine the need to repeat them after completing the primary training.

### 5.3.5 Job rotation frequency and sequence

There is no job rotation for trusted roles.

### 5.3.6 Sanctions for unauthorized actions

Any employee failure whose result is a situation that is not in accordance with the provisions of this CP or CPS, whether it concerns negligence or bad intent, will be the subject of appropriate administrative and disciplinary proceedings by the Provider.

### 5.3.7 Independent Contractor Controls

Where independent contractors are assigned to implement trusted roles, they must be subject to the obligations and specific requirements for these roles within the meaning of section 5.3 and are equally subject to the sanctions referred to in point 5.3.6.

### 5.3.8 Documentation supplied to personnel

Employees in trusted roles must have the documents needed to perform the function they are assigned to, including a copies of this CP and CPS and all technical and operational documentation necessary to maintain the integrity of operation of the Provider's.

## 5.4 Audit logging procedures

The Provider must record and have available all important information regarding the issued certificates during the necessary time and even after termination of operation.

Provider has to record accurate time in the trust service concerning key management, and clock synchronization. The time recorded for each event must be synchronized with UTC at least every 24 hours.

### 5.4.1 Types of events recorded

The Provider shall record and evaluate the following important events

- Life cycle processes of Provider's keys (generation, backup, recovery, disposal, etc.);
- Processes related to the HSM module itself;
- Data obtained at the provision of trusted services by Customers / Holders (Requests for Issuance, Cancellation, etc.);
- System logs of individual parts of the Provider system.

### 5.4.2 Frequency for Processing and Archiving Audit Logs

Administrators of the Provider are required to keep track of the system logs posted in a timely manner to identify in time the potential threat to the Provider's service provision. All recorded logs in electronic form must be kept at regular intervals, at least once a month, on the recording media in order to be available to the auditor. Likewise, the auditor must be provided with all written audit records concerning to the life cycle processes of the keys of Root and Subordinate Certification Authorities, Time stamp Authorities, and OCSP responders of the Provider.

### 5.4.3 Retention Period for Audit Logs

Provider must keep audit logs in accordance with the requirements of current legislation. Audit logs shall be kept at least until the end of the following regular annual external audit of their services.

### 5.4.4 Protection of Audit Log

Audit records must be kept and protected so that they are not impaired.

### 5.4.5 Audit Log Backup Procedure

No stipulation.

### 5.4.6 Audit Log Accumulation System

Provider must have a built-in log backup system.

### 5.4.7 Notification to event-causing subject

No stipulation.

### 5.4.8 Vulnerability assessments

See 5.4.2.

## 5.5 Records archival

### 5.5.1 Types of records archived

Provider must keep all records of the issued certificates as well as the certificates themselves according to the requirements of the current legislation during the period specified in 5.5.2.

The records can be kept in paper form or, in electronic form. All records that shall be submitted by the Customer / Holder for the issuing of required type of certificate (e.g., business listing, power of attorney, domain ownership, etc.) shall also be part of the retained records.

Provider must also keep all audit records (logs), written records of CA events (CA key generation, subordinate CA, TSA certificate issuance, and OCSP responder certificates).

Viewing records can be allowed individual components of the Provider fully of the PMA and to the persons performing the compliance audit.

### 5.5.2 Retention period for archive

Provider must keep the original of the application for the certificate together with the relevant documents confirming the identity of the Holder in the paper or in the electronic form at minimum 10 years.

### 5.5.3 Protection of archive

The archive records of the Provider must be stored in a safe off-premises location and must be maintained in a manner that prevents unauthorized modification, replacement or destruction.

### 5.5.4 Archive backup procedures

No stipulation.

### 5.5.5 Requirements for time-stamping of records

No stipulation.

### 5.5.6 Archive collection system

No stipulation.

### 5.5.7 Procedures to obtain and verify archive information

No stipulation.

## 5.6 Key changeover

Provider must use his signature (private) keys only for the purpose for which they are intended. Private CA subordinate keys can only be used only for the purpose for which they are intended i.e. signing end-user certificates or signing certificates issued for technological purposes (timestamp, OSCP responder, etc.). Root CA private keys can only be used when signing certificates for subordinate CAs or technology certificates belongs to Root CA (OCSP responder).

A new Provider's certificate (Root CA, subordinate CA) shall be published at the Provider's Web site after creating.

## 5.7 Compromise and disaster recovery

### 5.7.1 Incident and compromise handling procedures

In order to ensure the integrity of services, the Provider must implement data backup and recovery procedures.

Provider shall have developed disaster recovery plans for the performance of trusted services.

Trusted services should be provided from two geographically separated CA systems, one of which is led as master and the other as backup for the case of failure or disaster of master one.

Disaster recovery procedures shall be regularly reviewed and tested (at least on an annual basis) and reviewed and updated as necessary.

### 5.7.2 Recovery Procedures if Computing resources, software, an/or data are corrupted

In the event of damage or suspicion of damage to hardware, software or data, the Provider must use procedures to recover damaged assets. Procedures must include activities that ensure a complete restoration of the environment.

### 5.7.3 Recovery Procedures after Key Compromise

In the case of compromise of a private CA key, the Provider shall have procedures for

- Recovering a secure environment;
- End-user public key distribution procedures;
- Issuing new certificates to end-users.

### 5.7.4 Business continuity capabilities after a disaster

The Provider must have procedures in place to ensure continuity of action in the event of an accident due to natural disasters that will ensure its ability to resume its activity. Procedures must include a recovery place, procedures for asset protection at the site of the accident or natural disaster respectively, etc.

## 5.8 CA or RA termination

Upon termination of the Provider's activities for reasons other than those caused by force majeure (e.g. natural disaster, state of war, state power, etc.), the procedure shall be followed in accordance with part 5.7.

Before terminating providing the services, the Provider shall

- At least 6 months in advance notify by the suitable way the supervisory Authority, the all Holders of valid certificates, the Relying Parties and to the public planned closure of its activities. This notice must be made through the Provider's website, electronic mail, ordinary mail, registration authorities, or electronic media and printing. Terminate all existing mandate contracts, powers of attorney under which other legal persons could act on behalf of the Provider.
- To conclude a contract with another CA that would ensure continuity in providing trusted services, if possible.
- To collect and prepare all documents associated with the trusted services provided for archiving according the PMA guidelines.
- To check compliance with privacy rules e. g. Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation and Act No. 18/2018 Z. z. on the Protection of Personal Data (hereinafter referred to as "Personal Data Protection Regulations") [13].
- Eliminate all private keys, including all their copies, in such a way that they can no longer be restored.

Upon termination of its activity, the Provider will not issue any certificate and will probably guarantee impossibility to re-use the Provider's private keys.

Before terminating their activities, each RA will provide all archived data to the Provider as instructed by the PMA.

The Provider must have a solution to cover all the costs associated with meeting the minimum termination requirements in the event of bankruptcy or any other cause when it will be unable to cover the costs by its own means, in accordance with applicable bankruptcy legislation.

# 6. TECHNICAL SECURITY CONTROLS

The technical part of the provider's infrastructure (hardware and software) must consist only of secure systems and official software. The infrastructure architecture of the provider must be designed with components that meet safety standards at the level of current knowledge.

Particular attention must be paid to the cryptographic module (HSM), which serves to generate, store and use the Provider's private keys and is one of the most vulnerable assets. The private keys of the provider must be stored in an HSM module that is certified at least according to the FIPS 140-2 Level 3 standard.

The Provider must use a combination of physical, logical and procedural measures to ensure its security to protect its private key. These measures must be described, for example, in the published CPS.

The Provider's system must contain a device for the continuous detection, monitoring, and signaling of unauthorized and unusual attempts to access its resources.

Publishing applications must provide access control before trying to add or delete a certificate or modifying other associated data.

Revocation status reporting must provide access control before attempts to modify revocation status information.

All Provider features that use a computer network must be secured against unauthorized access and other malicious activities.

## 6.1 Key pair generation and installation

### 6.1.1 Key pair generation

#### 6.1.1.1 Certificate issuer

Generating and installing a provider's key pair must be done in a standardized way detailed in the Provider's documentation. The key pair generating shall provide sufficient confidence in the process and the whole process must be recorded in writing. Authorized staff in trusted roles who are eligible to participate in the key generation and request generation process must ensure key generation. Key generation must be done in a secure cryptographic module.

#### 6.1.1.2 Registration authority

The generation of key pairs of certificates for registration authorities shall be performed under the control of the Provider's authorized staff and the keys must be stored in QSCD.

#### 6.1.1.3 End users

See section 4.1.

### 6.1.2 Private key delivery to subscriber

Key pair containing the RA employee's private key must be delivered to the holder in a secure way.

The generated end-holder certificate holder's key pair, which is stored in a QSCD, must be handed in personally as soon as the certificate is issued.

### 6.1.3 Public key delivery to certificate issuer

The public key must be securely delivered to the certification authority, for example, on-line via TLS/SSL connection through communications authorized by the registration authority.

### 6.1.4 CA public key delivery to relying parties

For relying parties, the Provider must securely provide public keys of all his issuing Certification Authorities issuing the certificates.

### 6.1.5 Key sizes

The CPS determines the recommended key lengths, minimum key lengths for all types of entities, and all algorithms used (e.g., RSA) respectively.

### 6.1.6 Public key parameters generation and quality checking

Parameters and quality of the Provider's public key (root and slave CAs) determine the PMA, and quality control is controlled during the key generation ceremony. The Provider must use Cryptographic Hardware Modules meeting the requirements of FIPS 186-2 to generate and store keys to ensure random generation of RSA keys with a minimum of 2048-bit size.

For each type of end-user certificate, the Provider must specify the parameters and quality of the public key (length, type) and must check compliance with these parameters prior to issue.

### 6.1.7 Key usage purposes

Certificates of the Certification Authorities of the Provider include extensions, which determine its usage.

## 6.2 Private Key Protection and Cryptographic Module Engineering

### 6.2.1 Cryptographic module standards and controls

To protect their private keys (root CAs, subordinate CAs) Provider shall use hardware cryptographic modules certified to FIPS 140-2 level 3. Modules shall be stored in secured spaces accessible only to persons in trusted roles.

Provider's CA private keys can only be used to sign certificates and CRLs issued by the Provider.

CA equipment must be permanently protected from unauthorized access, even from unauthorized physical access.

The HSM module must meet the protection against electromagnetic radiation capture.

### 6.2.2 Private key (N out of M) multi-person control

In the case of operations with the private keys of the Provider (e.g. generation, backup, disposal), shall always be participating the appropriate number of eligible persons on the principle "N" out of "M".

### 6.2.3 Private key escrow

No stipulation.

### 6.2.4 Private key backup

Private keys of Provider shall be generated and stored inside hardware cryptographic modules.

Private keys shall always be encrypted in case authorized personnel within the meaning of section 6.2.2 perform transfer them for backup and recovery purposes, Transferring private keys and restoring them to another hardware cryptographic module may only.

### 6.2.5 Private key archival

No stipulation.

### 6.2.6 Private key transfer into or from a cryptographic module

See section 6.2.4

### 6.2.7 Private key storage on cryptographic module

Private keys of subordinate CA used to sign certificates issuing to end-users shall be stored in the HSM. Private keys may leave the module only in encrypted form that will not allow their restore without the appropriate number of authorized persons on the principle "K" out of "N". All The HSM Modules of the Provider shall be operated in secure environment with the access control.

### 6.2.8 Activating Private Keys

Authorized persons in the sense of the section 6.2.2 can only activate the private keys of the Provider.

Upon activation, shall each authorized person from the required number of eligible persons insert his smart card to the HSM module and enter a password.

The protection of private key by the Holder whom Provider issued certificate is his/her sole responsibility. The Provider shall advise all Holders to protect their private keys by using a strong password to prevent their private key being misused.

### 6.2.9 Deactivating Private Keys

Deactivation of the private key in the HSM module can only be done by an authorized person (CA administrator) or the private keys can be deactivated automatically in the event of a session failure or the power supply failure of the HSM module.

### 6.2.10 Destroying Private Keys

The Provider must ensure by technical and organizational measures that the Provider's Private Key cannot be used after the end of his life cycle. The end of the life cycle of the CA private key and the technical and organizational measures taken shall be done with a record signed by all the actors present.

### 6.2.11 Cryptographic Module Capabilities

See section 6.2.1.

## 6.3 Other aspects of key pair management

### 6.3.1 Public key archival

Provider must keep all public keys for which the certificate was issued in accordance to section 5.5.2.

### 6.3.2 Certificate operational periods and key pair usage periods

The validity of the Certificate issued by the Provider and the usability of the key pair shall not exceed the following

| Certificate type | Validity (maximum) |
|---|---|
| Root CA | 30 years |
| Subordinate CA | 15 years |
| End user certificate (except TLS/SSL) | 5 years |
| End user TLS/SSL certificate | 395 days |

## 6.4 Activation data

### 6.4.1 Activation data generation and installation

Activation data is data that is necessary to allow access to the private key that is either stored in software on a computer file, in a QSCD device or in the HSM module. The activation data can be in the form of a PIN, password, or password divided into several parts on the K / N principle and so on.

The activation data for the Provider's Cryptographic Module used must be created in the sense of section 6.2.2.

### 6.4.2 Activation data protection

Only Holders are solely responsible for protecting his private keys.

When issuing a certificate, the Holder shall be notify by the Providers of the need to protect the private key with a strong password.

Key pair dedicated for certificate issuer

- Shall be generated in a security module that meets the minimum requirements of the FIPS 140-2 level 2 standard;

- Any manipulation with a private key can only be allowed under the multiple control principle, and minimum three (3) persons are needed. Handling involves recovering a key to another HSM module if the module in which the keys are currently stored.

Further details regarding the private key of the Provider CA are provided in the "Working with Cryptographic Modules" document.

### 6.4.3 Other aspects of activation data

It shall be ensured that asymmetric private keys never occur in an unencrypted form outside the module where they are stored.

No one shall have access to a private signature key other than its Holder.

During backup and transfer, the keys must be encrypted. Holder of the key is responsible for ensuring that all copies of private keys are protected, including the protection of all workstations where any of his/her private keys occurs.

Pass-phrases, PINs, biometric data or other mechanisms equivalent to authentication robustness must be used to protect access to the private key. Activation data may be distributed to the Holder in person or by post, but only separately from the cryptographic module they activate.

If the activation data is written, it must be secured at the data protection level for which the cryptographic module is used and must not be stored with it.

Activation data for private keys belonging to certificates confirming individual identity may never be shared.

Those who are authorized to use the given private keys in the organization should only know activation data for private keys belonging to certificates confirming the identity of an organization.

## 6.5 Computer security controls

### 6.5.1 Specific computer security technical requirements

The Provider must perform all the functions of a trusted service provider using a trusted system that must meet the requirements defined in its Security Project for information system.

Provider issuing certificates must meet the specific information security requirements of a trusted service provider as defined in ETSI EN 319411-1 "Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1 General requirements“ [14]

All systems must be regularly verified for malicious code and protected against spyware and viruses.

### 6.5.2 Computer security rating

No stipulation.

## 6.6 Life cycle technical controls

### 6.6.1 System development controls

Applications for the needs of the Provider's system must take account of the security of the development environment, personal security, security of the configuration management in system maintenance, technical software development practices, software development methodology, and modularity and layering.

### 6.6.2 Security management controls

The Provider must use the tools and procedures to ensure that the operating systems and network connections match the set security.

These tools and procedures should include security integrity, firmware, and hardware integrity checks to ensure their proper functioning.

### 6.6.3 Life cycle security controls

No stipulation.

## 6.7 Network security controls

The provider must have taken measures to ensure network security, including security of firewalls.

## 6.8 Time-stamping

No stipulation.

# 7. CERTIFICATE, CRL, AND OCSP PROFILES

## 7.1 Certificate profile

### 7.1.1 Version number

This CP only allows issuing certificates conforming to X.509 version 3.

#### 7.1.1.1 Provider Root CA Certificates

Algorithms and key lengths applied in the Root Certificate of the Provider

| Signature Algorithm |
|---|
| sha256RSA |

| Public key |
|---|
| RSA, length 2 048 bit or 4 096 bit |

| Validity of Root CA certificate |
|---|
| maximum 30 years |

Table 7 Content of items in the Root Certificate of the Provider

| Name abbr. | OID | Name | Content |
|---|---|---|---|
| C | 2.5.4.6 | countryName | SK |
| L | 2.5.4.7 | localityName | Bratislava |
| | 2.5.4.97 | organizationIdentifier | *Reference to the identification of the legal entity operating the CA* [1)] |
| O | 2.5.4.10 | organizationName | Disig a.s. |
| CN | 2.5.4.3 | commonName | *depending on the CA type* [2)] |

[1)] It shall be part of the Root CA certificate, which validity begins after 1.7.2016

[2)] The CN shall contain the business name of the certification authority t. j. CA Disig complemented as required root distinguishing name of CA Disig with e.g. Root R1, Root R2 etc.

Table 8 Certificate extensions in root CA certificates

| Extension / OID | Presence | Critical |
|---|---|---|
| basicConstraints / 2.5.29.19 | YES | YES |
| keyUsage / 2.5.29.15 | YES | YES |
| subjectKeyIdentifier / 2.5.29.14 | YES | NO |

### 7.1.1.2 Subordinate Certification Authority of the Provider

Algorithms and key lengths applied in the subordinate CA

| Signature Algorithm |
|---|
| sha256RSA |

| Public key |
|---|
| RSA, length 2 048 bit |

| Validity of subordinate CA |
|---|
| maximum 15 years |

Table 9 The content of the items in the certificate of the Subordinate CA

| Name abbr. | OID | Name | Content |
|---|---|---|---|
| C | 2.5.4.6 | countryName | SK |
| L | 2.5.4.7 | localityName | Bratislava |
| | 2.5.4.97 | organizationIdentifier | *Reference to the identification of the legal entity operating the CA* [1)] |
| O | 2.5.4.10 | organizationName | Disig a.s. |
| CN | 2.5.4.3 | commonName | *depending on the CA type* [2)] |

[1)] It shall be part of the Subordinate CA certificate, which validity begins after 1.7.2016

[2)] The CN shall contain the business name of the certification authority t. j. CA Disig complemented as required root distinguishing name of CA Disig with e.g. R2I2 Certification Service, R2I3 Certification Service etc.

Table 10 Certificate extensions in subordinate CA

| Extension / OID | Presence | Severity |
|---|---|---|
| authorityInfoAccess / 1.3.6.1.5.5.7.1.1 | YES | NO |
| Authority Key Identifier / 2.5.29.35 | YES | NO |
| basicConstraints / 2.5.29.19 | YES | YES |
| keyUsage / 2.5.29.15 | YES | YES |
| subjectKeyIdentifier / 2.5.29.14 | YES | NO |
| crlDistributionPoints / 2.5.29.31 | YES | NO |
| certificatePolicies / 2.5.29.32 | YES | NO |
| subjectAltName / 2.5.29.17 | YES | NO |

#### 7.1.1.3 End user certificates

For details on the content of the distinguishing name (DN) of each type of certificate issued under this CP, refer to the section 3.1.4.

### 7.1.2 Certificate Content and Extensions

Table 11 lists the extensions used in all types of certificates issued.

Table 11 Basic extensions in certificates

| Extension name | ASN.1 name and OID / Description | Presence | Critical |
|---|---|---|---|
| Subject Key Identifier | {id-ce-subjectKeyIdentifier}<br>{2.5.29.14}<br>This extension identifies the public key being certified. | YES | NO |
| Authority Key Identifier | {id-ce-authorityKeyIdentifier}<br>{2.5.29.35}<br>It identifies the public key to be used to verify the signature on this certificate or CRL. | YES | NO |
| Key Usage | {id-ce-keyUsage}<br>{2.5.29.15}<br>This extension indicates the purpose for which the certified public key is used. | YES | NO |
| CRL Distribution Points | {id-ce-CRLDistributionPoints}<br>{2.5.29.31}<br>This field identifies the CRL distribution point or points to which a certificate user should refer to ascertain if the certificate has been revoked | YES | NO |
| Extended Key Usage | {id-ce-extKeyUsage}<br>[2.5.29.37]<br>This field indicates one or more purposes for which the certified public key may be used, in addition to | YES | NO |

| | | | |
|---|---|---|---|
| | or in place of the basic purposes indicated in the key usage extension field. | | |
| Certificate Policies | {id-ce-certificatePolicies}<br>{2.5.29.32}<br>This extension lists certificate policies, recognized by the issuing CA, that apply to the certificate, together with optional qualifier information pertaining to these certificate policies. | YES | NO |
| subjectAltName | id-ce-subjectAltName<br>[2.5.29.17]<br>This extension contains one or more alternative names, using any of a variety of name forms, for the entity that is bound by the CA to the certified public key. | YES | NO |
| AuthorityInfoAccess | {id-pe-authorityInfoAccess}<br>{1.3.6.1.5.5.7.1.1}<br>Specifies the address (http// ... p7c, certificate or ldap//...) where is possible to obtain the certificates issued to the publisher of this certificate and the address of the OCSP. | YES | NO |

### 7.1.3 Algorithm object identifiers

| Signature Algorithm |
|---|
| sha256RSA |
| OID 1.2.840.113549.1.1.11 |

### 7.1.4 Name Forms

Requirement for the form of names for the individual types of certificates are listed in section 3.1.4.

In the publisher CA certificate, the certification path of which contains a root certificate distributed as a trust anchor in widely available application software, the name "CA Disig" is always used.

The following algorithms and key lengths are applied to all issued end-user certificates under this CP

| Signature Algorithm |
|---|
| sha256RSA |

| Public key |
|---|
| RSA, length - minimum 2 048 bit |

| Validity of certificate signature/seal certificate |
|---|
| Max. 5 years (1825 days) |

The following algorithms and key lengths are used for TLS / SSL certificates made under this CP

| Signature Algorithm |
| --- |
| sha256RSA |
| **Public key** |
| RSA, length - minimum 2 048 bit |
| **Validity of certificate TLS/SSL certificate** |
| Max. 395 days |

### 7.1.5 Name constraints

No stipulation.

### 7.1.6 Certificate policy object identifier

See section 1.2.

### 7.1.7 Usage of Policy Constraints extension

This extension is not used.

### 7.1.8 Policy qualifiers syntax and semantics

Each certificate issued under this policy must contain its identifier in the form of OID (see 1.3.158.35975946.0.0.0.1.1 ) in the id-ce-certificatePolicies (2.5.29.32).

In addition, each TLS/SSL certificate must contain an OID identifier (2.23.140.1.2.2) what means that the certificate is issued as a TLS/SSL certificate where the organization (a legal entity or a natural person) is verified that have the right to use, or have control of, the FQDN.

Each e-seal certificate must have a notice in the NoticeText (OID 1.3.6.1.5.5.7.2.2) that it is an electronic seal certificate within the meaning of the eIDAS Regulation [6].

### 7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

### 7.1.10 Other provisions

The structure (profile) of other certificates issued by the Provider, which are exclusively intended for internal use by contractual partners, is detailed in the relevant CPS, including the Certificate Extensions used.

The structure of certificates issued by the Provider may be changed only based on the PMA's decision and in the case of personal certificates issued for the purposes of the contractual partners under an agreement with the partner.

Used certificate extensions in each certificate type may be expanded according to the actual needs based on the PMA decision. Such an extension is not considered as a change in the profile of the certificates as defined in section 7.1. As required by the Provider, all issued certificate types may be extended to other items according the RFC 5280.

## 7.2 CRL profile

### 7.2.1 Version number

All CRLs issued by the Provider must be CRL version 2.

CRLs must be issued and signed by the same CA Provider as certificates listed in the CRL.

Issued CRLs must comply with RFC 5280 „Internet X.509 Public Key Infrastructure Certificate and CRL Profile“ [2]

### 7.2.2 CRL and CRL entry extensions

Table 12 lists the CRL extensions that were issued by the CAs of the Provider to which this CP applies, along with information on their presence and criticality.

Table 12 CRL extensions

| Extension name | Required | Critical |
|---|---|---|
| Authority Key Identifier (OID 2.5.29.35) | YES | NO |
| CRL Number (OID 2.5.29.20) | YES | NO |

## 7.3 OCSP profile

### 7.3.1 Version number

Provider must issue OCSP responses according to RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“ [15].

Separate OCSP responders whose signing certificates will be signed by the corresponding certification authorities of the Provider, and must include OCSP Signing (1.3.6.1.5.5.7.3.9) extension must issue OCSP responses for individual CAs issuing publicly trusted certificates.

### 7.3.2 OCSP extensions

Table 13 contains possible extensions in the OCSP responses of the Provider's OCSP Responder, their reporting obligation and their criticality.

Table 13 OCSP response extensions

| Extensions name | Required | Critical |
|---|---|---|
| id-pkix-ocsp-nonce<br>(OID 1.3.6.1.5.5.7.48.1.2) | NO | NO |
| Online Certificate Status Protocol (OCSP) Stapling TLS extension SignedCertificateTimestampList*<br>(OID 1.3.6.1.4.1.11129.2.4.5) | YES | NO |

* - This extension is included only in OSCP response issued by CA Disig R2I2 Certification Service/OCSP responder

# 8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

The purpose of the compliance audit is to ensure that the Provider has a satisfactory system of work that guarantees the quality of the trusted services provided by the Provider, and guarantees that he is acting in compliance with all the requirements of this CP, CPS, eIDAS Regulation [6] and CA/Browser forum [3]. All aspects of the CA operation relating to this CP are to be subject to compliance audits.

## 8.1 Frequency or circumstances of assessment

The Provider must undergo an audit of the compliance of the trusted services provided within the meaning of the section 1.4.1 at least once a year. In addition, each CA has the right to request regular and irregular reviews of the activities of its subordinate CMAs to confirm that subordinate CMAs operate in accordance with the security practices and procedures described in the applicable CPS.

## 8.2 Identity/qualifications of assessor

The auditor must be competent in the field of compliance audits and must be thoroughly acquainted with the audited CPS CMA, and meet the qualification requirements described in the document [3].

## 8.3 Assessor's relationship to assessed entity

See section 8.2.

## 8.4 Topics covered by assessment

The provider will be audited in accordance with a national scheme that assesses compliance with the latest versions of ETSI EN 319 411-1, including normative references from ETSI EN 319 401

The audit must be carried out by a qualified auditor within the meaning of paragraph 8.2.

## 8.5 Actions taken as a result of deficiency

When the auditor finds a discrepancy between the CMA's operation and the CPS's provisions, the following actions must be taken

- The auditor record a discrepancy;
- The auditor notifies the entities defined in section 8.6;
- Provider will propose the PMA the appropriate correction actions, including the expected time for its implementation.

The PMA will determine the appropriate correction actions, even up to possibly revocation of the CA certificate.

## 8.6 Communication of results

The Audit Report shall state explicitly that it covers the relevant systems and processes used in the issuance of all Certificates that assert one or more of the policy identifiers listed in section 7.1.6.

Audit report shall be publicly available no later than three months after the end of the audit period.

## 8.7 Self-Audits

During the period in which the CA Disig issues Certificates shall monitor adherence to this Certificate Policy, its Certification Practice Statement and CA/Browser forum requirement [3] and strictly control service quality by performing self-audits. Self-audit shall take place at least on a quarterly basis and against a randomly selected sample of the greater of 1 certificate or at least three percent of the TLS/SSL Certificates issued during the period commencing immediately after the previous self-audit sample was taken.

# 9. OTHER BUSINESS AND LEGAL MATTERS

## 9.1 Fees

There is duty of the Provider to publish a valid price list of trusted services and information under which these services can be ordered.

### 9.1.1 Certificate issuance or renewal fees

Fee for certificates must be paid on the terms agreed with the Customer / Holder.

Provider has to publish a valid price list of his services through his company's web site (see section 1).

In the case of the provision of its services only to the contractual partner, the price list need not be published.

### 9.1.2 Certificate access fees

See section 9.1.1

### 9.1.3 Revocation or status information access fees

See section 9.1.1

### 9.1.4 Fees for other services

See section 9.1.1

### 9.1.5 Refund policy

In justified cases, the Provider can reimburse the payment for the services provided based on an individual assessment.

## 9.2 Financial responsibility

The Provider must have sufficient resources to perform the trust services in order to remain solvent and be able to pay indemnities in the case of a court decision or, settlement of claims arising from the provision of these services.

### 9.2.1 Insurance coverage

The Provider shall be insured for possible damage that may be caused to the Holder of Certificates or third parties in relation to the provision of trusted services.

The Provider shall be liable for damages arising from the use of a certificate issued by him under applicable legislation (e.g., Commercial Code, Civil Code). The assumption is that the relevant provisions of this CP have been complied.

Liability for damage and the resulting settlement can only be accepted provided that

- The Holder has not violated his / her obligations (especially protection of his / her private key);

- Anyone who relied on a certificate issued by the Provider has done everything to prevent any damage, in particular by having verified the status of the certificate in question i.e. whether the certificate was not revoked at the decisive time when it was relied upon to.

The Provider does not have any financial responsibility for any damages that would arise to the Certificate Holder or the relying party in connection with the use of the certificate in a specific software application or in connection with the fact that the certificate cannot be used with the specific application or hardware.

Any claim for damages must be filed in writing.

### 9.2.2 Other assets

No stipulation.

### 9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

## 9.3 Confidentiality of business information

### 9.3.1 Scope of confidential information

Confidential information subject to appropriate protection shall be

- Private keys of the Provider used to sign certificates issued to subordinate CAs;
- Private keys of subordinate CAs used to sign certificates issued to end-users;
- Private keys of TSA services or OCSP;
- Private keys belonging to the executive components of the Provider (RA staff);
- Infrastructure (e.g. documents, procedures, procedures, files, scripts, passwords, etc.) serving to ensure the operation of the Provider's CA, including all its RAs;
- Personal data of holders of certificates subject to protection under the Personal Data Protection Regulations [13].

The certificate may only contain the information that is important and necessary for performing secure communication by the certificate.

CMA may require that the Provider can also exploit information that is not listed in the certificates (such as document ID, address, and telephone number) to properly manage certificates.

Any such information must be explicitly defined in the CPS.

All information stored at the Provider, which are not in the repository, must be treated as sensitive information and access to them shall be restricted to those who necessarily need this information to perform its official duties.

All information that is listed in the certificate and is therefore published through the repository is not classified as confidential and is considered public.

A list of revoked certificates (CRLs) is not considered confidential.

### 9.3.2 Information not within the scope of confidential information

The Provider may not disclose information relating to the Customer or the Certificate Holder to any third party. Disclosure is possible only if it is permit by this CP; it is required by law or by the order of the Competent Court or given in contract between the Provider and his Customer. Each requirement for release of information must be authenticated and documented.

The Provider shall treat the Customer's personal data in accordance with applicable laws and shall not provide it to any third party except for entities legally entitled to assess the activity of the Provider or competent governmental bodies such as the police, court or prosecutor respectively.

### 9.3.3 Responsibility to protect confidential information

Participants who receive confidential information are responsible for their protection against disclosure and must refrain from providing them to a third party.

## 9.4 Privacy of personal information

### 9.4.1 Privacy plan

The Provider shall process the Personal Data of the Customers / Certificate Holders or authorized persons respectively in accordance with the requirements of Personal Data Protection Regulations [13].

### 9.4.2 Information treated as private

The provider must have a defined scope of personal data that process when providing qualified trusted services.

### 9.4.3 Information not deemed private

The Provider may, in accordance with the Personal Data Protection Regulations [13] define the types of information he carries out in providing trusted services and are not considered personal data.

### 9.4.4 Responsibility to protect private information

Participants who obtain personal data are responsible for their protection against disclosure and must refrain from providing them to a third party.

### 9.4.5 Notice and consent to use private information

The Provider is obliged to proceed in accordance with the Personal Data Protection Regulations in fulfilling the information obligation towards the persons concerned and in obtaining their consent to the processing of personal data [13].

### 9.4.6 Disclosure pursuant to judicial or administrative process

The Provider may also provide these data to third parties if the relevant legislation is imposed or permitted do this.

### 9.4.7 Other information disclosure circumstances

No stipulation.

## 9.5 Intellectual property rights

This CP and the relate documents represent important Provider's expertise and are protected by copyright.

The Provider is the holder of the exclusive rights to the IS of the Provider and to the content of its web site.

## 9.6 Representations and warranties

Provider through this CP, Terms of Service [5] and, where applicable, the certificate issuance agreement expresses legal assumptions regarding the use of issued certificates by the Customer / Holder and the relying party.

### 9.6.1 CA representations and warranties

Regarding Trusted Services, the Provider does not provide any representations or warranties except as provided in this CP and the General Terms [5].

### 9.6.2 RA representations and warranties

All external Entity registration authorities shall provide trusted services based on a contractual relationship with the Provider and in accordance with this CP.

See also section 9.6.

### 9.6.3 Subscriber representations and warranties

Customer or Certificate Holder uses the trusted services of the Provider on his own responsibility and carries all the costs of remote means of communication or other technical means necessary for the use of these services (e.g. the software needed for making the electronic signature / seal, software for the authentication of the website etc.);

### 9.6.4 Relying party representations and warranties

The Relying party shall note that they is solely free to decide whether to trust and rely on the certificate issued by the Provider and hence on the information contained therein. The Relying party is required to comply with the obligations described in section 10 of the General Terms [5], in the case of a decision to trust the Provider's certificates; otherwise, it is solely responsible for the legal consequences thereby caused.

### 9.6.5 Representations and warranties of other participants

No stipulation.

## 9.7 Disclaimers of warranties

The Provider is solely responsible for damages caused by failure to comply with obligations according Article 13 of eIDAS Regulations [6].

## 9.8 Limitations of Liability

The Provider is not liable for indirect or contingent losses or damages incurred to the Customers or to the Relying Parties in connection with the use of trusted services.

The Provider is not liable for any damages (including lost profits) incurred by the Customer / Holder of the certificate, relying party or to any third party due to

a) violation of the obligations by the Customer / Holder or by the relying party under the legal, contractual, General Terms or Provider's obligations, including the obligation to exercise reasonable care when relying on the certificates;

b) failure to provide the necessary cooperation on the part of the Customer or Certificate Holder;

c) by the technical features, configuration, incompatibility, inadequacy or other defects in software or hardware means used by them;

d) use or reliance on the expired or revoked certificate;

e) Use of the certificate by the Customer / Holder of the certificate in violation of the contract, the General Terms or the Provider's policies;

f) that the certificate was used contrary to its purpose or limitations stated in the certificate, in General Terms or in the CP respectively;

g) delay or non-delivery of request about Certificate status to the Provider for reasons not on the Provider's side (in particular in cases of unavailability or overloading of the Internet or defects in the equipment or technical equipment used by the verifier);

h) failure to provide any of the trusted services or their unavailability during the scheduled maintenance or reorganization announced at the Provider's web site;

i) due to Force Majeure;

The Provider is not liable for damages incurred to the Relying party because, when relying on the certificate and trustworthy services of the Provider or relying on the electronic signature or seal made on their basis, did not proceed according section 10 of the General Terms [5] or according of requirements of this policy.

## 9.9 Indemnities

Any person who violates his or her obligation or any obligation under this CP, The Agreement, and the General Terms shall be liable to compensate for damage caused to the other party, except in cases where the liability of the entity is excluded for damages. Damage shall be deemed actual damage, loss of earnings and costs incurred by the injured party in respect of the damage event.

Whoever violates his or her obligation or any obligation under this CP, The Contract, and the General Terms may be relieved of liability for damages only if it proves that a breach of duty or any obligation has occurred as a result of circumstances excluding responsibility e.g. Force Majeure.

## 9.10 Term and termination

### 9.10.1 Term

This version of CP is effective from the date of its entry into force, which is September 1, 2020 until it is replaced by a new version. For details on the history of changes to this CP, see the "Revision" section 1.2.1.

### 9.10.2 Termination

This CP version will expire on the date of publication of a new version higher than 5.4, or termination of the Provider's trusted service.

### 9.10.3 Effect of termination and survival

In the event that this document is not replaced by a new version and its validity expires after the finishing of providing trustworthy service by Provider, all provisions of this CP relating to the Provider, which he is obliged to observe after termination of his activity shall be fulfilled. (See section 9).

## 9.11 Individual notices and communications with participants

Provider communication with individual RAs must be officially conducted through an authorized e-mail communication between the Provider's authorized person and the authorized person of RA.

## 9.12 Amendments

### 9.12.1 Procedure for amendment

The CP update is based on its review, which must be done at least once a year from the approval of the current valid version. An authorized person of Provider who, based on the results of the review, must prepare a written proposal for any proposed changes must perform the review.

An authorized PMA member must do approval of proposed changes. The proposed changes must be considered within 14 days of their delivery. After the deadline for

review of the change proposal, the PMA has to accept the proposed change, accept it or refuse it.

Errors, update requests, or proposed CP changes must be communicated to the contact listed in 1.5.2. Such communication must include a description of the change, the reason for the change, and the contact details of the person requesting the change or suggesting the change respectively.

All approved CP changes must be notified to the entities concerned within one week prior to their entry into force through the channel for publishing and notifying (see section 2).

Each modified version of this CP must be numbered and registered, so the newer version must have a higher version number than the one it replaces.

Corrections of clutter, grammar and stylistic errors are not considered as changes initiating a change to the version of this CP.

### 9.12.2 Notification mechanism and period

Provider must publish information about the current version of CP through its website (see section 1.5.2).

The Authorized Representative of the Provider must inform all contractually bound RAs of the Provider about the approval of the new version of the CP, by sending a new version by e-mail before it enters into force in accordance with section 9.12.1. The Provider shall request feedback from the RA in the form of a confirmation e-mail message about the download of the electronic version of the Provider's CP.

Current version of CP must be available on each contractually bound RA of the Provider at least in electronic form. Internal employees must be equally informed about the new version of this CP.

### 9.12.3 Circumstances under which OID must be changed

Every policy must have its OID assigned by the Provider. The OID of this policy is listed in section1.2 and for each new CP version remains unchanged.

## 9.13 Dispute resolution provisions

The Customer / Holder has the right to send to the Provider a complaint about the provided trusted service by email at radisig@disig.sk. The Provider shall process the complaint no later than 30 days after its receipt, unless otherwise agreed by the parties. Complaint process refers only to a description of the defect referred to by the Customer. The Provider has to respond within 30 days of complaint receipt. The Provider reserves the right to extend this period in case of more complicated complaints.

The courts of the Slovak Republic have exclusive jurisdiction to settle any disputes between the Provider and the Customer / Holder of the certificate. If the Customer / Certificate Holder is a consumer, any dispute may also be settled out of court. In such a case, it is entitled to contact an out-of-court dispute resolution body, Slovak trade inspection or other legal entity registered in the list pursuant to Article 5 2 of Act no. 391/2015 Coll. on alternative dispute resolution of consumer disputes,

as amended. Prior to joining a court or out-of-court dispute settlement, the parties are required to try to resolve this dispute by mutual agreement first.

## 9.14 Governing law

The laws of the Slovak Republic govern legal relations between the Provider and the Customer / Holder of the certificate.

The rights and obligations of the parties which are not governed by the General Terms, or by The Agreement are governed, in particular, by the relevant provisions of Act No. 513/1991 Coll., Commercial Code, as amended, Act no. 40/1964 Coll., The Civil Code in the wording of later regulations and other generally binding legal regulations of the Slovak Republic.

## 9.15 Compliance with applicable law

Provider provides trustworthy services in accordance with valid legal regulations in force in the Slovak Republic.

## 9.16 Miscellaneous provisions

### 9.16.1 Entire agreement

No stipulation.

### 9.16.2 Assignment

The Customer / Holder may not assign, transfer or transfer (or otherwise deal with) any third party's rights, obligations or claims under the Agreement or the General Conditions without the written consent of the Provider.

### 9.16.3 Severability

If any provision of this CP is, or becomes, invalid or unenforceable, it will not cause invalidity or unenforceability of the entire CP if it is completely separable from the other provisions of this CP. The Provider will immediately replace the invalid or unenforceable provision of the CP with new valid and enforceable provisions, the subject of which will be as close as possible to the subject matter of the original provision while preserving the purpose of this CP and the content of the individual provisions of this CP.

### 9.16.4 Enforcement

In the event that a certain right is not exercised during the duration of the contractual relationship between the parties, this right shall not be terminated due to its non-application unless otherwise stated.

Because of the cancellation of contractual relationship between the Contracting Parties, The parties are not deprived of the obligation to fulfill all the obligations arising from the rights exercised so far and to take all necessary legal acts which do not delay the delay and which are indispensable to prevent damage.

### 9.16.5 Force Majeure

Provider, Customer, and Holder are not responsible for delaying the fulfillment of their obligations due to circumstances excluding liability (Force Majeure).

Circumstance for excluding is an impediment that occurs independently of the will of the obligated party and prevents it from fulfilling its duty if it is impracticable to assume that the obligated party will avert or overcome this impediment or its consequences and that, at the time of the occurrence of obstacle could foresee the obstacle or not.

If the circumstances for excluding of the liability arise, then the party on which such circumstances occurs shall immediately inform the other of the nature, the beginning and the end of such an obstacle to the fulfillment of its obligations. Provider, Customer, and Holder are committed to doing their utmost to avert and overcome circumstances that exclude liability.

However, liability is not excluded if such a circumstance has occurred only when the obligated party has been late in fulfilling its obligation or if the party concerned fails to fulfill its obligation immediately inform the other of the nature and the beginning of the duration of the obstacle or if it originated from economic conditions. Effects that exclude liability are limited only to the period that an obstacle with which these effects are associated.

## 9.17 Other provisions

No stipulation.