Certificate Policy
for issuing TLS certificate

Disig, a.s.

Version **6.0**

Valid from **February 1, 2024**

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 City Court Bratislava III Section: Sa Insert No.: 3749/B
Telephone	+ 421 2 208 50 140
E-mail	disig@disig.sk

This document is a translation of the Slovak version of the document and has not undergone language editing. In case of contradictions, the provisions stated in the Slovak version of this document apply.

Trademarks
Product names mentioned herein may be trademarks of the firms.

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 Business Register of the City Court Bratislava III Section: Sa Insert No.: 3749/B, as a Trusted Service Provider (hereinafter referred to as "Provider"). This CP applies to root CAs and subordinate CAs mentioned in chapter 1.4.1 operated by the Provider, which provides 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 Publicly-Trusted TLS Server 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 TLS Certificates [3] (hereinafter "TLS BR"), requirements of individual programs for root certificates distributed by certificate consumers as is Microsoft [4], Mozilla [5], Apple [6], Google [7] 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") [8] and the requirements of the ETSI EN 319 411-1 standard. [9]

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 [10].

1.2 Document Name and Identification

Document Name:	**Certificate Policy for issuing TLS certificate**
Name abbreviation:	**CP CA Disig**
Version:	**6.0**
Approved on:	**January 29, 2024**
Valid from:	**February 1, 2024**
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; Miškovič
1.5	December 20, 2006	Formal text editing - Formatting, correcting links, editing text in section 4 "Operational requirements"; Miškovič
2.0	January 23, 2007	CP expansion in relation to the new type of certificate issued for the contracted client. Addition of section 7 "Certificate Profiles"; Miškovič.
2.1	March 29, 2007	Correcting text in chap. 2.8 and Chap. 4.9 Text editing related to a minor change in a partner's certificate; Miškovič
3.0	March 19, 2008	Overall revision of the CP for each type of certificate. Ďurišová, Miškovič
3.1	June 24, 2008	A new type of certificate adding.; Miškovič
3.2	November 10, 2008	Change certificate validity for domain user PKI VsZP Termination of operation at Záhradnícka 153; Miškovič
3.3	November 25, 2008	Editing the wording: section 3.1.9 - Domain ownership verification section 4.1.1; 4.1.2, - validation of the Applicant's e-mail address; Miškovič
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). Change the email address location in the certificate profile (section 3.1.2; 6.1.2); Miškovič
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; Miškovič
4.1	May 11, 2010	Inclusion of proposed audit corrective actions of 13.11.2009 (audit according ETSI TS 102042 V1.3.4); Miškovič
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; Miškovič
4.3	January 25, 2012	Supplementing the possibility to issue certificate for subordinate CAs, adding signature algorithms, and regular annual review of content; Miškovič
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; Miškovič
4.5	August 15, 2013	Refining of CA Disig CA root CA Certificate Profile and other Certified Types of Certificates; Miškovič
6.0	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); Enable issuing "wildcard" TLS/SSL certificates to be issued at the third level of the domain name (3.1.2); Miškovič

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
5.5	May 20, 2021	Addition of the method of reporting incidents (2.2); Shelf life of data used to verify domain ownership (3.2.2.4); Method of reporting compromise of the CA private key by third parties (4.9.12); Miskovic
5.6	May 20, 2022	Removing an OU field from the TLS certificate profile (3.1.4.3); Modification of the requirements for obtaining audit records in accordance with the requirements [3] version 1.8.4 (5.4); changing the TLS / SSL certificate type designation to TLS; Mišković
5.7	October 1, 2022	Changes in connection with the requirement to publish revocation reasons in CRL when revoking issued TLS certificates (4.9.1.1; 4.9.2; 4.9.3; 7.2.2)
5.8	April 20, 2023	Changes in connection with the creation of a new subordinate CA Disig R2I5; Mišković
5.9	September 1, 2023	Changes in connection with the entry into force of "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"; Mišković
6.0	February 1, 2024	Allocation of CP exclusively for the policy of issuing Publicly-Trusted TLS Certificates; 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 conducts certain selected activities in the provision of trusted services on behalf of the Provider.

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

Provider may establish following types of RA:

- **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

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

The Certificate holder may be:

- A device or system operated by a natural or legal person or operated on behalf of a natural or legal person.

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

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") [11] 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 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.

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 the 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 for:

- TLS communication security (web site authentication).

Provider issued following types of certificates to the Subscribers:

- Publicly-Trusted TLS certificate (TLS 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 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) i.e. 2.23.140.1.2.2 in the meaning of TLS BR [3].

- 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)(DER)	B561EBEAA4DEE4254B691A98A55747C234C7D971
Hash (sha256) (DER)	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) (DER)	19F2783DEDD8561A61C682932EE9D5B4D86B00CE
Hash (sha256) (DER)	C96F24C45113FD91AE2F9E40E106653BFA0FFBCFA07E209524C844E7C8DA4148
Comment	It only issues TLS end-user certificates (see 3.1.4.3).

1.4.2 Prohibited Certificate Uses

Certificates issued under this CP are not EU qualified certificates for website authentication according the eIDAS Regulation [8] and cannot be used where EU qualified certificates for website authentication are required .

1.5 Policy administration

1.5.1 Organization Administering the Document

Table 1 contains 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** see more at **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,

b) the creation, verification, and validation of certificates for website authentication,

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.

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.

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 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
TLS	-	Transport Layer Security
SSL	-	Secure Sockets Layer

1.6.3 Bibliography

[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] Baseline Requirements for the Issuance and Management of Publicly-Trusted TLS certificates version 2.0.2. s.l. : https://cabforum.org/baseline-requirements-documents/.

[4] Program Requirements - Microsoft Trusted Root Program. s.l. : https://learn.microsoft.com/en-us/security/trusted-root/program-requirements.

[5] Mozilla Root Store Policy, Version 2.9, Effective September 1, 2023. s.l. : https://www.mozilla.org/en-US/about/governance/policies/security-group/certs/policy/.

[6] Apple Root Certificate Program, Effective August 15,2023. https://www.apple.com/certificateauthority/ca_program.html.

[7] Chrome Root Program Policy, Version 1.5. s.l. : https://www.chromium.org/Home/chromium-security/root-ca-policy/.

[8] Regulation (EU) No 910/2014 of the European Parliament 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.

[9] ETSI EN 319 411-1 Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements.

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

[11] General terms and conditions of provision and use of a trusted services Disig, a.s.

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

[13] RFC 6960 „X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP“.

[14] RFC 5019 The Lightweight Online Certificate Status Protocol (OCSP) Profile.

[15] RFC 8954 Online Certificate Status Protocol (OCSP) Nonce Extension.

[16] RFC 6962 Certificate Transparency.

[17] ETSI EN 319 401 Electronic Signatures and Infrastructures (ESI); General Policy Requirements for Trust Service Providers.

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 according with section 8.

The Provider confirms that all requirements of the current version of the document [3], which is published on the website http://www.cabforum.org, are considered in this CP. In case of any discrepancies between these requirements and this CP, the requirements given by the current version of the document shall prevail [3].

The Provider must have a website available that will allow application vendors to assess their software with the Provider's certificates issued, which are linked to a publicly trusted root certificate.

When a CA fails to comply with any requirement of the current version of "Mozilla Root Store Policy" [5], whether it be a misissuance, a procedural or operational issue, or any other variety of non-compliance - the event is classified as an incident. At a minimum, Provider must promptly report all incidents to Mozilla in the form of an Incident Report and must regularly update the Incident Report until a Mozilla representative marks the corresponding bug as resolved in the mozilla.org Bugzilla system. The Provider should cease issuance until the problem has been prevented from reoccurring.

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).

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

The Provider shall protect any information stored in a repository that is not available to the public. The 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

No stipulation.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonym of subscribers

No stipulation.

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 certificate issued by the Provider may consist of items that are described in the following section.

3.1.4.1 Certificate

Table 3 contains a list of fields that may be contained in the relative order in the subject of certificate type "*Organization Validated*" issued by Provider

Each 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 certificate will be referred to as a "wildcard " certificate.

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

Table 3 "*Organization Validated*" certificate subject fields and their description

Filed name	OID	Abb.	Description	Note
countryName	**2.5.4.6**	**C**	Two-character abbreviation for country name according to ISO 3166-1 associated with the Subject. SK for Slovak republic	**Mandatory field**
localityName	2.5.4.7	L	Subject's locality information	**Mandatory field**

organizationName	2.5.4.10	O	The Subject's name or DBA.	**Mandatory field**
commonName	**2.5.4.3**	**CN**	Value derived from the subjectAltName extension according to Section 0	**Mandatory field**

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

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

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

No stipulation.

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 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, to the Customer requesting a certificate.

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

Verification must be performed at the specified time before the 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 performed by the Provider using one of the methods specified in this paragraph.

3.2.2.4.1 Validating the Applicant as a Domain Contact

No stipulation.

3.2.2.4.2 Email, Fax, SMS, or Postal Mail to Domain Contact

Confirming the Applicant's control over the FQDN by sending a Random Value via email, fax, SMS, or postal mail and then receiving a confirming response utilizing the Random Value. The Random Value MUST be sent to an email address, fax/SMS number, or postal mail address identified as a Domain Contact.

Each email, fax, SMS, or postal mail MAY confirm control of multiple Authorization Domain Names.

The CA MAY send the email, fax, SMS, or postal mail identified under this section to more than one recipient provided that every recipient is identified by the Domain

Name Registrar as representing the Domain Name Registrant for every FQDN being verified using the email, fax, SMS, or postal mail.

The Random Value SHALL be unique in each email, fax, SMS, or postal mail.

The CA MAY resend the email, fax, SMS, or postal mail in its entirety, including re-use of the Random Value, provided that the communication's entire contents and recipient(s) remain unchanged.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation.

Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.3 Phone Contact with Domain Contact

No stipulation.

3.2.2.4.4 Constructed Email to Domain Contact

The Provider does not use this method.

3.2.2.4.5 Domain Authorization Document

No stipulation.

3.2.2.4.6 Agreed-Upon Change to Website

No stipulation.

3.2.2.4.7 DNS Change

The Provider does not use this method.

3.2.2.4.8 IP Address

The Provider does not use this method.

3.2.2.4.9 Test Certificate

No stipulation.

3.2.2.4.10 TLS Using a Random Value

No stipulation.

3.2.2.4.11 Any Other Method

No stipulation.

3.2.2.4.12 Validating Applicant as a Domain Contact

The Provider does not use this method.

3.2.2.4.13 Email to DNS CAA Contact

The Provider does not use this method.

3.2.2.4.14 Email to DNS TXT Contact

The Provider does not use this method.

3.2.2.4.15 Phone Contact with Domain Contact

Confirm the Applicant's control over the FQDN by calling the Domain Contact's phone number and obtain a confirming response to validate the ADN. Each phone call MAY confirm control of multiple ADNs provided that the same Domain Contact phone number is listed for each ADN being verified and they provide a confirming response for each ADN.

In the event that someone other than a Domain Contact is reached, the CA MAY request to be transferred to the Domain Contact.

In the event of reaching voicemail, the CA may leave the Random Value and the ADN(s) being validated. The Random Value MUST be returned to the CA to approve the request.

The Random Value SHALL remain valid for use in a confirming response for no more than 30 days from its creation. The CPS MAY specify a shorter validity period for Random Values.

Once the FQDN has been validated using this method, the CA MAY also issue Certificates for other FQDNs that end with all the Domain Labels of the validated FQDN. This method is suitable for validating Wildcard Domain Names.

3.2.2.4.16 Phone Contact with DNS TXT Record Phone Contact

The Provider does not use this method.

3.2.2.4.17 Phone Contact with DNS CAA Phone Contact

The Provider does not use this method.

3.2.2.4.18 Agreed-Upon Change to Website v2

The Provider does not use this method.

3.2.2.4.19 Agreed-Upon Change to Website - ACME

The Provider does not use this method.

3.2.2.4.20 TLS Using ALPN

The Provider does not use this method.

3.2.2.5 Authentication for an IP Address

The Provider does not issue 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 consider, 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 8659 and the processing instructions provided in RFC 8659 for all records found.

If the Provider issues, they must do so within the TTL of the CAA record, or 8 hours, whichever is greater.

3.2.3 Authentication of individual identity

The Provider must guarantee, in the event that the certificate is issued for a device or system that can use the certificate, that the identity of the device or of the system with its public key are linked accordingly.

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

This natural person must provide the CMA with the following information:

- 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.

The 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 this section.
- 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).

The Provider must specify in the relevant CPS the procedures for authenticating the identity of the Certificate Holder. The CA must record this process for each certificate in written or electronic form. Documentation on authentication must contain at least:

- the identity of the person performing the authentication,
- unambiguous identification data from documents proving the identity of the Certificate Holder,
- date of identification.

Identity verification must be conducted by the CMA based on a document containing the following data of the Holder:

- full name and surname,
- address of permanent residence,
- social security number (persons who have it assigned),
- date of birth (persons who have not been assigned a birth number).

At the same time, the Customer/Holder must provide another document that contains at least the name and surname of the Holder and other personal data (date of birth, social security number). This does not apply if it is a service card.

The Provider must also record the following data from the documents:

- identity card number,
- identity card issuer,
- the date of validity of the identity card, if marked.

The Provider must accept the following documents when verifying the Holder's identity:

- ID card,
- passport,
- driver's license,
- birth certificate,
- service card,
- public health insurance policyholder's card
- weapon license.

In the case of providing a birth certificate, firearms license, service license or public health insurance policyholder's card, one of the following documents must also be provided: identity card, passport.

If a natural person represents another natural person, he must also present an officially verified power of attorney, from the text of which it is clearly clear that the representing natural person was authorized by the authorizing natural person to act in the given matter on his behalf.

Part of the Holder's authentication is the mandatory provision of the selected e-mail address, which will be stored together with his personal data in the Provider's IS, and which will serve expressly for communication between the Provider and the Certificate Holder and will not be part of the issued certificate. The Provider will not verify whether the specified e-mail address really belongs to the Holder.

All documents provided to RA by Customers must be either originals or officially certified copies of originals. No information may be added, changed, crossed out, etc. to them. Documents on which their validity period is marked must be valid.

If the RA employee has doubts about the identity of the potential Customer (e.g., an obvious discrepancy between the photo in the personal document and the appearance of the Customer, contradiction between the two submitted documents, etc.), he can refuse his registration.

Any documents in a foreign language (except Czech) must be translated into Slovak by an official translator - an expert.

At the request of the Customer or the RA, any disputed cases in the proof of identity must be resolved by the procedure according to section 9.13.

When providing documents, it is required that the originals of these documents for inspection and copies of the originals (do not have to be verified), except for personal documents identifying the Customer's identity, used for archiving for the Provider's needs, must be provided to the RA. Provision of an extract from the commercial register obtained from the Internet by the Customer is not sufficient, as this extract is only informative and cannot be used for legal actions.

The RA employee must check the following on the documents:

- Personal documents of a natural person:
  a) compliance of the data specified in the application with the data specified in the personal documents,
  b) validity of the submitted document,
  c) coming of age of a natural person (i.e., age 18),
  d) correspondence between the photo in the personal document and the appearance of the owner of the personal document,
  e) conformity in the submitted documents t. j. whether the data on one document does not contradict the data on another document.
- Extracts from the commercial register or of another register of legal entities:
  a) validity of the statement - must not be older than 3 months,
  b) proceeding on behalf of a legal entity - i.e., whether the natural person(s) who submitted the given statement has the right to act (sign) on behalf of the given legal entity,
  c) statement form – original or officially (notary/registered) certified copy of the statement.
- Consent to issuing a certificate:
  a) authorization to act on behalf of the company - the person signing the consent must be authorized to represent the Customer. Eligibility is checked according to the extract from the trade register or other register specified by law (or the establishment document, power of attorney, appointment decree). If the signing person is not entered in this statement, he must provide another document on the

basis of which he can act on behalf of the Customer (usually a power of attorney certified by a notary).

b) Validity - if the validity period of the consent is stated in the consent, this information is also checked.

- Powers of Attorney:

a) verification of power of attorney (by a notary/registry)

b) matching of the data specified in the power of attorney, which define the representative physical or legal entity, with the data indicated on the personal documents of the representing natural person or with the data indicated on the statement from the business or another register of the representing legal entity,

c) extent of power of attorney - i.e., j. whether the power of attorney authorizes the authorized natural or legal person to perform the required action on the RA on behalf of the authorizing natural or legal person,

d) time limit or another condition stated in the power of attorney

The Provider can also accept documents submitted by the Customer in electronic form, signed with a valid qualified electronic signature or a qualified electronic seal (extract from the commercial register, power of attorney, declaration, authorization, etc.).

3.2.4 Non-verified subscriber information

During the initial release, the email address is not verified.

3.2.5 Validation of authority

If the Applicant for a Certificate containing Subject Identity Information is an organization, the Provider shall use a reliable method of communication to verify the authenticity of the Applicant Representative's certificate request.

The Provider may use the resources listed in section 3.2.2.1 as a reliable method of communication. Provided that the Provider uses a reliable method of communication, the Provider may establish the authenticity of the certificate request directly with the Applicant representative or with an authoritative source within the Applicant's organization, such as the Applicant's main business offices, corporate offices, human resource offices, information technology offices, or other department that the CA deems appropriate.

In addition, the Provider shall establish a process that allows an Applicant to specify the individuals who may request certificates. If an Applicant specifies, in writing, the individuals who may request a certificate, then the Provider shall not accept any certificate requests that are outside this specification. The Provider shall provide an Applicant with a list of its authorized certificate requesters upon the Applicant's verified written request.

3.2.6 Criteria for Interoperation or Certification

The Provider shall disclose all cross-certified Subordinate CA certificates that identify the Provider as the subject, provided that the CA arranged for or accepted the establishment of the trust relationship

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

No stipulation.

3.3.2 Identification and authentication for re-key after revocation

No stipulation.

3.4 Identification and authentication for revocation request

No stipulation.

4. Certificate Life-Cycle Operational Requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

A certificate may be requested by a natural or legal person operating a device or system, who demonstrates in the certificate request that they are eligible to request a certificate with an FQDN and that all FQDNs which are listed in the SAN of certificate.

The Provider must maintain an internal database of all revoked TLS certificates and rejected requests due to suspicion of phishing or other fraudulent activity.

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 for the visit.

4.1.2.2 Request generation

When requesting a TLS 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 certificate request and save it on suitable medium.

The Provider issues certificates exclusively at the company's headquarters in Bratislava

Notes and warnings: Please note that the request for a certificate or the public key in it, for which a certificate has already been issued, cannot be used repeatedly to issue another certificate for security reasons and will be rejected at the RA! The request for a certificate must include the

subject:commonName (the so-called entity name) item, filled in appropriately. The individual items must be filled in so that the entered values are in accordance with this document, with an emphasis on its section 3.1.2, and to clearly identify the entity that will use the given certificate (typically the fully qualified domain name (FQDN)). If item O (subject:organizationName) is filled in the application, item L (subject:localityName) must also be filled in.

4.1.2.3 Sending a certificate request

The request for the issuance of the certificate is sent by the Customer to RA (radisig@disig.sk) which must perform all procedures related to the process of issuing the certificate

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 [11];
- 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 verify any identifying information to be entered into the certificate.

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 into the Provider's information system.

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.

The Provider may not issue 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).

Any request meeting the requirements of this CP must be processed without delay if the issue is made in the presence of the customer or at the latest at the time agreed with the customer in the certificate application process.

The Provider shall not issue certificates containing internal names or reserved IP addresses,

4.2.3 Time to process certificate issuance

No stipulation.

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.

Certificate issuance by the Root CA shall require an individual authorized by the Provider (i.e., the CA system operator, system officer, or PKI administrator) to deliberately issue a direct command in order for the Root CA to perform a certificate signing operation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

No stipulation.

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

No stipulation.

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 [11];
- 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.
- 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.

The 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 relies on the certificate issued under this CP and in accordance with the General Terms and Conditions [11] 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 consistent with the restrictions of the certificate, which are contained in the certificate itself, the General Conditions [11] 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

The 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

No stipulation.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

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

No stipulation.

4.8 Certificate modification

4.8.1 Circumstance for certificate modification

No stipulation.

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
- 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.
- 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 TLS BR [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 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.
- 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.

When an end entity certificate is revoked for one of the reasons below, the specified CRLReason MUST be included in the reasonCode extension of the CRL entry corresponding to the end entity certificate. When the CRLReason code is not one of the following, then the reasonCode extension MUST NOT be provided:

- keyCompromise (RFC 5280 CRLReason #1).
- privilegeWithdrawn (RFC 5280 CRLReason #9);**
- cessationOfOperation (RFC 5280 CRLReason #5).
- affiliationChanged (RFC 5280 CRLReason #3); or
- superseded (RFC 5280 CRLReason #4).

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 decided 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 decided to continue maintaining the CRL/OCSP Repository; or
- Revocation is required by this CP and/or CPS.
- The Provider's right to issue certificates under TLS BR [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) can request the cancellation of the certificate at any time, even without specifying the reason for the revocation of the certificate, with the exception of the reasons that must be published in the CRL, while the applicant must indicate them in his request.

RA shall revoke the certificate of Subscriber if 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).

Additionally, Subscribers, relying parties, application software suppliers, and other third parties may submit Certificate Problem Reports informing the Provider of reasonable cause to revoke 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 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.
- In the case of a request to revoke a certificate for the reasons listed in section 4.9.1.1, the certificate holder must submit/deliver a "Request for TLS Certificate Cancellation", which is available on the Provider's website: https://dsrv.disig.sk/download/forms/tls_revoke_form.pdf

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

No stipulation.

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 collaborate 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 did not 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 certificates 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 [11].

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 using 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 4 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 the 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

No stipulation.

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.

OCSP responses must conform to RFC6960 [13] and/or RFC5019 [14]. OCSP responses must either be signed by:

1. the CA that issued the certificates whose revocation status is being checked, or
2. an OCSP Responder whose certificate is signed by the CA that issued the certificate whose revocation status is being checked.

In the latter case, the OCSP signing certificate must contain an extension of type id-pkix-ocsp-nocheck, as defined by RFC6960 [13].

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 [13].

OCSP responders operated by the Provider shall support the HTTP GET method, as described in RFC 6960 [13] and/or RFC 5019 [14]. The Provider may process the Nonce extension (1.3.6.1.5.5.7.48.1.2) in accordance with RFC 8954 [15].

The validity interval of an OCSP response is the difference in time between the *thisUpdate* and *nextUpdate* field, inclusive. For purposes of computing differences, a difference of 3,600 seconds shall be equal to one hour, and a difference of 86,400 seconds shall be equal to one day, ignoring leap-seconds.

For the status of Subscriber certificates:

1. OCSP responses must have a validity interval greater than or equal to eight hours.
2. OCSP responses must have a validity interval less than or equal to ten days.
3. For OCSP responses with validity intervals less than sixteen hours, then the Provider shall update the information provided via an OCSP prior to one-half of the validity period before the *nextUpdate*.
4. For OCSP responses with validity intervals greater than or equal to sixteen hours, then the Provider shall update the information provided via an OCSP at least eight hours prior to the *nextUpdate*, and no later than four days after the *thisUpdate*.

For the status of Subordinate CA Certificates:

- The Provider shall update information provided via an OCSP
  - at least every twelve months; and
  - within 24 hours after revoking a Subordinate CA Certificate.

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

Compromise of the private key of certification authorities (root, subordinate) operated by the Provider (see 1.5.1) in accordance with this certification policy may be notified by third parties to the Provider to the contact details specified in section 1.5.1 or 1.5.2 respectively at the discretion of the third parties (by telephone, e-mail, post, etc.). The third parties may also choose any other method he deems appropriate for such notification.

4.9.13 Circumstances for suspension

The 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.

Revocation entries on a CRL or OCSP Response must not be removed until after the expiry date of the revoked certificate.

4.10.2 Service availability

The Provider shall operate and maintain its CRL and optional OCSP capability with resources sufficient to provide a response time of ten seconds or less under normal operating conditions.

The distribution points on which CRLs are published must be available in 24x7 mode.

OCSP must be available in 24x7 mode.

The Provider shall maintain a continuous 24x7 ability to respond internally to a high-priority certificate problem report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a Certificate that is the subject of such a complaint.

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

No stipulation.

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 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 the 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 conducted.

The Security Policy of the Provider and the Summary of Security Assets shall be reviewed at regular intervals and always when 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 in protected areas accessible only to authorized persons and separated from other areas by appropriate security features (security doors, grilles, fixed walls, etc.). The provided 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 managed 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 of the 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 roles 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 consider 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

An 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

No stipulation.

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 copy 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.

The Provider must 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 CA SHALL record at least the following events:

- CA certificate and key lifecycle events, including:
  - Key generation, backup, storage, recovery, archival, and destruction.
  - Certificate requests, renewal, and re-key requests, and revocation.
  - Approval and rejection of certificate requests.
  - Cryptographic device lifecycle management events.
  - Generation of Certificate Revocation Lists.
  - Signing of OCSP Responses (as described in Section 4.9 and Section 4.10); and
  - Introduction of new Certificate Profiles and retirement of existing Certificate Profiles.
- Subscriber Certificate lifecycle management events, including:
  - Certificate requests, renewal, and re-key requests, and revocation.
  - All verification activities stipulated in TLS BR [3] and CPS.
  - Approval and rejection of certificate requests.

- Issuance of Certificates.
- Generation of Certificate Revocation Lists; and
- Signing of OCSP Responses in accordance with TLS BR [3] section 4.9 and 4.10

- Security events, including:
  - Successful and unsuccessful PKI system access attempts.
  - PKI and security system actions performed.
  - Security profile changes.
  - Installation, update, and removal of software on a Certificate System.
  - System crashes, hardware failures, and other anomalies.
  - Firewall and router activities; and
  - Entries to and exits from the CA facility.

Log records MUST include the following elements:

- Date and time of event.
- Identity of the person making the journal record; and
- Description of the event.

5.4.2 Frequency for Processing and Archiving Audit Logs

No stipulation.

5.4.3 Retention Period for Audit Logs

The CA and each Delegated Third Party SHALL retain, for at least two (2) years:

- CA certificate and key lifecycle management event records in the meaning of 5.4.1 after the later occurrence of:
  - the destruction of the CA Private Key; or
  - the revocation or expiration of the final CA certificate in that set of certificates that have an X.509v3 *basicConstraints* extension with the *cA* field set to true and which share a common *public key* corresponding to the CA private key.
- Subscriber certificate lifecycle management event records (see 5.4.1) after the expiration of the Subscriber certificate.
- Any security event records (as set forth in section 5.4.1) after the event occurred.

5.4.4 Protection of Audit Log

No stipulation.

5.4.5 Audit Log Backup Procedure

No stipulation.

5.4.6 Audit Log Accumulation System

No stipulation.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

Additionally, the Provider's security program must include an annual risk assessment that:

1. Identifies foreseeable internal and external threats that could result in unauthorized access, disclosure, misuse, alteration, or destruction of any certificate data or certificate management processes.
2. Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the certificate data and certificate management processes; and
3. Assesses the sufficiency of the policies, procedures, information systems, technology, and other arrangements that the Provider has in place to counter such threats.

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.

The 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

The Provider is obliged to keep the contract with the holder or customer respectively and confirmation of the issuance of a certificate under this contract at least 7 years from the expiry of the certificate issued under this contract.

In addition, the Provider must keep for at least two (2) years:

1. all archived documentation related to the security of CA systems, certificate management systems, root CA systems (as specified in Section 5.5.1); and
2. all archived documentation related to certificate application verification, certificate issuance and certificate revocation, and certificates themselves (as specified in Section 5.5.1), whichever occurs later:

- such records and documentation were last relied upon in the verification, issuance, or revocation of applications for certificates and certificates; or
- expiration of end-user certificates issued based on such records and documentation.

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

The 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 belonging 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

To ensure the integrity of services, the Provider must implement data backup and recovery procedures.

The Provider must have developed emergency procedures and recovery plans for the performance of trusted services in accordance with the requirements of section 5.7.1 of TLS BR [3].

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 assessed (at least on an annual basis) and reviewed and updated, as necessary.

The Provider is not obliged to publish its business continuity plans but must provide its business continuity plan and security plan upon request to the auditor of the Provider's services.

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

No stipulation.

5.7.3 Recovery Procedures after Key Compromise

No stipulation.

5.7.4 Business continuity capabilities after a disaster

No stipulation.

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, 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 to 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") [12].
- 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 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 modify 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 in accordance with the requirements in section 6.1.1.1 of TLS BR [3]. The key pair generating shall provide sufficient confidence in the process and the entire 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 End users

The Provider shall reject a certificate request if one or more of the following conditions are met:

1. The Key Pair does not meet the requirements set forth in Section 6.1.5 and/or Section 6.1.6.
2. There is clear evidence that the specific method used to generate the Private Key was flawed.

3. The Provider is aware of a demonstrated or proven method that exposes the Applicant's private Key to compromise.
4. The Provider has previously been made aware that the Applicant's private key has suffered a key compromise, such as through the provisions of section 4.9.1.1;
5. The Provider is aware of a demonstrated or proven method to easily compute the Applicant's Private Key based on the Public Key (such as a Debian weak key, see https://wiki.debian.org/SSLkeys).

If the Subscriber Certificate will contain an *extKeyUsage* extension containing either the values *id-kp-serverAuth* [RFC5280] [2] or *anyExtendedKeyUsage* [RFC5280] [2], the Provider shall not generate a key pair on behalf of a subscriber, and shall not accept a certificate request using a key pair previously generated by the Provider.

6.1.2 Private key delivery to subscriber

Parties other than the Subscriber shall not archive the Subscriber private key without authorization by the Subscriber.

If the Provider become aware that a Subscriber's private key has been communicated to an unauthorized person or an organization not affiliated with the Subscriber, then the Provider shall revoke all certificates that include the public key corresponding to the communicated private key.

6.1.3 Public key delivery to certificate issuer

No stipulation.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

For RSA key pairs the Provider shall ensure that the modulus size:

- when encoded, is at least 2048 bits,
- in bits, is evenly divisible by 8.

6.1.6 Public key parameters generation and quality checking

The parameters and quality of the Provider's public key (root and subordinate CA) are determined by the PMA and quality control is checked during the key generation ceremony. The Provider must use cryptographic hardware modules that meet the requirements of FIPS 186-2 to generate and store keys, which ensure the random generation of RSA keys with a size of at least 2048 bits.

RSA: The Provider shall confirm that the value of the public exponent is an odd number equal to 3 or more. Additionally, the public exponent should be in the range between 2^16 + 1 and 2^256 - 1.

The modulus should also have the following characteristics: an odd number, not the power of a prime, and have no factors smaller than 752. [Source: Section 5.3.3, NIST SP 800-89].

6.1.7 Key usage purposes

Private keys corresponding to Root Certificates must not be used to sign certificates except in the following cases:

1. Self-signed certificates to represent the Root CA itself.
2. Certificates for Subordinate CAs and Cross-Certified Subordinate CA Certificates.
3. Certificates for infrastructure purposes (administrative role certificates, internal CA operational device certificates); and
4. Certificates for OCSP Response verification.

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 people 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 principal "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 principal "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 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 into 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 presents.

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

No stipulation.

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	9125 days
Subordinate CA	5475 days
TLS certificate	395 days

To calculations, a day is measured as 86,400 seconds. Any amount of time greater than this, including fractional seconds and/or leap seconds, shall represent an additional day.

6.4 Activation data

6.4.1 Activation data generation and installation

No stipulation.

6.4.2 Activation data protection

No stipulation.

6.4.3 Other aspects of activation data

No stipulation.

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 systems.

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“ [9]

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

The Provider shall enforce multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

No stipulation.

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.

7.1.2 Certificate Content and Extensions

7.1.2.1 Provider's 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 bits
Validity of Root CA certificate
maximum 30 years

From September 15, 2023, the minimum validity period of 2922 days and the maximum validity period of 9132 days apply to root CAs, and for RSA signature algorithms given in section 7.1.2.7.1.

Table 5 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* (optional field)
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*depending on the CA type* [1)]

[1)] 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.

From 15.9.2023, the subject of the root CA certificate can only contain items given in section 7.1.2.10.2 of TLS BR [3].

Table 6 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

From 15.9.2023, the subject of the root CA certificate can only contain items given in section 7.1.2.1.2 of TLS BR [3].

7.1.2.2 Cross-Certified Subordinate CA Certificate Profile

No stipulation.

7.1.2.3 Technically Constrained Non-TLS Subordinate CA Certificate Profile

No stipulation.

7.1.2.4 Technically Constrained Precertificate Signing CA Certificate Profile

No stipulation.

7.1.2.5 Technically Constrained TLS Subordinate CA Certificate Profile

No stipulation.

7.1.2.6 Subordinate Certification Authority of the Provider

Algorithms and key lengths applied in the subordinate CA

Signature Algorithm
sha256RSA
Public key
RSA, minimal length 2 048 bit
Validity of subordinate CA
maximum 15 years

Table 7 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**
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*depending on the CA type* [1)]

[1] 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 etc.

From 15.9.2023, the subject of the subordinate CA's certificate can only contain items given in section 7.1.2.10.2 TLS BR [3].

Table 8 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

From 15.9.2023, the certificate of the subordinate CA can only contain the extensions given in section 7.1.2.6.1 TLS BR [3].

7.1.2.7 End user certificates

Details on the content of the subject of certificates issued pursuant to this CP are given in the section 3.1.4.

Table 9 lists the extensions used in issued certificates.

Table 9 Basic extensions in certificates

Extension name	ASN.1 name and OID / Description	Presence	Critical
AuthorityInfoAccess	{id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1} 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
Authority Key Identifier	{id-ce-authorityKeyIdentifier} {2.5.29.35} It identifies the public key to be used to verify the signature on this certificate or CRL.	YES	NO
Extended Key Usage	{id-ce-extKeyUsage} [2.5.29.37] This field indicates one or more purposes for which the certified public key may be used, in addition to or in place of the basic purposes indicated in the key usage extension field.	YES	NO

subjectAltName	id-ce-subjectAltName [2.5.29.17] 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
Subject Key Identifier	{id-ce-subjectKeyIdentifier} {2.5.29.14} This extension identifies the public key being certified.	YES	NO
Certificate Policies	{id-ce-certificatePolicies} {2.5.29.32} This extension lists certificate policies, recognized by the issuing CA, which apply to the certificate, together with optional qualifier information pertaining to these certificate policies.	YES	NO
Key Usage	{id-ce-keyUsage} {2.5.29.15} This extension indicates the purpose for which the certified public key is used.	YES	NO
CRL Distribution Points	{id-ce-CRLDistributionPoints} {2.5.29.31} 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

7.1.2.7.1 Subscriber Certificate Types

Pursuant to this CP, the Provider only issues "Organization Validated (OV)" type certificates.

7.1.2.7.2 Domain Validated

The Provider does not issue this type of certificate.

7.1.2.7.3 Individual Validated

The Provider does not issue this type of certificate.

7.1.2.7.4 Organization Validated

The "*Organization Validated*" profile of the certificate must meet the requirements given in section 7.1.2.7.4 of TLS BR [3].

7.1.2.7.5 Extended Validation

The Provider does not issue this type of certificate.

7.1.2.7.6 Subscriber Certificate Extensions

Certificates issued to the end user may only contain the extensions given in section 7.1.2.7.6 TLS BR [3].

7.1.2.7.7 Subscriber Certificate Authority Information Access

The "*Authority Information Access*" entry in the end-user certificate must comply with the requirements given in section 7.1.2.7.7 of the TLS BR [3].

7.1.2.7.8 Subscriber Certificate Basic Constraints

No stipulation.

7.1.2.7.9 Subscriber Certificate Policies

The "*Certificate Policies*" entry in the end-user certificate must comply with the requirements given in section 7.1.2.7.9 of the TLS BR [3].

7.1.2.7.10 Subscriber Certificate Extended Key Usage

The "*Extended Key Usage*" entry in the end-user certificate must comply with the requirements given in section 7.1.2.7.10 of the TLS BR [3].

7.1.2.7.11 Subscriber Certificate Key Usage

The "*Key Usage*" entry in the end-user certificate must comply with the requirements given in section 7.1.2.7.11 of the TLS BR [3].

7.1.2.7.12 Subscriber Certificate Subject Alternative Name

The "*Subject Alternative Name*" entry in the end-user certificate must comply with the requirements given in section 7.1.2.7.12 of the TLS BR [3].

7.1.2.8 OCSP Responder Certificate Profile

If the Provider does not directly sign OCSP responses, it may make use of an OCSP authorized responder, as defined by RFC 6960 [13]. The issuing CA of the responder must be the same as the issuing CA for the certificates it provides responses for.

The OCSP responder's certificate profile must comply with the requirements given in section 7.1.2.8 of TLS BR [3].

7.1.2.8.1 OCSP Responder Validity

The validity of the OCSP responder's certificate must comply with the requirements given in section 7.1.2.8.1 of TLS BR [3].

7.1.2.8.2 OCSP Responder Extensions

The extensions in the responder's OCSP certificate must comply with the requirements given in section 7.1.2.8.2 of TLS BR [3].

7.1.2.8.3 OCSP Responder Authority Information Access

The "Authority Information Access" in the responder's OCSP certificate must comply with the requirements given in section 7.1.2.8.3 of TLS BR [3].

7.1.2.8.4 OCSP Responder Basic Constraints

"Basic Constraints" in the responder's OCSP certificate must comply with the requirements given in section 7.1.2.8.4 of TLS BR [3].

7.1.2.8.5 OCSP Responder Extended Key Usage

"Extended Key Usage" in the responder's OCSP certificate must comply with the requirements given in section 7.1.2.8.5 of TLS BR [3].

7.1.2.8.6 OCSP Responder id-pkix-ocsp-nocheck

"id-pkix-ocsp-nocheck" in the responder's OCSP certificate must comply with the requirements given in section 7.1.2.8.6 of TLS BR [3].

7.1.2.8.7 OCSP Responder Key Usage

"Key Usage" in the responder's OCSP certificate must comply with the requirements given in section 7.1.2.8.7 of TLS BR [3].

7.1.2.8.8 OCSP Responder Certificate Policies

"Certificate Policies" in the responder's OCSP certificate must comply with the requirements given in section 7.1.2.8.8 of TLS BR [3].

7.1.2.9 Precertificate profile

A precertificate is a signed data structure that can be submitted to a Certificate Transparency log, as defined by RFC 6962 [16]. A precertificate appears structurally identical to a certificate, except for a special critical poison extension in the extensions field, with the OID of 1.3.6.1.4.1.11129.2.4.3. This extension ensures that the precertificate will not be accepted as a certificate by clients conforming to RFC 5280. The existence of a signed precertificate can be treated as evidence of a corresponding certificate also existing, as the signature represents a binding commitment by the Provider that it may issue such a certificate.

A precertificate is created after the Provider has decided to issue a certificate, but prior to the actual signing of the certificate. The Provider may construct and sign a precertificate corresponding to the certificate, for the purpose of submitting to Certificate Transparency Logs. The Provider may use the returned signed Certificate Timestamps to then alter the Certificate's extensions field, adding a Signed Certificate Timestamp List, as defined in Section 7.1.2.11.3, and as permitted by the relevant profile, prior to signing the certificate.

Precertificate profile describes the transformations that are permitted to a certificate to construct a precertificate. The Provider must not issue a precertificate unless they are willing to issue a corresponding certificate, regardless of whether they have done so. Similarly, the Provider must not issue a precertificate unless the corresponding certificate conforms to the TLS BR [3], regardless of whether the Provider signs the corresponding certificate.

A precertificate may be issued either directly by the Issuing CA or by a technically constrained precertificate signing CA, as defined in Section 7.1.2.4 TLS BR [3].

7.1.2.9.1 Precertificate Profile Extensions - Directly Issued

Extensions must comply with the requirements given in section 7.1.2.9.1 of the TLS BR [3].

7.1.2.9.2 Precertificate Profile Extensions - Precertificate CA Issued

No stipulation.

7.1.2.9.3 Precertificate Poison

The precertificate must contain the precertificate poison extension (OID: 1.3.6.1.4.1.11129.2.4.3).

This extension must have an extnValue OCTET STRING which is exactly the hex-encoded bytes 0500, the encoded representation of the ASN.1 NULL value, as specified in RFC 6962 [16], Section 3.1.

7.1.2.9.4 Precertificate Authority Key Identifier

No stipulation.

7.1.2.10 Common CA Fields

Before issuing a certificate, the Provider must ensure that the content of the CA certificate, including the content of each item, fully meets all the requirements of at least one certificate profile documented in section 7.1.2 in accordance with the description of items in section 7.1.2.10 of TLS BR [3].

7.1.2.11 Common Certificate Fields

Before issuing a certificate, the Provider must ensure that the content of the certificate, including the content of each item, fully meets all the requirements of at least one certificate profile documented in section 7.1.2 in accordance with the description of items in section 7.1.2.11 of TLS BR [3].

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the *subjectPublicKeyInfo* field within a certificate or precertificate. No other encoding is allowed.

7.1.3.1.1 RSA

The Provider must mark the RSA key with the algorithm identifier *rsaEncryption* (OID: 1.2.840.113549.1.1.1). Parameters must be present and must be explicitly *NULL*.

The Provider must not use another algorithm, such as the algorithm identifier id-RSASSA-PSS (OID: 1.2.840.113549.1.1.10), to mark the RSA key.

When encoded, the *AlgorithmIdentifier* for RSA keys must be byte-for-byte identical to the following hexadecimal-encoded bytes:
300d06092a864886f70d0101010500

7.1.3.1.2 ECDSA

No stipulation.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed with the CA Provider's private key must meet the requirements for using "*AlgorithmIdentifier*" or a type derived from "*AlgorithmIdentifier*" in the context of signatures if specified in Section 7.1.3.2 of TLS BR [3].

7.1.3.2.1 RSA

The Provider must use a single signature algorithm and encoding in accordance with the requirements specified in section 7.1.3.2.1 of TLS BR [3].

The encoded "*AlgorithmIdentifier*" must be byte-for-byte identical to the specified hex-encoded bytes as specified in Section 7.1.3.2 of TLS BR [3].

7.1.3.2.2 ECDSA

No stipulation.

7.1.4 Name Forms

For all certificates issued by the Provider in terms of this CP, the encoding of the names must be in accordance with the requirements given in section 7.1.4 TLS BR [3].

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

7.1.6.1 Reserved Certificate Policy Identifiers

The certificate policy OID 2.23.140.1.2.2 is reserved for the "*Organization validated*" certificate type - see 1.4.1 of this CP.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

Before 15.3.2024, the Provider must issue CRLs in accordance with the profile specified in the requirements of section 7.2 TLS BR [3] or the profile specified in version 1.8.7 of the requirements for issuing and managing publicly trusted certificates. With effect from 15.3.2024, the Provider must issue CRLs in accordance with the profile specified in section 7.2 of TLS BR [3].

7.2.1 Version number

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

7.2.2 CRL and CRL entry extensions

Extensions in the issued CRL must comply with the requirements specified in section 7.2.2 of the TLS BR [3].

7.3 OCSP profile

If the OCSP response refers to a root CA or a subordinate CA certificate, including cross-certified CA certificates, and this certificate has been revoked, then the reason for the revocation must be specified in the *RevokedInfo CertStatus* field.

The specified revocation reason *CRLReason* must contain a value allowed for CRLs as specified in Section 7.2.2 of TLS BR [3].

7.3.1 Version number

No stipulation.

7.3.2 OCSP extensions

The *singleExtensions* of an OCSP response must not contain the *reasonCode* (OID 2.5.29.21) CRL entry extension.

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 [8] 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 section 8.2 TLS BR [3].

8.3 Assessor's relationship to assessed entity

No stipulation.

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 [9], including normative references from ETSI EN 319 401 [17].

The audit must be conducted 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 records a discrepancy.
- The auditor notifies the entities defined in section 8.6;
- The 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 7.1.6.1 The Provider make the audit report publicly available.

The Provider makes its audit report publicly available no later than three months after the end of the audit period. In the event of a delay greater than three months, the Provider shall provide an explanatory letter signed by the qualified auditor.

The audit report must contain at least the following clearly-labelled information:

1. name of the organization being audited,
2. name and address of the organization performing the audit,
3. the SHA-256 fingerprint of all roots and subordinate CA certificates, including cross-certified subordinate CA certificates, which were in-scope of the audit,
4. audit criteria, with version number(s), that were used to audit each of the certificates (and associated keys),
5. a list of the Provider policy documents, with version numbers, referenced during the audit,
6. whether the audit assessed a period of time or a point in time,
7. the start date and end date of the audit period, for those that cover a period of time.
8. the point in time date, for those that are for a point in time,
9. the date the report was issued, which will necessarily be after the end date or point in time date; and
10. for audits conducted in accordance with any of the ETSI standards - a statement to indicate if the audit was a full audit or a surveillance audit, and which portions of the criteria were applied and evaluated, e.g. DVCP, OVCP, NCP, NCP+, LCP, EVCP, EVCP+, QCP-w, Part 1 (General Requirements), and/or Part 2 (Requirements for Trust Service Providers).
11. for audits conducted in accordance with any of the ETSI standards - a statement to indicate that the auditor referenced the applicable CA/Browser Forum criteria, such as TLS BR [3], and the version used.

An authoritative English language version of the publicly available audit information must be provided by the qualified auditor and the Provider shall ensure it is publicly available.

The audit report must be available as a PDF and shall be text searchable for all information required. Each SHA-256 fingerprint within the audit report must be uppercase letters and must not contain colons, spaces, or line feeds.

8.7 Self-Audits

During the period in which the CA issues certificates, the Provider must monitor compliance with its CP and CPS and the requirements specified in TLS BR [3] and

control the services provided by conducting internal audits at least on a quarterly basis on a randomly selected sample of issued certificates in a number higher than one and at most in the number of three percent of the issued certificates in the period since the previous internal audit.

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 with.

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 OCSP services,
- 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,
- Personal data of holders of certificates subject to protection under the Personal Data Protection Regulations [12].

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

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 permitted 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 the 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 it 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 [12].

9.4.2 Information treated as private

The Provider must have a defined scope of personal data that is processed when providing qualified trusted services.

9.4.3 Information not deemed private

The Provider may, in accordance with the Personal Data Protection Regulations [12] 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 it 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 [12].

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 to do this.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

This CP and the related 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 [11] 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 [11].

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 are 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 [11], 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 to Article 13 of eIDAS Regulations [8] and failure to fulfill obligations in accordance with this CP.

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 [11] 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. The 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 February 1, 2024 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 6.0, 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.

The 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 to radisig@disig.sk. The Provider shall process the complaint no later than 30 days after its receipt, unless otherwise agreed by the parties. The 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 the liability arise, then the party on which such circumstances occur 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.