Certificate Policy

Disig, a.s.

Version 1.0

Valid from September 1, 2023

OID 1.3.158.35975946.0.0.0.1.11

Table of Content

Business Name	Disig, a. s.
Residence	Záhradnícka 151, 821 08 Bratislava, Slovakia
Registration	Business Register of the Municipal Court Bratislava III, Section: Sa, Insert No.: 3794/B.
Telephone	+ 421 2 208 50 140
E-mail	disig@disig.sk

1. INTRODUCTION

This document defines the Certificate Policy (hereinafter referred to as "CP") of company Disig, a.s., with its registered office at Záhradnícka 151, 821 08 Bratislava, National Trade Register number: 35975946, registered in the Commercial Register of Municipal Court Bratislava III, section: Sa, insert no. 3794/B, as a Trusted Service Provider (hereinafter referred to as "Provider"). This CP applies to all root CAs and subordinate CAs operated by the Provider, which provides trust services of issuance S/MIME certificates in accordance with the Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [1] (hereinafter referred to as "Certificate").

The certificate issued for the end user (hereinafter referred to as the "Subscriber") uniquely identifies the entity to which the certificate is issued and binds this entity to the corresponding pair of keys. Unless it is explicitly stated in the policy that it refers to the certificate of the root certification authority or subordinate certification authority, then the word Certificate means the certificate of the end entity.

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

https://eidas.disig.sk

1.1 Overview

This CP defines the creation and management of public key certificates (X.509 version 3), in accordance with RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile" [2] and the requirements of Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [1] , 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") [3], and ETSI TS 119 411-6 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates [4]. S/MIME certificates are issued in accordance with NCP and NCP+ policy requirements according to ETSI EN 319 411-1 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 1: General requirements“ [5]

This policy is structured in accordance with RFC 3647 [6].

1.2 Document Name and Identification

Document Name	Certificate Policy
Name abbreviation	CP SMIME CA Disig*
Version:	1.0
Approved on:	August 25, 2023
Valid from:	September 1, 2023
This document is assigned an object identifier (OID):	1.3.158.35975946.0.0.0.1.11

* - in this document, only the abbreviated form CP is mostly used

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

1.3.158.35975946.0.0.0.1.11 - CP SMIME CA Disig

1.2.1 Revisions

Revision	Revision date	Description; Reviewer
1.0	September 1, 2023	First version; Mišković

1.3 PKI Participants

1.3.1 Certification Authorities

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

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

1.3.2 Registration Authorities

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

The RA shall carry out its activities in accordance with the approved CP and the Certification Practice Statement (hereinafter "CPS") [7].

Provider may establish following types of RA:

- Commercial RA - is intended to mediate selected trustworthy services of the Provider to the general public and is operated by a third party, on the basis of a written agreement with the Provider;
- Enterprise RA - is intended to mediate selected trustworthy services exclusively for the own needs of a particular legal body, For the needs of its operated systems requiring the use of certificates and is operated, on the basis of a written contract with the Provider;
- Internal RA - is operated by the Provider and is intended to provide trusted services for all interested parties. This RA is not a separate legal body.

If the term "RA of the Provider" is used in the text, it refers to all types of RA mentioned above.

1.3.2.1 Enterprise RA

The Provider can delegate to the Enterprise RA the verification of certificate requests for natural persons within their own organization. The Provider will not accept requests for a certificate authorized by an Enterprise RA unless the following requirements are met:

- If the Certificate Request is for an **"***Organization-validated***"** or **"***Sponsor-validated***"** profile, the Provider shall confirm that the Enterprise RA has authorization or control of the requested email domain(s) in accordance with Section 3.2.2.1or Section 3.2.2.3.
- The Provider shall confirm that the **"***subject:organizationName***"** name is either that of the delegated enterprise, or an Affiliate of the delegated enterprise, or that the delegated enterprise is an agent of the named Subject. The Provider shall impose these limitations as a contractual requirement on the Enterprise RA and monitor compliance by the Enterprise RA in accordance with Section 8.8.

1.3.3 Subscribers

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

The Certificate holder may be:

- A natural person - apply for S/MIME digital signature certificate;
- A natural person identified in association with a legal person - apply for S/MIME digital signature certificate;
- A legal person (that can be an Organization or a unit or a department identified in association with an Organization) - apply for S/MIME digital certificate for seal.

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

When the subscriber is acting on behalf of one or more distinct subjects to whom it is linked (e.g. the subscriber is a company requiring certificates for its employees to allow them to participate in electronic business on behalf of the company),

responsibilities of the subscriber and of the subject are addressed in the General Terms of Service and Use of the Trusted Certificate Issuance and Verification Service " (the "General Terms") [8] 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 S/MIME digital signature certificate the subscriber is:
  - The natural person itself;
  - A legal person mandated to represent the subject; or
  - Any entity with which the natural person is associated (such as the company employing the natural person or a non-profit legal person the natural person is member of).
- To request a S/MIME digital certificate for seal the subscriber is:
  - Any entity as allowed under the relevant legal system to represent the legal person; or
  - A legal representative of a legal person subscribing for its subsidiaries or units or departments.

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 RA 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.

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

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

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

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

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

CAs of the Provider issue following types of certificates to the Subscribers:

- S/MIME digital signature certificate or S/MIME digital certificate for seal - include public key associated with the email address and can also include the identity of natural person or legal person, which has control of the requested email address. The cryptographic keys associated with this type of certificate are primarily intended for the security of electronic mail, the creation of an advanced electronic signature. The issued certificate will include, inter alia, the following certification policy identifiers:
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated(2) multipurpose (2)} (2.23.140.1.5.2.2);
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) organization-validated (2) strict (3)} (2.23.140.1.5.2.3);
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) multipurpose (2)} (2.23.140.1.5.3.2); and
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) sponsor-validated (3) strict (3)} (2.23.140.1.5.3.3); and
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) multipurpose (2)} (2.23.140.1.5.4.2); and
  - {joint-iso-itu-t(2) international-organizations(23) ca-browser-forum(140) certificate-policies(1) smime-baseline(5) individual-validated (4) strict (3)} (2.23.140.1.5.4.3),

In accordance with Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates [1].

The Provider issues management certificates for its needs (Certificate for Subordinate CA, and 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 (sha256) (DER)	E23D4A036D7B70E9F595B1422079D2B91EDFBB1FB651A0633EAA8A9DC5F80703
Comment	It issues certificates only for subordinate certification authorities of the Provider.

Name	CA Disig R2I5 Certification Service
Certificate serial number	081b06df4c7965509d000000000000000e
Issuer	CA Disig Root R2
Hash (sha256) (DER)	90BA720B376FB9FDCF8A1037A5316FB493B5ACF656AD79C6839008BD43343FDD
Comment	It issues SMIME digital signature certificates and certificates for seals for end users in accordance with the requirements stated in "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates, Version 1.0.1 [1]

1.4.2 Prohibited Certificate Uses

Certificates issued under this CP are not EU Qualified Certificates according the eIDAS Regulation [3] and cannot be used where EU Qualified Certificates 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	https//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 2 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	https//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;

CA of the Provider - certification authorities of the Provider that are used to issue S/MIME certificates;

Trust service means an electronic service normally provided for remuneration, which consists of

a) the creation, verification, and validation of electronic signatures, electronic seals or electronic time stamps, electronic registered delivery services and certificates related to those services, or

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

c) the preservation of electronic signatures, seals or certificates related to those services;

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

Electronic signature means data in electronic form which is attached to or logically associated with other data in electronic form and which is used by the signatory to sign;

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

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

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;

RA of the Provider - a term that includes all types of RA (commercial, enterprise, internal);

S/MIME Certificate - contains a Public Key bound to a Mailbox Address and MAY also contain the identity of a Natural Person or Legal Entity that controls such email address.

S/MIME STRICT profile - profiles for S/MIME Certificates with "*extKeyUsage*" limited to "*id-kp-emailProtection*", and stricter use of Subject DN attributes and other extensions;

S/MIME MULTIPURPOSE profile - profiles are aligned with the more defined Strict Profiles, but with additional options for extKeyUsage and other extensions. This is intended to allow flexibility for crossover use cases between document signing and secure email.

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

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

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

Advanced electronic seal means an electronic seal, which meets the requirements set out in Article 36 of eIDAS Regulation; [3];

Advanced electronic signature means an electronic signature, which meets the requirements set out in Article 26 of eIDAS Regulation; [3];

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

ASCII	-	American Standard Code for Information Interchange
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
LEI	-	Legal Entity Identifier
OCSP	-	Online Certificate Status Protocol
OID	-	Object Identifier
PKCS#10		Certificate request format based on Public Key Cryptographic Standards (RFC 2986)
PKI		Public Key Infrastructure
PMA	-	Policy Management Authority
RA	-	Registration Authority
RFC	-	Request for Comments
S/MIME	-	Secure MIME (Multipurpose Internet Mail Extensions)
TSA	-	Time Stamp Authority

URL	-	Uniform Resource Locator
UTC	-	Coordinated Universal Time

1.6.3 Bibliography

[1] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates version 1.0.1. s.l. : https://cabforum.org/smime-br/.

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

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

[4] ETSI TS 119 411-6 „Electronic Signatures and Infrastructures (ESI); Policy and security requirements for Trust Service Providers issuing certificates; Part 6: Requirements for Trust Service Providers issuing publicly trusted S/MIME certificates.

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

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

[7] S/MIME Certificate Practice Statement Part: Registration Authority . s.l. : Disig.

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

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

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

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

[12] RFC5322 "Internet Message Format".

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

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

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

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

[17] Recommendation for ObtainingAssurances for Digital SignatureApplications.

[18] Network and Certificate System Security Requirements. s.l. : CA/B Forum.

[19] RFC 5280 "Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile".

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

[21] 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.

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

[23] Mozilla Root Store Policy, Version 2.9.0, Effective September 1, 2023.

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

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

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

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

2.2 Publication of information

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

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

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

The Provider confirms that all requirements of the current version of the document [1], which is published on the website https://cabforum.org/smime-br/ , are taken into account in this CP. In case of any inconsistency between those requirements and this CP, the requirements given by the current version of the document take precedence over this document [1].

2.3 Time or frequency of publication

The CA shall develop, implement, enforce, and annually update a Certificate Policy and/or Certification Practice Statement (CP and/or CPS) that describes in detail how the CA implements the latest version of these Requirements.

The CA shall review and update its CP and/or CPS at least every 365 days, incrementing the version number and adding a dated changelog entry, even if no other changes are made to the document.

2.4 Access controls on repositories

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

The information stored in a repository shall be available in a read-only manner.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

Each CA shall be able to create certificates that contain distinguished name according to X.500 (X.500 Distinguished Name, hereafter "Distinguished Name") [9] , namely X.501 [10] or X.520 [11] respectively and names according to RFC5322 Internet Message Format [12].

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

3.1.2 Need for names to be meaningful

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

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

3.1.3 Anonymity or pseudonym of subscribers

The use of pseudonyms and nicknames in S/MIME certificates is not allowed.

3.1.4 Rules for interpreting various name forms

3.1.4.1 Non ASCII character substitution

It is possible to use diacritical marks (non ASCI characters) in the distinguished name of S/MIME certificates.

Following tables show equivalent ASCII characters that can be used instead of non ASCII characters.

Character	ASCII representation		Character	ASCII representation
á, ä	a		ó, ô	o
č	c		ŕ	r
ď	d		š	s
dž	dz		ť	t
é	e		ú	u
í	i		ý	y
ľ, ĺ	l		ž	z
ň	n			

Character	ASCII representation		Character	ASCII representation
Á, Ä	A		Ó, Ô	O
Č	C		Ŕ	R
Ď	D		Š	S
DŽ	DZ		Ť	T
É	E		Ú	U
Í	I		Ý	Y
Ľ,Ĺ	L		Ž	Z
Ň	N			

3.1.4.2 Geographic names

No stipulation.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

The CA Disig shall authenticate the identity attributes of the Subject and their control over the Mailbox Addresses to be included in the S/MIME Certificate according to the requirements of the following sections:

Certificate type	Mailbox Control	Organization Identity	Individual Identity
S/MIME digital signature certificate [Individual-validated]	Section 3.2.2	NA	Section 3.2.4
S/MIME digital signature certificate [Sponsor-validated]	Section 3.2.2	Section 3.2.3	Section 3.2.4
S/MIME digital certificate for seal [Organization-validated]	Section 3.2.2	Section 3.2.3	NA

3.2.1 Method to prove possession of private key

No stipulation.

3.2.2 Validation of mailbox authorization or control

This section defines the permitted processes and procedures for confirming the Applicant's control of Mailbox Address to be included in issued Certificate.

The RA of the Provider shall verify that Applicant controls the email accounts associated with all Mailbox Fields referenced in the Certificate.

The Provider shall not delegate the verification of mailbox authorization or control. This does not apply to contractually bound RAs which provide trust services on behalf of the Provider.

RA of the Provider shall maintain a record of which validation method, including the relevant version number from the TLS Baseline Requirements or S/MIME Baseline Requirements [1], was used to validate every domain or email address in issued Certificates.

Completed validations of Applicant authority MAY be valid for the issuance of multiple Certificates over time. In all cases, the validation shall have been initiated within the time period specified in the relevant requirement (such as Section 4.2.1) prior to Certificate issuance.

Note: Mailbox Fields MAY be listed in Subscriber Certificates using „*rfc822Name*“ or „*otherName*“ of type „*id-on-SmtpUTF8Mailbox*“ in the „*subjectAltName*“ extension.

3.2.2.1 Validating authority over mailbox via domain

When issuing a certificate for a contractual partner of the "sponsor-validated" type, where e-mail address verification will not be performed for each applicant individually, it is possible to verify the control over the e-mail address by verifying that the contractual partner has control over the domain part of the e-mail address, to be used in the certificate.

The Provider shall use only the approved methods in Section 3.2.2.4 of the TLS Baseline Requirements [13] to perform this verification.

3.2.2.2 Validating control over mailbox via email

The RA of the Provider MAY confirm the Applicant's control over each Mailbox Field to be included in a Certificate by sending a Random Value via email and then receiving a confirming response utilizing the Random Value.

Control over each Mailbox Address shall be confirmed using a unique Random Value. The Random Value shall be sent only to the email address being validated and shall not be shared in any other way.

The Random Value shall be unique in each email. The Random Value shall remain valid for use in a confirming response for no more than 24 hours from its creation. The CA MAY specify a shorter validity period for Random Values in its CP and/or CPS.

The Random Value shall be reset upon each instance of the email sent by the CA to a Mailbox Address, however all relevant Random Values sent to that Mailbox Address MAY remain valid for use in a confirming response within the validity period described in this Section. In addition, the Random Value shall be reset upon first

use by the user if intended for additional use as an authentication factor following the Mailbox Address verification.

3.2.2.3 Validating applicant as operator of associated mail server(s)

No stipulation.

3.2.2.4 CAA records

No stipulation.

3.2.3 Authentication of organization identity

The following requirements shall be fulfilled to authenticate Organization identity included in the Organization-validated and Sponsor-validated profiles.

3.2.3.1 Attribute collection of organization identity

The CA or RA shall collect and retain evidence supporting the following identity attributes for the Organization:

- Formal name of the Legal Entity;
- A registered Assumed Name for the Legal Entity (if included in the Subject);
- An organizational unit of the Legal Entity (if included in the Subject);
- An address of the Legal Entity (if included in the Subject);
- Jurisdiction of Incorporation or Registration of the Legal Entity; and
- Unique identifier and type of identifier for the Legal Entity.

The unique identifier shall be included in the Certificate "*subject:organizationIdentifier*" as specified in Section 7.1.4.2.2 and Appendix A of [1].

3.2.3.2 Validation of organization identity

3.2.3.2.1 Verification of name, address, and unique identifier

The CA or RA shall verify the full legal name and an address (if included in the Certificate Subject) of the Legal Entity Applicant using documentation provided by, or through communication with, at least one of the following:

1. A government agency in the jurisdiction of the Legal Entity's creation, existence, or recognition;
2. A Legal Entity Identifier (LEI) data reference;
3. A site visit by the CA or a third party who is acting as an agent for the CA; or
4. An Attestation which includes a copy of supporting documentation used to establish the Applicant's legal existence, such as a certificate of registration, articles of incorporation, operating agreement, statute, or regulatory act.

The CA or RA MAY use the same documentation or communication described in 1 through 4 above to verify both the Applicant's identity and address.

An organization (legal entity) with its registered office in the Slovak Republic must prove its identity with an extract from the Business Register of the Slovak Republic (https://www.orsr.sk/) or another valid register of legal entities, e.g. Register of legal entities, entrepreneurs and public authorities, which is maintained by the Statistical Office of the Slovak Republic (https://rpo.statistics.sk/). An original or an officially certified copy of the original, not older than three months, must be required from the Provider's RA. The document must contain the full business name or title, identification data (usually ID number), seat, name/s of the person/persons acting for the legal entity and the method of acting and signing for the given legal entity. The RA of the Provider also accepts the electronic form of the extract from the used register, which will be authorized by a qualified electronic seal of the state authority responsible for keeping the register.

In case that the legal entity does not have its seat in Slovak Republic, its identity must be verified in the same way as stated above. An extract from a valid register of legal entities must be officially translated into the Slovak language (except for organizations based in the Czech Republic).

In the event that a legal entity cannot prove its identity with an extract from the commercial register or the register of legal entities, such a legal entity must prove in writing, in addition to its identity, the legality or "reason" for its existence, even if the legal entity cannot prove your identity. using and referring to a law or other regulation that deals with the subject of a given type, document, etc.

In the case of issuing a certificate, the legal entity must prove the identification data specified in the certificate request by submitting an original document proving this fact.

3.2.3.2.2 Verification of assumed name

The provider does not use this verification. S/MIME certificates are issued only with valid registered organization name.

3.2.3.3 Disclosure of verification sources

The RA shall verify the unique identifier used in the Certificate from a register that is maintained or authorized by the relevant government agency. The Provider shall disclose the authorized sources it uses through an appropriate and readily accessible online means (see section 3.2.3.2.1

3.2.4 Authentication of individual identity

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

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

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

- Full name and surname;
- Permanent residence (if it is listed in the document);
- Birth registration number (applicants who have it assigned);
- Date of birth (applicants without birth registration number);
- Further information as defined in section 3.2.4.1.

The RA of the Provider shall comply with applicable data protection legislation in the gathering and retention of evidence relating to Individual identity supporting this Requirement in accordance with Section 9.4.

3.2.4.1 Attribute collection of individual identity

The Provider shall document and publish the methods it uses to collect Individual identity attributes.

3.2.4.1.1 From a physical identity document

Individual identity can be provided by the following physical (primary) identity documents:

- eID (issued by government authority), or residence permit in the Slovak republic (in case of foreigners); or
- Passport.

The Subscriber/Holder shall provide another (secondary) identity document that has his/her name, and date of birth (or personal number) :

- Driving license;
- Birth certificate;
- Service card;
- Health insurance card;
- Firearm license;
- Passport.

The RA of the Provider shall collect these data:

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

If birth certificate, firearms license, service card, health insurance card are used as evidence then eID or passport must be also submitted.

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

3.2.4.1.2 From a digital identity document

The Provider does not use this method of initial identity authentication at this moment.

3.2.4.1.3 Using electronic identification schemes

The Provider does not use this method of initial identity authentication at this moment.

3.2.4.1.4 From a certificate supporting a digital signature applied by the Applicant

The Provider does not use this method of initial identity authentication at this moment.

3.2.4.1.5 From Enterprise RA records

In the case of Sponsor-validated Certificates approved by an Enterprise RA, records maintained by the Enterprise RA shall be accepted as evidence of Individual identity.

The Enterprise RA shall maintain records to satisfy the requirements of Section 1.3.2 and Section 8.8.

3.2.4.1.6 Affiliation from company attestation

In the case of Sponsor-validated Certificates not approved by an Enterprise RA, the RA MAY verify the authority or affiliation of an Individual to represent an Organization to be included in the *"subject:organizationName"* of the Certificate using an Attestation provided by the Organization

RA shall verify natural person identity according to section 3.2.4 and verify company identity according to section 3.2.3

3.2.4.1.7 From a general attestation

Evidence for Individual identity attributes MAY be gathered using an Attestation from a qualified legal practitioner or notary in the Applicant's jurisdiction.

3.2.4.1.8 From authorized reference sources as supplementary evidence

Evidence for Individual identity attributes shall use at least one of the following sources for authoritative evidence: a physical or digital identity document, digital signature supported by certificate, Enterprise RA records, or suitable Attestation.

The RA of the Provider MAY additionally gather and verify supplementary evidence using authorized sources such as additional official documents, government or regulatory registers, or national population registers.

The RA of the Provider shall internally document the accepted reference sources, including a description of the documents or Attestations accepted as supplementary evidence.

3.2.4.2 Validation of individual identity

The RA of the Provider shall validate all identity attributes of the Individual to be included in the Certificate.

If the evidence has an explicit validity period, the CA shall verify that the time of the identity validation is within this validity period. In context this can include the "*validFrom*" and "*validTo*" attributes of a digital signature Certificate or the date of expiry of an identity document.

The RA of the Provider may reuse existing evidence to validate Individual identity subject to the age restrictions in Section 4.2.1.

3.2.4.2.1 Validation of a physical identity document

The physical identity document shall be presented in its original form. The RA of the Provider only accepts a personally submitted document and does not support its remote verification, e.g. through the video.

The RA registration agent shall make a visual comparison of the physical appearance of the Applicant and the face photo and/or other information on the physical identity document.

The RA registration agent shall have access to authoritative sources of information on document appearance

The Provider or RA of the Provider retains information sufficient to evidence the fulfillment of the identity validation process and the verified attributes. In addition to identity attributes, the Provider record the following information: issuer, validity period, and the document's unique identification number.

3.2.4.2.2 Validation of a digital identity document

The Provider does not use this method of initial identity authentication at this moment.

3.2.4.2.3 Validation of eID

The Provider does not use this method of initial identity authentication at this moment.

3.2.4.2.4 Validation of digital signature with certificate

The Provider does not use this method of initial identity authentication at this moment.

3.2.4.2.5 Validation of an Attestation

If the Attestation is used as evidence to validate the identity attributes of a natural person, then its reliability must be verified according to the section 3.2.8.

3.2.4.2.6 Validation using an Enterprise RA record

An Enterprise RA issuing a "Sponsor-validated" Certificate shall validate all identity attributes of an Individual to be included in the Certificate. The Enterprise RA MAY rely upon existing internal records to validate Individual identity.

3.2.5 Non-verified subscriber information

Subscriber information that has not been verified in accordance with this CP shall not be included in Publicly-Trusted S/MIME Certificates.

3.2.6 Validation of authority

Before commencing to issue Organization-validated and Sponsor-validated Certificates for an Applicant, the Provider shall use a Reliable Method of Communication to verify the authority and approval of an Applicant Representative to perform one or more of the following:

- to act as an Enterprise RA;
- to request issuance or revocation of Certificates; or
- to assign responsibilities to others to act in these roles.

The Provider MAY establish a process that allows an Applicant to specify the individuals who may act as Applicant Representatives on an ongoing basis. The Provider shall provide an Applicant with a list of its authorized Applicant Representatives upon the Applicant's verified written request.

The Provider MAY use the sources listed in Section 3.2.3.2.1 to verify the 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 Provider deems appropriate.

3.2.7 Criteria for Interoperation

The Provider shall disclose all Cross Certificates that identify the Provider as the Subject.

3.2.8 Reliability of verification sources

Before relying on a source of verification data to validate Certificate Requests, the RA of the Provider shall verify its suitability as a Reliable Data Source.

Enterprise RA records are a reliable data source for the attributes of a natural person included in "sponsor-validated" digital signature certificates issued within an organization that is the Provider's Enterprise RA.

The RA of the Provider MAY rely upon a letter attesting that Subject Information or other fact is correct. The CA or RA shall verify that the letter was written by an accountant, lawyer, government official, or other reliable third party in the Applicant's jurisdiction customarily relied upon for such information.

An Attestation shall include a copy of documentation supporting the fact to be attested. The RA of the Provider shall use a Reliable Method of Communication to contact the sender and to confirm the Attestation is authentic.

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

No stipulation.

A certificate request can be submitted by:

- S/MIME digital signature certificate [Individual validated]:
  - Natural person
- S/MIME digital signature certificate - employee [Sponsor-validated]:
  - Natural person authorized by customer,
  - any entity with which a natural person is associated, e.g. her employer, non-profit organization of which she is a member, etc
- S/MIME digital certificate for seal [Organization-validated]:
  - any entity that acts on behalf of the given legal entity (organization) in accordance with applicable national legislation.

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 RA of 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)" [8] and "Informáciou o spracúvaní osobných údajov (Information on Personal Data Processing)" [14], 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 prepared a certificate request in form of PKCS #10, which will be send in advance to the RA of the Provider (see paragraph 4.1.2.3);
- To have prepared the selected identity documents and other necessary documents, i.e. Extract from business register, Power of Attorney, etc.;
- To arrange a date of the visit.

4.1.2.2 Request generation

4.1.2.2.1 Certificate Request generation

The Certificate can be issued only for PKCS#10 certificate request format. The Customer is required to generate a request for a Certificate on the computer, using

the appropriate browser and the Provider's website (see URL in section 1) and store it on the appropriate media.

A request for S/MIME digital signature certificate, must be forwarded to the appropriate RA of the Provider by e-mail in advance and from the e-mail address given in the certificate request in the "*subject:emailAddress*".

A request for S/MIME digital certificate for seal, must be forwarded to the appropriate RA of the Provider by e-mail in advance and from the e-mail address given in the certificate request in the "*subject:emailAddress*". The e-mail address in the certificate request for S/MIME digital certificate for seal must not be the address of a natural person. The Provider's RA only accepts a general e-mail address of a legal entity, such as obchod@disig.sk , faktury@disig.sk etc.

The RA of the Provider reserves the right to refuse a request for S/MIME digital certificate for seal where this requirement is not met.

The email addresses of each Provider's RA are available at the Provider's website (see section 1).

A certificate request 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 must be rejected at RA!

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

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

4.1.2.3 Sending a certificate request

The Applicant sends a certificate request to appropriate RA of the Provider (https://eidas.disig.sk/en/contact/registration-authorities/) where all necessary steps, which are part of certificate issuance must be performed.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Before issuing the certificate, the RA of the Provider shall:

- Inform the Subscriber about the General Terms and Conditions [8];
- 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 validate any information to be entered into the certificate.

In the case of the certificate for electronic signature or electronic seal where the cryptographic keys are not in the QSCD, the RA of the Provider shall verify the delivered request, which can be in the PKCS #10 format and then he can verify the Subscriber identity. The content of the request items and the obligation to complete them see section 7.

An employee of RA of the Provider must verify that the electronically submitted certificate request of a given Customer does include "*subject:emailAddress*" field and has been sent from the same e-mail address as found in the certificate request. In the event of discrepancies, it may refuse to issue a certificate.

4.2.1.1 Validation of mailbox authorization or control

Completed validation of the ownership and control of a mailbox or validation of applicant as operator of associated mail servers in accordance with Section 3.2.2.1 or Section 3.2.2.3 may be obtained no more than 398 days prior to issuing the Certificate.

Completed validation of control of a mailbox in accordance with Section 3.2.2.2 shall be obtained no more than 30 days prior to issuing the Certificate.

4.2.1.2 Authentication of organization identity

Completed validation of organization identity in accordance with Section 3.2.3 shall be obtained no more than 825 days prior to issuing the Certificate.

Validation of authority in accordance with Section 3.2.6 shall be obtained no more than 825 days prior to issuing the Certificate, unless a contract between the CA and the Applicant specifies a different term.

4.2.1.3 Authentication of individual identity

Completed validation of Individual identity in accordance with Section 3.2.4 shall be obtained no more than 825 days prior to issuing the Certificate.

A prior validation shall not be reused if any data or document used in the prior validation was obtained more than the maximum time permitted for reuse of the data or document prior to issuing the Certificate.

4.2.2 Approval or rejection of certificate applications

No stipulation.

4.2.3 Time to process certificate issuance

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

Certificate issuance by the Root CA shall require at least two individuals authorized by the CA (i.e., the CA system operator, system officer, or PKI administrator) one of whom deliberately issues 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

No stipulation.

4.4.2 Publication of the certificate by the CA

No stipulation.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

See Section 9.6.3, provisions 2. and 4.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

Every S/MIME certificate is always issued as new certificate for newly generated keys and certificate request, where the procedure is in accordance with the provisions stated in sections 4.1 to 4.5.

4.6.1 Circumstance for certificate renewal

No stipulation.

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

Every S/MIME certificate is always issued as new certificate for newly generated keys and certificate request, where the procedure is in accordance with the provisions stated in sections 4.1 to 4.5.

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

No stipulation.

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

4.9.1 Circumstances for revocation

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

4.9.1.1 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 the Provider to 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;
- The CA is made aware of a demonstrated or proven method that can easily compute the Subscriber's Private Key based on the Public Key in the Certificate (such as a Debian weak key, see https://wiki.debian.org/SSLkeys); or
- The Provider obtains evidence that the validation of domain authorization or mailbox control for any Mailbox Address 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 an email address or 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 an email address or Domain Name, a relevant licensing or services agreement between the Subscriber has terminated, or the account holder has failed to maintain the active status of the email address or Domain Name);
- The Provider is made aware of a material change in the information contained in the Certificate;
- The Provider is made aware that the Certificate was not issued in accordance with S/MIME Requirements or the Provider's CP and/or CPS;
- The Provider determines or is made aware that any of the information appearing in the Certificate is inaccurate;
- The Provider's right to issue certificates under these CA/Browser forum requirements [1] 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, or if there is clear evidence that the specific method used to generate the Private Key was flawed;
- The Provider terminates the business for any reason and does not arrange that another CA will provide information on revoked certificates on its behalf.

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

Revoked certificate cannot be restored in any circumstances.

4.9.1.2 Reasons for Revoking a Subordinate CA Certificate

The Provider 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 CP or CPS;
- The Issuing CA determines that any of the information appearing in the Certificate is inaccurate or misleading;
- The Issuing CA or Subordinate CA ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the Certificate;
- The Issuing CA's or Subordinate CA's right to issue Certificates under these Requirements expires or is revoked or terminated, unless the Issuing CA has made arrangements to continue maintaining the CRL/OCSP Repository; or
- Revocation is required by this CP and/or CPS.

4.9.2 Who can request revocation

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

Certificate revocation may also request

- Provider - the RA personnel shall document this fact in writing, including the reason for his/her proceedings,
- the court, by means of its judgment or interim measure (a copy of the relevant court decision must be attached to the certificate revocation documents),
- entity (natural or legal person) by virtue of inheritance (a copy of the documents showing the right of the entity to apply for the certificate to be revoked).

Additionally, Subscribers, Relying Parties, Application Software Suppliers, and other third parties MAY submit Certificate Problem Reports informing the Issuing CA of reasonable cause to revoke a Certificate.

4.9.3 Procedure for revocation request

If the Subscriber's authentication requirements are met, which requests the revocation of the certificate, the certificate revocation request can be submitted:

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

in the sentence "I hereby ask to cancel my certificate with the serial number XXXXXX";

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

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

The certificate that expired cannot be revoked.

Reporting and incident reporting procedures for possible compromise of a private key, misuse of a certificate or other type of fraud, unauthorized issuance 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

The Provider shall within 24 hours after receiving a Certificate Problem Report investigate the facts and circumstances related to a Certificate Problem Report and provide a preliminary report on its findings to both the Subscriber and the entity who filed the Certificate Problem Report.

After reviewing the facts and circumstances, the Provider shall work with the Subscriber/Subject and any entity reporting the Certificate Problem Report or other revocation-related notice to establish whether or not the certificate will be revoked, and if so, a date which the Provider will revoke the certificate.

The period from receipt of the Certificate Problem Report or revocation-related notice to published revocation must not exceed the time frame set forth in Section 4.9.1.1.

The date selected by the Provider 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 should be addressed with higher priority); and
- Relevant legislation.

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 [8].

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

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

4.9.7 CRL issuance frequency

CRL issuance frequency varies depending on whether it concerns a root CA a subordinate CA. Table 3 contains information on maximum CRL issuance frequency.

Table 3 CRL issuance frequency

CRL issuer	Issuance frequency	nextUpdate vs. thisUpdate	Notes
Root CA	max 365 days	< 365 days	Always within 24 hours after revoking a subordinate CA
Subordinate CA	max 7 days	< 10 days	

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

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

Root CA issuing certificates to subordinate CAs must issue CRLs:

- At least every 7 days with nextUpdate no more than 10 days;
- Always within 24 hours after revoking a Subordinate CA certificate.

4.9.8 Maximum latency for CRLs

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

4.9.9 On-line revocation/status checking availability

When provided, OCSP responses shall conform to RFC 6960 [15] and/or RFC 5019 [16]. OCSP responses shall either:

- Be signed by the CA that issued the Certificates whose revocation status is being checked, or
- Be signed by 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 shall contain the "*ocspSigning EKU (1.3.6.1.5.5.7.3.9)*" and an extension of type "*id-pkix-ocsp-nocheck*", as defined by RFC 6960 [15].

4.9.10 On-line revocation/status checking requirements

Providers's OCSP responders shall support the HTTP GET method, as described in RFC 6960 [15] and/or RFC 5019 [16].

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 S/MIME Certificates:

- OCSP responses shall have a validity interval greater than or equal to eight hours;
- OCSP responses shall have a validity interval less than or equal to ten days;
- For OCSP responses with validity intervals less than sixteen hours, then the CA shall update the information provided via an Online Certificate Status Protocol prior to one-half of the validity period before the nextUpdate; and
- For OCSP responses with validity intervals greater than or equal to sixteen hours, then the CA shall update the information provided via an Online Certificate Status Protocol 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 CA shall update information provided via OCSP:

- at least every twelve months; and
- within 24 hours after revoking a Subordinate CA Certificate.

If the OCSP responder receives a request for the status of a Certificate serial number that is "unused", then the responder should not respond with a "*good*" status.

The CA should monitor the OCSP responder for requests for "unused" serial numbers as part of its security response procedures.

A Certificate serial number within an OCSP request is "assigned" if a Certificate with that serial number has been issued by the Issuing CA, using any current or previous key associated with that CA subject, or "unused" if otherwise.

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

4.9.11 Other forms of revocation advertisements available

No stipulation.

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

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 accordance with the 4.9.10.

Revocation entries on a CRL or OCSP Response shall 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 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 shall be available in 24x7 mode.

OCSP shall be available in 24x7 mode.

4.10.3 Optional features

No stipulation.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

The Provider does not escrow or recover the Subscriber's Private Key.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. MANAGEMENT, OPERATIONAL, AND PHYSICAL CONTROLS

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

Security measures shall be available to staff concerned.

Provider shall

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

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

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

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

5.1 Physical security controls

5.1.1 Site location and construction

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

5.1.2 Physical access

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

5.1.3 Power and air conditioning

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

5.1.4 Water exposures

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

5.1.5 Fire prevention and protection

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

5.1.6 Media storage

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

5.1.7 Waste disposal

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

5.1.8 Off-site backup

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

5.2 Procedural controls

5.2.1 Trusted roles

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

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

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

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

5.2.2 Number of Individual Required per Task

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

5.2.3 Identification and authentication for each role

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

5.2.4 Roles requiring separation of duties

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

5.3 Personnel controls

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

5.3.1 Qualifications, experience, and clearance requirements

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

Persons in managerial positions shall

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

5.3.2 Background check procedures

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

5.3.3 Training Requirements and Procedures

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

5.3.4 Retraining frequency and requirements

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

5.3.5 Job rotation frequency and sequence

There is no job rotation for trusted roles.

5.3.6 Sanctions for unauthorized actions

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

5.3.7 Independent Contractor Controls

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

5.3.8 Documentation supplied to personnel

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

5.4 Audit logging procedures

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

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

5.4.1 Types of events recorded

The CA shall record at least the following events.

5.4.1.1 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.

5.4.1.2 Subscriber Certificate lifecycle management events, including:

- Certificate requests, renewal, and re-key requests, and revocation;

- All verification activities stipulated in this CP and the CA's Certification Practice Statement;
- Approval and rejection of certificate requests;
- Issuance of Certificates;
- Generation of Certificate Revocation Lists; and
- Signing of OCSP Responses (as described in Section 4.9 and Section 4.10).

5.4.1.3 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 (as set forth in Section 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 (as set forth in Section 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

The Provider's security program shall include an annual Risk Assessment that:

- 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;
- Assesses the likelihood and potential damage of these threats, taking into consideration the sensitivity of the Certificate Data and Certificate Management Processes; and
- 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

The Provider shall archive all audit logs (as set forth in Section 5.4.1).

Additionally, the Provider shall archive:

- Documentation related to the security of their Certificate Systems, Certificate Management Systems, Root CA Systems, and Delegated Third Party Systems; and
- Documentation related to their verification, issuance, and revocation of Certificate Requests and Certificates.

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

Archived audit logs shall be retained for a period of at least two (2) years from their record creation timestamp, or as long as they are required to be retained per Section 5.4.3, whichever is longer.

Additionally, the Provider shall retain, for at least two (2) years:

- All archived documentation related to the security of Certificate Systems, Certificate Management Systems, Root CA Systems and
- All archived documentation relating to the verification, issuance, and revocation of Certificate Requests and Certificate.

5.5.3 Protection of archive

No stipulation.

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 (internal or external)

No stipulation.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

No stipulation.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Provider shall have an Incident Response Plan and a Disaster Recovery Plan.

The Provider shall document a business continuity and disaster recovery procedures designed to notify and reasonably protect Application Software Suppliers, Subscribers, and Relying Parties in the event of a disaster, security compromise, or business failure. The Provider is not required to publicly disclose its business continuity plans but shall make its business continuity plan and security plans available to the Provider 's auditors upon request. The Provider shall annually test, review, and update these procedures.

The business continuity plan shall include:

1. The conditions for activating the plan;
2. Emergency procedures;
3. Fallback procedures;
4. Resumption procedures;
5. A maintenance schedule for the plan;

6. Awareness and education requirements;
7. The responsibilities of the individuals;
8. Recovery time objective (RTO);
9. Regular testing of contingency plans;
10. The CA's plan to maintain or restore the CA's business operations in a timely manner following interruption to or failure of critical business processes;
11. A requirement to store critical cryptographic materials (i.e., secure cryptographic device and activation materials) at an alternate location;
12. What constitutes an acceptable system outage and recovery time;
13. How frequently backup copies of essential business information and software are taken;
14. The distance of recovery facilities to the CA's main site; and
15. Procedures for securing its facility to the extent possible during the period of time following a disaster and prior to restoring a secure environment either at the original or a remote site.

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

No stipulation.

6. TECHNICAL SECURITY CONTROLS

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

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

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

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

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

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

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

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

For CA Key Pairs that are used as a CA Key Pair for a Root CA Certificate; or

Provider shall:

- prepare and follow a Key Generation Script;
- either
  - (i) have a Qualified Auditor witness the CA Key Pair generation process, or
  - (ii) video-record the entire CA Key Pair generation process for review by its Qualified Auditor.

The Provider shall also:

- generate the CA Key Pair in a physically secured environment as described in the CA's CP and/or CPS;
- generate the CA Key Pair using personnel in Trusted Roles under the principles of multiple person control and split knowledge;

- generate the CA Key Pair within cryptographic modules meeting the applicable technical and business requirements as disclosed in the CA's CP and/or CPS;
- log its CA Key Pair generation activities; and
- maintain effective controls to provide reasonable assurance that the Private Key was generated and protected in conformance with the procedures described in its CP and/or CPS and (if applicable) its Key Generation Script.

6.1.1.2 RA key pair generation

No stipulation.

6.1.1.3 Subscriber key pair generation

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

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

The Provider does not generate the Private Key on behalf of the Subscriber.

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 CA or any of its designated RAs become aware that a Subscriber's Private Key has been communicated to a person or organization not authorized by the Subscriber, then the CA 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; and
- Ensure that the modulus size, in bits, is evenly divisible by 8.

6.1.6 Public key parameters generation and quality checking

For RSA key pairs: 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. (See NIST SP 800-89, Section 5.3.3.) [17] .

6.1.7 Key usage purposes (as per X.509 v3 key usage field)

Private Keys corresponding to Root CA Certificates shall not be used to sign Certificates except in the following cases:

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

6.2 Private Key Protection and Cryptographic Module Engineering Controls

The Provider shall implement physical and logical safeguards to prevent unauthorized Certificate issuance. Protection of the CA Private Key outside the validated system or device specified above shall consist of physical security, encryption, or a combination of both, implemented in a manner that prevents disclosure of the Private Key.

The Provider shall encrypt its Private Key with an algorithm and key-length that, according to the state of the art, are capable of withstanding cryptanalytic attacks for the residual life of the encrypted key or key part.

6.2.1 Cryptographic module standards and controls

No stipulation.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

See Section 5.2.2.

6.2.5 Private key archival

Parties other than the Provider shall not archive the Subordinate CA Private Keys without authorization by the Provider.

6.2.6 Private key transfer into or from a cryptographic module

If the Issuing CA of the Provider generated the Private Key on behalf of the Subordinate CA, then the Issuing CA shall encrypt the Private Key for transport to the Subordinate CA.

If the Issuing CA becomes aware that a Subordinate CA's Private Key has been communicated to an unauthorized person or an organization not Affiliated with the Subordinate CA, then the Issuing CA shall revoke all certificates that include the Public Key corresponding to the communicated Private Key.

6.2.7 Private key storage on cryptographic module

The Provider shall protect its Private Key in a system or device that has been validated as meeting at least FIPS 140-2 level 3, FIPS 140-3 level 3, or an appropriate Common Criteria Protection Profile or Security Target, EAL 4 (or higher), which includes requirements to protect the Private Key and other assets against known threats.

6.2.8 Method of Activating Private Key

No stipulation.

6.2.9 Method of Deactivating Private Key

No stipulation.

6.2.10 Method of Destroying Private Key

No stipulation.

6.2.11 Cryptographic Module rating

No stipulation.

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	Maximum Validity Period
Strict and Multipurpose	825 days

For the purpose of 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 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

The CA/Browser Forum's Network and Certificate System Security Requirements [18] are incorporated by reference as if fully set forth herein.

6.8 Time-stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

The Provider shall meet the technical requirements set forth in Section 2.2, Section 6.1.5, and Section 6.1.6.

The Provider shall generate non-sequential Certificate serial numbers greater than zero (0) and less than 2^159 containing at least 64 bits of output.

7.1.1 Version number

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

7.1.2 Certificate content and extensions; application of RFC 6818

This section specifies the additional requirements for Certificate content and extensions for Certificates.

7.1.2.1 Root CA certificates

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

Signature Algorithm
sha256RSA
Public key
RSA, length 2 048 bit or 4 096 bit
Validity of Root CA certificate
maximum 30 years

Table 4 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.

Table 5 Certificate extensions in root CA certificates

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

7.1.2.2 Subordinate CA certificates

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 6 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, R2I3 Certification Service etc.

Table 7 Certificate extensions in subordinate CA

Extension / OID	Presence	Critical
certificatePolicies / 2.5.29.32	shall	NO
crlDistributionPoints / 2.5.29.31	shall	NO
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	should	NO
basicConstraints / 2.5.29.19	shall	YES
keyUsage / 2.5.29.15	shall	YES
extKeyUsage / 2.5.29.37	shall	NO
authorityKeyIdentifier / 2.5.29.35	shall	NO
subjectKeyIdentifier / 2.5.29.14	shall	NO

7.1.2.3 Subscriber certificates

For details on the content of the distinguishing name (DN) of each type of certificate issued under this CP, refer to the section 7.1.4.2.

Table 8 lists the extensions used in all types of certificates issued.

Table 8 Basic extensions in subscriber certificates

Extension name / ASN.1 name and OID	Description	Presence	Critical
Certificate Policies {id-ce-certificatePolicies} {2.5.29.32}	It shall include exactly one of the reserved policyIdentifiers listed in Section 7.1.6.1.	shall	NO
CRL Distribution Points {id-ce-CRLDistributionPoints} {2.5.29.31}	Strict and Multipurpose profiles shall contain at least one distributionPoint whose fullName value includes a GeneralName of type uniformResourceIdentifier that includes a URI where the Issuing CA's CRL can be retrieved. Every uniformResourceIdentifier shall have the URI scheme HTTP. Other schemes shall not be present.	shall	NO
AuthorityInfoAccess {id-pe-authorityInfoAccess} {1.3.6.1.5.5.7.1.1}	1. id-ad-ocsp The extension MAY contain one or more accessMethod values of type id-ad-ocsp that specifies the URI of the Issuing CA's OCSP responder. Strict and Multipurpose profiles shall for every accessMethod have the URI scheme HTTP. Other schemes shall not be present. 2. id-ad-calssuers The extension should contain at least one accessMethod value of type id-ad-calssuers that specifies the URI of the Issuing CA's Certificate. Strict and Multipurpose profiles shall for every accessMethod have the URI scheme HTTP. Other schemes shall not be present.	should	NO

basicConstraints {id-ce-basicConstraints} {2.5.29.19}	This extension MAY be present. The cA field shall not be true. pathLenConstraint field shall not be present.	should	NO
Key Usage {id-ce-keyUsage} {2.5.29.15}	Strict profile: For signing only, bit positions shall be set for digitalSignature and MAY be set for nonRepudiation. For key management only, bit positions shall be set for keyEncipherment. For dual use, bit positions shall be set for digitalSignature and keyEncipherment and MAY be set for nonRepudiation. Multipurpose profile: applies same as for Strict profil with modification that for key management and dual use may be set for dataEncipherment. Other bit positions shall not be set.	shall	should
Extended Key Usage {id-ce-extKeyUsage} [2.5.29.37]	Strict profile: id-kp-emailProtection shall be present. Other values shall not be present Multipurpose profile: id-kp-emailProtection shall be present. Other values MAY be present. Any profile: The values id-kp-serverAuth, id-kp-codeSigning, id-kp-timeStamping, and anyExtendedKeyUsage shall not be present.	shall	NO
Authority Key Identifier {id-ce-authorityKeyIdentifier} {2.5.29.35}	The keyIdentifier field shall be present. authorityCertIssuer and authorityCertSerialNumber fields shall not be present.	shall	NO
subjectAltName id-ce-subjectAltName [2.5.29.17]	The value of this extension shall be encoded as specified in Section 7.1.4.2.1.	shall	NO
Subject Key Identifier {id-ce-subjectKeyIdentifier} {2.5.29.14}	It should contain a value that is derived from the Public Key included in the Subscriber Certificate.	should	NO

7.1.2.4 All certificates

All fields and extensions shall be set in accordance with RFC 5280 [19]. The Provider shall not issue a Certificate that contains a keyUsage flag, extKeyUsage value, Certificate extension, or other data not specified in Section 7.1.2.1, Section 7.1.2.2, or Section 7.1.2.3 unless the Provider is aware of a reason for including the data in the Certificate. If the Provider includes fields or extensions in a Certificate that are not specified but are otherwise permitted by these Requirements, then the Provider shall document the processes and procedures that the Provider employs for the validation of information contained in such fields and extensions in its CP and/or CPS.

Provider shall not issue a Certificate with:

- Extensions that do not apply in the context of the public Internet
- Field or extension values which have not been validated according to the processes and procedures described in this CP and/or CPS.

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

The following requirements apply to the "*subjectPublicKeyInfo*" field within a Certificate. No other encodings are permitted.

7.1.3.1.1 RSA

The Provider shall indicate an RSA key using the "*rsaEncryption* (OID: 1.2.840.113549.1.1.1)" algorithm identifier. The parameters shall be present, and shall be an explicit "*NULL*".

The Provider shall not use a different algorithm, such as the "*id-RSASSA-PSS* (OID: 1.2.840.113549.1.1.10)" algorithm identifier, to indicate an RSA key.

When encoded, the AlgorithmIdentifier for RSA keys shall be byte-for-byte identical with the following hex-encoded bytes: *300d06092a864886f70d0101010500*

7.1.3.1.2 ECDSA

The Provider does not issue certificates for this type of keys.

7.1.3.1.3 EdDSA

The Provider does not issue certificates for this type of keys.

7.1.3.2 Signature AlgorithmIdentifier

All objects signed by a CA Private Key shall conform to these requirements on the use of the "*AlgorithmIdentifier*" or "*AlgorithmIdentifier*" -derived type in the context of signatures.

In particular, it applies to all of the following objects and fields:

- The "*signatureAlgorithm*" field of a Certificate.
- The "*signature*" field of a "*TBSCertificate*" (for example, as used by a Certificate).
- The "*signatureAlgorithm*" field of a "*CertificateList*"
- The "*signature*" field of a "*TBSCertList*"
- The "*signatureAlgorithm*" field of a "*BasicOCSPResponse*".

No other encodings are permitted for these fields.

7.1.3.2.1 RSA

The CA of the provider shall use one of the following signature algorithms and encodings. When encoded, the "*AlgorithmIdentifier*" shall be byte-for-byte identical with the specified hex-encoded bytes.

AlgorithmIdentifier	Encoding
RSASSA-PKCS1-v1_5 with SHA-256	300d06092a864886f70d01010b0500
RSASSA-PKCS1-v1_5 with SHA-384	300d06092a864886f70d01010c0500
RSASSA-PKCS1-v1_5 with SHA-512	300d06092a864886f70d01010d0500
RSASSA-PSS with SHA-256, MGF-1 with SHA-256, and a salt length of 32 bytes	304106092a864886f70d01010a3034a00 f300d060960864801650304020105 00a11c301a06092a864886f70d010108300d0 609608648016503040201050 0a203020120
RSASSA-PSS with SHA-384, MGF-1 with SHA-384, and a salt length of 48 bytes	304106092a864886f70d01010a3034a00 f300d060960864801650304020205 00a11c301a06092a864886f70d010108300d06096 086480165030402020500a203020130
RSASSA-PSS with SHA-512, MGF-1 with SHA-512, and a salt length of 64 bytes	304106092a864886f70d01010a3034a00 f300d060960864801650304020305 00a11c301a06092a864886f70d010108300d06096 086480165030402030500a203020140

7.1.3.2.2 ECDSA

The Provider does not use this type of signature algorithm.

7.1.3.2.3 EdDSA

The Provider does not use this type of signature algorithm.

7.1.4 Name Forms

Attribute values shall be encoded according to RFC 5280 [19].

7.1.4.1 Name encoding

For every valid Certification Path (as defined by RFC 5280, Section 6):

- For each Certificate in the Certification Path, the encoded content of the "Issuer Distinguished Name" field of a Certificate shall be byte-for-byte identical with the encoded form of the "Subject Distinguished Name" field of the Issuing CA Certificate.
- For each CA Certificate in the Certification Path, the encoded content of the "Subject Distinguished Name" field of a Certificate shall be byte-for-byte identical among all Certificates whose "Subject Distinguished Names" can be compared as equal according to RFC 5280, Section 7.1, and including expired and revoked Certificates.

7.1.4.2 Subject information - subscriber certificates

By issuing the Certificate, the CA of the Provider represents that it followed the procedure set forth in its CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

The Provider shall not include a Mailbox Address in a Mailbox Field except as verified in accordance with Section 3.2.2.

Subject attributes shall not contain only metadata such as '.', '-', and ' ' (i.e., space) characters, and/or any other indication that the value is absent, incomplete, or not applicable.

7.1.4.2.1 Subject alternative name extension

Certificate field	Required / Optional	Contents
extensions: subjectAltName	shall be present	This extension shall contain at least one *GeneralName* entry of the following types: • Rfc822Name and/or • otherName of type id-on-SmtpUTF8Mailbox, encoded in accordance with RFC 8398

7.1.4.2.2 Subject distinguished name fields

The Provider issues these types of SMIME Certificates:

- S/MIME digital signature certificate
  - Individual-validated (STRICT and MULTIPURPOSE)
  - Sponsor-validated (STRICT and MULTIPURPOSE)
- S/MIME digital certificate for seal (STRICT and MULTIPURPOSE).

The following subject distinguished name fields are included in the specified types of Certificates:

Subject distinguished name field	SMIME digital signature certificate				S/MIME digital certificate for seal	
	Individual-validated		Sponsor-validated		Organization-validated	
	Multipurpose	Strict	Multipurpose	Strict	Multipurpose	Strict
commonName	YES	YES	YES	YES	YES	YES
givenName	YES	YES	YES	YES		
surname	YES	YES	YES	YES		
serialNumber	YES	YES	YES	YES		
countryName	YES	YES	YES	YES	YES	YES
organizationName			YES	YES	YES	YES
organizationIdentifier			YES	YES	YES	YES
localityName			YES	YES	YES	YES
emailAddress	YES	YES	YES	YES	YES	YES

a) Certificate Field: **"***subject:commonName* (OID 2.5.4.3)**"**

This attribute shall contain one of the following values verified in accordance with Section 3.2.

Certificate type	Contents
Organization-validated	*subject:organizationName* Mailbox Address
Sponsor-validated	Personal Name, Pseudonym, or Mailbox Address
Individual-validated	Personal Name, Pseudonym, or Mailbox Address

The Personal Name should be presented as "*subject:givenName*" and/or "*subject:surname*". The Personal Name MAY be in the Subject's preferred presentation format or a format preferred by the CA or Enterprise RA, but shall be a meaningful representation of the Subject's name as verified under Section 3.2.4.

If present, the Mailbox Address shall contain a rfc822Name or otherName value of type id-on-SmtpUTF8Mailbox from extensions:subjectAltName.

Like all other Certificate attributes, "*subject:commonName*" and "*subject:emailAddress*" shall comply with the attribute upper bounds defined in RFC 5280 [19].

b) **Certificate Field: "*subject:organizationName* (OID 2.5.4.10)"**

If present, field shall contain the Subject's full legal organization (legal person) name as verified under Section 3.2.3. RA of the provider MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations, or removing character "," (comma) or character substitutions according to section 3.1.4.1.

c) **Certificate Field: "*subject:organizationalUnitName* (OID: 2.5.4.11)"**

The provider does not include this field in SMIME Certificates.

d) Certificate Field**: "*subject:organizationIdentifier* (2.5.4.97)"**

If present, the field shall contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme.

The "*subject:organizationIdentifier*" shall be encoded as a PrintableString or UTF8String.

The Registration Scheme identified in the Certificate shall be the result of the verification performed in accordance with Section 3.2.3.

The Registration Scheme shall be identified using the following structure in the presented order:

- 3 character Registration Scheme identifier (e.g. NTR);
- 2 character ISO 3166 country code for the nation in which the Registration Scheme is operated, or if the scheme is operated globally ISO 3166 code "XG" shall be used.

The following Registration Schemes are recognized as valid under Requirements [1] for use in the "*subject:organizationIdentifier*" attribute :

- NTR: For an identifier allocated by a national or state trade register to the Legal Entity named in the *subject:organizationName*.
- VAT: For an identifier allocated by the national tax authorities to the Legal Entity named in the *subject:organizationName*.
- PSD: For a national authorization number allocated to the payment service provider named in the *subject:organizationName* under Payments Services Directive (EU) 2015/2366. This shall use the extended structure as defined in ETSI TS 119 495, clause 5.2.1.

- LEI: For a Legal Entity Identifier as specified in ISO 17442 for the entity named in the *subject:organizationName*. The 2 character ISO 3166 country code shall be set to 'XG'.

The country code used in the Registration Scheme identifier shall match that of the "*subject:countryName*" in the Certificate as specified in Section 7.1.4.2.2.

e) **Certificate Field: "subject:givenName (2.5.4.42)" and/or "subject:surname (2.5.4.4)"**

If present, the "*subject:givenName*" field and "*subject:surname*" field shall contain a Natural Person Subject's name as verified under Section 3.2.4. Subjects with a single legal name shall provide the name in the "*subject:surname*" attribute. The "*subject:givenName*" and/or "*subject:surname*" shall not be present if the "*subject:pseudonym*" is present.

f) **Certificate Field: "*subject:pseudonym* (2.5.4.65)"**

The Provider does not include this field in SMIME Certificates.

g) Certificate Field: **"*subject:serialNumber* (2.5.4.5)"**

If present, it MAY be used to contain an identifier assigned by the CA or RA to identify and/or to disambiguate the Subscriber.

In addition, the *subject:serialNumber* MAY be used in the Sponsor-validated and Individual-validated profiles to contain a Natural Person Identifier as described in ETSI EN 319 412-1 Section 5.1.3 [20].

The Provider shall confirm that the Individual represented by the Natural Person Identifier is the same as the Certificate Subject.

h) **Certificate Field: "*subject:emailAddress* (1.2.840.113549.1.9.1)"**

It shall contain a single Mailbox Address as verified under Section 3.2.2.

i) **Certificate Field: "*subject:title* (2.5.4.12)"**

The Provider does not include this field in SMIME Certificates.

j) **Certificate Field: Number and street: "*subject:streetAddress* (OID: 2.5.4.9)"**

The Provider does not include this field in SMIME Certificates.

k) **Certificate Field: "*subject:localityName* (OID: 2.5.4.7)"**

If present, it shall contain the Subject's locality information as verified under Section 3.2.3 for "Organization-validated" and "Sponsor-validated" Certificate Types or Section 3.2.4 for "Individual-validated" Certificate Types.

l) **Certificate Field: "*subject:stateOrProvinceName* (OID: 2.5.4.8)"**

The Provider does not include this field in SMIME Certificates.

m) Certific**ate Field: "*subject:postalCode* (OID: 2.5.4.17)"**

The Provider does not include this field in SMIME Certificates.

n) **Certificate Field: "*subject:countryName* (OID: 2.5.4.6)"**

If present, it shall contain the two-letter ISO 3166-1 country code associated with the location of the Subject verified under Section 3.2.3 for "Organization-validated" and "Sponsor-validated" Certificate Types or Section 3.2.4 for "Individual-validated" Certificate Types.

7.1.4.3 Subject information - root certificates and subordinate CA certificates

By issuing a Subordinate CA Certificate, the Provider represents that it followed the procedure set forth in its CP and/or CPS to verify that, as of the Certificate's issuance date, all of the Subject Information was accurate.

7.1.4.3.1 Subject distinguished name fields

a) **Certificate Field: "***subject:commonName* **(OID 2.5.4.3)"**

This field shall be present and it should contain an identifier for the Certificate such that the Certificate's Name is unique across all Certificates issued by the Issuing CA.

b) **Certificate Field: "***subject:organizationName* **(OID 2.5.4.10)"**

This field shall be present and it shall contain either the Subject CA's name or DBA as verified under Section 3.2.3.2.2. The Provider MAY include information in this field that differs slightly from the verified name, such as common variations or abbreviations.

c) **Certificate Field: "***subject:countryName* **(OID: 2.5.4.6)"**

This field shall be present and it shall contain the two-letter ISO 3166-1 country code for the country in which the Provider's place of business is located.

d. Other Subject Attributes

Other attributes MAY be present within the subject field. If present, other attributes shall contain information that has been verified by the Provider.

7.1.5 Name constraints

For a Subordinate CA Certificate to be considered Technically Constrained, the Certificate shall include an *Extended Key Usage (EKU)* extension specifying all extended key usages for which the Subordinate CA Certificate is authorized to issue Certificates.

The *anyExtendedKeyUsage* KeyPurposeId shall not appear within this extension.

7.1.6 Certificate policy object identifier

This section describes the content requirements for the Root CA, Subordinate CA, and Subscriber Certificates as they relate to the identification of Certificate Policy.

7.1.6.1 Reserved certificate policy identifiers

The following CA/Browser Forum Certificate Policy identifiers are reserved for use by Provider to assert that a Certificate complies with these Requirements.

Certificate Type	Subtype	Policy Identifier
S/MIME digital signature certificate type „Individual-validated“	STRICT	2.23.140.1.5.4.3
	MULTIPURPOSE	2.23.140.1.5.4.2
S/MIME digital signature certificate type “Sponsor-validated“	STRICT	2.23.140.1.5.3.3
	MULTIPURPOSE	2.23.140.1.5.3.2
S/MIME digital certificate for seal	STRICT	2.23.140.1.5.2.3
	MULTIPURPOSE	2.23.140.1.5.2.2

7.1.6.2 Root CA certificates

A Root CA Certificate should not contain the *certificatePolicies* extension. If present, the extension shall conform to the requirements set forth for Certificates issued to Subordinate CAs in Section 7.1.6.3.

7.1.6.3 Subordinate CA certificates

A Certificate issued to a Subordinate CA that is an Affiliate of the Issuing CA shall include a set of policy identifiers from one of the two options below:

- One or more explicit policy identifiers defined in Section 7.1.6.1 that indicate the Subordinate CA's adherence to and compliance with SMIME Requirements [1] and MAY contain one or more identifiers documented by the Subordinate CA in its CP and/or CPS; or
- The “*anyPolicy (2.5.29.32.0)*” identifier.

The Subordinate CA and the Issuing CA shall represent, in their CP and/or CPS, that all Certificates containing a policy identifier indicating compliance with SMIME Requirements [1] are issued and managed in accordance with these Requirements.

7.1.6.4 Subscriber certificates

A Certificate issued to a Subscriber shall contain, within the Certificate's *certificatePolicies* extension, a policy identifier that is specified in Section 7.1.6.1.

The Certificate MAY also contain additional policy identifier(s) defined by the Provider. The Provider shall document in its CP and/or CPS that the Certificates it issues containing the specified policy identifier(s) are managed in accordance with this CP Requirements.

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

7.2.1 Version number

No stipulation.

7.2.2 CRL and CRL entry extensions

Table 9 lists the CRL extensions that were issued by the CAs of the Provider to which this CP applies, along with information on their presence and criticality.

Table 9 CRL extensions

Extension name	Required	Critical
Authority Key Identifier (OID 2.5.29.35)	YES	NO
CRL Number (OID 2.5.29.20)	YES	NO
ReasonCode (OID 2.5.29.21)	YES*	NO

* If a CRL entry is for a Root CA or Subordinate CA Certificate, including Cross Certificates, this CRL entry extension shall be present. If a CRL entry is for a Certificate not technically capable of causing issuance, this CRL entry extension should be present, but MAY be omitted, subject to the following requirements.

  The CRLreason of certificateHold (6) SHALL NOT be used for Root CA or Subordinate CA Certificates.

  The CRLReason indicated shall not be unspecified (0). If the reason for revocation is unspecified, CAs shall omit the reasonCode entry extension.

  The Repository may include CRL entries that have a CRLreason of certificateHold (6) for Certificates that include the Certificate Policy identifiers for the Legacy or Multipurpose Generations. The Repository shall not include CRL entries that have a CRLreason of certificateHold (6) for Certificates that include the Certificate Policy identifiers for the Strict Generation.

  If a reasonCode CRL entry extension is present, the CRLReason SHALL indicate the most appropriate reason for revocation of the Certificate, as defined by the CA within its CP/CP.

If present, the reasonCode (OID 2.5.29.21) extension shall not be marked critical.

7.3 OCSP profile

If an OCSP response is for a Root CA or Subordinate CA Certificate, including Cross Certificates, and that Certificate has been revoked, then the revocationReason field within the RevokedInfo of the CertStatus SHALL be present.

The CRLReason indicated SHALL contain a value permitted for CRLs, as specified in Section 7.2.2.

7.3.1 Version number

No stipulation.

7.3.2 OCSP extensions

Table 10 contains possible extensions in the OCSP responses of the Provider's OCSP Responder, their reporting obligation and their criticality.

Table 10 OCSP response extensions

Extensions name	Required	Critical
id-pkix-ocsp-nonce (OID 1.3.6.1.5.5.7.48.1.2)	NO	NO

The "*singleExtensions*" of an OCSP response shall 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 [3] and CA/Browser forum [1]. All aspects of the CA operation relating to this CP are to be subject to compliance audits.

The Provider shall at all times:

- Issue Certificates and operate its PKI in accordance with all law applicable to its business and the Certificates it issues in every jurisdiction in which it operates;
- Comply with Requirements of this CP;
- Comply with the audit requirements set forth in this section; and
- Be licensed as a trust services provider (CA) in each jurisdiction where it operates, if licensing is required by the law of such jurisdiction for the issuance of Certificates.

8.1 Frequency or circumstances of assessment

Certificates that are capable of being used to issue new Certificates shall either be Technically Constrained in line with Section 7.1.5 and audited in line with Section 8.8 only, or unconstrained and fully audited in line with all remaining requirements from this section. A Certificate is deemed as capable of being used to issue new Certificates if it contains an X.509v3 "*basicConstraints*" extension, with the "*cA Boolean*" set to "*true*" and is therefore by definition a Root CA Certificate or a Subordinate CA Certificate.

The period during which the Provider issues Certificates shall be divided into an unbroken sequence of audit periods. An audit period shall not exceed one year in duration.

If the Provider has a currently valid Audit Report indicating compliance with an audit scheme listed in Section 8.4, then no pre-issuance readiness assessment is necessary.

If the Provider does not have a currently valid Audit Report indicating compliance with one of the audit schemes listed in Section 8.4, then, before issuing Publicly-Trusted S/MIME Certificates, the Provider shall successfully complete a point-in-time readiness assessment performed in accordance with applicable standards under one of the audit schemes listed in Section 8.4. The point-in-time readiness assessment shall be completed no earlier than twelve (12) months prior to issuing Publicly-Trusted S/MIME Certificates and shall be followed by a complete audit under such scheme within ninety (90) days of issuing the first Publicly-Trusted S/MIME Certificate.

8.2 Identity/qualifications of assessor

The Provider's audit shall be performed by a Qualified Auditor. A Qualified Auditor means a Natural Person, Legal Entity, or group of Natural Persons or Legal Entities that collectively possess the following qualifications and skills:

- Independence from the subject of the audit;
- The ability to conduct an audit that addresses the criteria specified in an Eligible Audit Scheme (see Section 8.4);
- Employs individuals who have proficiency in examining Public Key Infrastructure technology, information security tools and techniques, information technology and security auditing, and the third-party attestation function;
- For audits conducted in accordance with any one of the ETSI standards accredited in accordance with ISO 17065 applying the requirements specified in ETSI EN 319 403 or ETSI EN 319 403-1;
- Bound by law, government regulation, or professional code of ethics; and
- Except in the case of an Internal Government Auditing Agency, maintains Professional Liability/Errors & Omissions insurance with policy limits of at least one million US dollars in coverage.

8.3 Assessor's relationship to assessed entity

See section 8.2.

8.4 Topics covered by assessment

For Audit Periods starting after the Effective Date defined in Section 1.2.1 of the SMIME Requirements [1] the Provider shall undergo an audit in accordance with the following scheme:

- ETSI EN 319 411-1 v1.3.1 or newer, which includes normative references to ETSI EN 319 401 (the latest version of referenced ETSI documents should be applied).

The audit shall be conducted by a Qualified Auditor, as specified in Section 8.2.

8.5 Actions taken as a result of deficiency

No stipulation.

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 shall make the Audit Report publicly available.

The Provider shall make 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 shall contain at least the following clearly-labelled information:

- Name of the organization being audited;
- Name and address of the organization performing the audit;
- The SHA-256 fingerprint of all Roots and Subordinate CA Certificates, including Cross Certificates, that were in-scope of the audit;
- Audit criteria, with version number(s), that were used to audit each of the Certificates (and associated keys);
- A list of the Provider policy documents, with version numbers, referenced during the audit;
- Whether the audit assessed a period of time or a point in time;
- The start date and end date of the Audit Period, for those that cover a period of time;
- The point in time date, for those that are for a point in time;
- The date the report was issued, which will necessarily be after the end date or point in time date;
- 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., ETSI EN 319 401, ETSI EN 319 411-1 policy LCP, NCP or NCP+, ETSI EN 319 411-2 policy QCP-n, QCP-n-qscd, QCP-l or QCP-l-qscd; and
- 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 this document, and the version used.

An authoritative English language version of the publicly available audit information shall be provided by the Qualified Auditor and the Provider shall ensure that it is publicly available.

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

8.7 Self audits

During the period in which the Provider issues Certificates, the Provider shall monitor adherence to its CP and/or CPS and these Requirements and control its service quality by performing self audits on at least a quarterly basis against a randomly selected sample including a minimum of the greater of thirty (30) Certificates or three percent (3%) of the Certificates issued by it during the period commencing immediately after the previous self-audit sample was taken.

8.8 Review of delegated parties

No stipulation.

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.

The Provider shall publish a valid price list on company's web site (see section 1).

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

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

No stipulation.

9.1.4 Fees for other services

No stipulation.

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

9.2.1 Insurance coverage

No stipulation.

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

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

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 [21].

The Provider shall publish a Privacy Policy that provides information on the Provider 's data protection practices. The Privacy Policy should include information on how the Provider collects, uses, shares, store, and deletes or retains data, as well as contact information for the exercise of privacy rights.

The data protection practices are available on:
https://eidas.disig.sk/pdf/info_oou_gdpr.pdf .

9.4.2 Information treated as private

The Provider shall treat all personal information about an Individual that is not publicly available in the contents of a Certificate as private information. This includes information that links a "*subject:pseudonym*" to the real identity of the Subject Individual.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

The Provider shall protect private information using appropriate safeguards and a reasonable degree of care. The Provider shall require the same from any service providers who handle private information on behalf of the Provider.

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 [21].

9.4.6 Disclosure pursuant to judicial or administrative process

No stipulation.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

No stipulation.

9.6 Representations and warranties

9.6.1 CA representations and warranties

By issuing a Certificate, the Provider makes the warranties listed herein to the following Certificate Beneficiaries:

- The Subscriber that is a party to the Subscriber Agreement or Terms of Use for the Certificate;
- All Application Software Suppliers with whom the Root CA has entered into a contract for inclusion of its Root CA Certificate in software distributed by such Application Software Supplier; and
- All Relying Parties who reasonably rely on a Valid Certificate.

The Provider represents and warrants to the Certificate Beneficiaries that, during the period when the Certificate is valid, the Provider has complied with this CP and/or CPS in issuing and managing the Certificate.

The Certificate Warranties specifically include, but are not limited to, the following:

1. Right to Use Mailbox Address: That, at the time of issuance, the Provider:
   i. implemented a procedure for verifying that the Applicant either had the right to use, or had control of, the Mailbox Addresses listed in the Certificate's subject field and *subjectAltName* extension (or was delegated such right or control by someone who had such right to use or control);
   ii. followed the procedure when issuing the Certificate; and
   iii. accurately described the procedure in the Provider 's CP and/or CPS;
2. Authorization for Certificate: That, at the time of issuance, the Provider:
   i. implemented a procedure for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
   ii. followed the procedure when issuing the Certificate; and
   iii. accurately described the procedure in the Provider 's CP and/or CPS;
3. Accuracy of Information: That, at the time of issuance, the Provider:
   i. implemented a procedure for verifying the accuracy of all of the information contained in the Certificate (with the exception of the *"subject:serialNumber"* attribute);
   ii. followed the procedure when issuing the Certificate; and
   iii. accurately described the procedure in the Provider 's CP and/or CPS;

4. Identity of Applicant: That, if the Certificate contains Subject Identity Information, the Provider:
   i. implemented a procedure to verify the identity of the Applicant in accordance with Section 3.2 and Section 7.1.4.2.2 ;
   ii. followed the procedure when issuing the Certificate; and
   iii. accurately described the procedure in the Provider 's CP and/or CPS;
5. Subscriber Agreement: That, if the Provider and Subscriber are not Affiliated, the Subscriber and Provider are parties to a legally valid and enforceable Subscriber Agreement that satisfies these Requirements, or, if the Provider and Subscriber are the same entity or are Affiliated, the Applicant Representative acknowledged the Terms of Use;
6. Status: That the Provider maintains a 24 x 7 publicly-accessible Repository with current information regarding the status (Valid or Revoked) of all unexpired Certificates; and
7. Revocation: That the Provider will revoke the Certificate for any of the reasons specified in these Requirements.

9.6.2 RA representations and warranties

No stipulation.

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.);

Customer or Certificate Holder comply with all provisions regarding commitments and warranties as stated in Terms of Use [8].

Prior to the issuance of a Certificate, the Provider shall obtain, for the express benefit of the Provider and the Certificate Beneficiaries, either the Applicant's:

- Agreement to the Subscriber Agreement with the Provider; or
- Acknowledgement of the Terms of Use [8].

The Provider shall implement a process to ensure that each Subscriber Agreement or Terms of Use is legally enforceable against the Applicant. In either case, the Agreement shall apply to the Certificate to be issued pursuant to the Certificate Request. The Provider MAY use an electronic or "click-through" Agreement provided that the Provider has determined that such agreements are legally enforceable. A separate Agreement MAY be used for each Certificate Request, or a single Agreement MAY be used to cover multiple future Certificate Requests and the resulting Certificates, so long as each Certificate that the Provider issues to the Applicant is clearly covered by that Subscriber Agreement or Terms of Use.

The Subscriber Agreement or Terms of Use shall contain provisions imposing on the Applicant itself (or made by the Applicant on behalf of its principal or agent under a subcontractor or hosting service relationship) the following obligations and warranties:

- Accuracy of Information: An obligation and warranty to provide accurate and complete information at all times to the Provider, both in the Certificate Request and as otherwise requested by the Provider in connection with the issuance of the Certificate(s) to be supplied by the Provider;
- Protection of Private Key: An obligation and warranty by the Applicant to take all reasonable measures to assure control of, keep confidential, and properly protect at all times the Private Key that corresponds to the Public Key to be included in the requested Certificate(s) (and any associated activation data or device such as a password or token);
- Acceptance of Certificate: An obligation and warranty that the Subscriber will review and verify the Certificate contents for accuracy;
- Use of Certificate: An obligation and warranty to use the Certificate only on MailBox Addresses listed in the Certificate, and to use the Certificate solely in compliance with all applicable laws and solely in accordance with the Subscriber Agreement or Terms of Use;
- Reporting and Revocation: An obligation and warranty to:
  i. promptly request revocation of the Certificate, and cease using it and its associated Private Key, if there is any actual or suspected misuse or compromise of the Subscriber's Private Key associated with the Public Key included in the Certificate, and
  ii. promptly request revocation of the Certificate, and cease using it, if any information in the Certificate is or becomes incorrect or inaccurate;
- Termination of Use of Certificate: An obligation and warranty to promptly cease all use of the Private Key corresponding to the Public Key included in the Certificate upon revocation of that Certificate for reasons of Key Compromise.
- Responsiveness: An obligation to respond to the Provider's instructions concerning Key Compromise or Certificate misuse within a specified time period.
- Acknowledgment and Acceptance: An acknowledgment and acceptance that the Provider is entitled to revoke the Certificate immediately if the Applicant were to violate the terms of the Subscriber Agreement or Terms of Use, or if revocation is required by the Provider's CP and/or CPS.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

No stipulation.

9.8 Limitations of Liability

For delegated tasks to RA, the Provider and RA MAY allocate liability between themselves contractually as they determine, but the Provider shall remain fully responsible for the performance of all parties in accordance with this CP, as if the tasks had not been delegated.

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 [8] or according of requirements of this policy.

9.9 Indemnities

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

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

Notwithstanding any limitations on its liability to Subscribers and Relying Parties, the Provider understands and acknowledges that the Application Software Suppliers who have agreed to distribute the Root CA Certificate do not assume any obligation or potential liability of the CA under these Requirements or that otherwise might exist because of the issuance or maintenance of Certificates or reliance thereon by Relying Parties or others. Thus, except in the case where the Provider is a government entity, the Provider shall defend, indemnify, and hold harmless each Application Software Supplier for any and all claims, damages, and losses suffered by such Application Software Supplier related to a Certificate issued by the Provider, regardless of the cause of action or legal theory involved. This does not apply, however, to any claim, damages, or loss suffered by such Application Software Supplier related to a Certificate issued by the CA where such claim, damage, or loss was directly caused by such Application Software Supplier's software displaying as not trustworthy a Certificate that is still valid, or displaying as trustworthy:

(1) a Certificate that has expired, or

(2) a Certificate that has been revoked (but only in cases where the revocation status is currently available from the CA online, and the application software either failed to check such status or ignored an indication of revoked status).

9.10 Term and termination

9.10.1 Term

This version of CP is effective from the date of its entry into force, which is September 1, 2023 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 1.0, 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

No stipulation.

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 section 1.5.2. Such communication must include a description of the change, the reason for the change, and the contact details of the person requesting the change or suggesting the change respectively.

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

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

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

9.12.2 Notification mechanism and period

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

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

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

9.12.3 Circumstances under which OID must be changed

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

9.13 Dispute resolution provisions

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

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

9.14 Governing law

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

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

9.15 Compliance with applicable law

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

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

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

9.16.3 Severability

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

9.16.4 Enforcement

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

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

9.16.5 Force Majeure

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

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

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

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

9.17 Other provisions

No stipulation.