Certificate Practice Statement
Part: Registration Authority

Disig, a.s.

Version 5.1

Valid from 23.5.2018

OID 1.3.158.35975946.0.0.0.1.3

Content

Trade name	Disig, a.s.
Residence	Záhradnícka 151, 821 08 Bratislava
Registration	OR Okresného súdu Bratislava I, odd. SA 3794/B
Telephone	+ 421 2 208 50 140
E-mail	disig@disig.sk

1. Introduction

This document defines the Certificate Practice Statement (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 District Court Bratislava I, Sa, insert no. 3794/B, as a Trusted Service Provider (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 5.1 with effective date from 23.5.2018.

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]; Act no. 272/2014 Coll. on trustworthy services [4] and EU Regulation No. 910/2014 [5].

The Provider confirms that these CPSs take into account all the requirements of the document [6], 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 [6] shall prevail.

1.2 Document Name and Identification

Document Name:	Certificate Practice Statement Part: Registration Authority
Name abbreviation:	CPS RA CA Disig
Version:	5.1
Approved on:	18.5.2018
Valid from:	23.5.2018
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 CA Disig

This CPS is relate to certificate for natural person, legal person and publicly trusted certificates for Web site authentication (SSL certificate) issued by the Provider. Other types of certificates are described in separate CPSs.

The term "certificate" or "the Provider' certificate" in this document refers to any mentioned above certificates issued by the Provider.

1.2.1 Revisions

Revision	Revision date	Description; Reviewer
1.0	25.03.2006	Firs version; Mišković
1.5	20.12.2006	Formal text editing - Formatting, correcting links, editing text in section 4 "Operational requirements"; Mišković
2.0	23.01.2007	CP expansion in relation to the new type of certificates issued for the contracted client. Addition of section 7 "Certificate Profiles"; Mišković.
2.1	29.03.2007	Correcting text in chap. 2.8 and Chap. 4.9 Text editing related to a minor change in a partner's certificate; Mišković
3.0	19.03.2008	Overall revision of the CP for each type of certificate; Ďurišová, Mišković

3.1	24.06.2008	A new type of certificate adding.; Miškovič
3.2	10.11.2008	Change certificate validity for domain user PKI VsZP Termination of operation at Záhradnícka 153; Miškovič
3.3	25.11.2008	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	02.06.2009	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	14.10.2009	Editing in connection with Mozilla Foundation requirements when applying for a CA Disig certificate to the Mozilla Root Certificate Store; Miškovič
4.1	11.05.2010	Inclusion of proposed audit corrective actions of 13.11.2009 (audit according ETSI TS 102042 V1.3.4);; Miškovič
4.2	11.03.2011	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	25.01.2012	Supplementing the possibility to issue certificate for subordinate CAs, adding signature algorithms, and regular annual review of content; Miškovič
4.4	22.06.2012	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	15.08.2013	Refining of CA Disig CA root CA Certificate Profile and other Certified Types of Certificates; Miškovič
4.6	21.06.2013	Correction of the OID of the document - deleting the version of the document from the OID (section 1.2). Editing Profiles for subordinate CAs - certificatePolicies Identifier (section 7.1.2); Enable issuing "wildcard" SSL certificates to be issued at the third level of the domain name (3.1.2); Miškovič
4.7	2.2.2015	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	22. 5. 2015	Verification of CAA records (4.1.5); Mišković
4.9	21. 10. 2016	Changes made in connection with the eIDAS Regulation and in connection with the expiry of Act no. 215/2002 Coll. and the entry into force of Act no. 272/2016 Z. z .; Inclusion of Baseline Requirements for Issuance and Management of Publicly-Trusted Certificates, to Version v.1.4.1; Mišković
5.0	25. 9. 2017	Conversion of CP to RFC 3647 format; Inclusion of eIDAS requirements and incorporation of the requirements of the current version of Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.5.2; Mišković
5.1	23. 5. 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); Mišković

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 and CA Disig Root R1 - See section 1.4.1CP CA Disig.

1.3.2 Registration authorities

The components of the Provider detailed in these rules is:

- Commercial Registration Authority
- Internal Registration Authority

If the registration authorities are established based on a written contract with a business partner and it will be run its own registration authorities, a separate CPS will be issued for this type.

1.3.3 Subscriber and Certificate Holder

See section 1.3.3 CP CA Disig.

1.3.4 Relaying 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

Provider within the meaning of this CPS issues to end customers the following types of certificates:

- certificates for natural person intended in particular for the purpose of securing electronic mail or signing electronic documents,
- certificates for legal person intended to make an electronic seal,
- SSL certificates designed to secure Web site authentication.

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:	**Záhradnícka 151, 821 08 Bratislava 2**
Company ID:	359 75 946
Phone:	+421 2 20850140
e-mail:	disig@disig.sk
Web site:	http://www.disig.sk

1.5.2 Contact Person

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

Registration Authority	
Address:	**Záhradnícka 151, 821 08 Bratislava 2**
E-mail:	radisig@disig.sk
Phone:	+421 2 20850140
Web site:	http://eidas.disig.sk/

The list of other Registration Authorities of Provider is available at web site: http://eidas.disig.sk/en/ralist/.

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

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. Act No. 272/2016 Coll. on Trust Services for Electronic Transactions in the Internal Market and on Amendment and Supplementing of certain Acts (Trust Services Act).

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

6. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates.

7. General Terms of Service for Trusted Services, Disig, a.s.

8. 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.

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 Certification Information

See section 2.2 CP CA Disig.

Information on Registration Authorities providing trusted services on behalf of the Provider is available at the Provider's website - See section 1.5.2.

2.3 Time or Frequency of Publication

The certificate is published as soon as it is issued and Customer / Certificate Holder can download it immediately. Information about the issued certificate are 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 their creation (issuing, revocation, etc.).

Certificates issued for closed systems or for the internal purposes of the Provider are not publicly available and information about their release is not published in the repository.

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

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

3.1.1 Types of Names

In general, CA does not assign distinguishing names in the sense of X.500 (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.

3.1.2 Need for Names to be Meaningful

See section 3.1.2 CP CA Disig.

3.1.3 Anonymity or Pseudonym of Subscribers

See section 3.1.3 CP CA Disig.

3.1.4 Rules for Interpreting Various Name Forms

See section 3.1.4 CP CA Disig.

3.1.5 Uniqueness of names

See section 3.1.5 CP CA Disig.

In the event that a certificate for two different entities could be produced that would contain the same distinguished name of the subject, a unique identifier in the form of the serialNumber entry is inserted into the certificate.

3.1.6 Recognition, authentication and role of trademarks

The Provider will not knowingly issue a certificate containing a name if it is suspected that the Customer / Holder has no authorization to use such a trademark in the certificate application.

3.2 Initial identity validation

3.2.1 Method to Prove Possession of Private Key

In the case of a request for a new (subsequent) certificate that was generated for new cryptographic keys by the Customer / Holder, the ownership of the private key is formally validated by the Customer / Holder by sending the signed certificate

request as an attachment of the message from the e-mail address given in the certificate request . The RA worker verifies whether it has been delivered from an email address that is identical to the address specified in the request.

A signed certificate request is then automatically authenticated in the Provider's system, where it is verified that the request has been signed using a private key that matches the public key in the request.

If the Provider generates the key directly to a Qualified Signature / Seal Creation Device (QSCD), there is no need to verify the ownership of the private key.

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 copy 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 3.2.3.

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 on 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 3.2.3. 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 authorize 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 worker 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 an SSL certificate where CountryName is country code, the RA worker 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

Validation is done in one of the ways listed in section 3.2.2.4 of the current version of CP CA Disig, where the preferred method is to send randomly generated value by email according to the following procedure:

An RA worker through the KeePass software application will generates a random text string with a minimum length of 20 characters that will contain upper and lower case 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 Registrarfor 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 / SSL 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 / SSL certificates that end with the same FQDN at the second and higher level. The RA worker then archives the appropriate email communication for the TLS / SSL certificates issued in electronic form. This method can also be used to validate the "wildcard" TLS/SSL certificate request for Web site authentication.

The second method is phone contact and the procedure is as follows:

An RA worker verifies the eligibility of the TLS / SSL certificate request by the customer by calling the phone number of the authorized contact that is listed as a legitimate contact for that domain at the Registrar for that domain (e.g., for a top level domain ".sk" it is whois.sk-nic.sk). If successful FQDN validation is performed in this way, the Provider can also issue other TLS / SSL certificates that end with the same FQDN at the second and higher level. The RA worker performs a record in electronic form about the telephone conversation, indicating the telephone number to which it was executed and the name of the person who confirmed the

eligibility of the TLS / SSL certificate. This method can also be used to validate the "wildcard" TLS/SSL request.

3.2.2.5 IP Address Authentication

No provisions.

3.2.2.6 Validation of a domain containing a "wildcard" character

An RA worker will validate a request for a "wildcard" SSL 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 worker will validate a request for a "wildcard" SSL 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 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

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

3.2.2.8 CAA record

The RA worker shall check the published CAA record before issuing an SSL 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 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 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.

3.2.3.1 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 an SSL 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.

Typical value of this entry will be a complete domain name.

The RA performs verification of all items in the DN certificate except organizationUnitName (Organization Name). In the case of this item, only a check shall be made as to whether it does not include the name of a legal person, business name, trademark, address, location, or other text referring to an identifiable natural or legal person.

3.2.3.2 Contractors identity authentication

Authentication of the identity of a natural person or components of Disig contractual partners (business partners) is carried out in cooperation with the responsible persons of this company.

Some procedures are simplified in this case and do not have to be done, for example, domain ownership verification, email account verification, and more.

3.2.3.3 Documents submitted

3.2.3.3.1 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 worker 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.

3.2.3.3.2 Natural person

See section 3.2.3 and section 3.2.3.3.2 CP CA Disig.

3.2.3.3.3 Natural person - employee

See section 3.2.3.3.4 CP CA Disig.

3.2.3.3.4 Legal person

In this case, the applicant for the certificate shall submit the documents listed in the section 3.2.3.3.2. At the same time, he must submit the document according to the section 3.2.2.

3.2.3.4 Component or system

See section 3.2.3.1.

3.2.3.5 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) are 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 are 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 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 on 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.).

3.2.3.6 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.

3.2.4 Non-verified Subscriber Information

See section 3.2.4 CP CA Disig.

3.2.5 Validation of Authority

See section 3.2.3.

3.2.6 Criteria for Interoperation or Certification

No provisions.

3.3 Identification and authentication when issuing a subsequent certificate

The conditions for issuing a subsequent certificate are described in detail in section 3.2.7 CP CA Disig.

The RA will issue the certificate without a personal visit to the holder only in the case of a certificate for a physical person or, certificate for a legal entity only after the conditions specified in section 3.2.7 of CP CA Disig. For verification of the request sent, in the case of unsigned e-mail from an e-mail address which is identical to the address given in the received application or sent from a different email than the one received in the request, the RA will send an e-mail to the email address that will contain secret unpredictable information (verification information). The certificate applicant must return the verification information as proof of the verification of the request for the issue of the subsequent certificate. The response must be sent within a specified period sufficient to send the e-mail. If the verification of the request is unsuccessful, the Provider refuses to issue the certificate.

3.3.1 Identification and authentication when issuing a subsequent certificate after cancellation of the previous one

Once the certificate has been revoked, the applicant for the subsequent certificate must submit to all the initial registration requirements.

3.4 Identification and authentication for re-key requests

See section 3.3 CP CA Disig.

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.

4.1.3 Request generation

See section 4.1.3 CP CA Disig.

4.1.4 Sending a certificate request

See section 4.1.4 CP CA Disig.

4.2 Enrollment process and responsibilities

4.2.1 Performing identification and authentication functions

4.2.1.1 The RA procedure when sending an application electronically

1. The RA worker verifies that a certificate request of a given Customer's (mandatory requirement for issuing certificates with the extension "Secure Email (1.3.6.1.5.5.7.3.4)") was sent from the same email address as found in the certificate application. In the event of discrepancies, it will refuse to issue the certificate.
2. If the pre-submitted application for a certificate contains the same email address, as is address from which was send, the RA worker will verify this email address. Verification will be accomplished by sending an e-mail to the email address that will contain secret unpredictable information (verification information). The certificate applicant shall send the verification information as proof of the verification of the e-mail address. The reply must be sent within a specified period sufficient to send the e-mail. If the email address verification is unsuccessful, the Provider will refuse to issue the certificate. The detailed procedure is described in the relevant manuals for RA staff and is subject to the initial training of RA staff. Verification of an email address is not necessary if a subsequent certificate request is sent electronically by e-mail, which is signed by a valid applicant's certificate issued by the Provider's certification authority and the email address from which the request was sent is identical to the email in the request.

3. For Provider's contractual partners who submit requests for issuance of a certificate from a contractually agreed domain, the e-mail address verification is not performed.

4.2.1.2 The procedure for registering a customer directly on the RA

1. An RA worker informs the physical person present about the General Terms of Service for Trusted Services [7].
2. The RA worker verifies the identity of the Customer or, the entity representing him, according to the provisions of the section 3.2.2 and 3.2.3.
3. he RA employee selects a pre-sent certificate request identified by the Customer. An application for the issuance of a personal certificate for the signature and encryption of e-mail shall be sent to the RA concerned electronically from the address, which will is included in the DN of the request in the E-mail field.
4. The RA worker checks out the completeness and accuracy of the accepted certificate request (e.g., if some items do not contain clearly erroneous data).

   Warning: All items must be filled in without diacritics. Small and large letters are distinguished. Items "City:", "Company:" and "Business Unit:" are optional. Mandatory field "E-mail" of certificate request shall be filled in by an email address of the customer.

   The customer must demonstrate to the RA in a satisfactory manner all the data he / she has entered into each item of the certificate request. If the Customer submits other documents (other than personal documents of natural persons, such as extract from the Commercial Register or other evidence of a legal entity, power of attorney if another entity is represented), the RA will take over and keep copies of all documents submitted, compares them with the originals, and writes the text "I confirm the match to the original" for each copy and adds the date and signature. The submission of an extract from the commercial register obtained from the Internet by the Customer is not sufficient as this statement has only informative and not applicable to legal acts.

5. Through the information system of the Provider, it is automatically verified whether a certificate was issued in the past for the public key found in the submitted certificate request. If it was, RA will refuse the certificate request for security reasons because the previously certified public key can no longer be used in another certificate.
6. The RA employee shall submit to the Customer a contract for the issue and use of the certificate and services in two copies for signature, one for the Provider and one for the Customer. Customer's agreement with the text of this agreement is a condition for receiving a certificate request and issuing a certificate.
7. The customer shall pay for the certificate the amount according to the valid price list of the provider's services, unless otherwise agreed.
8. The RA worker inserts a request for the certificate and other required personal data into the Provider's information system.
9. Once the certificate is issued, the certificate applicant will be able to take over the certificate. In this case, the certificate applicant and the RA worker sign a confirmation about the issuance of the certificate. This confirmation shall be write out two copies - one for the applicant and one for the RA, who

then forward it to the Provider. For contract partners whose certificates are issued on a contractual basis, only the confirmation is signed.

4.2.1.3 Detailed procedure for obtaining an SSL certificate

4.2.1.3.1 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 an SSL 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 SSL certificate request or a public key for that has certificate already been issued respectively cannot be used repeatedly to issue another SSL certificate for safety reasons and will be refused to RA! An SSL certificate 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 SSL 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, 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 CA Disig, otherwise CA Disig reserves the right to reject this request. All data must be entered without diacritics. You cannot use a comma in the Organization field. An SSL certificate applicant can only be the organizations statutory or an authorized person to whom the SSL certificate is issued. All data in the application must be validly demonstrated by the applicant, except subject subject: organizationUnitName (OU). The OU item may not contain the name of a legal person, business name, trademark, address, location, or other text referring to a particular natural or legal person, unless the use of such information is reasonably substantiated by the applicant.

- will prepare the selected identity documents and other necessary documents, e.g. extract from business register (we recommend to verify 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 contact RA to verify before visiting the RA and clarify itself any doubts and problems, especially those relating to the suitability of the individual items in the SSL certificate request.

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

4.2.1.4 Procedure of the RA before issuing an SSL certificate

Based on a pre-submitted application, an RA worker 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 SSL certificate request. If an RA worker has seriously suspected of unauthorized use of any FQDN by Customer, it has the

right to require the Customer shall to demonstrate in a credible way that he/she may use given FQDN, otherwise RA may refuse to accept the SSL certificate request.

4.2.2 Approval or rejection of certificate applications

The certificate request shall be processed by the RA worker 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.

An RA worker 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.

If the top level domain (gTLD) specified in the TLS / SSL certificate (e. g. ".ipsum") is unknown to the worker, 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 in the list, it refuses to issue the certificate.

4.2.3 Delivering a public key to the issuer of the certificate

See section 4.1.4 CP CA Disig.

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 certificate. If the certificate does not contain an e-mail address e-mail is send 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

If the certificate is not issued on a QSCD, the certificate issued is available for download via the Provider's repository at http://eidas.disig.sk/sk/crtsearch/ or in the notifying e-mail is the link with the address from which the Holder can directly download issued certificate

If certificate is issued on a QSCD, it is handed over to the Customer / Holder immediately after issue along with the QSCD.

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 been agreed not to disclose it.

4.4.3 Notification of certificate issuance by the CA to other entities

See section 4.4.3 CP CA Disig.

4.5 Key pair and certificate usage

See section 4.5 CP CA Disig.

4.6 Certificate renewal

See section 4.6 CP CA Disig.

4.7 Certificate re-key

When issuing a certificate on a new key, is procedure the same as when issuing the initial certificate - See section 4.3.

4.7.1 Circumstance for certificate re-key

No provisions.

4.7.2 Who may request certification of a new public key

An existing Holder, for whom the Provider has previously been issued a certificate by and who meets the identification and authentication requirements according section 3 may request certificate for the new key.

4.7.3 Processing certificate re-keying requests

The RA worker issues the certificate in the same way as the original certificate was issued.

4.7.4 Notification of new certificate issuance to Subscriber

After the certificate is issued, the Holder is notified of its issuing by sending an e-mail message to an e-mail address notified during the authentication and identification process.

4.7.5 Conduct constituting acceptance of a re-keyed certificate

In the case of issuing certificate during the holder's personal presence to the RA, the method of taking over described in the section is applied 4.4.

In the case of submitting a request for a certificate on a new key by electronic means, the certificate is delivered to the Holder to the e-mail address given in the certificate.

4.7.6 Publication of the re-keyed certificate by the CA

See section 4.4.2.

4.7.7 Notification of certificate issuance by the CA to other entities

See section 4.4.3.

4.8 Certificate modification

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

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.

An RA worker 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.

An RA worker declines the request if the applicant fails to meet the authentication conditions (see sections 3.2.2 resp. 3.2.3).

4.9.4 Revocation request grace period

See section 4.9.4 CP CA Disig.

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 worker 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

See section 4.9.6 CP CA Disig.

4.9.7 CRL issuance frequency

No provisions.

4.9.8 Maximum latency for CRLs

No provisions.

4.9.9 On-line revocation/status checking availability

No provisions.

4.9.10 On-line revocation/status checking availability

No provisions.

4.9.11 Other forms of revocation advertisements available

No provisions.

4.9.12 Special requirements re key compromise

No provisions.

4.9.13 Circumstances for suspension

Provider does not provide such a service.

4.9.14 Who can request suspension

Provider does not provide such a service.

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 24/7/365 mode.

OCSP is available in 24/7/365 mode.

4.11 End of subscription

See section 4.11 CP CA Disig.

4.12 Key escrow and recovery

See section 4.12 CP CA Disig.

5. Facility, Management, and Operational Controls

5.1 Physical controls

Access to information system of the Provider through the application "RA Client" that RA uses in its activity is protected against unauthorized access such way that RA worker use its own authentication certificate.

An important security measure that significantly restricts the possibility of abuse of the RA worker identity (the RA certificate and, in particular, the associated private key) is that the RA key pair is stored on the chip card. Access to a private key stored on the card is protected by a password.

Additional security mechanisms appropriate to the level of threat in RA environment are used to protect RA.

5.2 Procedural controls

When choosing a person to a RA worker 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 is required to comply with CPS.

The RA worker 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.

5.3 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 worker shall be selected based on reliability, loyalty, and credibility.

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

5.4 Audit logging procedures

5.4.1 Types of events recorded

No provisions.

5.4.2 Frequency of processing log

No provisions.

5.4.3 Retention period for audit log

No provisions.

5.4.4 Protection of audit log

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

5.4.5 Audit log backup procedures

No provisions.

5.4.6 Audit collection system

Provider must have a built-in log backup system.

5.4.7 Notification to event-causing subject

No provisions.

5.4.8 Vulnerability assessments

No provisions.

5.5 Records archival

5.5.1 Types of records archived

RAs shall 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 can be kept in paper form or, in electronic form. All records that must be submitted by the Customer / Holder to be issued with the required type of certificate (e.g., business listing, power of attorney, etc.) must also be part of the retained records.

5.5.2 Retention period for archive

See section 5.5.1.

5.5.3 Protection of archive

Archived RA Records must be stored in a safe place until delivery and must be maintained in a manner that prevents unauthorized modification, replacement or destruction.

5.5.4 Archive backup procedures

No provisions.

5.5.5 Requirements for time-stamping of records

No provisions.

5.5.6 Archiving system

No provisions.

5.5.7 Procedures to obtain and verify archive information

No provisions.

5.6 Key changeover

RA worker 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 worker'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 worker's key is compromised, loss of the key, disclosure of access passwords, etc., this incident shall be immediately reported by the RA worker 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 Computing resources, software, and/or data are corrupted

No provisions.

5.7.3 Entity private key compromise procedures

In the event of compromise on the RA worker 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 provisions.

5.8 RA termination

Upon termination of RA:

- RA in advance, within the meaning of the RA agreement, by appropriate manner notify the intention to cease its activity to the Provider,
- RA follow the instructions of the Provider to concentrate and prepare for submission all documents related to the provided trusted services,
- RA get rid all private keys of RA workers and pass RA tokens back to the Provider.

6. Technical Security Controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

6.1.1.1 Certificate issuer

No provisions.

6.1.1.2 Registration authority

Generating access keys and issuing authentication certificates for RA Workers 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 provisions.

6.1.2 Private key delivery to subscriber

See section 6.1.2 CP CA Disig.

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

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 worker is checked by the CA side in automatic mode.

6.1.4 CA public key delivery to relying parties

All certificates of issuing Certification Authorities of Provider are available through the Provider's Web site at: https://eidas.disig.sk/sk/cacert/.

6.1.5 Key sizes

Algorithms and key lengths applied in Administrator certificates:

Signature Algorithm
Sha256RSA

Public key
RSA, length 2048 bit

Algorithms and key lengths applied in the CA Disig root certificate:

Signature Algorithm
sha256RSA

Public key
RSA, length 4096 bit

Algorithms and key lengths applied in the subordinate CA Disig certificate:

Signature Algorithm
sha256RSA

Public key
RSA, length at least 2 048 bit

Validity of certificate
Max 15 years*

* - the "Valid to“ value of subordinate CA shall not exceed the value "Valid to" of root CA.

The key lengths in end-user certificates are listed in the section 7.1.4 CP CA Disig.

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 workers 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 are available.

6.2 Private Key Protection and Cryptographic Module Engineering

No provisions.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No provisions.

6.3.2 Certificate operational periods and key pair usage periods

Validity of RA workers certificate shall not exceed the following:

Certificate type	Validity (max)
RA worker	365 days

6.4 Activation data

6.4.1 Activation data generation and installation

Activation data for the RA worker private key is selected by the RA worker 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 worker is solely responsible for the protection of RA worker' private keys.

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

6.4.3 Other aspects of activation data

See section 6.4.3 CP CA Disig.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

See section 6.5.1 CP CA Disig...

6.5.2 Information security assessment

No provisions.

6.6 Computer security rating

6.6.1 System development controls

See section 6.6.1 CP CA Disig.

6.6.2 Security management controls

No provisions.

6.6.3 Life cycle security controls

No provisions.

6.7 Network security controls

No provisions.

6.8 Time-stamping

No provisions.

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

The certificate profiles are listed in the currently valid CP CA Disig section 7.1.

7.2 CRL profile

See section 7.2 CP CA Disig.

CRL issued by CA Disig are CRL versions 2.

Signature Algorithm:	sha256RSA

The CRL includes all revoked certificates, including those that are not valid at the time of issue of the CRL.

7.3 OCSP profile

See section 7.3 CP CA Disig.

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 provisions.

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

During the period in which the external RA performs its activity, the Provider must monitor RA activity and check RA services by performing periodic inspection of the supplied documents to issued certificates. If Provider finds serious deficiencies, it can always perform an audit of the RA to identify the causes of the deficiencies. Other Business and Legal Matters

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 - http://eidas.disig.sk/en/pricelist/.

9.1.1 Certificate issuance or renewal fees

See section 9.1.1. CP CA Disig.

9.1.2 Certificate access fees

No provisions.

9.1.3 Revocation or status information access fees

These services are provided free of charge.

9.1.4 Fees for other services

No provisions.

9.1.5 Fees for other services

No provisions.

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 Insurance coverage

No provisions.

9.2.3 Insurance or warranty coverage for end-entities

No provisions.

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") [8].

9.4.2 Information treated as private

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

9.4.3 Information not deemed private

No provisions.

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. [8]

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 these CPS.

Refer to the section 9.6.

9.6.3 Subscriber representations and warranties

No provisions.

9.6.4 Relying party representations and warranties

No provisions.

9.6.5 Representations and warranties of other participants

No provisions.

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. 18.5.2018 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 5.1, 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

Provider communication with individual RAs is officially carried out through authorized email communications between the Provider's authorized persons and the authorized person from RA.

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 in accordance with 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 provisions.

9.16.2 Assignment

RA shall not transfer its rights or duties (or otherwise deal with them) to any third party without the written consent of the Provider.

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 immediately 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 provisions.