S/MIME Certificate Practice Statement Part: RA

Disig, a.s.

Version 1.0

Valid from September 1, 2023

OID 1.3.158.35975946.0.0.0.1.12

Content

Trade name	Disig, a.s.
Residence	Záhradnícka 151, 821 08 Bratislava
Registration	Business Register of the Municipal Court Bratislava III Section: Sa Insert No.: 3749/B
Telephone	+ 421 2 208 50 140
E-mail	disig@disig.sk

This document is a translation of the Slovak version of the document and has not undergone language editing. In the event of any inconsistency between Slovak version and English version of this document, Slovak version takes precedence over English version of this document.

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

.

1. INTRODUCTION

This document defines the S/MIME Certificate Practice Statement Part: Registration Authority (hereinafter referred to as "CPS") 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, Sa, insert no. 3794/B, as a Trusted Service Provider (hereinafter referred to as "Provider"). This CPS is based on the document "Certificate Policy (CP SMIME)“ (OID=1.3.158.35975946.0.0.0.1.11) [1] of the Provider. The current CP SMIME version to which this CPS is linked is Version 1.0 with effective date from September 1, 2023.

The Provider's web site for the provided trusted services is available at

https://eidas.disig.sk.

1.1 Overview

This CPS defines the creation and management of public key certificates (X.509 version 3), according to Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280) [2]; Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME [3]; and EU Regulation No. 910/2014 [4].

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

This CPS is structured in accordance with RFC 3647 [5].

1.2 Document Name and Identification

Document Name	S/MIME Certificate Practice Statement Part: RA
Name abbreviation	CPS RA SMIME CA Disig*
Version:	1.0
Approved on:	August 28, 2023
Valid from:	September 1, 2023
This document is assigned an object identifier (OID):	1.3.158.35975946.0.0.0.1.12

* in this document, only the abbreviated form CPS 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

1.3.158.35975946.0.0.0.1.12 - CPS RA SMIME CA Disig

1.2.1 Revisions

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

1.3 PKI Participants

1.3.1 Certification Authorities

See section 1.3.1 CP SMIME.

1.3.2 Registration Authorities

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

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

Provider may establish following types of RA:

- Commercial RA - is intended to mediate selected trustworthy services of the Provider to the general public and is operated by a third party, on the basis of a written agreement with the Provider;
- 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 delegated 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 requirements in section 1.3.2.1 CP SMIME.

1.3.3 Subscribers

See section 1.3.3 CP SMIME.

1.3.4 Relying Parties

See section 1.3.4 CP SMIME.

1.3.5 Other Participants

See section 1.3.5 CP SMIME

1.4 Certificate Usage

1.4.1 Appropriate Certificate Uses

See section 1.4.1 CP SMIME.

1.4.2 Prohibited Certificate Uses

See section 1.4.2 CP SMIME.

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 CP SMIME).

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

Certification Authority CA Disig	
Address:	Záhradnícka 151, 821 08 Bratislava 2
E-mail:	caoperator@disig.sk
Phone:	+421 2 20850140
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 CP SMIME).

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.

CPS is published and available to relaying parties at the web site of Provider: https://eidas.disig.sk/en/provider/policies-and-documents/ .

1.6 Definitions and Acronyms

1.6.1 Definitions

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; [4] ;

Advanced electronic signature means an electronic signature, which meets the requirements set out in Article 26 of eIDAS Regulation; [4] ;

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 as defined in X.509 [6] 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	-	A DNS record that specifies the Certificate Authorities (CA), who can issue a specific domain name certificate.
CMA	-	Certificate Management Authority
CP	-	Certificate Policy
CPS	-	Certificate Practice Statement
CRL	-	Certification Revocation List
HSM	-	Hardware Security Modul
IČO	-	Organization identification number ,Organization Identifier
OID	-	Object Identifier
PKI		Public Key Infrastructure
PMA	-	Policy Management Authority
RA	-	Registration Authority
QSCD	-	Qualified Signature Creation Device
S/MIME	-	Secure MIME (Multipurpose Internet Mail Extensions)

1.6.3 Bibliography

[1] Certificate Policy, Disig a.s.

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

[3] Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME .

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

[5] RFC 3647 - Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework.

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

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

[8] CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.2.0.0.

[9] General Terms of Service for Trusted Services, Disig, a.s.

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

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

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The URL https://eidas.disig.sk is the Provider repository. The repository is publicly accessible to Certificate holders, Relying parties and the public.

2.2 Publication of information

The following information is available at the Providers repository on a 24x7 basis:

- Certificates issued in accordance with this CPS,
- 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 SMIME and this CPS,
- information on the outcome of a regular audit of the performance of the trusted services provided.

2.3 Time or frequency of publication

See section 2.3 CP SMIME.

2.4 Access controls on repositories

Through the technical and accepted organizational arrangements, the Provider protects any information stored in a repository that are not intended for public expansion. For this purpose, the exact rules included in the Provider's security project and related directives have been developed.

Publicly available information provided by the Provider's repository has a controlled access character.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

CA Disig only accepts PKCS # 10 or SPKAC request unless otherwise agreed with the customer.

3.1.2 Need for names to be meaningful

In general, CA does not assign distinguishing names in the sense of X.500 [7] (X.500 Distinguished Name, hereafter referred to as "Distinguished Name") for customer certificates.

Certificate applicants choose the distinguishing name they want to be on their certificate according to the requirements listed in section 7.1.4.2.2 CP SMIME.

3.1.3 Anonymity or pseudonym of subscribers

The use of pseudonyms, aliases and nicknames in S/MIME certificates issued by the Provider is not allowed.

3.1.4 Rules for interpreting various name forms

3.1.4.1 Non ASCII character substitution

See section 3.1.4.1 CP SMIME.

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 RA employee on behalf of the Provider will perform the authentication of all the identity attributes of the S/MIME certificate Subject and the control over the e-mail address according to the following requirements:

S/MIME 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.

Note: Mailbox Address will be listed in Subscriber Certificates using „*rfc822Name*“ in the „*subjectAltName*“ extension.

3.2.2.1 Validating authority over mailbox via domain

When issuing certificates of the "*sponsor-validated*" type for a contractual partner, where validation of individual e-mail addresses of applicants will not be performed, the RA verifies that the contractual partner has control over the domain name of the e-mail address to be used in the certificate.

Validation will be performed by the RA employee, in accordance with section 3.2.2.4.2 of the current version "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates" [8], by sending a random text string with a minimum length of 20 characters, which will contain uppercase, and lowercase letters, numbers and special characters. The generated random value will be send to an email address identified as a authorized contact for that domain at the Registrar (for example, for top level domain ".sk" it is whois.sk-nic.sk). Random value must be unique for each sent e-mail. Validation of the domain portion of the email address will be successful if the RA receives a confirmation email back from the authorized contact that will contain the sent random text string. The RA employee then archives the relevant email communication from the validation in electronic form.

3.2.2.2 Validating control over mailbox via email

Before the issuance of the Certificate, the RA Provider's employee must validate the ownership and control over the e-mail address included in the certificate request.

Validation is done through RA Client application by sending a random value to the email address found in the certificate request. The sending is done automatically after loading the profile for the S/MIME certificate and the corresponding certificate request to the RA Client application and choosing the option to verify the e-mail address (verify Email). After sending the Validation email, the Applicant has 24 hours to confirm the random value. The validation status is checked by the RA employee in the RA Client application in the "Search" menu and the "eMail Verification" tab. If the Validation is in the "approved" state, then the Validation of the e-mail address was successful.

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

The Provider does not support this method.

3.2.2.4 CAA records

No stipulation.

3.2.3 Authentication of organization identity

The RA employee complies with the following requirements 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;
- Unique identifier and type of identifier for the Legal Entity.

The unique identifier is the identifier included in the Certificate "*subject:organizationIdentifier*" as specified in Section 7.1.4.2.2 and Appendix A of [3].

3.2.3.2 Validation of organization identity

3.2.3.2.1 Verification of name, address, and unique identifier

The RA verifies the full legal name of the Applicant (legal entity) based in Slovak republic and the unique identifier according to:

- submitted original of company record from the Business Register of the Slovak Republic (https://www.orsr.sk/) (hereinafter referred to as "OR SR");
- in the case of an Applicant (legal entity) that is not registered in the OR SR, the name is verified by submitted original of company record from the Register of Legal Entities, Entrepreneurs and Public Authorities maintained

by the Statistical Office of the Slovak Republic (https://rpo.statistics.sk/) (hereinafter "RPO SR");

- if an Applicant (legal entity) does not have its seat in Slovak Republic, its identity is verified by submitting an extract from the register of the government agency in the jurisdiction of the creation, existence and therefore recognition of the legal entity. RA will then verify data through the website "Business registers - search for a company in the EU".

The original or an officially certified copy of the original of the submitted documents must not be older than three months. The document must contain the full business name or name and identification information.

The RA of the Provider also accepts the electronic form of the documents, that will be authorized by a qualified electronic seal of the state authority responsible for the register.

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.

3.2.3.2.3 Disclosure of verification sources

See section 3.2.3.2.1.

3.2.4 Authentication of individual identity

3.2.4.1 Attribute collection of individual identity

The RA of the Provider verifies the identity of the natural person on the basis of the submitted identification document, which must contain the following data of the Applicant:

- Full name and surname;
- Permanent residence;
- Birth registration number (applicants who have it assigned);
- Date of birth (applicants without birth registration number).

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.

3.2.4.1.2 From a digital identity document

No stipulation.

3.2.4.1.3 Using electronic identification schemes

No stipulation.

3.2.4.1.4 From a certificate supporting a digital signature applied by the

Applicant

No stipulation.

3.2.4.1.5 From Enterprise RA records

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

The Enterprise RA maintains 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 verifies 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 verifies 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, e.g. if a natural person represents another natural person, he must prove the identity of the principal by an officially verified power of attorney, from the text of which it is clear that the representing natural person was authorized by the principal to act in the given matter on his behalf, and which contains all the data mentioned in section 3.2.4.1.1.

3.2.4.1.8 From authorized reference sources as supplementary evidence

No stipulation.

3.2.4.2 Validation of individual identity

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

The passport and eID has an explicit validity period, the RA of the Provider verifies that the time of the identity validation is within this validity period. It means that the time of the identity validation is earlier than the date of expiry of an identity document.

The RA of the Provider may reuse existing evidence but no more than 825 days since completed validation of Individual identity.

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 employee makes 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 employee has access to authoritative sources of information on document appearance.

The RA of the Provider fills in the information system with the 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: type of the identity document, issuer, validity period, and the document's unique identification number.

3.2.4.2.2 Validation of a digital identity document

No stipulation.

3.2.4.2.3 Validation of eID

No stipulation.

3.2.4.2.4 Validation of digital signature with certificate

No stipulation.

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 Error! Reference source not found..

3.2.4.2.6 Validation using an Enterprise RA record

An Enterprise RA issuing a "Sponsor-validated" Certificate validates 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 and does not require identity document, on the condition that the internal records must contain all personal data required by the Provider and the data that will be recorded in the certificate.

3.2.5 Non-verified subscriber information

Subscriber information that has not been verified in accordance with this CPS and CP SMIME 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 uses a Reliable Method of Communication to verify the authority of issuance of particular certificate type for natural person or legal entity.

3.2.7 Criteria for Interoperation

No stipulation.

3.2.8 Reliability of verification sources

The RA of the Provider relies on a source of verification as a Reliable Data Source. data to validate Certificate Requests,

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 relies upon a data of Applicants, which are send by contact person of contractual partner. This contact person is listed in signed contract of trust services.

The RA of the Provider uses a Reliable Method of Communication to contact the sender and to confirm the Attestation is authentic.

The RA of the Provider relies also upon a data, which are officially authorized in accordance with the applicable legislation.

3.3 Identification and authentication for re-key request

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 requests

No stipulation.

4. CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

See section 4.1.1 CP SMIME.

4.1.2 Enrollment process and responsibilities

4.1.2.1 Preparation

See section 4.1.2.1 CP SMIME.

4.1.2.2 Request generation

4.1.2.2.1 Certificate Request generation

See section 4.1.2.2.1 CP SMIME.

4.1.2.3 Sending a certificate request

See section 4.1.2.3 CP SMIME.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Before issuing the certificate, the RA of the Provider performs in RA Client application:

- checking whether the e-mail address specified in the certificate request corresponds to the e-mail address from which the request was sent,
- checking the completeness and correctness of the data in the received certificate application, whether it contains only permitted items in the sense of section 7.1.4.2.2 CP SMIME,
- verification of ownership and control over the Applicant's e-mail address in accordance with section 4.2.1.1,
- checking whether the verification of ownership of the Applicant's e-mail address was successful and a certificate can be issued.

During a personal visit of the Applicant or a person authorized by him RA employee:

- informs the person about the General Conditions [9],
- verifies the identity of the future Certificate Holder in accordance with section 3.2.4.2 and enters his personal data into the Provider's IS through the RA Client application, filling in all mandatory items required by the Provider's system,

- verifies other documents to validate any identification data to be included in the certificate, e.g. the identity of the organization in accordance with section 3.2.3.2.

In case of detected discrepancies, it may refuse to issue a certificate.

When verifying the identity of a natural person or legal entity, it is possible to use the existing validation of these identities as long as they meet the deadlines given in section 4.2.1.3 or 4.2.1.2.

4.2.1.1 Validation of mailbox authorization or control

Completed validation of the mailbox control in accordance with Section 3.2.2.2 SHALL be obtained no more than 30 days prior to issuing the Certificate. If the RA employee finds that the existing verification is older than 30 days, he must perform a new validation of ownership and control of the e-mail address.

Completed validation of the mailbox control in accordance with Section 3.2.2.1 SHALL be obtained no more than 398 days prior to issuing the Certificate. If the RA employee finds that the existing verification is older than 398 days, he must perform a new validation of ownership and control of the e-mail domain.

4.2.1.2 Authentication of organization identity

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

Validation of authority in accordance with Section 3.2.6 can 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.

If the RA employee finds that the existing verification is older than 825 days, he must perform a new validation of organization identity.

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.

If the RA employee finds that the existing verification is older than 825 days, he must perform a new validation of Individual identity.

4.2.2 Approval or rejection of certificate applications

The certificate request shall be processed by the RA personnel immediately upon receipt in accordance with the procedures set out in section 4.2.1 . The certificate will be issued if all conditions for issuance are met.

RA personnel rejects a certificate request if he has reasonable doubts about the identity of the customer and identifies deficiency in identity papers, if customer provide incomplete information, or if the provider has previously issued a public key certificate on submitted request.

4.2.3 Time to process certificate issuance

No stipulation.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

See section 4.3.1 CP SMIME.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Subscriber (certificate holder) is immediately notified once the certificate is issued, by sending an e-mail message directly from the CA management system to the e-mail address included in the Certificate.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The issued certificate is available for download via the Provider's repository at

https://eidas.disig.sk/en/provider/certification-authority/certificate-search/

The link with the address from which the Subscriber can directly download issued certificate is send within the notification email.

4.4.2 Publication of the certificate by the CA

Each issued certificate is published in the Provider's repository immediately after issue, unless Customer / Applicant has been agreed not to disclose it.

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 CP SMIME, items 2 and 4.

4.5.2 Relying party public key and certificate usage

No stipulation.

4.6 Certificate renewal

See section 4.6 CP SMIME.

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

See section 4.7 CP SMIME.

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 RA of the Provider revokes the certificate if it has relevant information that the relationship between the entity and its public key defined in the certificate is no longer considered valid.

4.9.1.1 Revocation of the Customer / Holder's certificate

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

- The Subscriber/Subject requests in writing 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").

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

See section 4.9.2 CP SMIME.

4.9.3 Procedure for revocation request

See section 4.9.3 CP SMIME.

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 relying parties.

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 when 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. CP SMIME.

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

See section 4.9.6 CP SMIME.

4.9.7 CRL issuance frequency

No stipulation.

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

OCSP responses and service is managed in accordance with RFC 6960 [10] . OCSP responses are signed by:

- an OCSP Responder whose Certificate is signed by the CA that issued the Certificate whose revocation status is being checked.

The OCSP signing Certificate contains 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 [10].

4.9.10 On-line revocation/status checking availability

No stipulation.

Providers's OCSP responders support the HTTP GET method, as described in RFC 6960 [10] and/or RFC 5019 [11].

For the status of S/MIME Certificates:

- OCSP responses have a validity interval greater than or equal to eight hours;
- OCSP responses have a validity interval less than or equal to eight days;
- The provider updates the information provided through OCSP immediately after the certificate status changes in the database system.

For the status of Subordinate CA Certificates, the CA updates 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 does not respond with a "*good*" status.

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

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

See section 4.9.12 CP SMIME.

4.9.13 Circumstances for suspension

See section 4.9.13 CP SMIME.

4.9.14 Who can request suspension

See section 4.9.14 CP SMIME.

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 current CRL is available at the Provider's Web site (See section 1) and is accessible through the HTTP protocol on port 80.

The OCSP service is available at the URL specified in the issued certificate.

Revoked certificates are not removed from CRL or OCSP response.

4.10.2 Service availability

The Provider operates and maintains 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 are available in 24x7 mode.

OCSP is 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

See section 4.12.1 CP SMIME.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical security controls

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

No stipulation.

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

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

5.1.7 Waste disposal

See section 5.1.7 CP SMIME.

5.1.8 Off-site backup

No stipulation.

5.2 Procedural controls

5.2.1 Trusted roles

Within CA, the trusted roles responsible for each aspect of the trusted service are defined, and the duties of each role are defined in the contract with the RA.

5.2.2 Number of Individual Required per Task

No stipulation.

5.2.3 Identification and authentication for each role

Each role has a defined method of identification and authentication when accessing the Provider's IS.

Access by the RA personnel to the Provider's IS through the RA Client application, which is created by the Provider. RA employee is authenticated when accessing RA Client application by his certificate. The certificate is issued by the Provider and key pair is stored in smart card (USB token).

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

Personnel of external RA is authorized to perform RA duties by executive management of the legal entity. The contract must be signed between the Provider and legal entity.

Personnel of internal RA are appointed to the role by the Provider's executive management.

5.3.1 Qualifications, experience, and clearance requirements

See section 5.3.1 CP SMIME.

5.3.2 Background check procedures

See section 5.3.2 CP SMIME.

5.3.3 Training requirements and Procedures

Every RA personnel must go through compulsory training, prior to performing his / her function, by the Provider's authorized staff.

5.3.4 Retraining frequency and requirements

The frequency of training for RA personnel is defined in the internal directive "RA Life Cycle".

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

See section 5.3.6 CP SMIME.

5.3.7 Independent Contractor Controls

See section 5.3.7 CP SMIME.

5.3.8 Documentation supplied to personnel

See section 5.3.8 CP SMIME.

5.4 Audit logging procedures

5.4.1 Types of events recorded

No stipulation.

5.4.2 Frequency for Processing and Archiving Audit Logs

No stipulation.

5.4.3 Retention Period for Audit Log

No stipulation.

5.4.4 Protection of Audit Log

No stipulation.

5.4.5 Audit Log Backup Procedures

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

No stipulation.

5.5 Records archival

5.5.1 Types of records archived

No stipulation.

5.5.2 Retention period for archive

No stipulation.

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 Archiving collection system

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

No stipulation.

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 RA termination

No stipulation.

6. TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 CA key pair generation

No stipulation.

6.1.1.2 Registration authority

No stipulation.

6.1.1.3 End users

RA of the Provider rejects 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 CP SMIME and/or Section 6.1.6 CP SMIME;
- 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 CP SMIME.

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

6.1.2 Private Key delivery to subscriber

No stipulation.

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

See the section 6.1.5 CP SMIME.

6.1.6 Public key parameters generation and quality checking

See the section 6.1.6 CP SMIME.

6.1.7 Key usage purposes

No stipulation.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

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

No stipulation.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key transfer into or from a cryptographic module

No stipulation.

6.2.7 Private Key storage on cryptographic module

No stipulation.

6.2.8 Method of Activating Private Keys

No stipulation.

6.2.9 Method of Deactivating Private Keys

No stipulation.

6.2.10 Method of Destroying Private Keys

No stipulation.

6.2.11 Cryptographic Module Capabilities

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

See section 6.3.2 CP SMIME.

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 has implemented multi-factor authentication for all accounts capable of directly causing certificate issuance.

6.5.2 Computer security rating

No stipulation.

6.6 Live cycle technical controls

6.6.1 System development controls

See section 6.6.1 CP SMIME.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Time-stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

7.1.1 Version number

No stipulation.

7.1.2 Certificate Content and Extensions; application of RFC 6818

No stipulation.

7.1.2.1 Root CA certificates

No stipulation.

7.1.2.2 Subordinate CA certificates

No stipulation.

7.1.2.3 Subscriber certificates

No stipulation.

7.1.2.4 All certificates

No stipulation.

7.1.3 Algorithm object identifiers

7.1.3.1 SubjectPublicKeyInfo

See section 7.1.3.1 CP SMIME.

7.1.3.1.1 RSA

See section 7.1.3.1.1 CP SMIME.

7.1.3.1.2 ECDSA

No stipulation.

7.1.3.1.3 EdDSA

No stipulation.

7.1.3.2 Signature AlgorithmIdentifier

See section 7.1.3.2 CP SMIME.

7.1.3.2.1 RSA

See section 7.1.3.2.1 CP SMIME.

7.1.3.2.2 ECDSA

No stipulation.

7.1.3.2.3 EdDSA

No stipulation.

7.1.4 Name Forms

No stipulation.

7.1.4.1 Name encoding

No stipulation.

7.1.4.2 Subject information - subscriber certificates

No stipulation.

7.1.4.2.1 Subject alternative name extension

Certificate field	Required/Optional	Contents
extensions:subjectAltName	SHALL be present	This extension will contain one *GeneralName* entry of the following type: Rfc822Name

7.1.4.2.2 Subject distinguished name fields

The Provider issues these types of S/MIME 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 dogotal 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 will contain one of the following values verified in accordance with Section 3.2.

Certificate type	Contents
Organization-validated	*subject:organizationName*
Sponsor-validated	Personal Name
Individual-validated	Personal Name

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

The field will 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 CP SMIME.

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

No stipulation.

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

The field will contain a Registration Reference for a Legal Entity assigned in accordance to the identified Registration Scheme.

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

The Registration Scheme will 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.

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*.

The country code used in the Registration Scheme identifier will 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)"**

The field will contain a name of natural person verified according to section 3.2.4 in common form "name surname", separated by space.

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

No stipulation.

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

The field will contain a unique number associated with a Subscriber to distinguish each Subscriber.

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

The field will contain a single Mailbox Address as verified under Section 3.2.2.

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

No stipulation.

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

No stipulation.

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

The field will 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)"**

No stipulation.

m) **Certificate Field: "***subject:postalCode* **(OID: 2.5.4.17)"**

No stipulation.

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

The field will 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

No stipulation.

7.1.4.3.1 Subject distinguished name fields

No stipulation.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

See section 7.1.6 CP SMIME.

7.1.6.1 Reserved certificate policy identifiers

The following CA/Browser Forum Certificate Policy identifiers will be used 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

No stipulation.

7.1.6.3 Subordinate CA certificates

No stipulation.

7.1.6.4 Subscriber certificates

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

The Certificate will also contain CP SMIME policy identifier defined by the Provider in the form OID=1.3.158.35975946.0.0.0.1. as well as URI address, where the policy can be found.

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

No stipulation.

7.3 OCSP profile

7.3.1 Version number

No stipulation.

7.3.2 OCSP extensions

No stipulation.

8. COMPLIANCE AUDIT AND OTHER ASSESSMENTS

No stipulation.

8.1 Frequency or circumstances of assessment

No stipulation.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

No stipulation.

8.6 Communication of results

No stipulation.

8.7 Self-Audits

During the period in which the Provider issues Certificates, the Provider will monitor adherence to its CP SMIME and this CPS 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

No stipulation.

9.1.1 Certificate issuance or renewal fees

No stipulation.

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

No stipulation.

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

No stipulation.

9.4.2 Information treated as private

No stipulation.

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

No stipulation.

9.4.5 Notice and consent to use private information

No stipulation.

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

See section 9.6, CP SMIME.

9.6.1 CA representations and warranties

See section 9.6.1 CP SMIME.

9.6.2 RA representations and warranties

No stipulation.

Refer to the section 0.

9.6.3 Subscriber representations and warranties

See section 9.6.3 CP SMIME.

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

No stipulation.

9.9 Indemnities

No stipulation.

9.10 Term and Termination

9.10.1 Term

This version of the CPS is effective from the date of its entry into force i.e. September 1, 2023 until it is replaced by a new version. For details on the history of changes to this CPS, refer to section 1.2.1 **"**Revisions**".**

9.10.2 Termination

Validity of this CPS will expire on publication of a new version with a higher number than 1.0, or termination of the trusted service provision by the Provider at the time of validity.

9.10.3 Effect of termination and survival

In the event that this document is not replaced by a new version and during its validity the Provider terminated providing of trusted services, all provisions of these CPS regarding 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

Updates to the CPS are based on their review, which is done at least once a year from the approval of the current valid version. The review is carried out by a designated person of Provider who, based on the results of the review, prepares a written proposal for any proposed changes.

Approval of the proposed changes shall be carried out by the designated PMA member. Proposed changes must be assessed within 14 days of their delivery. After the deadline set for the assessment of the change proposal, the PMA must accept, accept with modification, or reject the proposed change.

Errors, update requests, or proposed changes to the CPS must be communicated to the contact mentioned 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.

All approved CPS changes shall be notified to the entities concerned within one week prior to their entry into force through the channels of the publication and notifying policy.

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

Repairs to mistyping, grammatical and stylistic errors are not considered as initiating changes to the version of this CPS.

9.12.2 Notification mechanism and period

The Provider publishes CPS-related information through its web site

https://eidas.disig.sk/en/provider/policies-and-documents/

The Authorized Representative of the Provider shall inform all of the contractually bound RAs of the Provider about the approval of the new version of the CPS, by sending a new version by e-mail.

The current version of the CPS is available at every contractual RA of the Provider, at least in electronic form. Internal employees are informed of the new version of this CPS.

9.12.3 Circumstances under which OID must be changed

No stipulation.

9.13 Dispute resolution provisions

No stipulation.

9.14 Governing law

No stipulation.

9.15 Compliance with applicable law

See section 9.13 CP SMIME.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

No stipulation.

9.16.4 Enforcement

No stipulation.

9.16.5 Force Majeure

No stipulation.

9.17 Other provisions

No stipulation.