Certificate Practice Statement for issuing TLS certificates Part: Registration Authority

Disig, a.s.

Version 6.3

Valid from January 10, 2025

OID 1.3.158.35975946.0.0.0.1.3

Content

Trade name	Disig, a.s.
Residence	Galvaniho 17/C, 821 04 Bratislava
Registration	Business Register of the City Court Bratislava III Section: Sa Insert No.: 3749/B
Telephone	+ 421 2 208 50 140
E-mail	disig@disig.sk

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

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

.

1. INTRODUCTION

This document defines providing a trusted service for the creation and verification of TLS certificates - part: RA (Certificate Practice Statement, hereinafter referred to as "CPS") for the registration authorities (hereinafter referred to as "RA") of Disig, a.s., Galvaniho 17/C, 821 04 Bratislava as a provider of trusted services (hereinafter referred to as "Provider"). This CPS are based on the document "Certificate Policy (CP CA Disig)“ (OID=1.3.158.35975946.0.0.0.1.1) [1] of the Provider. The current CP CA Disig version to which these CPSs are linked is Version 6.3 with effective date from January 10, 2025.

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

https://eidas.disig.sk.

1.1 Overview

CPSs were created based on Internet X.509 Public Key Infrastructure Materials (RFC3647) [2]; Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280) [3]; Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates [4], requirements of individual programs for root certificates distributed by Microsoft [5], Mozilla [6], Apple [7], Google [8] and EU Regulation No. 910/2014 [9].

The Provider confirms that these CPSs take into account all the requirements of the document [4], which is published at http://www.cabforum.org. In the event of any inconsistency between these requirements and these CPS, the requirements of the current version of the document [4] shall prevail.

This practice statement is structured in accordance with RFC 3647 [2].

1.2 Document Name and Identification

Document Name:	**Certificate Practice Statement for issuing TLS certificates Part: Registration Authority**
Name abbreviation:	**cps_ra_cadisig_en**.pdf
Version:	**6.3**
Approved on:	**December 31, 2024**
Valid from:	**January 10, 2025**
This document is assigned an object identifier (OID):	**1.3.158.35975946.0.0.0.1.3**

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.**3** – **cps_ra_cadisig_en**.pdf

This CPS is related to publicly trusted certificates for Web site authentication (TLS certificate) issued by the Provider.

Unless it is expressly stated in the rules that it refers to the certificate of the root certification authority or subordinate certification authority, so the word "certificate" means the TLS certificate of the end entity.

1.2.1 Revisions

Revision	Revision date	Description; Reviewer
1.0	March 25, 2006	First version; Miškovič
1.5	December 20, 2006	Formal text editing - Formatting, correcting links, editing text in section 4 "Operational requirements"; Miškovič
2.0	January 23, 2007	CP expansion in relation to the new type of certificate issued for the contracted client. Addition of section 7 "Certificate Profiles"; Miškovič.
2.1	March 29, 2007	Correcting text in chap. 2.8 and Chap. 4.9 Text editing related to a minor change in a partner's certificate; Miškovič
3.0	March 19, 2008	Overall revision of the CP for each type of certificate. Ďurišová, Miškovič

3.1	June 24, 2008	A new type of certificate adding.; Miškovič
3.2	November 10, 2008	Change certificate validity for domain user PKI VsZP Termination of operation at Záhradnícka 153; Miškovič
3.3	November 25, 2008	Editing the wording: section 3.1.9 - Domain ownership verification section 4.1.1; 4.1.2, - validation of the Applicant's e-mail address; Miškovič
3.4	Jun 2, 2009	Modification regarding the requirement for the minimum length of the public key to be issued by CA Disig (section 5.1.3; 6.1.2); Change the email address location in the certificate profile (section 3.1.2; 6.1.2); Miškovič
4.0	October 10, 2009	Editing in connection with Mozilla Foundation requirements when applying for a CA Disig certificate to the Mozilla Root Certificate Store; Miškovič
4.1	May 11, 2010	Inclusion of proposed audit corrective actions of 13.11.2009 (audit according ETSI TS 102042 V1.3.4); Miškovič
4.2	March 3, 2011	Changing the validity of certificates; incorporating Mozilla Foundation's new security policy requirements and Microsoft code signing requirements; formal edits of tables and texts; Miškovič
4.3	January 25, 2012	Supplementing the possibility to issue certificate for subordinate CAs, adding signature algorithms, and regular annual review of content; Miškovič
4.4	June 22, 2012	Incorporating Requirements for the Baseline Requirements for Issuing and Managing Publicly-Trusted Certificates, v.1.0, issued by the CA / Browser Forum; Miškovič
4.5	August 15, 2013	Refining of CA Disig CA root CA Certificate Profile and other Certified Types of Certificates; Miškovič
4.6	June 21, 2013	Correction of the OID of the document - deleting the version of the document from the OID (section 1.2). Editing Profiles for subordinate CAs - certificate Policies Identifier (section 7.1.2); Enable issuing "wildcard" SSL certificates to be issued at the third level of the domain name (3.1.2); Miškovič
4.7	February 2, 2015	Z Inclusion of the requirements of the current version of the Baseline Requirements for the Issue and Management of Publicly-Trusted Certificates, v.1.2.3; Revision of the CP in connection with the amendment to the Electronic Signature Act, pursuant to Act no. 305/2013 Coll.; Miškovič
4.8	May 22, 2015	Verification of CAA records (4.1.5); Miškovič
4.9	October 10, 2016	Changes made in connection with the eIDAS Regulation and in connection with the expiry of Act no. 215/2002 Coll. and the entry into force of Act no. 272/2016 Z.z.; Inclusion of Baseline Requirements for Issuance and

		Management of Publicly-Trusted Certificates, to Version v.1.4.1; Miškovič
5.0	September 25, 2017	Conversion of CP to RFC 3647 format; Inclusion of eIDAS requirements and incorporation of the requirements of the current version of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.5.2; Miškovič
5.1	May 23, 2018	Entry into force of Regulation no. 2016/679 - GDPR; Modification of the wording of point 3.2.2.4 (new verification method); addition of clause 4.2.2 (gTLD); Miškovič
5.2	May 17, 2019	Document revision and modification as required [6], changes in 4.9.3; 5; 5.2; 5.3, 5.4 and 5.5; Miškovič
5.3	December 2, 2019	Document revision; Change of document titles related to the issue of certificates (4.2.1.2); Miškovič
5.4	September 1, 2020	Specification of domain ownership verification methods in section 3.2.2.4; Changing the titles of chapters according to their titles in [4]; Miškovič
5.5	May 1, 2021	Addition of the person responsible for reporting incidents (2.2); Miškovič
5.6	June 18, 2021	Update wording of section 3.2.2.4.
5.7	May 20, 2022	Change the TLS / SSL certificate type designation to TLS; Additions and modifications in section 5.4 concerning record keeping; Miškovič
5.8	October 1, 2022	Change in connection with the requirement of publishing revocation reason in CRL when revoking issued TLS certificates (4.9.3); Miškovič
5.9	September 1, 2023	Changes in connection with the entry into force of "Baseline Requirements for the Issuance and Management of Publicly-Trusted S/MIME Certificates"; Miškovič
6.0	February 1, 2024	Allocation of CP exclusively for the policy of issuing Publicly-Trusted TLS Certificates; Miškovič
6.1	July 18, 2024	Change of headquarters of Disig, a.s.
6.2	August 15, 2024	Extension of domain verification methods by DNS Change method in accordance with TLS Baseline Requirements section 3.2.2.4.7; Miškovič
6.3	January 10, 2025	Change in the methods used for domain validation as of 15.1.2025 (3.2.2.4); Multi-Perspective Issuance Corroboration (3.22.2.9); Miškovič

1.3 PKI Participants

1.3.1 Certification Authorities

These CPSs concern the provision of trustworthy services by subordinate CAs belonging under the CA Disig Root R2– See section 1.4.1CP CA Disig.

1.3.2 Registration Authorities

The components of the Provider detailed in these rules is:

- Internal Registration Authority

1.3.3 Subscribers

See section 1.3.3 CP CA Disig.

1.3.4 Relying Parties

See section 1.3.4 CP CA Disig.

1.3.5 Other Participants

See section 1.3.5 CP CA Disig

1.4 Certificate Usage

See section 1.4.1 CP CA Disig.

1.4.1 Appropriate Certificate Uses

See section 1.4.1 CP CA Disig.

1.4.2 Prohibited Certificate Uses

See section 1.4.2 CP CA Disig.

1.5 Policy administration

1.5.1 Organization Administering the Document

Provider	
Company:	**Disig, a. s.**
Address:	**Galvaniho 17/C, 821 04 Bratislava**
Company ID:	**359 75 946**
Phone:	**+421 2 20850140**
e-mail:	**disig@disig.sk**
Web site:	**http://www.disig.sk**

1.5.2 Contact Person

The contact person responsible for the operation of the Provider's registration authorities is:

Registration Authority	
Address:	**Galvaniho 17/C, 821 04 Bratislava**
E-mail:	**radisig@disig.sk**
Phone:	**+421 2 20850140**
Web site:	**http://eidas.disig.sk/**
Incident reporting:	**tspnotify@disig.sk** see more at: **https://eidas.disig.sk/pdf/incident_reporting.pdf**

1.5.3 Person Determining CPS Suitability for the policy

See section 1.5.3 CP CA Disig.

1.5.4 CPS approval procedures

These CPSs are approved by a person appointed as PMA.

CPS are published in accordance with the Publishing and Notification Policy at the Provider's website (See section 1).

1.6 Definitions and Acronyms

1.6.1 Definitions

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

1.6.2 Acronyms

CP	-	Certificate Policy
CPS	-	Certificate Practice Statement
CA	-	Certification Authority
OID	-	Object Identifier
PKI		Public Key Infrastructure
PMA	-	Policy Management Authority
RA	-	Registration Authority
CRL	-	Certification Revocation List
HSM	-	Hardware Security Module
CMA	-	Certificate Management Authority
IČO	-	Organization identification number

SSL	-	Secure Sockets Layer
TLS	-	Transport Layer Security
SWACA	-	Certification Authority software

1.6.3 Bibliography

[1] *Certificate Policy, Disig a.s.*

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

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

[4] ***CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v.2.1.2.***

[5] ***Microsoft Trusted Root Program.***

[6] ***Mozilla Root Store Policy, Version 2.9, Effective September 1, 2023.***

[7] ***Apple Root Certificate Program platný od 15.8.2023.*** **s.l. : https://www.apple.com/certificateauthority/ca_program.html.**

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

[9] ***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 as amended by Regulation 1183/2024.***

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

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

[12] 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.

[13] ***CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates v. 2.1.2.***

2. PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The Providers web site the URL of which is listed in Section 1 has a repository function. The repository is publicly accessible to Certificate holders, Relying parties and the public at all.

2.2 Publication of information

See section 2.2 CP CA Disig.

If the conditions set by the current "Mozilla Root Store Policy" [6] are not complied with, the Manager of the Provider's certification authority appointed to the role of PMA shall reporting the incident.

2.3 Time or frequency of publication

The certificate is published as soon as it is issued, and the Customer / Certificate Holder can download it immediately. Information about the issued certificate is available in the Provider's repository. – See section 2.1.

CRLs are published as specified in 4.9.8. Information about the revoked certificate can be found in the Provider's repository.

All information in the repository is published as soon as possible after its creation (issuing, revocation, etc.).

2.4 Access controls on repositories

Through the technical and accepted organizational arrangements, the Provider protects any information stored in a repository that is 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

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

3.1.1 Types of names

No stipulation.

3.1.2 Need for names to be meaningful

No stipulation.

3.1.3 Anonymity or pseudonym of subscribers

No stipulation.

3.1.4 Rules for interpreting various name forms

See section 3.1.4 CP CA Disig.

3.1.5 Uniqueness of names

No stipulation.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove Possession of private key

No stipulation.

3.2.2 Authentication of Organization and Domain Identity

3.2.2.1 Authentication of identity

For a Customer / Holder requesting a certificate for a legal entity, the RA checks the submitted documents proving the existence of the legal entity. This is usually an extract from the commercial register or, another equivalent extract from another officially valid register of legal entities.

Documents submitted must be either original or officially authenticated copies of the original, maximum three months old. The document must include the full business name or name, identification (usually IČO), seat, name (s) of the person

(s) acting as legal person, and manner of proceedings and signing for the legal entity.

If the legal person is not domiciled in the Slovak Republic, its identity is verified in the same manner as above. An extract from the current register of legal entities must be officially translated into the Slovak language (except for organizations based in the Czech Republic).

Natural persons, who acting on the RA on behalf of the legal entity must prove their identity according to section 3.2.4.

Only authorized person of the user can act on behalf of a legal entity on the RA i.e., the person who is its statutory representative (or more of these persons at the same time, if required by the extract from the commercial register), or the legal entity may be represented by a natural or other legal entity.

If a legal entity is represented in the RA, the natural or legal person acting on its behalf must always submit for inspection a verified extract from the commercial register of a legal entity not older than three months.

If a legal authorize a natural person to act on its behalf on RA, that person must prove his identity under section 3.2.4. In addition, shall prove himself with an officially verified (notary or registered) power of attorney from whose text it is clearly clear that a representative was empowered by a legal person to act on the matter on its behalf.

If a legal entity authorizes another legal entity to act on its behalf on the RA, that legal representative, apart from relevant power of attorney (see the previous paragraph), must prove its identity in the same way as the represented legal entity as required above.

A subject (natural or legal person) representing a legal person may not in any case be represented by another subject.

If a legal entity cannot prove its identity by a extract from commercial register (applies to non-business entities such as the municipality, the church, the civic association, the foundation, the state body, etc.), such legal person must also prove legally, in addition to his / her identity or "reason") of its existence (using and referring to a law or other regulation dealing with a subject of a given type, a charter, etc.).

3.2.2.2 DBA/Business name

If the content of the DBA / Business Name certificate is, the RA personnel verifies that the Customer / Holder has the right to use the given TBA / Business Name by translating one of the documents listed in section 3.2.2.2CP CA Disig.

3.2.2.3 Verification of Customer / Holder Country

When issuing a certificate where CountryName is country code, the RA personnel verifies the eligibility of connection between the country with the Customer / Holder based on information provided by the domain registrar / based on other documents submitted – See section 3.2.2.1 of these CPS.

3.2.2.4 Verifying Domain Name or Domain Control

The RA employee will verify the authorization for the domain or control over the domain by the method specified in the document [4] in section 3.2.2.4.2 resp. if this method cannot be used, it should alternatively use the method given in document [4] in section 3.2.2.4.15. The method specified in document [4] in section 3.2.2.4.2 or in section 3.2.2.4.15 may only be used until January 15, 2025.

From January 15, 2025, instead of the method specified in document [4] in section 3.2.2.4.2 or section 3.2.2.4.15, one of the methods specified in document [4] in section 3.2.2.4.13 or section 3.2.2.4.14 shall be used to verify domain authority or control over the domain.

In the case of verification in accordance with section 3.2.2.4.2 [4], the RA shall generate a random text string with a minimum length of 20 characters using the KeePass software application, which shall contain uppercase and lowercase letters, numbers and special characters. The generated value will be emailed to an email address identified as a legitimate contact for that domain at the Registrar for, that domain (for example, for top level domain ".sk" it is whois.sk-nic.sk). The random value generated must be sent along with the TLS certificate's eligibility confirmation in the e-mail message returned from the email address to which the verification email was sent. Random value must be unique for each sent e-mail. If successful FQDN eligibility validation is performed in this way, the Provider can also issue other TLS certificates that end with the same FQDN at the second and higher level. The RA personnel then archives the appropriate email communication for the TLS certificates issued in electronic form. This method can also be used to validate the "wildcard" TLS certificate request for Web site authentication.

In the case of verification in accordance with section 3.2.2.4.15 [4], the RA employee verifies the legitimacy of the request for the issuance of a TLS certificate by the Customer by telephone. RA employee should call the phone number of the authorized contact that is listed as a legitimate contact for that domain to the Registrar for that domain (e.g., for a top-level domain ".sk" it is whois.sk-nic.sk). In the event that there is a person on the telephone contact other than the contact listed for the given domain, the RA employee must request a contact with the person who is the given contact. If there is an answering machine on the telephone contact, the RA employee will leave information on the answering machine with the content of a randomly generated value (see the procedure according to method 3.2.2.4.2 [4]) and a verified ADN (Authorization Domain Name). If successful FQDN validation is performed in this way, the RA employee shall make an electronic record of the telephone conversation with the telephone number to which it was made and the name of the person who confirmed the validity of the TLS certificate request. The RA employee will record a randomly generated value if the answering machine was on a telephone number and record the response to the message left. The provider can also issue other TLS certificates that end with the same FQDN at the second and higher level. This method can also be used to validate the "wildcard" TLS request.

In the case of verification pursuant to Section 3.2.2.4.13 [4], the RA employee shall generate a random text string of at least 20 characters long using the KeePass software application, which shall contain uppercase and lowercase letters, numbers and special characters. The value thus generated shall be sent via email

to the email address identified as the domain contact for the domain obtained from the DNS CAA record for the domain (the “contactemail” CAA record entry) being verified. The randomly generated value shall be sent together with confirmation of the eligibility of the TLS certificate application in a return email message from the email address to which the verification email was sent. The random value shall be unique for each email message sent. If the eligibility of the FQDN use is successfully validated in this manner, the Provider may also issue other TLS certificates that end with the same FQDN at the second and higher levels. The RA staff then archives the relevant email communication for the issued TLS certificates in electronic form. This method can also be used to validate the request for the issuance of a "wildcard" TLS certificate.

In the case of verification pursuant to Section 3.2.2.4.14 [4], the RA employee shall generate a random text string with a minimum length of 20 characters using the KeePass software application, which shall contain uppercase and lowercase letters, numbers and special characters. The value generated in this way is sent via email to the email address identified as the domain contact for the given domain - the DNS TXT entry on the "_validation-contactemail" subdomain of the validated domain. The randomly generated value must be sent together with confirmation of the eligibility of the TLS certificate application in a returned email message from the email address to which the verification email was sent. The random value must be unique for each email message sent. If the eligibility of the FQDN use is successfully validated in this way, the Provider may also issue other TLS certificates that end with the same FQDN at the second and higher levels. The RA staff then archives the relevant email communication for the issued TLS certificates in electronic form. This method can also be used to validate the request for the issuance of a "wildcard" TLS certificate.

We also have an automated domain ownership and validation method in accordance with section 3.2.2.4.7 [4], where a unique random value is sent by the system used to issue TLS certificates for each FQDN that is expected to be in the SAN of the issued TLS certificate, with the proviso that this unique random value must be entered in the DNS TXT record for each FQDN and at the same time must also be entered for all lower levels, up to the second level, of the given FQDNs. Subsequently, the CA system automatically checks the presence of the TXT value in the DNS records. Validation of a unique random value for a given FQDN will be used for validation within a maximum of 30 days from its submission. Validation data obtained using this method (3.2.2.4.7 [4]) can be used to validate ownership and control of the same FQDN if it is not older than 398 days.

3.2.2.5 IP Address Authentication

No stipulation.

3.2.2.6 Validation of a domain containing a "wildcard" character

An RA personnel will validate a request for a "wildcard" TLS certificate such way that check whether in the CN or SAN is a wildcard star ("*") located in the first position on the left and followed immediately by a dot (".").

An RA personnel will validate a request for a "wildcard" TLS certificate such way that check whether in the CN or SAN is a wildcard star ("*") located in the first

position on the left and followed immediately by a dot ("."). It also checks if a certificate is issued for a third and a higher level of domain and if the first level is only the national domain ".sk" i.e., an acceptable request must be a "wildcard" domain name for the third level "*.*domainname.sk*". Authentication of the domain authorization is done in the sense of the section 3.2.2.4.

3.2.2.7 Data source accuracy

RA personnel shall proceed according to section 3.2.2.7 of CP CA Disig before using any source as a trusted source.

3.2.2.8 CAA record

The RA personnel shall check the published CAA record before issuing a TLS certificate. If it finds that such a record exists, it may not issue the certificate unless it is confirmed that the certificate request complies with the relevant set of records in the CAA.

Verification of the record is made for each FQDN listed in the CN or SAN of the certificate request respectively in such a way that it proceeds in the name tree from the left to the right, to check the CAA record. If the request contains the FQDN in the form X.Y.X, the check is performed in the order X.Y.X -> Y.Z -> Z if Z is not the national level e.g., ".sk".

A written record containing all the FQDNs checked, and the result of the inspection is created.

3.2.3 Multi-Perspective Issuance Corroboration

See section 3.2.2.9 of CP CA Disig.

3.2.4 Authentication of individual identity

A natural person may be a citizen of the Slovak Republic or a foreign national.

A physical person must prove his / her identity with two of the following personal documents:

- ID card,
- passport,
- driving license,
- birth certificate,
- temporary residence permit (or permanent residence) in the case of an alien
- firearms license
- service card

It is required that at least one of the submitted documents be a document that includes the photograph of the person concerned. In case of submission of a birth certificate, a firearms card, or a service card, one of the following documents must also be presented: a citizen's card or a passport.

If a natural person represents another natural person at the RA, he must also prove himself with an officially authenticated (notarized or registered) power of attorney from whose text it is clearly clear that the representative natural person was empowered by the person empowered to act on the matter on his behalf.

If a legal entity represents a natural person except of a power of attorney (see the previous paragraph), the authorized legal person shall prove its identity under section 3.2.2.

3.2.4.1 Authentication of device or system identity

The CMA must also guarantee that the identity of the component and its public key are properly matched.

For the hardware or software component that will use certificates it is possible to create a TLS certificate. In this case, the component must be assigned to the natural or legal person (organization) administering it.

This person or organization is required to provide the RA with the following information:

- Device identification (name of the software component);
- The public key of the device (included in the certificate request);
- Device authorization and its attributes (if any should be included in the certificate);
- Contact details to enable the CMA to communicate with that person, if necessary.

The RA must authenticate the accuracy of any authorization (the value of the distinguishing name item) to be included in the certificate and verify those data.

Methods for performing this authentication and data control include:

- Verification of identity of the person in accordance with the requirements in section 3.2;
- Verifying the identity of the organization to which the component belongs, in accordance with the requirements of the section 3.2.2;
- Verifying the eligibility of the data to be listed in each certificate item, with an emphasis on the content of the item commonName.

The typical value of this entry will be a complete domain name.

The RA performs verification of all items in the subject of certificate.

3.2.4.2 Documents submitted

3.2.4.2.1 General

All documents submitted to RA by applicants must be either original or officially authenticated copies of the originals. There must be no information added, altered, overridden, and the like. Documents marked with a period of validity must be valid.

If a RA personnel has a doubt as to the identity of the potential customer (e.g., a clear mismatch between the photograph in the personal document submitted and

the customer's appearance, the inconsistency of the two documents submitted, etc.), he may refuse his registration.

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

At the request of a potential customer or an RA, any contingencies in identifying are dealt with in accordance with section 9.13.

Provided documents are required be the originals and a copy of the originals (they do not need to be authenticated), except personal documents identifying the applicant's identity, authorized person, serving for archiving for the needs of the Provider. Providing of the extract from the commercial register or a trade license respectively obtained from the Internet is not sufficient, since it is only informative and not applicable to legal acts.

3.2.4.2.2 Natural person

See section 3.2.3 CP CA Disig.

3.2.4.2.3 Natural person - employee

See section 3.2.3 CP CA Disig.

3.2.4.2.4 Legal person

See section 3.2.3 CP CA Disig.

3.2.4.3 Component or system

See section 3.2.3 CP CA Disig.

3.2.4.4 Checking the data on the submitted documents

In the event of any reasonable doubt as to the identity of the potential customer, the RA may refuse his registration. RA staff shall check on the submitted documents the following:

- Personal documents of natural persons:
  - The validity of the document submitted - in the case of an invalid personal document, proceed as if the personal document was missing - the RA registration refused;
  - The age of 18 years of age - RA refuses to register minors; the legal guardian (usually the parent) is entitled to act on behalf of minors
  - Whether there is no apparent discrepancy between the photograph in the personal document and the holder of the personal document - if so, the RA may refuse registration
  - Inconsistency of submitted documents i.e., whether the data on one document is inconsistent with the data on another document.
- Business Register Extracts:
  - Whether is not older than 3 months;
  - Whether natural persons (only one natural person, unless stated otherwise in the statement) who filed the statement, have the right to

act (sign) for the legal entity (i.e., whether they are its statutory representatives);

- Whether the statement is officially certified (notary or registrar) if it is not an original;

- Power of Attorney:
  - Whether the power of attorney is officially certified (notary or registrar);
  - Whether the data given in the power of attorney, which defines the representative of natural or legal person coincide with the data on the personal documents of natural person or with the information given on the statements from the commercial register of the legal entity respectively;
  - Scope of the power of attorney - i.e., whether the power of attorney entitles an authorized natural or legal person to the requested act on the RA on behalf of the empowered natural or legal person;
  - Whether the power of attorney is not limited in time or whether it contains another condition and whether it is fulfilled;
- Statutory declaration:
  - Authorization to sign - the person who signed the declaration is entitled to represent the legal person. Eligibility is checked according to commercial register or other registration of legal entities. If the person who will be signing is not enrolled in this statement, he must submit another document under which he may act for the company (usually a notarized power of attorney).

The type of documents submitted (such as an id card, passport) and the relevant data from them are recorded by the RA employee electronically into the CA information system.

In the case of found deficiencies in the submitted documents, submission of incomplete documents, the RA employee must refuse the applicant's registration. The issuing of certificate will be disapproved in this case.

An RA employee must also accept the documents submitted by the applicant in electronic form signed by a valid qualified electronic signature (listing with business register, power of attorney, statement, mandate, etc.).

3.2.4.5 Initial RA registration

Initial registration of a person in the RA role is done under the same conditions described above as in the case of the person requesting the personal certificate. Self-verification of the identity of the RA staff shall be performed by the Provider's staff unless otherwise agreed by the Provider.

3.2.5 Non-verified subscriber information

See section 3.2.4 CP CA Disig.

3.2.6 Validation of authority

See section 3.2.3.

3.2.7 Criteria for Interoperation or Certification

No stipulation.

3.3 Identification and authentication for re-key request

No stipulation.

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 CA Disig.

4.1.2 Enrollment process and responsibilities

4.1.2.1 Preparation

See section 4.1.2.1 CP CA Disig.

4.1.2.2 Request generation

See section 4.1.2.2 CP CA Disig.

4.1.2.3 Sending a certificate request

See section 4.1.2.3 CP CA Disig.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

4.2.1.1 Detailed procedure for obtaining a certificate

4.2.1.1.1 Preparation for a visit to RA

The customer will take the following steps:

- Shall be familiar with this procedure or with the principles and instructions for obtaining the certificate;
- Generates a certificate request (typically e.g., by Microsoft IIS or Apache / Openssl) and sends it electronically to RA (radisig@disig.sk) and, at the same time, stores it for backup purposes on a suitable portable medium;

Notes and Warnings: Please note that certificate request or a public key for that certificate has already been issued respectively cannot be used repeatedly to issue another certificate for safety reasons and will be refused to RA! A certificate request must include an appropriately filled subject: commonName (so-called entity name). Individual fields must be completed so that the values entered are consistent with this document, with emphasis on section 3.1.2, and uniquely identify the entity that will use the TLS certificate (typically the full domain name (FQDN)). If the item O (subject: organizationName) is filled in, the item L (subject: localityName) must also be filled in. If item O (subject: organizationName) is not filled in, item L (subject: localityName) must not be filled in.

The use of special characters (such as comma, hyphen, =, / and others) should be limited to the minimum required, and we recommend using these characters only after agreement with the Provider, otherwise the Provider reserves the right to reject this request.

- Will prepare the selected identity documents and other necessary documents, e.g., extract from business register (we recommend verifying the validity of documents) according to the provisions of section 3;

  Note: It is necessary for the customer will prepare copies (not necessarily verified) of all documents (other than personal documents of natural persons) which they intend to submit to the RA (e.g., extract from the commercial register and other documents about the legal entity, authorization etc.) to be able to submit this to the RA. The submission of an extract from the commercial register obtained from the Internet by the applicant is not sufficient, as this statement is merely informative and not applicable to legal acts.

  It is advisable for the customer to contact RA to verify before visiting the RA and clarify any doubts and problems, especially those relating to the suitability of the individual items in the certificate request.

- He / she will agree on the date of the RA visit (by phone, e-mail).

4.2.1.2 Procedure of the RA before issuing a certificate

Based on a pre-submitted application, RA personnel performs domain ownership verification within the meaning of section 3.2.2.4 and at the same time check the completeness and accuracy of the accepted certificate request. If RA personnel have seriously suspected of unauthorized use of any FQDN by Customer, it has the right to require the Customer shall demonstrate in a credible way that he/she may use given FQDN, otherwise RA may refuse to accept the TLS certificate request.

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 and if all the conditions for issue are met. If a request was, send by electronic means the certificate shall be issued immediately after verifying of all requirements. In case of need of a personal participation of the Customer / Holder, the issuing of the certificate shall take place on his/her personal participation, if all required documents are submitted.

RA personnel reject 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.

If the top-level domain (gTLD) specified in the certificate (e. g. ".ipsum") is unknown to the personnel, it must verify that it is in the "Root Zone Database" of the Internet Assigned Numbers Authority (IANA) (https://www.iana.org/domains/root/db). If it finds that the gTLD is not on the list, it refuses to issue the certificate.

RA personnel will not issue a TLS certificate for a request containing a domain name if, when verifying the CAA DNS record (see section 3.2.2.8 CP CA Disig), he finds that such a record exists and the Provider is not authorized to issue TLS certificates, in terms of its content, i.e. the record does not contain authorization in the form "disig.sk".

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 CA Disig.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The holder is notified of issuing the certificate by sending an e-mail message directly from the CA to the e-mail address given in the personal data of the Certificate Holder.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

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

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

in the notifying e-mail is the link with the address from which the Holder can directly download issued certificate or it is provided to him through an email message or by transferring it on a portable medium.

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 / Holder has 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

No stipulation

4.5.2 Relying party public key and certificate usage

No stipulation

4.6 Certificate renewal

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

No stipulation.

4.7.1 Circumstance for certificate re-key

No stipulation.

4.7.2 Who may request certification of a new public key

No stipulation.

4.7.3 Processing certificate re-keying requests

No stipulation.

4.7.4 Notification of new certificate issuance to subscriber

No stipulation.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

No stipulation.

4.7.6 Publication of the re-keyed certificate by the CA

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

See section 4.9.1 CP CA Disig.

4.9.1.1 Revocation of the Customer / Holder's certificate

See section 4.9.1.1 CP CA Disig.

4.9.2 Who can request revocation

See section 4.9.2 CP CA Disig.

4.9.3 Procedure for revocation request

The person requesting the certificate to be revoked must either undergo on the RA to the same authentication process as is required when the certificate holder first registration or must demonstrate by standing proof that he is an authorized person who may request the revocation of the certificate.

If the holder of the certificate is to be represented on RA in the case of the revocation of the certificate, the representative body shall submit the power of attorney (legalized by notary or registrar), from which it is clearly clear the certificate holder's wish to cancel his / her certificate. The representative body shall leave the power of attorney or a copy thereof (not necessarily verified) to RA. The RA will take over and retain this document; in the case of an unverified copy, it will compare it with the original and write the text "I'm confirming match with the original" with the date and signature.

RA personnel shall assess the eligibility of the certificate revocation request and, if it is clear that the applicant for revocation is not an authorized person, the RA may refuse the cancellation request.

RA personnel declines the request if the applicant fails to meet the authentication conditions (see sections 3.2.2 resp. 3.2.4).

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

In the case of request to revoke a certificate for any of the reasons listed in section 4.9.1.1 of the current CP CA Disig (keyCompromise (RFC 5280 CRLReason #1), privilegeWithdrawn (RFC 5280 CRLReason #9), cessationOfOperation (RFC 5280 CRLReason #5), affiliationChanged (RFC 5280 CRLReason #3) or superseded (RFC 5280 CRLReason #4) the RA must require the sending of a written request in accordance with section 4.9.3 of the current CP CA Disig.

4.9.4 Revocation request grace period

No stipulation.

4.9.5 Time within which CA must process the revocation request

See section 4.9.5 CP CA Disig.

Revocation is made no later than within 24 hours of the validation of rightfulness of the revocation request.

Upon receipt of a request for revocation of the certificate that the RA deems to be eligible (that is, which complies with the relevant provisions of these policies), the RA personnel inserts the received certificate revocation request into the Provider's information system through the RA Client application and perform full procedure of revocation.

After the certificate revocation, the provider will automatically send the e-mail notification of its certificate revocation to the holder as well as information on the reasons for his revocation.

4.9.6 Revocation checking requirement for relying parties

No stipulation.

4.9.7 CRL issuance frequency

No stipulation.

4.9.8 Maximum latency for CRLs

No stipulation.

4.9.9 On-line revocation/status checking availability

No stipulation.

4.9.10 On-line revocation/status checking availability

No stipulation.

4.9.11 Other forms of revocation advertisements available

No stipulation.

4.9.12 Special requirements re key compromise

No stipulation.

4.9.13 Circumstances for suspension

No stipulation.

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 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.

4.10.2 Service availability

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

OCSP is available in 24x7 mode.

Reporting problems with the certificate is available 24x7 at the address podpora@disig.sk.

4.10.3 Optional Features

No provisions.

4.11 End of subscription

No stipulation.

4.12 Key escrow and recovery

4.12.1 Key escrow and recovery policy and practices

No stipulation.

4.12.2 Session key encapsulation and recovery policy and practices

No stipulation.

5. FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical security controls

5.1.1 Site location and construction

Technological facilities in which the Provider's basic infrastructure is located are located in protected areas accessible only to authorized persons and separated from other areas by appropriate security features (security doors, grilles, fixed walls, etc.). The provider’s equipment consists only of equipment reserved for certification authority functions and does 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 are 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 is 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 is adequately supplied with electricity and air-conditioned and provide a reliable operating environment.

5.1.4 Water exposures

The spaces in which the Provider's equipment is located is located so that it is not endangered by water from any source.

5.1.5 Fire prevention and protection

The spaces in which the Provider's equipment is located are reliably protected from direct fire sources and from heat.

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

There is no environmental pollution from the waste arising from the operation of the Provider.

5.1.8 Off-site backup

In the event of irreversible damage to headquarters premises where infrastructure is provided, the Provider has a copy of all of the most important assets on the backup site that is geographically remote from the main site.

5.2 Procedural controls

When choosing a person to an RA personnel role the emphasis is on being accountable and trustworthy because this role requires credibility. The functions performed by this role are functions that form the basis of trust in the Provider on a personal level.

Any RA that works in accordance with these CPS complies with CPS.

The RA personnel responsibility is primarily:

- Verification of identity either through personal contact or through a representative entity;
- Recording information from certificate applicants and verifying their accuracy;
- Secure communication with the Provider;
- Communication to the Customer / Holder and documenting of a communication.

5.2.1 Trusted roles

Within CA, the trusted roles responsible for each aspect of the trusted service are defined, and the roles of each role are defined.

Persons selected for roles are responsible and trustworthy.

All persons in trusted roles engage without 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, is identified a number of individuals assigned to perform that task (rule K of N).

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.

5.2.4 Roles requiring separation of duties

Each role has criteria that take into account the need to separate functions from the role of i.e., there are roles that cannot be performed by the same individuals.

5.3 Personnel controls

Personal security measures are provided by internal mechanisms of a legal entity that has a contract with the Provider to provide its services through his registration authority.

Personnel for role RA personnel is selected based on reliability, loyalty, and credibility.

All RA personnel are properly instructed and trained to the extent necessary to perform the RA personnel's work and always have up-to-date versions of the Provider's Documents for the performance of the RA personnel's work, which are available at the Web site https://razona.disig.sk.

Access by the RA personnel to the Provider's IS through the RA Client application that RA uses for its operation is protected from unauthorized access by using RA's own RA certificate through which it is identified and authorized.

An important precautionary measure that significantly reduces the possibility of electronic identity abuse is that an RA key pair is stored on a smart card. Access to the private key stored on the card is password protected.

Other security mechanisms appropriate to the level of threat in the RA equipment environment are also used to protect RA equipment.

5.3.1 Qualifications, experience, and clearance requirements

Registration Authority roles meet the qualification requirements required for this role.

5.3.2 Background check procedures

For RA staff a security clearance is not required.

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. These trainings are mandatory for all types of RA (see section 1.3.2 CP CA Disig).

5.3.4 Retraining frequency and requirements

Repeating of RA staff training is based on a PMA decision and is performed when there are significant changes, whether in legislation or in the software of the RA workstations.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

Failure of any RA personnel whose result is a condition that is not in accordance with the provisions of this CPS and/or CP, whether it is negligence or malicious

intent, is subject to appropriate administrative and disciplinary proceedings by the Provider based on internal regulations or by the Providers existing contracts with external RAs

5.3.7 Independent Contractor Controls

No stipulation.

5.3.8 Documentation supplied to personnel

RA personnel have at their disposal the documents necessary for the performance of the function to which they are assigned, including a copy of this CPS and the CP and all technical and operational documentation necessary to maintain the integrity of the Provider's operations. This documentation is available on the special razona.disig.sk portal.

5.4 Audit logging procedures

5.4.1 Types of events recorded

All events related to operations performed in the RA Client application are recorded directly by the application. Likewise, all information sent from the RA Client application is recorded on the server side of the Service Provider.

5.4.2 Frequency for Processing and Archiving Audit Logs

No stipulation.

5.4.3 Retention Period for Audit Log

See section 5.4.3 CP CA Disig.

5.4.4 Protection of Audit Log

All records must be stored and protected on the RA in such a way so as not to impair their destruction.

5.4.5 Audit Log Backup Procedures

No stipulation.

5.4.6 Audit Log Accumulation System

The provider has a built-in log backup system.

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

RAs keep all records about issued certificates for the period specified in the relevant RA agreement and deliver them to the Provider at the intervals stipulated in the RA agreement.

The records are kept in paper form or in electronic form. All records that were submitted by the Customer / Holder at the issuing of required type of certificate (e.g., business listing, power of attorney, etc.) are also part of the retained records.

5.5.2 Retention period for archive

The Provider shall keep records in accordance with the requirement in Section 5.5.2 of CP CA Disig.

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

RA personnel can only use access keys to access the information system of Provider through "RA Client" application, sign operations in the "RA Client" application, and access the razona.disig.sk portal.

The RA personnel's access keys are regularly updated each year.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

In the event that the RA personnel's key is compromised, loss of the key, disclosure of access passwords, etc., this incident shall be immediately reported by the RA personnel to the Provider so that appropriate measures can be taken to minimize the possibility of misuse of access rights to the IS of the Provider.

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

No stipulation.

5.7.3 Recovery Procedures after Key Compromise

In the event of compromise on the RA personnel private key, the Provider shall immediately revoke the relevant certificate and revoke its authorization in it IS.

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 Certificate issuer

No stipulation.

6.1.1.2 Registration authority

Generating access keys and issuing authentication certificates for RA Personnel are performed by authorized Provider staff. All access keys are stored on a qualified electronic signature device (QSCD) where access to the keys is protected by an access password chosen by the RA Operator. This ensures double-factor authentication when issuing a certificate through IS Provider.

6.1.1.3 End users

No stipulation.

6.1.2 Private Key delivery to subscriber

See section 6.1.2 CP CA Disig.

All QSCD for RA personnel either are handed in person at the Provider's office or are sent by registered mail to the RA personnel. In the case of registered mail, the initiation of access rights for RA personnel in the IS of Provider is only performed after confirmation of the delivery of QSCD by the RA personnel.

6.1.3 Public key delivery to certificate issuer

The public key is delivered to the Certification Authority safely on-line via the "RA Client" application during the certification process. The communication between the "RA Client" application and the issuing CA is authorized by signing all the data by the RA. The authorization for the RA personnel is checked by the CA side in automatic mode.

6.1.4 CA public key delivery to relying parties

No stipulation.

6.1.5 Key sizes

No stipulation.

6.1.6 Public key parameters generation and quality checking

See section 6.1.5 of these CPS as well as section 7 of CP CA Disig.

6.1.7 Key usage purposes

Keys issued to RA personnel shall only be used for access to the IS of Provider through the "RA Client" application, and to sign the data sent during certificate issuance process. They can also be used to access the razona.disig.sk portal, where all the necessary information for RA is available.

6.2 Private Key Protection and Cryptographic Module Engineering

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 Activating Private Keys

No stipulation.

6.2.9 Deactivating Private Keys

No stipulation.

6.2.10 Destroing 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

Validity of RA personnel certificate shall not exceed the following:

Certificate type	Validity (max)
RA personnel	365 days

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data for the RA personnel private key is selected by the RA personnel itself as soon as the QSCD has been acquired and before its first use to access the Provider's IS.

6.4.2 Activation data protection

The RA personnel are solely responsible for the protection of RA personnel' private keys.

Each RA personnel is alerted by the Provider's responsible person about the need to protect the private key with a strong password against potential misuse.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

See section 6.5.1 CP CA Disig.

6.5.2 Computer security rating

No stipulation.

6.6 Live cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

No stipulation.

6.8 Time-stamping

No stipulation.

7. CERTIFICATE, CRL, AND OCSP PROFILES

Certificate profiles and certificate revocation lists are set centrally - neither the customer nor the RA can change the certificate structure.

7.1 Certificate profile

7.1.1 Version number

See section 7.1.1 CP CA Disig.

7.1.2 Certificate Content and Extensions

See section 7.1.2 CP CA Disig.

7.1.3 Algorithm object identifiers

See section 7.1.3 CP CA Disig.

7.1.4 Name Forms

No stipulation.

7.1.5 Name constraints

No stipulation.

7.1.6 Certificate policy object identifier

See section 1.2.

7.1.7 Usage of Policy Constraints extension

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.

7.1.10 Other provisions

No stipulation.

7.2 CRL profile

7.2.1 Version number

See section 7.2 CP CA Disig.

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

See section 8 CP CA Disig.

Based on the decision of an external organization that assesses the compliance of Provider's trusted services, each external RA has to undergo an audit of the services provided and provide maximum interoperability if the audit is requested. Any refusal will result in termination of the contract and cooperation with the RA concerned.

8.1 Frequency or circumstances of assessment

See section 8.1 CP CA Disig.

8.2 Identity/qualifications of assessor

See section 8.2 CP CA Disig.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

See section 8.4 CP CA Disig.

8.5 Actions taken as a result of deficiency

See section 8.5 CP CA Disig.

8.6 Communication of results

See section 8.2 CP CA Disig.

8.7 Self-Audits

No stipulation.

9. OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

The price list of trusted services or information on about contractual terms can be ordered for these services is published on the Provider's website - https://eidas.disig.sk/en/provider/pricelists/.

9.1.1 Certificate issuance or renewal fees

See section 9.1.1. CP CA Disig.

9.1.2 Certificate access fees

No stipulation.

9.1.3 Revocation or status information access fees

These services are provided free of charge.

9.1.4 Fees for other services

No stipulation.

9.1.5 Refund policy

No stipulation.

9.2 Financial responsibility

The Provider has sufficient resources to perform its trustworthy services.

9.2.1 Insurance coverage

The Provider is insured against possible damages that may be caused to the Customer / Holder of Certificates, respectively or to third parties in relation to the provision of trusted services.

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

See section 9.3.1 CP CA Disig.

9.3.2 Information not within the scope of confidential information

See section 9.3.2 CP CA Disig.

9.3.3 Responsibility to protect confidential information

External RAs are responsible for protecting confidential information under the terms of a contract they have concluded with the Provider.

9.4 Privacy of personal information

9.4.1 Privacy plan

See section 9.4.1 CP CA Disig.

The Provider processes the Personal Data of the Customers / Holders of Certificates or his authorized representatives in accordance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council - General Data Protection Regulation and Act No. 18/2018 Z. z. on the Protection of Personal Data (hereinafter referred to as "Personal Data Protection Regulations") [10].

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

No stipulation.

9.4.4 Responsibility to protect private information

External RAs are responsible for protecting the personal data of Customers / Certificate Holders, shall protect them against disclosure, and must refrain from providing them to a third party.

9.4.5 Notice and consent to use private information

The Provider fulfills the information obligation towards the persons concerned in accordance with the requirements of the Personal Data Protection Regulations [10].

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

This CPS and its associated documents represent important Provider's knowledge, so they are protected by copyright.

9.6 Representations and warranties

See section 9.6, CP CA Disig.

9.6.1 CA representations and warranties

See section 9.6.1 CP CA Disig.

9.6.2 RA representations and warranties

All external Entity registration authorities provide trusted services under a contractual relationship with the Provider and in accordance with their CPS.

Refer to the section 9.6.

9.6.3 Subscriber representations and warranties

No stipulation.

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

The Provider is solely responsible for the damage caused by the non-fulfillment of its obligations under the eIDAS Regulation, 13 eIDAS.

9.8 Disclaimers of warranties

See section 9.6.1 CP CA Disig.

9.9 Indemnities

For these CPS is section 9.9 of CP CA Disig fully applicable.

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., January 10, 2025 until it is replaced by a new version. For details on the history of changes to this CP, 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 6.3, 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 see 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 conducted by a designated person of the Provider who, based on the results of the review, prepares a written proposal for any proposed changes.

Approval of the proposed changes shall be conducted by the designated PMA member following the requirements set out in section 9.12.1 CP CA Disig.

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 these CPSs 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 these CPS.

9.12.2 Notification mechanism and period

The Provider publishes CPS-related information through its web site (see section 1).

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.

9.12.3 Circumstances under which OID must be changed

All CP or CPS have OID set by the Provider. The OID of this CPS is listed in Section 1.2 and is valid for each new version of these CPS.

9.13 Dispute resolution provisions

See section 9.13 CP CA Disig.

9.14 Governing law

See section 9.14 CP CA Disig.

9.15 Compliance with applicable law

See section 9.13 CP CA Disig.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

No stipulation.

9.16.2 Assignment

No stipulation.

9.16.3 Severability

If any provision of these CPS is or becomes invalid or unenforceable, it will not invalidate or invalidate the entire CPS if it is completely separable from the other provisions of the CPS. The Provider will at once replace the invalid or unenforceable provision of the CPS with a new valid and enforceable provision the subject of which will be as relevant as possible to the subject matter of the original provision while preserving the purpose of these CPS and the content of the individual provisions of these CPS.

9.16.4 Enforcement

See section 9.16.4 CP CA Disig.

9.16.5 Force Majeure

See section 9.16.5 CP CA Disig.

9.17 Other provisions

No stipulation.