CA Disig Certification Practice Statement - Part: Registration Authority

Practice
Version 4.9
Valid from 21.11. 2016

Disig, a. s.
Záhradnícka 151
821 08 Bratislava 2
Slovakia

Change History

Version	Revision date	Description of the revision; revised by
1.0	25.03.2006	The first version of the document; Mišković
1.5	20.12.2006	Formal emendation of the document - formatting, links repairs, emendation in Chapter 4, "Operational requirements"; Mišković
3.0	19.03.2008	Overall review of CP in relation to various types of issuing certificates; Ďurišová, Mišković
3.1	24.06.2008	Adding of a new certificate type; Mišković
3.2	10.11.2008	Cancellation of operations at 153rd Záhradnícka street
3.3	25.11.2008	Adjustment as follows: Chapter 3.1.9 - domain ownership verification Chapter 4.1.1, 4.1.2, - validation of the e-mail address of the applicant
3.4	02.06.2009	Adjustment in connection with the requirement of a minimum length of a public key, on which Disig CA issued the certificate (paragraph 5.1.3; 6.1.2); Change of the e-mail address location in the profile of the certificate (paragraph 3.1.2; 6.1.2); Mišković
4.0	14.10.2009	Modification in relation to the Mozilla Foundation requirement to apply for CA Disig certificate location to the Root Certificate into the Mozilla Store; Mišković
4.1	11.05.2010	Incorporation of the proposed corrective actions from audits of 11/13/2009 (audited according to ETSI TS 102 042 v1.3.4); MIškovič
4.2	11.03.2011	Certificate validity period change; Mozilla Foundation security policy requirements and Microsoft (code signing certificate) requirements incorporation; formal modification of text and tables; Mišković
4.3	25.01.2012	Subordinate CA issuing possibility; new signing algorithm adding; regular annual revision; Mišković
4.4	22.06.2012	CA/Browser Forum document „Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.0" requirements implementation; Mišković
4.5	15.08.2012	Subordinate CA issuing possibility; new signing algorithm adding; regular annual revision; Mišković
4.6	21.06.2013	Document OID refine – cut out version of document (chapter 1.2); Small text changes; Mišković

4.7	16.03.2015	Incorporating the requirements of the current version of the document "Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates",v.1.2.3; Change the certificate issued to a legal person system certificate for electronic seal (3.1.2); Miškovič
4.8	1.6.2015	CAA records review (4.1.3); Miškovič
4.9	21.11. 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 1.4.1; Miškovič

Content

Business Name	Disig, a. s.
Residence	Záhradnícka 151, 821 08 Bratislava, Slovakia
Registration	Registered in the District Court Bratislava I, odd. Sa 3794/B
Telephone	+ 421 2 208 50 140
Fax	+ 421 2 208 50 141
E-mail	disig@disig.sk

Reference

1. Recommendation ITU-T X.509; Information technology – Open Systems Interconnection – The Directory: Public-key and attribute certificate frameworks
2. ACT No. 215/2002272/2016 Coll. on Trust Services for Electronic SignatureTransactions in the Internal Market and on the Amendment and Supplementing of certain Acts as amended.(Trust Services Act).
3. The NSA Decree No. 133/2009 (pdf, 103.5 kB) Coll. on the content and extent of operational documentation kept by the certification authority and on the security rules for the execution of certification activities.
4. RFC3647, Request for Comments: 3647, Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework, S. Chokhani, Orion Security Solutions, Inc.; W. Ford, VeriSign, Inc.; R. Sabett, Cooley Godward LLP; C. Merrill, McCarter & English, LLP; S. Wu, Infoliance, Inc.; November 2003.
5. RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
6. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.4.1, CA / Browser Forum, 2016
7. ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates, European Telecommunications Standards Institute 2013.
8. Act No. 122/2013 on Protection of Personal data and supplementing of certain acts as amended.

List of Terms and Abbreviations

Terms

Contractual partner - a legal entity with which the company Disig has concluded a written contract to provide CA Disig certification service.

Abbreviation

CA	–	Certification Authority
CMA	–	Certificate Management Authority
CP	–	Certificate Policy
CPS	–	Certificate Practice Statement
CRL	–	Certification Revocation List
EFTA	-	European Free Trade Association (Iceland, Lichtenstein, Norway, Switzerland)
HSM	–	Hardware Security Module
IČO	–	Organization identification number
NBÚ	–	National Security Authority
OID	-	Object Identifier
PEM	-	**Privacy Enhanced Mail**
PKCS#10	-	Certification Request Standard according Public Key Cryptographic Standards (RFC 2986)
PKI		Public Key Infrastructure
PMA	–	Policy Management Authority
RA	–	Registration Authority
SSCD	-	Secure Signature Creation Device
SC	-	System certificate for legal person

1. Introduction

This document defines the rules for the performance of certification activities (Certificate Practice Statement, hereinafter "CPS") for registration authority (hereinafter refer to as “RA”) which provide certification services on behalf Certification Authority CA Disig (hereinafter "CA Disig“), which is operated by Disig, a. s. (hereinafter “Disig”).

The rules are based on the Certification Policy (hereinafter "CP"; OID=1.3.158.35975946.0.0.0.1.1) CA Disig applied in the implementation of Public Key Infrastructure (hereinafter referred to as "PKI") consisting of products and services provided and managed according to standard X.509 certificates for public key cryptography.

A certificates issued for end entity are uniquely identifies an entity, for which is a certificate issued and linking this entity to the appropriate key pair.

If in this document is not explicitly state that this is related to the Root Certificate Authority or subordinate Certification Authority certificates, the word ”certificate” means an end entity certificate.

1.1 Overview

These CPS are the rules for the performance of certification practices on the basis of which the company Disig established and operated certification authority CA Disig and also describes RA function.

The rules were created in accordance with 133 Decree of the National Security Authority of March 29, 2009 on the content and scope of operating documentation administered by a certification authority[2] and on the security rules and rules for performing certification activities and materials on the Internet X.509 Public Key Infrastructure - Certificate Policy and Certification Practices Framework (RFC3647) [3] and Internet X.509 Public Key Infrastructure - Certificate and Certificate Revocation List (CRL) Profile (RFC5280).[4]

These rules define the creation and management of certificates with public keys according to the X.509 version 3 standards for their use in applications that require secure communication between computer systems connected to a computer network.

Skeletal part of such a network may be the unprotected network, such as internet.

1.2 Identification

Title:	**CA Disig Certification Practice Statement - Part: Registration Authority**
Short title:	**CPS RA CA Disig**
Version:	**4.9**
Approved Date:	**November 14, 2016**
Valid from:	**21.11.** 2016
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 – ICO))

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 relating to personal certificates, certificates for legal person, SSL certificates and certificates for software components issued by the CA Disig. Other types of certificates are described in separate CPS.

Term certificate or certificate CA Disig herein refers to any of the above certificates issued by the CA Disig.

Up to 1.7.2013 was used for this document OID 1.3.158.35975946.0.0.0.1.3.x.y where x.y means the exact version of a particular CPS RA e.g. version valid from August 22, 2012 to July 1, 2012 was identifying by OID in form of 1.3.158.35975946.0.0.0.1.3.4.5.

Since version 4.6 of CPS RA is used only identifier of this document in his basic form as written above e.g. OID=1.3.158.35975946.0.0.0.1.3.

1.3 Community and applicability

1.3.1 Certification Authorities

1.3.1.1 Policy Management Authority

Policy Management Authority - PMA is a component provided for the purpose of:

- supervising the creation and updating of the CP‘s, including the evaluation of plans to implement any of the changes,

- revision of certificate practice statement (hereinafter CPS) of CA Disig through the analysis of CPS to ensure that the practice meets the CA Disig CP,
- reviewing of audits findings, to determine whether CA Disig adequately comply with approved CPS,
- giving recommendations for CA Disig regarding corrective actions and other appropriate measures,
- determine the appropriateness of the use of foreign orders,
- giving advice regarding the suitability of the certificates associated with the CP for specific management applications and managing activities of the certification authority and registration authority,
- interpretation of the CPS and its instructions for RA and CA,
- auditing Disig CA,
- ensuring that this Certificate Practice Statement (CPS) is duly and properly implemented.

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

1.3.1.2 Certification Authority

Certification Authority (CA) is an entity authorized by PMA to create sign and issue certificates with public key for Root CA, SubCA and end entity certificates.

CA is responsible for all aspects of the issuance and management of all types of certificates mentioned above, including control over the process of registration, identification and authentication, the process of creating, publishing and revocation of certificates, changes of certificate key pair.

CA ensures that all aspects of its services, operations and infrastructure geared to certificates issued under this CP are performed in accordance with the requirements and provisions of this CP.

1.3.1.3 Registration Authorities

Component of CA Disig, which deal in detail the CPS are:

- Commercial RA
- In-house RA

If the registration authority will be created under a written contract with business partners and this will operate their own registration authorities, separate CPS for this RA will be issued.

CA and RA together constitute the Certificate Management Authority (hereinafter referred to as "CMA"). The term CMA is to be used when the function can be attributed to either the CA or RA, or when the claim concerns while CA and RA.

1.3.2 End entities

1.3.2.1 Applicants for the certificate of CA Disig and certificate holders

Applicants for a certificate shall mean the natural person who is eligible to apply for a certificate on behalf of entity whose name appears as an entity in the certificate.

Entity whose name appears as an entity in the certificate may be:

- Natural person,
- Legal person,
- Component.

The applicant for a certificate after the acceptance of the certificate becomes the holder of the certificate. Conditions to be met by the applicant for the receiving certificate are defined by CP CA Disig.

Certificate holder shall mean the natural person who undertakes to use the corresponding private key and certificate in accordance with CP CA Disig and this CPS.

1.3.2.2 The relying parties

Party relying on the certificate is the entity which, by using a foreign certificate to verify the integrity of electronically signed messages, or to establish secure communications with the holder of the certificate, relies on the validity of the certificate holder's ties with the public key.

Party relying on the certificate should use the information from the certificate to determine the suitability of the certificate for that use.

Synonymous with the concept of party relying on the certificate is the concept the certificate user. Certificate user acts on the basis of trust to the certificate and/or on the basis of an electronic signature verified by the certificate.

1.3.3 Applicability

CA Disig issued to the clients following types of certificates:

- personal certificates – designed primarily for the electronic mail security for a natural person or electronic document signing,
- SSL certificates - designed primarily for the purpose of ensuring secure communication with the web servers,
- personal certificates for domain user - used for domain logging respectively communication between domain users,
- system certificates for the legal person(seal originator) for electronic seal
- certificate for the domain controller - designed exclusively for security communications of domain controllers
- personal certificates for corporate clients - designed for mutual communication within the organization and for ensure mutual

communication between specific applications used by this organization and its clients.

- code signing certificates – this certificate is using for digitally signing executable and scripts to confirm the software author and guarantee that the code has not been altered or corrupted since it was signed

CA Disig conforms to the current version of the Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates published at http://www.cabforum.org.[5] In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.4 Contact details

Registration authority CA Disig	
Address:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**radisig@disig.sk**
phone	**+421 2 20850140**
fax:	**+421 2 20850141**
www:	**http://www.disig.sk**

Founder, owner and operator of CA Disig	
Company:	**Disig, a. s.**
Address:	**Záhradnícka 151, 821 08 Bratislava 2**
Company ID:	**35975946**
phone	**+421 2 20850140**
fax:	**+421 2 20828141**
e-mail:	**disig@disig.sk**
www:	**http://www.disig.sk** (Slovak version) **http://www.disig.eu** (English version)

List of other registration authority of Certification authority CA Disig is available on the web site of CA Disig at:
http://www.disig.sk/index.php?id=120

2. General provisions

2.1 Obligations

2.1.1 RA obligations

RA acts as a registry for the certification authority CA Disig - especially for the collection and verification of information from applicants for certification which will be placed to the certificates.

RA is implementing direct contact between applicants and CA Disig.

RA receives certificate request, deliver issued certificates to the holder or to the holder authorized parties, mediates the transfer of certificates and certificate revocation list of customers, receive and handles their complaints, collecting fees from customers for CA Disig provided services.

In its activities, the RA governed by this CPS.

RA is responsible for ensuring that her RA has verified the information collected and that these details are correct at the time.

RA staff is required, inter alia:

- operate according CP of CA Disig, this CPS and instructions of the PMA,
- keep RA private key confidentiality - compromising the private key, the loss of their smart card or forgotten password to access to your private key immediately report to the PMA,
- keep RA correspondence effected in written or electronic form and send written documents for archiving to the CA Disig according to the instruction,
- keep records of RA activities RA in the book "Records of the registration authority CA Disig"
- to the "Records of the registration authority CA Disig" record any other events for RA, mainly events relating to the RA private key (the compromising, the adoption or the loss of the smartcard, forgotten password), RA workplace safety, acceptance (and how handled) initiative, comments or request for interpretation of CP and CPS,
- to do email communication exclusively by signed and possibly encrypted message,
- perform the registration of clients - applicants for a certificate and verify their identity, distinguishing name values in the certificate request, the request format, collect the documents used during the registration process and refuse documents which does not conform to the provisions of this CPS,
- received certificate request process such way that they are insert together with the necessary personal data into CA Disig information system,

- take full responsibility that the collected information were verified and that all the information were correct at the time,
- receive, register and proceed for handling suggestions, comments or requests for interpretation of the CP and CPS, and if a solution based on this document or other binding guidelines for RA is not clear, refer to the handling to PMA,
- accepting request for certificate revocation - proceed valid request, others refuse
- to collected fees from customers for services provided by CA Disig

RA is authorized due urgent technical or operational reasons to suspend its activities for the necessary length of time.

This fact is obliged to report PMA.

Special case of RA is RA called “Mobile registration authority”. Mobile RA functions as a mobile registry, mainly based on contracts with specific customers of CA Disig. Unless a separate agreement with the CA Disig customer exists, the mobile RA acts as a common RA.

RA who performs registration functions as described in this CPS must comply with the provisions of this document and to act accordingly. If it is found that RA fails to comply with these obligations CA Disig will apply to it the appropriate measures, including suspension of its operations as RA.

2.1.2 Subscriber obligations

Obligations of the subscriber:

- continually protect his private key in accordance with this CPS and in accordance with the provisions of the contract,
- immediately notify the CMA, which issued the certificate, on suspicion that the private key has been compromised or lost and this notification must be made through a mechanism that is consistent with this CPS,
- comply with all terms, conditions and restrictions imposed on the use of his private key and certificate,
- precisely identify himself and formulate on any communications with RA respectively CA,
- use provided certificate only for the relevant purposes.

These obligations relating also to the natural person who receives a certificate for managed components.

Subscriber who fails respectively failed to comply with its obligations, is not entitled to compensation for any damage.

2.1.3 Relying party obligations

See section 2.1.4 of actual version CP CA Disig.

2.1.4 Repository obligations

See section 2.1.5 of actual version CP CA Disig.

2.2 Liability

See section 2.2 of actual version CP CA Disig.

2.3 Financial responsibility

See section 2.3 of actual version CP CA Disig.

2.4 Interpretation and Enforcement

See section 2.4 of actual version CP CA Disig.

2.5 Fees

CA Disig disclosed its current price list through the web site Disig CA (see Section 1.4).

Price list for the contractual partner is not published.

2.6 Publication and Repository

2.6.1 Publication of CA information

CA publishes information on the Internet in online mode via its website (repository) which is accessible to holders of certificates and relying parties and which includes:

- all certificates issued by CA Disig to the end users, which are published through the certificates search service,
- current CRL and any CRL issued after the start of certification services by all issuing CA and SubCA,
- CA Disig Root CA and SubCA certificates belonging to their signature key,
- copy of the current CP CA Disig and CPS for RA in electronic form

Information about certificates issued by CA Disig is not disclosed where they are issued for the internal needs of contract partner and partners are contractually agreed to undisclosed.

2.6.2 Frequency of publication

The certificate is published immediately after its issuance and immediately can be downloaded by certificate holder. Information on the issuance of a certificate can be found at http://www.disig.sk, which serves as the repository of the certification authority CA Disig.

CRL is published as specified in section 4.4.3.1. Information about revoked certificate can be found on the Disig website (www.disig.sk), which serves as the repository of the certification authority CA Disig.

All information to be published in the repository, are published as soon as possible.

2.6.3 Access Controls

CA Disig adequate protects any information stored in the repository, which is not intended for public dissemination. To this end, has developed strict rules included in Disig CA security project and related directives.

2.6.4 Repositories

CA Disig repository function will hold the CA Disig web site located on the web site of company Disig (see. 1.4). CA Disig repository page is publicly accessible via the Internet to holders of certificates, to parties relying on certificates and to the public at all.

Publicly available information on the Disig website has the character-driven approach.

Disig make every effort to assure the integrity, confidentiality and availability of data under the provision of certification services. Were also made sense and precautions to prevent unauthorized access to persons who might in any way alter, damage, or erase data stored in the repository (see also 2.6.3).

2.7 Compliance Audit

2.7.1 Frequency of entity compliance audit

CA is undergoing an annual audit of compliance in accordance with the requirements of international standards (e.g. ETSI TS 102 042 "Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates" [6]).

2.7.2 Identity/qualifications of auditor

The auditor must be competent in the field of compliance audits, and must be thoroughly familiar with CP CA Disig and this CPS and must meet the qualification requirements described in document [5]. Auditor is appointed by the PMA.

Compliance audit may be performed only by a person who meets the following requirements:
as the person is:

a) ethical, i.e. fair, truthful, sincere, honest and discreet;
b) open-minded, i.e. willing to consider alternative ideas or points of view;
c) diplomatic, i.e. tactful in dealing with people;
d) a separate i.e. it operates independently and in communications with other partners;

e) holds a certificate authorizing him to perform audits of information systems;

as an auditor must have general knowledge in:

a) the principles, procedures and auditing techniques to ensure that the audit nude run consistently and systematically;
b) the legislative requirements imposed on the system, which is undergoing an audit.

The auditor must document their competency references to audits carried out similar IS.

2.7.3 Topics covered by audit

The purpose of the audit should be a guarantee that the CA Disig has satisfactory system of RA work, which guarantees the quality of services provided by CA Disig and which guarantees that RA acts in accordance with all requirements of these CPS. All aspects of the operation of CA related to this CP shall be subject to audit.

2.7.4 Actions taken as a result of deficiency

When the auditor finds a non-conformance between the RA operation and provisions of this CPS, the following actions must be taken:

a) auditor recorded non-conformance,
b) auditor shall notify the contrary entities defined in Section 2.7.5,
c) CA Disig proposes to the PMA appropriate corrective actions, including the expected time required for its implementation.

PMA shall determine the appropriate corrective actions as far as to the CA Disig certificate revocation. After corrective actions are performed, PMA restores activity of CA Disig or RA.

2.7.5 Communication of results

Auditor makes the audit report for the PMA on the results of audit. Results will be reported to the audited subject (CA Disig respectively RA) and in case of RA also to the CA Disig.

Implementation of corrective actions is brought to the attention of the responsible authority. To illustrate the implementation and effectiveness of corrective actions, may be required a special audit or partial audit focused on the aspect of the audited entity.

2.8 Confidentiality Policy

2.8.1 Types of information to be kept confidential

Confidential information subject to adequate protection are all described in the current CP CA Disig in Section 2.8.1 and:

- private keys belonging to CA Disig units (Administrator CA, RA).

2.8.2 Background release of confidential information

CA Disig not discloses any information relating to an applicant for a certificate or certificate holder to any third party if the information is considered public unless it is required by law or a competent court respectively it is stated in the contract between the CA Disig and its partners.

Any request for release of information not considered public, it must be authenticated and documented.

CA Disig should handle the customer's personal data in accordance with applicable laws and may not provide personal data to any third party except for entities within the meaning of the Act No. 215/2002 Coll. on Electronic Signature and on the amendment and supplementing of certain acts (hereinafter "Act No. 215/2002 Coll.") have the right to control the activities of CA Disig respectively under the Act No. 122/2013 Coll. may be entitled person.

CA Disig has developed its own analysis, plan and guidelines for the protection of personal data in accordance with Act no. 122/2013 Coll.

2.9 Intellectual Property Rights

CA Disig owner is the owner of all copyright in all documents, data, procedures, policies, certificates and private keys, which are part of the CA Disig infrastructure and it was created by him.

3. Identification and authentication

3.1 Initial Registration

Application for a certificate received by CA Disig must comply with the standard PKCS # 10 or SPKAC and must be in PEM format, if not otherwise agreed with the applicant.

3.1.1 Types of names

In general, CA Disig not assigns distinctive names meaning X.500 (X.500 Distinguished Name, "The Distinctive Name").

Applicants for the certificate choose themselves distinctive name, which should be in their certificate.

3.1.2 Need for names to be meaningful

See section 3.1.2 of actual version CP CA Disig.

3.1.3 Uniqueness of names

See section 3.1.3 of actual version CP CA Disig.

3.1.4 Name claim dispute resolution procedure

In case of disputes relating to the names will be transferred under the provisions of section 2.4.

3.1.5 Recognition, authentication and role of trademarks

See section 3.1.5 of actual version CP CA Disig.

3.1.6 Method to prove possession of private key

RA shall require an applicant for confirmation that it possesses the private key that corresponds to a public key contained in the certificate request.

In the case of issuing a new (subsequent) personal certificate on request, which was generated for new soft token cryptographic keys, is acceptable that the applicant for a certificate will confirm ownership of new private key that way that he/she sends new certificate request to RA via signed e-mail.

When signing the e-mail with the request, the applicant must use the private key for which the certification authority CA Disig issued certificate, and this is, at the time of received e-mail verification, valid.

In the event of receiving a certificate request electronically from the applicant who already holds a certificate issued by CA Disig which cannot be signed by private key of that certificate (certificate doesn’t have a secure e-mail extension), private key ownership will be verified by contacting the applicant by the CA Disig with the verification procedure that he/she is the originator of the request.

In the case where the person generates certificate request to the SSCD device then automatically holds the private key in time of his generation.

If the certificate holder does not have SSCD when the key is generated on SSCD on RA, then it SSCD must be received credible manner.

Restricted delivery is considered reliable enough.

CMA does not generate key pairs for foreign entities. Exceptions can only be generation of keys directly on the CMA to the customer SSCD. It can be done only in special cases based on a separate written contract with that customer, which confirms the customer's express desire that the CA Disig should generate key pair on his SSCD.

CA Disig in any case, does not archiving the private key belonging to the client (a foreign entity).

3.1.7 Authentication of legal identity (organization)

An applicant for a certificate, acting on behalf of the legal person shall submit a corporate name, other identifier, if one exists (usually organization ID), address and proof of the existence of the legal person (usually an extract from the Commercial Register).

RA verifies the data and the identity of the physical person (the requesting person) and also verifies that this person has the right to act on behalf of the legal person in case of certificate services.

Legal person (organization) established in the Slovak Republic is proving its identity by extract from the Companies Register of Slovak republic or other existing register of legal persons. RA will require the original or certified copy of the original, not the older than three months. Evidence must include full company name, identifier (usually company ID - ICO), seat, name of person acting as a legal person and the way of the signing procedure of a legal person.

In the event that a legal person not located in the Slovak Republic, its identity is verified in the same manner as described above. Extract from the current register of legal entities must be officially translated into Slovak language (except to organizations based in the Czech Republic).

Natural persons acting on RA in the case of obtaining a certificate on the basis of the extract from the Register on behalf a legal entity must prove their identity according to section 3.1.8.

On behalf of the legal person may act on RA only entitled person who is the statutory (or more of such persons at the same time, if required by an extract from the commercial register), or a legal person may be represented by another natural person or legal entity.

If a legal person is representing on RA by the natural or legal person both must always provide a certified extract from the commercial register for that legal person no older than three months.

If a legal person is representing on RA by the natural person, this natural person must prove their identity according section 3.1.8 and in addition must prove a

power of attorney (signed by a notary or the registrar office) from the text of which is made clear that a natural person is acting on behalf of legal person in the matter of RA services.

If a legal person is representing on RA by another legal person, the legal person except the power of attorney (see previous paragraph) must prove their identity in the same manner as legal person, as required above.

In the event that a legal person can prove his identity extracts from the commercial register (valid for non-commercial entities such as municipality, church, civic associations, foundations, public authority, etc.), that legal person, shall prove their identity and legality of its existence (with a reference to the law or other regulation, which the body of the type of deals) in written form.

When issuing system certificate legal person must prove the truth of an identifying information contained in the certificate request (NTR, VAT, SZ:) by providing the original document attesting the truthfulness.

3.1.8 Authentication of individual identity

Applicants for a certificate may be a citizen of Slovak Republic or a foreign national.

A natural person must prove his identity by two of the following personal documents:

- ID card
- Passport
- Driving license
- Birth certificate
- temporary residence permit (or residence) if the alien
- firearms certificate
- professional card

Is required that at least one of the submitted documents is a document which includes a photograph of the person. In case of submission of birth certificate, arms license or professional card it must also be submit one of the following documents: ID card or passport.

If a natural person is representing on RA by the another natural person, this natural person must prove a power of attorney (signed by a notary or the registrar office) from the text of which is made clear that a natural person is acting on behalf of another natural person in the matter of RA services.

If the legal person represents a natural person, besides the power of attorney (see previous paragraph) must prove their identity under section 3.1.7.

3.1.9 Authentication of the component identity

CMA must be guaranteed that the identity of the component and its public key are appropriately linked.

Hardware or software component that will use certificates will be subject to certification and CA Disig SSL certificate respectively code-signing certificate (not a personal certificate) can be created.

For this reason the component has to be assigned to a specific person or to a person that is authorized to deal on behalf of a company that is administrating the component. (see section 3.1.8 and 5.2).

Person or organization is obliged to provide following information to CMA, as described in sections 3.1.8 and 5.2:

- identification of component (name for software component),
- public key of the component (part of certificate request),
- authorization of component and its characteristics (URL and application description for software component),
- contact information, that CMA may, if necessary, to communicate with this person,

RA will be verify the accuracy of any authorization (values of distinguishing name) to be listed in the certificate and verify the data submitted.

Methods to implement this authentication and control data include:

- verify the identity of the person in accordance with the requirements of section3.1.8,
- verify the identity of the organization, which includes the component, in accordance with the requirements of section 3.1.7,
- verify the competency of using data to be introduced in individual items of the certificate, with an emphasis on CommonName.

The typical value of this item will be fully registered domain name.

The existence of a domain and its owner has been verified through WHOIS services provided by the web top level domain sponsoring organization (e.g. for domain ".sk" is the sponsoring organization SK-NIC - www.sk-nic.sk; for domain ".eu" is the sponsoring organization EURid vzw/asbl established in Belgium for the domain ".com" is sponsoring organization VeriSign Global Registry Services based in the U.S.).

Control over domain will be verified by sending an e-mail which will contain secret information to some unforeseeable e-mail accounts for the domain listed in the record obtained from the WHOIS service respectively on the e-mail from that domain for these possible accounts: admin, administrator, webmaster, hostmaster or postmaster.

An applicant for a SSL certificate for the domain shall send back verification information as proof of ownership of the domain and demonstration that it is under his/her control.

In the event that there is no e-mail address respectively there is no response from expected e-mail addresses because it does not exist, RA must take further steps to verify domain ownership for example use published contact data of domain registrar.

If from the data obtained from the above sources is not possible to reliably determine that the applicant is the owner of the domain or person acting on behalf of the owner of the domain, RA refuses to issue a certificate to that request.

RA performs verifying of all fields from DN of certificate request, except organizationUnitName field. In the case when organizationUnitName filed is not empty the RA performs check if this field not including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA has verified this information according section 4.1.

3.1.10 Authentication of identity among contractors

Identity authentication of individual component under control of the contractual partners of Disig (trading partners) is implemented in cooperation with the responsible party for this company.

Some procedures are simplified in this case and may not to be implementing e.g. verification of domain ownership, e-mail account verification checks and so forth.

3.1.11 Submitted documents

All documents submitted to the RA by applicants for service must be either originals or certified copies of the originals. It cannot be there any indication about add on data, changing data, cross out data etc. The documents which have expiration data must be valid.

If the RA worker has doubts about the identity of a potential customer (e.g. the apparent discrepancy between the photograph in the presentation of a personal document and view customer differences between the two documents etc.), he or she may refuse the registration.

Any documents in foreign languages (except Czech) must be translated into Slovak language by expert translators.

At the request of a potential customer or any RA contentious cases about proving the identity during the procedure of identification will deal under section 2.4.

When submitting the documents to RA it is required to present either the originals of these documents or copies of originals (not necessarily certified) except for personal ID documents. Extract from the Commercial register respectively trade register obtained from the Internet is not sufficient as it is informational only and is not applicable to legal acts

3.1.11.1 Physical person

A physical person shall submit two documents identifying his identity. The primary document is:

- Slovak citizens - a valid identity card or passport,
- Foreigners - proof of identity (namely identity card), residence permit in the Slovak Republic or passport respectively.

Secondary evidence may be:

- passport

- driving license
- health insurance card
- birth certificate
- personal license of professional soldier
- temporary residence permit (or resident) in the case of a foreigner
- firearms license issued by the police department
- service card

It is required, that at least one of the submitted documents was a document which includes a photograph of the person.

In the case of issuing or revocation certificate for contractual partner it suffices that the physical person will establish his identity with one of the following personal documents - an ID card or passport. The applicant for a certificate for contract partner shall meet other conditions for issuing of this type of certificate determined by the contract partner.

If physical person representing on the RA another person, must in addition show a certified (notary) powers. From the text it is clear that the representative was acting on behalf that physical person.

As an applicant for a certificate is the legal representative (usually the parent), must also submit the child's birth certificate, adopt parent must also submit a decision of a court or an extract from the registers. Sufficient proof is the identity card, in which the child is registered.

3.1.11.2 Physical person - employee

As an applicant for a certificate is the physical person who in the certificate request indicates the name of the organization, submit documents according Chapter 3.1.11.1. It must also submit consent to the issuance of a certificate from the employer.

This requirement does not apply to an employee of contract partner, who is contractually agreed upon a different authentication mechanism.

3.1.11.3 Legal person

In this case, the applicant shall submit the certificate documents referred to in Chapter 3.1.11.1. It must also submit a document according Chapter 3.1.7.

As a legal person act more than one person jointly, it is necessary to submit official (notary) the full power. From the text is should be clear that the physical person represents this legal person.

3.1.11.4 Component or code signing

See chapter 3.1.9.

All documents submitted to the RA by applicants for service must be either originals or certified copies of the originals. There cannot be any indication any

indication about add on data, changing data, cross out data etc. The documents which have expiration data must be valid.

If RA has doubts about the identity of a potential customer (e.g. the apparent discrepancy between the photograph in the presented ID card and a real present person) it may refuse registration.

Any documents in foreign languages (except Czech language) must be translated into Slovak language by the official language translators - expert.

All controversial issue about proving the identity will be according procedure written in chapter 2.4.

When submitting the documents on RA it is required present the originals of these documents for inspection or copies of originals (not necessarily certified), except for personal documents identifying the identity of the applicant respectively authorized persons. Extract from the commercial register respectively trade register obtained from the Internet is not sufficient as it is informational only and is not applicable to legal acts.

3.1.12 Submitted documents check

In case of any reasonable doubt about the identity of a potential customer RA may refuse the registration.

RA staff checked on the submitted documents the following:

- Personal documents of physical persons:
  - the validity of the document - in case of invalid personal documents it necessary to proceed as in the absence of such documents - RA refuses registration
  - legal age (i.e. age 18 years) - RA refuse registration of underage since for the underage have the right to act their legal representative (usually parent).
  - consistency between the photograph and personal view of the proprietor of identity documents – if there is evident discrepancy , RA can refuse registration,
  - consistency in the documentation that is whether the data in one document are not inconsistent to another one.
- Extracts from the Commercial Register or another register of legal persons:
  - If extract is not older than 3 months,
  - whether it has/have physical(s) person(s), who submitted a statement power to act (sign) for the legal person as a legal representative,
  - whether extract is a certified (by a notary or the registrar office), if not the original.
- Power of attorney:
  - whether the power of attorney is certified (by a notary or the registrar office)

- whether the information listed in the power of attorney, which defines the physical and/or representative of legal person, , comply with those set on the personal identification card of representative respectively with those set out in the extract or another register representing a legal person,
- the scope of the power of attorney - whether the power of attorney authorized empowered physical or legal person to act as required on the RA on behalf of the physical or legal persons,
- whether any time limit or other conditions specified in power of attorney are all right

- Statutory declaration:
  - The authority to sign – whether the person signing the declaration was authorized to represent the legal person. Eligibility is checked by an extract from companies register respectively another register of legal persons. As the person signing is not registered in this extract, he must submit other evidence on which it can act in the name of company (usually a notary certified power of attorney).

In the case of any reasonable doubt about the identity of a potential customer, also in the case of the deficiencies in the submitted documents respectively submission of incomplete documents, the RA staff shall to refuse registration of the applicant. Certificate services in this case will be refused.

CA Disig will accept also document in electronic form signed by valid Guaranteed Electronic Signature (ZEP) (Commerce register, Power of Attorney, declaration, authorization etc.)

3.1.13 Prior registration RA

Prior registration of persons in the role of RA is carried out under the same conditions as for the customer - the applicant's personal certificate, as is described above. Verify of the identity of RA staff is made by Disig employees unless is contractually agreed a different mechanism.

3.2 Subsequent issue of certificate

Requirements for subsequent certificate issuing are described in detail in actual CA Disig Certificate Policy section 3.2.

RA shall issue a certificate without an applicant personal visit for personal certificate or system certificate for legal person only when the requirements written in section 3.2 letter a) of current CP are fulfilled. Verification of the certificate request, in case of an unsigned e-mail from the e-mail address identical to that in the request, respectively sent from another e-mail as in the request made RA so that sent to a given e-mail address an electronic message which will contain a secret unpredictable information (authentication information). The applicant for a certificate must returned back authentication information as a proof of sending request for issuing of the subsequent certificate. The answer must be sent within

a specified period of time, sufficient to send e-mail. In case the verification of sending the request fail, CA Disig refuses issuance of a certificate.

3.3 Issue of subsequent certificate after expiration of the previous one

After the expiration of the certificate, the applicant must follow all requirements of the initial registration.

3.4 Revocation Request

Certificate revocation request shall be authenticated, see section 4.4. The request may be authenticated using the private key belonging to the certificate, regardless of whether the private key has been compromised or not.

4. Operational requirements

4.1 Certificate Application

When an applicant for a certificate will apply for a certificate, the applicant and the RA must perform the following steps:

- RA shall verify and record the identity of the applicant (according Section 3.1) and also verify any particular data which are in the certificate request from independent sources or alternative communication channels,
- applicant must have generated key pair (public and private key) for each requested certificate,
- applicant shall demonstrate that the public key create pair with the private key that is owned by the applicant (according Section 3.1.6),
- applicant shall provide sufficient documentation to verify any particulars data to be given to the certificate.

All communication between the different part of CA Disig concerning certificate request and issuing a certificate should be authenticated and protected from modification. Any electronic transmission of shared secrets must be encrypted.

4.1.1 The detailed procedure for obtaining a personal certificate or system certificate for legal person

4.1.1.1 Preparing to visit RA

Customer (applicant for a certificate) takes the following steps:

- Familiarize self with this procedure, possibly with the principles and instructions for obtaining a certificate.
- Generate on computer on the Disig web site using a supported browser a new certificate request (see URL at section 1.4) and stores it on the appropriate medium (HDD, USB drive, floppy, etc.).

We are given notice that due to security reason the certificate request respectively public key in it, for which a certificate has been issued, cannot be used for new certificate and the RA will refused issuance!

Request shall include an appropriately completed all mandatory items defined in section 3.1.2 of the current CP CA Disig. Mandatory items shall be completed in such a manner that the values are consistent with this CPS, with emphasis on the part of 3.1.2. When entering values into heading an application for a certificate should be the applicant for a certificate to bear in mind that RA will have a satisfactory way to prove all the data entered into the individual items of the application for a certificate.

All data must be entered without diacritics (softened, accents, etc.).

Using special characters (e.g. comma, dash = / and others) should be limited to the minimum amount necessary, recommend that if these characters to be used in agreement with CA Disig, otherwise the CA Disig reserves the right to refuse such an application for a certificate.

In the "Organization" shall not use a comma character.

- Prepare his/her chosen identity documents respectively other necessary documents, for example extract from the commercial register (we recommend to verify the validity of documents) under the provisions of Part 3

Note: It is recommended to the client to prepare the copy (not certified) of all documents (except for personal papers of individuals) who intends to submit to RA (e.g. an extract from the Commercial Register and other evidence of legal entity, power of attorney) to allow it to pass on RA. Extract from the commercial register obtained from the Internet is not sufficient, as is FOR information only and is not applicable for legal transactions. It is recommended that the applicant before visiting RA will verify and clarify any doubts and difficulties, especially those concerning the appropriateness of the values of individual items in the certificate request.

- Arrange his/her visit at RA via phone or email.
- Send electronically certificate request to the RA - RA e-mail addresses are available on the Disig website (see 1.4). Certificate request decided for signing and encryption of electronic mail extension "Secure Email (1.3.6.1.5.5.7.3.4)" shall be send from an e-mail address specified in the certificate request.

4.1.1.2 RA Visit

A customer comes to RA, taking with them or identify respectively submit:

- Certificate request generated by the browser in electronic form

Note: Customer must be able to identify on the RA RequestId indication value (as numeric string proceeded by the string "disigweb" that uniquely identifies the generated certificate request) of the certificate request. Application for a certificate for signing and encryption of electronic mail shall be send to the RA electronically in advance (see 4.1.1.1).

- Selected identity documents respectively other necessary documents, for example extract from the Commercial Register, credentials, etc. under the provisions of Part 3

Note: The customer submits to the RA the copy (not verified) of all documents (except for personal papers) necessary for registration (e.g. an extract from the Commercial Register and other evidence of legal entity, power of attorney, if representing another entity).

- Appropriate amount of money, if not previously agreed another form of payment for the certificate.

4.1.1.3 RA procedure for electronically sent certificate request

1. RA staff verify if electronically sent certificate request from an applicant (it is compulsory for certificates with extension "Secure Email (1.3.6.1.5.5.7.3.4)"), was sent from the same e-mail addresses, what is in the certificate request. If the differences observed refuses to issue the certificate.
2. In the case when certificate request sent in advance contains the same e-mail address as from which it was sent, the RA staff shall verify validity of this e-mail address. . Verification is carried out so that to the e-mail address is sending a mail message containing secret unpredictable information

(authentication information). An applicant for a certificate shall send back to the CA Disig verification information as evidence of control of the e-mail addresses. The answer shall be send within a specified period of time sufficient for sending email. In case that the verification of e-mail address runs unsuccessfully, CA Disig refuses to issue the certificate. Detailed procedure is described in the RA working manuals and is also subject to the initial training of RA staff.

3. Verification of e-mail address ownership for Disig contractual partner's employee who are sending certificate request from the contractor domain is not made.

4.1.1.4 Procedure for registering customers on RA

1. RA staff verifies the identity of the applicant or his/her representative according to the provisions of sections 3.1.7 and 3.1.8.
2. RA staff selects certificate request, identified by the applicant. Certificate request intended for signing and encryption of electronic mail must be sent electronically to the RA from the e-mail address which is written in the DN of the request.
3. RA staff checks the completeness and correctness of received certificate request (for example if some items do not include erroneous data).

Note: All fields must be completed without diacritics. Fields are sensitive to case. Field "City", "Organization" and "Organizational Unit" are optional. Application filed labeled as "e-mail" must be filled mandatory with the valid customer email address.

An applicant for a certificate shall satisfactorily demonstrate to the RA all the data entered into the certificate request fields. If the applicant shall also submit other documents (except for personal papers of individuals, e.g. Extract from the commercial register or other proof of legal entity, full power in case of representing another entity), the worker assumes RA and keep a copy (not certified) of all documents submitted, compare them with the original and each copy of the written text to confirm compliance with the original "and insert the date and your signature. Extract from the commercial register obtained from the Internet is not sufficient, as is information only and is not applicable to legal transactions.

4. Through a CA Disig to automatically verify the public key contained in the submitted application for a certificate has been previously issued certificate. Where, RA certificate request is rejected for security reasons to take, since once the certified public key can be used in a certificate.
5. RA worker applicant shall submit a certificate to sign the Treaty on the issue of a certificate of use and service CA Disig two copies - one for CA Disig and a customer. Consent by the applicant with this contract is subject to receipt of an application for a certificate and a certificate.
6. The customer pays the amount under the applicable Certificate lists service CA Disig paragraph under the Treaty, unless other agreed payment method.
7. RA worker placed in a Disig CA certificate request and other required information.

Note: In case of the application for a certificate for some reason it cannot be certified, CA Disig shall notify the RA, including giving a reason, which then notify the applicant of the

certificate. An applicant for a certificate can then either submit a new application for a certificate or it will be refunded the money paid.

8. Immediately after the issuance of a certificate applicant will be able to download your certificate. However, the applicant shall sign the certificate and the RA worker "Confirmation of personal certificate issuance and transfer of the applicant for a certificate, which is attached to" the issuance of a certificate of use and service CA Disig. This certificate shall be made in duplicate - one for the applicant and will remain an RA, which can then be forwarded to the issuing CA Disig. For contractors, whose employees are issued certificates on a contractual basis is only signed "Confirmation of personal certificate issuance and transfer of the applicant for a certificate.

The same procedure applies for application for a code-signing certificate.

4.1.2 The detailed procedure for obtaining a SSL certificate

4.1.2.1 Preparation for the visit of RA

Customer (applicant for a certificate) takes the following steps:

- become familiar with this procedure or with the principles and guidelines for obtaining a certificate,
- with appropriate software (typically. Microsoft IIS or Apache / OpenSSL) will generate a certificate request for the SSL certificate and send it electronically to the RA respectively save it on a suitable removable media for backup,

  Comments and Notes: Please note that a SSL certificate request respectively public key for which certificate has been issued before cannot be for safety reasons used to re-issue another SSL certificate and the RA will such request refused! SSL certificate request shall contain appropriately filled in field subject:commonName (the name of the component). Individual fields should be completed that way that entered values are consistent with this document, with emphasis on the part of 3.1.2, and to will clearly identify the device which will use issued SSL certificate (typically, for example. specifying details such as the fully qualified domain name). If organizationName is present, then localityName is required. If organizationName is absent, then the certificate must not contain a localityName.

  Use special characters (e.g. comma, dash, = / and others) should be limited to the minimum. We recommend use these characters only upon an agreement with CA Disig, otherwise Disig CA reserves the right to refuse such a SSL certificated request. All data must be entered without diacritics (softened, accents, etc.). In the organization filed may not be used the comma character. Applicants for a SSL certificate can only be a statutory of organization which is the owner of entity (e.g. fully qualified domain name, registered IP address, etc.) to be listed in the certificate or authorized person by him. All data in the certificate requests must be made by the applicant plausibly, except for items subject: organizationUnitName (OU). Item OU may include corporate name, trademark, address, location, or other text indicating the determinable physical or legal person, unless the use of this information, the applicant cannot credibly substantiate.

- prepare selected identity documents or the other necessary documents, e.g. extract from the Commercial Register (we recommend to verify the validity of documents) under the provisions of Part 3

Note: It is necessary that the customer will prepare copies (need not be verified) of all documents (except for personal documents), intends to submit to the RA (e.g. extract from the Commercial Register and the other documents of a legal person, power of attorney in case of represent at RA), so that it can deliver for RA. Submission of Commercial Registration obtained from the Internet by the applicant is not sufficient because this statement is for informational purposes only and is not used for legal purposes. It is recommended that the customer before of visiting RA verify and clarify possible doubts and problems, especially those concerning the appropriateness of the value of individual fields in the certificate request

- arrange an appointment RA (telephone, e-mail).

4.1.2.2 RA procedure before issuing a SSL certificate

1. The SSL certificates are on principle issued only by the Disig company staff only in the company location at Bratislava.
2. Based on previously sent request RA shall verify domain ownership within the meaning of paragraph. 3.1.9 and also check the completeness and correctness of the requests for an SSL certificate in accordance with the requirements of section 3.1.2.3 CP Table. 3, relating to items subject: organizationName a subject: localityName. If there is seriously suspected unauthorized use of the second level domain by the applicants RA shall be entitled to require from the applicant credible documented evidence of the authorization to use second level domain, otherwise the RA may refuse to accept this SSL certificate request. Verify domain ownership does not affect SSL certificate applicants who are Disig contractors.

Warnings and Notes: All fields shall be completed without diacritics. Uppercase and lowercase letters are distinguished. Fields "Organization", "Organization unit", “Locality” and "Email" are optional. The application must contain a properly completed entry commonName (i.e. entity name). Each field shall be completed, so that entered values are consistent with this document, with emphasis on the part of 3.1.2 In assessing the value of all fields meaningfulness of them shall be taken into account by RA staff (see section 3.1.2)- a breach of the principle of rationality may be a reason for refusing to issue the certificate. The full domain name must not be included in any other filed, except filed subject: CommonName (CN) and the certificate extension SubjectAlternativeName. If the field O (subject: organizationName) in request is filled in, also filed L (subject: localityName) shall be filled in. If the field O (subject: organizationName) is missing in the request, then field L (subject: localityName) shall not be in the request. OU filed may not include corporate name, trade name, trademark, address, location, or other text indicating the determinable physical or legal person, unless such information is not reliably verified and that the application also contains subject:organizationName, subject:localityName, and subject:countryName, which were also verified as credible. If an applicant submits other documents, other than personal documents of individuals, e.g. extract from the Commercial Register or other evidence of legal entity, power of attorney etc., RA staff takes over and retain copies (need not be verified) all submitted documents, compare them with the original and on each copy writes the text "certify compliance with the original" and insert the date and signature. Submission of extract from Commercial Register obtained from the Internet by the applicant is not sufficient because this extract is for informational purposes only and is not possible to use it for legal purposes. RA staff verifies that the issuance of a certificate will avoid duplication of certificate e.g. whether the entity has no valid personal certificate - emphasis is placed on the value subject:commonName.

Failure to meet the above conditions is a major reason for rejection of the certificate request.

3. Issuing a SSL certificate by external RA is possible only with the prior written consent of PMA CA Disig. Consent is given in the form of signed electronic message from a member of PMA Disig CA (see CP CA Disig section 1.3.1.1).
4. Before arrangement of meeting with their client by the external RA, they shall ask PMA CA Disig for authorization of issuing SSL certificate. Consent is sought by e-signed message, which will in appendix contain information about the applicant and the domain for which the issuance of a certificate is sought. Details about the extent of information transmitted will be sent to each RA by methodological guidelines by CA Disig.

4.1.2.3 Visiting of RA

1. Customer in the agreed time comes to RA, taking with him:
   - selected identity documents and other necessary documents, e. g. commercial registration, power of attorney etc. under the provisions of Part 3. Customer gives to the RA copies (may not be verified) of all documents (other than personal documents of individuals) to be submitted to the RA during registration (e. g. commercial registration and other documents of a legal person, power of attorney etc.
   - appropriate amount of money, if not agreed in advance any other form of payment for the certificate

4.1.2.4 The registration procedure on RA

1. RA staff verifies the identity of the applicant or other person who represents applicant, according to the provisions of sections 3.1.7 and 3.1.8.
2. RA staff asks the applicant to identify certificate request.
3. Through the information system of CA Disig is automatically verified that on the public key contained in the certificate request has not previously been issued a certificate. If yes, RA staff shall reject certificate request for security reasons, because once certified public key cannot be used for a new certificate.
4. RA staff shall submit to the applicant for signing the "Agreement on the issuance and use of CA Disig certificate services" in two copies - one for CA Disig and one for the customer. Consent of the applicant with the text of this agreement is subject to receipt of his/her certificate request.
5. Customer will pay for the issued certificate according the current price list of CA Disig in terms of the appropriate agreement paragraph, if not agreed otherwise method of payment.
6. The RA staff enter to the IS of CA Disig certificate request and other required information.

Note: In case of the application for a certificate for some reason it cannot be certified, CA shall notify the appropriate RA, including giving a reason, which then notifies the applicant of the certificate. The applicant for a certificate may then either submit a new application for a certificate or it will be refunded the money paid.

7. Immediately after the issuance of a certificate applicant will be able to download your certificate. In doing so, the applicant shall sign the certificate and the RA worker "Proof of issuance of a certificate and a certificate presented by the applicant", annexed to the Treaty on the issue of a certificate using a CA Disig services. This certificate shall be prepared in duplicate - one for the applicant and will remain an RA, which then forwarded to the issuing CA Disig.

4.1.3 CAA Records review

CA Disig requires for the issuance of SSL certificates personal presence of the applicant or his authorized person, where during the physical presence verifies the content of the SSL certificate request. For that reason does not perform verification CAA record for full domain name for which the SSL certificate to be issued, assuming that the applicant is aware of the limits laid down for that domain.

4.2 Certificate Issuance

CA Disig:

- not create a certificate, while not complete to the satisfaction of all verification and any changes, if necessary,
- is not responsible for any additional expense of the applicant that arise during the course of registration, for example, because of the need for repeated visits of RA, due to incomplete or missing documents or other deficiencies.

Although the applicant has prepared most of the data fields of the certificate request, the RA remains a responsibility to verify that the information is accurate and precise.

RA staff is responsible for the verifying of the applicant's data.

CA Disig has the right not to issue a certificate, although the applicant has passed registration process at RA, if subsequently is found significant fact that prevents the release of the certificate (e.g. error in the format of the certificate request).

4.2.1 Service of a private key to the certificate holder

The private key is generated by the applicant itself.

4.2.2 CA Disig public key delivered to users

CMA and the parties relying on certificates must act in cooperation to ensure authenticated and integral delivery of the CA Disig certificate.

Acceptable methods for delivery CA Disig certificate and authenticated are:

- upload the certificate from Disig web site (see 1.4),
- download the certificate directly to the Active Directory,
- using SSCD RA can upload trusted certificates to the delivered SSCD,

- receive CA Disig certificate personally at RA,

RA provide the party relying on the certificates or any other candidate with fingerprint (hash) of CA Disig namely via telephone, secure e-mail or personally at RA.

The specific choice of the method of providing fingerprints (hash) depends on the agreement with the interested parties. In addition, Disig will publish on their web site fingerprint of CA Disig certificate.

Fingerprint (or hash) sent together with the certificate is not acceptable as an authentication mechanism.

4.3 Certificate Acceptance

Since CA Disig is working in online mode e.g. certificates are created and issued, upon RA staff request, automatically and continuously, the applicant will usually be able to download the issued certificate during the same RA visit.

Immediately after the certificate issuance applicant can take his/her certificate. In doing so, the applicant shall sign document "Potvrdenie o vydaní certifikátu a jeho odovzdaní žiadateľovi o certifikát (Confirmation about certificate issuing and delivery to the applicant)" annexed document to "Zmluvy o vydaní a používaní certifikátu a služieb CA Disig (Agreement about certificate issuing and using CA Disig services". This document shall be made in two copies - one for the applicant and one will remain an RA, which then forwarded this copy to the CA Disig.

The certificate applicant can be represented at RA for certificate acceptance by another natural or legal person under the same conditions as when applying for a certificate (see section 3.1.7 respectively. 3.1.8). Receipt of the certificate is normally made at the same RA, where certificate request was made.

Notice about certificate issuance will be send to the email address specified in the certificate and passed the certificate holder or the entity it represents, along with the CA Disig root and intermediate certificate and CP document. For both certificates and documents is sufficient give a link to the Disig website, where they are available.

CA Disig can have any other procedure for certificate taking based on separate agreement with the applicant.

4.3.1 Initial upload the newly created certificate

4.3.1.1 Personal Certificate

Generally there are two ways to upload the newly created personal certificate into browser so that can be assigned by the browser to the corresponding private key that is created and stored on that PC, in the right user profile and used browser:

- Using links, which the applicant receives in an e-mail sending from CA Disig;
- Via opening the file containing the certificate in DER format (file must have the appropriate extension, e.g. der) and certificate installation.

Conditions for proper installation of the initial certificate are that shall be done:

- on the same computer,
- in the same user profile,
- in the same browser,

as where certificate request for that certificate was generated.

4.3.1.2 SSL certificate

The procedure for installing the newly created SSL certificate depends on the particular software or hardware respectively on which has the certificate should be used.

4.4 Certificate Revocation and Suspension

4.4.1 Circumstances for revocation

4.4.1.1 Background of revocation certificate

The certificate is revoked when the binding between the entity and its public key, defined in the certificate, is no longer considered valid. Examples of circumstances, which abolished this binding, are:

- the Subscriber requests or other authorized party requests in writing that the CA revoke the Certificate;
- the CA Disig obtains evidence that the subscriber's private key (corresponding to the public key in the certificate) has suffered a key compromise, or that the certificate has otherwise been misused;
- the CA Disig is made aware that a subscriber has violated one or more of its material obligations under the subscriber use Agreement;
- the CA Disig is made aware of a material change in the information contained in the Certificate;
- the CA Disig is made aware that the certificate was not issued in accordance with the CA Disig' s Certificate Policy or Certification Practice Statement;
- the CA Disig determines that any of the information appearing in the Certificate is inaccurate or misleading;
- the CA Disig ceases operations for any reason and has not made arrangements for another CA to provide revocation support for the certificate;
- circumstances that require the issue of the certificate (testing, verification, etc.) ended;
- there was a loss of private key;
- certificate holder the cancellation of the certificate;

- technical content or format of the certificate presents an unacceptable risk to Application Software Suppliers or Relying Parties (signature cryptographic algorithm change; cryptographic key length change etc.);
- death of the of the certificate subscriber;
- compromising of issuing CA Disig private key occurred;
- final judgment or preliminary court decision.

Whenever the CA Disig aware of any of the above circumstances, the certificate shall be revoked and shall be on the CRL.

Revoked certificates are present in all new editions of the CRL, at least until the certificates will not expire.

4.4.1.2 Who can request revocation

The holder of the certificate (or authorized physical or legal person) may request the revocation of its own certificate and without giving any reason for the request for revocation of certificate.

RA is put the suggestion to revoke holder's certificate, if he becomes aware that arise any of the circumstances described in Section 4.4.1.1.

If the certificate was issued under a special contract with the contractual partner, in this contract can be arranged, who in addition to the certificate holder has the right to ask for its revocation, how and under what circumstances.

The certificate revocation can also apply:

- CMA (the staffer is required to document this fact in writing, including reasons for its action),
- court through its judgments and preliminary decision (to documents on the certificate revocation shall include a copy of the court decision)
- entity (physical or legal person) on the basis of inheritance (to documents concerning the certificate revocation shall include a copy of the documents, which show the right to request revocation of the certificate

In the case of a certificate for RA may be the revocation of the certificate in addition to its holder (the RA) also applies to PMA, if it becomes a serious factor (see section 4.4.1.1) to revoke the certificate.

4.4.1.3 Procedure for revocation request

In the case of conditions for authentication applicant for certificate revocation (chapter 3.1.7. 3.1.8), revocation request may be submitted:

- Personally at any RA using the form "Application for revocation of certificate „which is available on RA - RA staff may request a password from the applicant to revoke the certificate if the applicant for revocation of the certificate is not the holder of a certificate, but the authorized person.

- By electronic mail - sending an electronic mail message, signed by the private key associated with the certificate, the revocation of the calls. In the message shall be clear intention for revocation of the certificate,

expressed by the words "I request the revocation of my certificate with serial number XXXXXX“.

- By electronic mail - sending an electronic mail message (not signed). In the message shall be clear intention for revocation of the certificate, expressed by the words "I request the revocation of the certificate with serial number XXXXXX“. This message must be sent together with the password for the certificate revocation.
- Through the post with password for the certificate revocation sent to the address of the RA which issued the certificate.
- Via telephone at the telephone number of a corresponding RA that issued the certificate, which to be revoked. Telephone number is published on the CA Disig web site. The applicant is required to enter a password to revoke the certificate.

Revocation request for certificate issued for the contractual partner purpose can be administered only at the RA which is mentioned in the contract and acts on behalf of the CA Disig.

If necessary, the RA will provide assistance to the applicant to identify the serial number of the certificate for revocation purpose. If the holder of a certificate will be represent at the RA by another person, representing person shall demonstrate proven powers (notary or registry) and from the text should be clearly evident that the holder of the certificate will revoke its certificate.

In certificate was revoke on the basis of a court decision, the RA staff is obliged to attach a photocopy of a court decision.

In the event that the certificate revocation decision made on the basis of CA Disig or RA, RA staff is obliged to attach record on which the revocation was made.

Expired certificate cannot be revoked

4.4.1.4 Revocation request grace period

This CP does not provide any specific time to revoke the certificate. CA Disig after receipt of a proper revocation request will revoke certificates as quickly as possible. CA Disig must revoke certificates within the time limits described in Section 4.4.3.1.

CA Disig automatically informs the holder of the certificate by e-mail about the revocation of its certificate. E-mail is send to the e-mail address included in the certificate and in the message text are details of the reason of the certificate revocation.

4.4.2 Circumstances for suspension

Certificate suspension means the temporary suspension of their validity.

CA Disig doesn’t support this service.

4.4.3 Certificate Revocation List

4.4.3.1 CRL issuance frequency

See section 4.4.3.1 of the current CP CA Disig.

4.4.3.2 CRL checking requirements

In the time between the competent certificate revocation requests and the publication of the revoked certificate to the CRL certificate holder bears all the responsibility for any damage caused by misuse of his or her certificate. After publishing certificate in the CRL bears all the responsibility for any damage caused by the use of revoked certificate party relied to this certificate.

Not verifying certificate status using CRLs is treated as a gross violation of this CP.

4.4.4 On-line revocation/status checking availability

Checking the current status of the certificate is done through:

- List of issued certificates at: http://www.disig.sk
- Certificate Revocation List at the following addresses:
  - http://www.disig.sk/ca/crl/ca_disig.crl
  - http://ca.disig.sk/ca/crl/ca_disig.crl

4.4.5 Other forms of revocation advertisements available

RA will respond by phone or email on inquiry regarding the status of a particular certificate, if this demand was made by phone, fax or email.

4.5 Security Audit Procedures

4.5.1 Types of events recorded

Recorded are all the events at CMA and all interactions between certificate applicants or holders and CMA.

Records may be in electronic or in written form and can be created either automatically or manually.

Viewing records will allow only to the individual components of the CMA regarding the scope of their activities, in full to PMA and persons performing the audit.

Records are regularly archived.

4.6 Records Archival

Record archiving is performed at regular intervals to ensure long-term deposit records as required by Act. No. 215/2002 Coll.

Full view of the archived records is allowing to PMA and to the persons performing the audit

Modification or removal of archived information is not acceptable.

4.7 Key Changeover

CA Disig uses his signature (private) key for creating certificates for end entity (holders). Parties relying on end entity certificates are using CA Disig root certificate during the whole period of validity of their certificates. For this reason, CA Disig will not issue certificate to the end entity, while its validity time exceeds the validity time of CA Disig root certificate. Validity period of CA Disig root certificate must exceed the validity of all issued certificates to the end-entity.

After creating a new root CA Disig certificate this one will be published on CA Disig web site.

The entire process must take place without negative impact on security.

4.8 Compromise and Disaster Recovery

In the case of compromising the CA Disig root or subCA private keys are the corresponding certificate issued on public key revoked and also the private keys are revoked.

Information about revocation must be publishing as fast as possible. Consequently, it has to be performed new installation of CA Disig key pairs.

CA Disig notifies all holders of the certificates which were signed by compromise key on its revocation as well as relying parties.

Revoked CA Disig certificate should be removed from each application, used by parties relying on certificates and should be replaced by a new CA Disig root certificate.

Distribution of new CA Disig root certificate should be made in a reliable manner and in accordance with Section 2.6.

In the event of a disaster in which the equipment of CA Disig is damaged and unable to operate, but the signature key is not destroyed, the operation of CA Disig shall be restored as quickly as possible, while the priority is giving to the revocation of the certificates and the ability to publish CRL.

In the event of a disaster in which the infrastructure of CA Disig is physically destroyed and also its signature key is destroyed, CA Disig certificate will be revoked.

Subsequently, the complete installation of CA Disig will be restoring as follows:

- renewal of CA equipment,
- generated new CA Disig keys
- creating a new CA Disig certificate
- creation of new RA certificates,

- issuance of all end-entity certificates by the new CA Disig certification authority,

> ***Note:*** *Costs per creation of new certificates of end-entities affected by the creation of a new CA certificate, shall be liable in this case to CA Disig.*

Parties relying on certificates may on their own risk continue the use of certificates signed using the destroyed private key to meet the urgent operational requirements.

4.9 CA Disig Termination

At the termination of the CA Disig certification authority for reasons other than events due act of God (e.g. natural disaster, war, the decision of state power and so on) proceed in accordance with Section 4.8.

CA Disig makes available information on terminating his activities to of all holders of valid certificates and parties relying on certificates.

After terminating of its activities CA Disig will not issue any certificate and ensure that his signature data (private key) will be demonstrably destroyed.

Before the finishing end CA activities all RA provide archived data to the CA Disig according the PMA instruction.

5. Physical, procedural, and personnel security controls

5.1 Physical Controls

Facilities CA Disig consists only of equipment dedicated to the functions of the CA and does not serve to any purposes not related to this function.

Unauthorized use of CA Disig equipment is prohibited. They should be implemented measures for the physical security to protect the CMA hardware and software from unauthorized use. CMA cryptographic modules shall be protected against theft, loss and unauthorized use.

CA Disig facilities must be constantly protected against unauthorized access and from unauthorized physical access too.

RA equipment shall be protected from unauthorized access, as it is installed and activated the cryptographic module. RA has implemented measures to control physical access in order to reduce the risk of diversion and counterfeiting. These security mechanisms should be appropriate to the level of threat in the RA equipment environment.

Detachable CMA cryptographic modules shall be deactivated prior to the imposition. When not in use, detachable cryptographic modules, and any activation information used to access or enable CMA cryptographic modules or other CMA equipment must be placed in locked facilities (security cabinets, safes, etc.). Activation data should be recorded and impose adequate security provided to the cryptographic module and should not be imposed together with the cryptographic module.

Equipment and area in which it is CA Disig equipment located shall be adequately supplied with electricity and air-conditioned to create a reliable operating environment.

Media should be stored so that they are protected from accidental, inadvertent damage (water, fire, electromagnetic). The media, which contain information relating to the security audit, archive or backup information, shall be stored in a location separate from the CMA equipment.

Backups of system sufficient for the recovery in the event of system failures are implemented by a periodic schedule. Backups are stored on-site physical and procedural measures appropriate to the operating CA.

5.2 Procedural Controls

Persons selected to the roles that require reliability, must be responsible and trustworthy.

The functions performed by these roles form the basis of trust in the entire PKI.

Two approaches are practice to increase the likelihood that these roles will be implemented successfully.

The first approach is to ensure that the person performing the role is trustworthy and properly trained and instructed.

The second approach is sharing functions between the roles of several people so that any harmful activities require an agreement with another person.

The primary role requiring credibility as defined in this CP is CA and RA.

Each CA, which operates under this CP, is subject to the provisions of this CP. CA is responsible to ensure, at first, that according this CP are performed the following functions:

- RA functions as described in the following paragraph, if not separated RA
- issuing and revocation of certificate
- publication and delivery of certificates and CRLs
- performing backups,
- administrative functions such as record about compromising and maintenance of database,
- operation of hardware cryptographic module

Each RA, which operates according this CP, is subject to the restrictions of this CP and CPS, by which it works.

The responsibility of the RA is in the first place:

- verification of identity, either through personal contact or through a third party if this is allowed,
- recording information about certificate applicants and verification of accuracy of recorded information,
- secure communications with the CA,
- reception and distribution of user certificates
- communication with certificate applicants and certificate holders of

The role of RA is highly dependent on the implementation of PKI and local requirements. Responsibility RA and management of RA should be described in detail in the CPS of the CA if the CA uses the RA.

Person responsible for component takes the role of an applicant for a certificate and the certificate holder when certificate is issued to the hardware or software components. Person responsible for component acts in synergy with RA in registering components (routers, firewalls, etc.) in accordance with Section 3.1.9 and is responsible for performing the duties of holders of certificates as defined in this CP.

5.3 Personnel Controls

Personnel security controls are provided by the internal mechanisms of the entity - founder.

Personnel for the CMA or any other role requiring credibility should be selected on the basis of loyalty, fidelity, credibility and integrity. All persons in the CMA would be a citizen of Slovak Republic.

All staff included in the CMA operation shall be properly trained. Topics are to include the operation of CMA software and hardware, operating and safety procedures, the provisions of this CP. Required specific training will depend on the use of equipment and selected staff.

6. Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

This CP does not exclude any source of keys which were generated in accordance with its provisions, and local safety requirements. It is expected that the private key will be generated by an entity that becomes its holder for example applicant for a certificate or RA and the SSCD equipment (e.g. computer, smart card, HSM module, etc.), which at the time of generating under the immediate control of the entity that holds the generated key.

The private key will not get out of the module, in which it was generated, with the exception that is encrypted because of its local transmission, or treatment or custody.

CA Disig essentially does not make a key pairs generation for the foreign entity on the facilities belonging to the CA Disig. This is also true for all RA.

6.1.2 Service to the certificate holder

If the private key is generated by a person other than the holder, private key shall be delivered to the holder on SSCD such way, that there is no possibility to pull it out unenciphered.

6.1.3 Key sizes

CPS recommended keys length respectively minimum key length for all types of entities and all used algorithms (e.g. RSA).

In the case of the RSA algorithm the minimum key length must be at least 2 048 bits.

In the case of the RSA algorithm, the minimum key length of root CA or subCA keys must be at least 2 048 bits.

Sha1RSA or sha256 RSA signing algorithms are used for subCA certificates.

SubCA validity shall be shorter than Root CA validity.

6.2 Private Key Protection

6.2.1 CA private key

CA Disig private key is stored in special equipment - HSM module, which is certified according to the standard FIPS 140-2 level 3.

At the operations with the CA Disig private key (e.g. generation, backup and destruction) will be always present defined number of authorized persons according the "k" of "n" principle. Only to authorized persons can operate with the CA Disig private key.

The private key is used solely for signing certificates and CRLs issued by CA Disig.

Before any operation with the CA Disig private key, the authentication of the defined number of authorized persons shall be performed. The defined number is according the "k" of "n" principle and authorized persons are using cards belonging to the HSM module, in which the CA Disig private key is stored. The backup of CA Disig private key is performed by the HSM software in encrypted form. For the decryption is necessary authentication of the defined number of authorized persons on the "k" of "n" principle who are holders of the administrator cards belonging to the HSM module, in which CA Disig private key is stored.

HSM module with the CA Disig private key inside together with the computer for issuing CA Disig certificates will be located at the regime workplace in a room that has security classification level, at least, the "Confidential" pursuant to Act 215/2004 Coll. on the Protection of classified information and on the amendment and supplementing of certain acts.

CA Disig facilities are continually protected against unauthorized access and from unauthorized physical access.

HSM module meets capture protection against electromagnetic radiation.

To avoid capture of electromagnetic radiation, including the sound outside the protected area, will require special safety equipment.

Room is located in the building, which is constantly guarded night and day by guard service and security technology.

6.2.2 Other private keys

It should be ensured that the asymmetric private key never leave the HSM module in the non-encrypted form.

No one is allowed to have access to a private signature key, except the holder.

Key holders are permitted to back up their own key pairs.

During the backup and transfer the keys shall be encrypted. Key holder is responsible for guaranteeing that all copies of private key are protected, including the protection of all workstations, which is located any of his private key. Pass-phrases, PINs, biometric data or other mechanisms of equivalent authentication robustness shall be used to protect access to use the private key.

The activation data may be distributed to holders face to face or by postal service, but separately from the cryptographic module, which activated.

If the activation data are in the written form, they should be protected at the same level as data which are secured by the cryptographic module and should not be kept together with him.

Activation data for the private keys belonging to a certificate confirming the identity of an individual shall never be shared.

Activation data for the private keys belonging to a certificate which conforming the identity of the organization shall be known only to those who in the organization are authorized to use those private key.

6.3 Keys pair management

All certificates issued by CA Disig will be deposited the next 10 years after the end of their validity respectively after termination of the CA Disig operation.

Private keys stored in the SSCD devices are not possible archived outside the assembly.

Archiving of the private keys is fully a matter of the holders of the keys, CA Disig cannot archive private keys, since they are not available to CA Disig and also CA Disig is not generating them for the external entities.

6.4 Computer Security Controls

CA Disig computer equipment is used exclusively for the purposes of conducting certification activities. Information security of CA Disig system is regularly control for compliance with the requirement of ISO 17799 and ISO 13335.

7. Certificate and CRL Profiles

7.1 Certificate profiles

This CP is managed only X.509 v3 digital certificates. All certificate profiles issued by CA Disig are described in actual and valid CA Disig Certification Policy in section 7.1.

7.2 CRL profile

CRL issued by CA Disig are CRL version 2.

Signature Algorithm:	**sha1RSA resp. sha256RSA**

CRL content all issued certificate regardless their expiration.

8. Specification Administration

8.1 Specification Change Procedures

PMA has the right to review and possibly revise this CP. Errors, requests for update or proposed changes to this CP shall be communicated to the contact given in section 1.5. Such communication must include a description of changes, justification of the change, and contact the person who requested the change.

Any changes to CP motivated PMA should be reported to the entity to which they relate in a period of at least a month.

After the time of examination has PMA adopt proposed change, adopt with modification or reject.

8.2 Publication and Notification Procedures

PMA has published information on this CPS RA (including the CPS) through the web and in accordance with the rules concerning the organization of web content.

If approved, the new version of CPS RA are published at the latest before the effective date through the repository (see 2.6) to make it available to all relying parties at the time of entry into force. The approved version of the CPS RA is sent electronically to all external RA in a sufficiently long time before they come into force, so that they can prepare for their implementation.

For new version of CPS RA sending is responsible the head of CA client services.

8.3 CPS Approval Procedures

PMA should made decision whether CPS is in accordance with this CP. Even before the start of the CA operation, CMA shall have approved CPS and this CPS shall meet all its requirements. PMA has inform on such decisions such way, that the information are easy available to the parties rely on the certificates.

8.4 Deductions

Under normal circumstances, PMA is to decide whether a deviation in the CMA practices is in accordance with current CP and if it is acceptable or whether a CMA should request to change the CP. PMA may allow relief from certain requirements of this CP in order to meet urgent, unforeseen operational requirements.

When the relief is allowed, PMA has disclosed that through the web accessible to parties relying on certificates and should either initiate a permanent change in this CP or set a specific time limit for such relief.