CA Disig Certification Policy

Version 4.6

Valid from 1.7.2013

OID 1.3.158.35975946.0.0.0.1.1

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; Miškovič
1.5	20.12.2006	Formal emendation of the document - formatting, links repairs, emendation in Chapter 4, "Operational requirements"; Miškovič
2.0	23.01.2007	Extending CP in the context of a new type of certificate (contract clients) Addition of Chapter 7 „Certificate profiles“; Miškovič.
2.1	29.03.2007	Text changes in Chapter 2.8 and 4.9 Modification of the text in connection with the minor change in the certificate for the contractual partner; Miškovič
3.0	19.03.2008	Overall review of CP in relation to various types of issuing certificates; Ďurišová, Miškovič
3.1	24.06.2008	Adding of a new certificate type; Miškovič
3.2	10.11.2008	Change in the length of validity of certificates for the domain user PKI VšZP 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); Miškovič
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; Miškovič
4.1	14.10.2010	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; Miškovič
4.3	25.01.2012	Subordinate CA issuing possibility; new signing algorithm adding; regular annual revision; Miškovič

Version	Revision date	Description of the revision; revised by
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; Miškovič
4.5	15.8.2012 12.10.2012	CA Disig Root certificates profile and CA Disig issued certificates profile correction; Miškovič Correction: withdrawing of obsolete text from chapter 3.1.9 which is no in equivalent Slovak version of CP as a primary CA Disig document; Miškovič
4.6	21.6.2013	Document OID refine – cut out version of document (chapter 1.2); Sub CA profile changing – certificatePolicies Identifier (chapter 7.1.2); Allowing wildcard SSL certificate on third level of domain name (chapter 3.1.2); 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. ACT No. 215/2002 Coll. on Electronic Signature and on the amendment and supplementing of certain acts as amended.
2. RFC5280, Request for Comments: 5280, Internet X.509 Public Key Infrastructure: Certificate and Certificate Revocation List (CRL) Profile, Cooper et al, May 2008.
3. CA/Browser Forum Baseline Requirements for the Issuance and Management of Publicly-Trusted Certificates, v.1.1.3 (Current through adoption of Ballot 97 on 21 February 2013), CA / Browser Forum, 2011-2013
4. ETSI TS 102 042 V2.1.1, Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates.
5. Act No. 122/2013 on Protection of Personal data and supplementing of certain acts as amended.
6. 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

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
CPS CA	–	Certificate Practice Statement – Part: Certification Authority
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

1. Introduction

This document describes the Certification Policy (hereinafter referred to as "CP") of the Certification Authority CA Disig (hereinafter "CA Disig“), which is operated by Disig, a. s. (hereinafter “Disig”) and is valid for all root Certification Authorities (CA) and all its subordinate Certification Authorities (subCA).

CP is used at the implementation of public key infrastructure (hereinafter referred to as PKI), which consists of products and services they provide and manage X.509 certificates, according to the standard X.509 (Internet X.509 Public Key Infrastructure - Public Key Infrastructure).

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.

Some applications for its intended use may require a higher security level than that indicated in this CP.

1.1 Overview

The aim of this CP is not the definition of a particular implementation of PKI or plans for future implementation or future certification procedure. This CP defines the creation and management of certificates with public keys according to the standard X.509 version 3.

1.2 Identification

Title:	**CA Disig Certification Policy**
Short title:	**CP CA Disig**
Version:	**4.6**
Approved Date:	**21.6.2013**
Valid from:	**1.7.2013**
This document is assigned an object identifier (OID):	**1.3.158.35975946.0.0.0.1.1**

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.**1** - **CP CA Disig**

All certificates issued before 1.6.2013 under this CP contain the base OID 1.3.158.35975946.0.0.0.1.1, which in the last two places was extended by the exact version of the CP at the time of issuance of the certificate e.g. certificates issued from 18.8.2012 to 1.6.2013 contain OID policy in form 1.3.158.35975946.0.0.0.1.1.4.5.

Since this version of the CP we will use the unique identifier (OID) of this document in the form as written above and all certificate profiles will be modified to incorporate this new OID.

1.3 Community and applicability

1.3.1 Authority

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 the adopted and approved Certification Policy (CP) and Certificate Practice Statement (CPS) are 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 Authority

Registration Authority (RA) is an entity which, based on the CA decision, will carry out activities, which are further described in Chapter 2.1.2.

RA must conduct its activities in accordance with the approved CPS.

CA Disig may establish the following types of RA:

- **Commercial RA** - will be used to provide CA Disig certificate services for those interested in all types of certificate from the public or independent third parties. Commercial RA operates under a written contract with the Disig, as an operator of CA Disig, and the other legal person and commercial RA is empowered to sign documents for provided contractual services on behalf of Disig (CA Disig).
- **Corporate RA** - will serve to issue certificates for its own needs (employees etc.) or systems operating by this company that require use of the certificate (customers etc.). Corporate RA operates under a written contract with the Disig as an operator of CA Disig, and the other legal person and corporate RA is empowered to sign documents for provided contractual services on behalf of Disig (CA Disig).
- **In-house RA** - will be hosted by Disig and is intended to provide a complex certification services provided by CA Disig for all candidates. This RA is not independent legal person.

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.

Sharing responsibility for the registration of the applicant for the certificate between CA and RA may be different in several implementations of this CP. This division of responsibilities will be described in the CPS for given RA.

CA Disig currently established RA only in the Slovak Republic, which are legal entities established in the Slovak Republic.

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 this CP.

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

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 Usability

CA Disig certificates are generally intended to ensure software respectively hardware communication, which supports the use of X.509 certificates conforming to the specification X.509 version 3.

The purpose of issuing the CA Disig certificates is generally to provide to the holder such security tools (certificates) that ensure the secure communication using commonly available software with minimal cost.

CA Disig certificates can generally be used primarily for:

- electronic mail security (signature and/or encryption of messages sent by electronic mail, the impossibility of negation (non-repudiation) of responsibility for the message sent by electronic mail)
- electronic documents signing
- SSL communications security (reliable web server or client identification)
- hedging mechanisms for workstations users
- internal PKI processes (secure communications between the components of PKI, etc.)

CA Disig issued, according of CA Type (root, sub CA), following types of certificates to the applicants:

- administration certificates (sub CA, TSA certificate, OCSP certificate),
- personal certificates – designed primarily for the electronic mail security for a natural person (hereinafter referred to as "personal certificate") respectively natural person acting on behalf of legal persons (hereinafter referred to as "certificate of legal person) and electronic document signing,
- server 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,
- 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 or
- 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 certificates that were issued for the CMA component may be used solely for the performance of activities of these components and only to their workplaces.

CPS can precisely define:

- list of applications where issued certificates are suitable
- list of applications for which using issued certificate is limited
- list of applications for which the use of issued certificates is prohibited

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. In the event of any inconsistency between this document and those Requirements, those Requirements take precedence over this document.

1.4 Contact details

Certification authority CA Disig	
Address:	**Záhradnícka 151, 821 08 Bratislava 2**
e-mail:	**caoperator@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)

2. General provisions

2.1 Obligations

2.1.1 CA Obligations

CA Disig, who issues certificates based on this CP, must comply with its provisions, including the following:

- provide PMA with his own CPS document, as well as any subsequent changes, to assess its compliance with this CP,
- act in accordance with the provisions of the approved CPS
- ensure that registration information are accepted solely from RA, which understand this CP and are obligated to act in accordance with it,
- quote in the certificates only correct and adequate information and archived documents proving the correctness of the data contained in certificates
- guarantee that the certificate holder is bound by the obligations in accordance with section 2.1.3 of this CP and is informed about the consequences of failure of these obligations,
- revoke holder certificate, if it is found that he acted contrary to his obligations,
- on-line operate repository that satisfies the provisions referred in section 2.1.5.

If it is found that the CA Disig does not comply with these obligations, the appropriate actions are enforced on it.

The CA Disig has sole responsibility to guarantee that the certificates they sign are created and managed in accordance with this CP and the processes of creating, managing and revocation of certificates shall only be exercised by persons who understand the relevant requirements of CP and are committed to them.

The CA Disig begins investigation of a Certificate Problem Report within twenty-four hours of receipt, and decides whether revocation or other appropriate action is warranted based on at least the following criteria:

1. The nature of the alleged problem;
2. The number of Certificate Problem Reports received about a particular Certificate or Subscriber;
3. The entity making the complaint (for example, a complaint from a law enforcement official that a Web site is engaged in illegal activities should

carry more weight than a complaint from a consumer alleging that she didn't receive the goods she ordered); and

4. Relevant legislation.

The CA Disig maintain a continuous 24x7 ability to respond internally to a high-priority Certificate Problem Report, and where appropriate, forward such a complaint to law enforcement authorities, and/or revoke a certificate that is the subject of such a complaint.

The CA Disig warrants to the Certificate Beneficiaries that, during the period before issuing the certificate and when the Certificate is valid implemented a procedure:

1. for verifying that the Applicant either had the right to use, or had control of, the Domain Name(s) listed in the Certificate's subject field and subjectAltName extension (or, only in the case of Domain Names, was delegated such right or control by someone who had such right to use or control);
2. for verifying that the Subject authorized the issuance of the Certificate and that the Applicant Representative is authorized to request the Certificate on behalf of the Subject;
3. for verifying the accuracy of all of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute);
4. for reducing the likelihood that the information contained in the Certificate's subject:organizationalUnitName attribute would be misleading;
5. to verify the identity of the Applicant in accordance with CP Sections 3 and CPS for RA Section 3;

The Subscriber and CA are parties to a legally valid and enforceable Subscriber Agreement in the form of „Agreement about issue and use a certificate and services of CA Disig" which satisfied all requirements for issued type of certificates.

Above procedures are accurately described in the CA's Certificate Policy and/or Certification Practice Statement;

2.1.2 RA Obligations

RA who performs registration functions described in this CP shall comply with its provisions and to act according to the approved CPS. If it is found that RA fails to comply with these obligations the appropriate actions are forced on it, including stopping RA operations.

The division of responsibilities between the CA and RA may be different in several implementations of this CP. This division of responsibilities will be described in the CPS for relevant CA.

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 implementing direct contact between applicants and Disig CA

RA receives certificate request, verifying the identity of applicants, mediates the transfer of certificates and a list of invalid certificates to the holder. Under certain circumstances (see chapter 4.4.1.1) initiates certificate revocation and implementing the processes associated with revocation request or request for issuance of a subsequent certificate. Adopts and handled complaints, collects fees from applicants for services provided by CA Disig, unless stipulated otherwise.
RA is responsible for ensuring that it collected information has been verified and that the information is correct at the time.

2.1.3 Subscriber obligations

The term authorized person means the holder of a certificate, these terms are synonymous.

Obligations of the certificate holder:

- continually protect his private key in accordance with this CP 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
- immediately request revocation of the certificate in the event that any indication referred to in the certificate had lapsed (except e-mail address)
- 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,
- in the case of using the certificate in another country to comply with legislative requirements for electronic signature valid for that country.

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

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

2.1.4 Relying party obligations

Relying parties on certificates issued according this CP are to:

- use certificate only for the purpose for which it was issued as is it states in the certificate,
- before they rely on the certificate, to verify the validity of each certificate (i.e. verify that the certificate is valid at the time and that is not on the current list of revoked certificates issued by CA Disig),
- establish a relationship of trust to the CA that issued the certificate verifying the certification path in accordance with the standard X.509 version 3,
- keep the original signed data, applications needed to read and process these data and the cryptographic applications needed to verify the electronic signatures of such data as may be necessary to verify the signature of the data.

2.1.5 Repository obligations

Repository management, which supports CA Disig during publication of information according this CP, is required:

- maintain the accessibility of the information under the provisions of this CP for publishing information on certificates,
- provide sufficient security mechanism to access management to the information stored in the repository under Section 2.6.3.

The operation and management of repository belongs to the CA obligations.

2.1.6 Obligations of external service providers

Responsibility of the CA Disig external service providers is to comply with terms of service contractually negotiated with the CA Disig.

2.2 Liability

This CP is governed by the applicable laws of Slovak Republic, first of all by Act no. 215/2002 Z. z. on electronic signature and on amendment of certain laws as amended and the related National Security Authority regulations.

CA Disig guarantees the uniqueness of the serial number for each certificate issued by it, i.e. guarantees that there are never two certificates issued by it, which would have the same serial number.

CA Disig provides assurance that issued certificate meet certificate standard X.509 version 3 and will be in accordance with this CP.

2.3 Financial responsibility

CA Disig is responsible for damages caused by using issued certificate in accordance with the existing legislation (e.g. the Commercial Code, Civil Code etc.). The prerequisite here is that they have complied with the provisions of this CP.
Liability and the resulting performance can be accepted only if the customer has not failed to comply with its obligations (especially protect his private key) and that everyone relying on a certificate issued by CA Disig did everything possible to prevent damage and especially to verify the current status of the certificate (i.e. whether the certificate has not been in a critical time on the certificate revocation list).

Not verifying certificate status through certificate revocation list (herein after „CRL“) is qualified as a gross breach of obligations deriving from this CP. Result is extinguish any claims to the possible application of the guarantees. CA Disig or creator CA Disig have no financial responsibility for damage incurred by the holder of the certificate or relying parties, in connection with the use of CA Disig certificate with some specific applications respectively hardware or in connection with the CA Disig certificate cannot be used with any particular application or hardware.

Any claim for damages must be filed in writing.

2.4 Interpretation and Enforcement

For the purposes of the interpretation of this CP or the settlement of disputes shall be subject to the next higher authority. Bodies are arranged in ascending order:

- RA
- CA

PMA decide definitively in the case of any dispute concerning the interpretation or applicability of this CP.

Every instance shall record case and give the applicant, respectively complainant explanation respectively proposal to settle the dispute. In case of disagreement, he could to refer the case to a higher instance.

Any decision of any of the instances defined here is not the right of the complainant to refer the complaint to an independent court.

2.5 Fees

Obligation of CA Disig is publish current services prices by appropriate way respectively publish information under which it is possible to order certification services. Prices are published on the Disig web site (see Section 1.4).

Fees for certificates shall be paid to the RA in cash, if not in advance respectively contractually agreed with the applicant otherwise.

Price list for the contractual partner is not published.

2.6 Publication and Repositories

2.6.1 Publication of CA information

CA Disig must provide on-line mode repository which is accessible to holders of certificates and the party relying on a certificate. Repository contains at least the following information:

- certificates issued in accordance with this CP,
- current CRL and any CRL issued after the start of certification services,
- CA Disig Root CA and SubCA certificates belonging to their signature key,
- copy of the current CP, including possible incentives for CA approved by PMA

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

2.6.2 Frequency of publication

The certificate shall be published as soon as possible after its issuing. Information on the issuance of a certificate can be found on the website of Disig (www.disig.sk), which serves as the repository of the certification authority CA Disig. Certificates issued for closed systems, respectively for internal purposes of CA Disig are not publicly available and information on their issue is not published in the CA Disig repository.

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 shall be published without delay as soon as the CA Disig such information becomes known. CA Disig specified in the CPS time limits within which it will publish various types of information.

Certificates issued for closed systems, respectively for internal purposes of CA Disig are not publicly available and information on their issue is not published in the CA Disig repository.

2.6.3 Access Controls

CA Disig must protect any information stored in the repository, which is not intended for public dissemination.

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 add. erase data stored in the repository.

2.6.4 Repositories

Repository should be located so as to be accessible to holders of certificates and to the party relying on certificates and in accordance with the overall safety requirements.

CA Disig repository function will hold the CA Disig web site located on the web site company Disig. The exact URL is mentioned in section 1.5. CA Disig 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.

2.7 Compliance Audit

2.7.1 Frequency of entity compliance audit

CA Disig must be audited for compliance with the international standards (e. g. ETSI TS 102 042 „Electronic Signatures and Infrastructures (ESI); Policy requirements for certification authorities issuing public key certificates“ [4]) at least once a year. In addition, every CA has the right to request review of regular and irregular activities of subordinate CMA, to confirm that the subordinate CMA operates in accordance with safety practices and procedures described in the relevant CPS.

2.7.2 Identity/qualifications of auditor

The auditor must be competent in the field of compliance audits, and must be thoroughly familiar with the CPS CMA, in which conducting audit and must meet the qualification requirements described in document [3].

2.7.3 Topics covered by audit

The purpose of the audit should be a guarantee that the CA Disig has satisfactory system of work, which guarantees the quality of services provided by CA Disig CA Audit also provides a guarantee that it is acting in accordance with all requirements of this CP and its 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 discrepancy between the CMA operation and provisions of its CPS, the following actions must be taken:

- auditor recorded discrepancy,
- auditor shall notify the contrary entities defined in Section 2.7.5,
- CA 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.

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 CA and its parent, if any, in accordance with section 2.6. Implementation of corrective actions should be 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 is:

- CA Disig Root CA private keys used to create an electronic signature when issuing subCA certificates or end entity certificates respectively,
- private keys of SubCA and private keys of providing services (TSA, OCSP)
- private keys belonging to CA Disig units,
- infrastructure (e.g. documents, procedures, processes, files, scripts, passwords, etc..) serving for CA Disig operation, including all its RA,
- personal data of customers according the Act No. 122/20132 on Protection of Personal Data.

The certificate should contain only such information that is relevant and necessary to implement secure communication using certificate.

For the purpose of proper administration certificates, CMA may require in the administration of certificates by the CA Disig using information that is not listed in the certificates (e.g. IDs from documents, addresses and phone numbers).

Any such information should be explicitly defined in the CPS. All the information stored in the CA Disig that are not in the repository is to be treated as sensitive information and access should be limited only to persons who need the information to perform their official duties.

All information listed in the certificate and thus are published through the repository are not classified as confidential and shall be considered public.

Certificate Revocation List (CRL) is not considered confidential.

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, unless it is authorized by this CP, as required by law or a competent court. Any request for release of information to be authenticated and documented.

CA Disig must handle customer personal information in accordance with applicable laws and may not be provided to any third party with the exception of bodies which by law have the right to control the activities of CA and the competent national authorities such as police, courts, and prosecutor's office respectively existing contract between the CA Disig and its partners permit disclosure.

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 with the applicant agreed otherwise

3.1.1 Types of names

Each CA should be able to generate certificates that contain the X.500 Distinguished Name (hereinafter referred to as the "distinctive name").

In general, CA Disig not assigns distinctive names.

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

3.1.2 Need for names to be meaningful

Used names should unambiguously identify the person or other subject or objects that are assigned. CMA is to ensure that there is a relationship of the certificate holder and any organization or organizational unit, which is identified by any part of any name in the holder's certificate.

When distinctive names are using, item CommonName has to represent the holder of the certificate that way that is easily understandable to man. In the case of a person will typically its valid name. In the case of legal persons to be its trade name or trade mark. In the case of component (server) it can be its full domain name, model name or serial number or name of the process and applications.

The concept of "meaningfulness" means that the form of the name is commonly used semantics to determine the identity of persons, organizations or equipment etc.

Using pseudonyms, nicknames, cover names, aliases, etc. in the certificates is allowed only if in the CN is clearly defined, that it is a pseudonym. Indication of "PSEUDONYM" should by written in CommonName (e.g. CN = alias – PSEUDONYM).

This is without prejudice to the provisions relating to uniquely identify the holder of the certificate so issued.

CA respectively RA has the right to refuse to issue a certificate, which would include information in breach of the principle of meaningfulness of names. Particular emphasis is placed on the entry in item CommonName.

When entering the items into certificate request, the applicant shall bear in mind that in the RA will have a satisfactory way to prove all the data that entered into the individual certificate request items.

All of the information contained in the Certificate (with the exception of the subject:organizationalUnitName attribute) are CA Disig verified.

Distinguished Name used in different type of certificates issued by CA Disig consists of the items described below:

3.1.2.1 Personal certificate

In the table is the list of standard fields in the DN of personal certificate with the mandatory in bold. Personal certificate can be extending with other fields according of RFC 5280 article 4.1.2.6. [2]

Table 1: Personal certificate fields and their description

Abbreviation name	Title	Description	Note
C	**countryName**	Two character abbreviation for country name **SK** for Slovak republic	**Entry is required!!!**
L	localityName	Locality name	Entry is not required
O	organizationName	Organization name	Entry is not required
OU	organizationUnitName	Organization unit name	Entry is not required
CN	**commonName**	Given name and surname	**Entry is required!!!**

Note: All data must be entered without diacritics. Use special characters (e.g. comma, dash, = / and others) should be limited to the minimum. It is recommended use these characters in agreement with CA Disig. Otherwise, the CA Disig has right to refuse such a request for a certificate.
In the Organization name shall not use the comma character!!!

Important!: If the personal certificate will be used for signing and encryption of electronic mail, it is essential that the request in PKCS # 10 include a valid **e-mail address** of the certificate holder.

3.1.2.2 Certificate for the legal person

In the table is the list of the standard fields in the DN of legal person certificate with the mandatory in bold. Certificate for the legal person can be extending with other fields according of RFC 5280 article 4.1.2.6.[2]

Table 2 : Legal person certificate fields and their description

Abbreviation name	Title	Description	Note
C	**countryName**	Two character abbreviation for country name **SK** for Slovak republic	**Entry is required!!!**
L	localityName	Locality name	Entry is not required

O	organizationName	Organization name	Entry is not required
OU	organizationUnitName	Organization unit name	Entry is not required
CN	**commonName**	Organization name	**Entry is required!!!**

Note: All data must be entered without diacritics. Use special characters (e.g. comma, dash, = / and others) should be limited to the minimum. It is recommended use these characters in agreement with CA Disig. Otherwise, the CA Disig has right to refuse such a request for a certificate.
In the field Organization name shall not use the comma character!!!

3.1.2.3 SSL Certificate add domain controller certificate

In the table is the list of the standard fields in the DN of SSL certificates with mandatory in bold. SSL certificates can be extending with other fields according of RFC 5280 article 4.1.2.6.[2] Each SSL certificate shall have a "subjecAltName" certificate extension with at least one entry with the Fully-Qualified Domain Name.

As a full domain name will be accepted also name containing the asterisk (*) in the third and higher position domain name (eg *.disig.sk; *.mail.disig.sk etc.) and this type of SSL certificate will be referred to as a "wildcard " SSL certificate.

CA Disig shall not include Fully-Qualified Domain Names in Subject attributes except CommonName and subjectAlternativeName (see 7.1.2.3 table 12)

Table 3: SSL certificates fields and their description

Abbreviation name	Title	Description	Note
C	**countryName**	Two character abbreviation for country name **SK** for Slovak republic	**Entry is required!!!**
ST	stateOrProvinceName	Name of state	Entry is not required
L*	localityName	Locality name	Entry is not required*
O*	organizationName	Organization name	Entry is not required*
OU	organizationUnitName	Organization unit name	Entry is not required
CN	**commonName**	Component or unit name	**Entry is required!!!**

* - If organizationName is present, then localityName is required. If organizationName is absent, then the certificate must not contain a localityName.

Note: All data must be entered without diacritics. Use special characters (e.g. comma, dash, = / and others) should be limited to the minimum. It is recommended use these characters in agreement with CA Disig. Otherwise, the CA Disig has right to refuse such a request for a certificate.
In the field Organization name shall not use the comma character!!!

3.1.2.4 Code-signing certificate

In the following table is list of the standard fields in the DN of code-signing certificate with mandatory in bold. This type of certificate can be extending with other fields according of RFC 5280 article 4.1.2.6.[2]

Table 4: Code-signing certificate fields and their description

Abbreviation name	Title	Description	Note
C	**countryName**	Two character abbreviation for country name **SK** for Slovak republic	**Entry is required!!!**
L	localityName	Locality name	Entry is not required
O	organizationName	Organization name	Entry is not required
OU	organizationUnitName	Organization unit name	Entry is not required
CN	**commonName**	Organization or surname and given name	**Entry is required!!!**

Note: All data must be entered without diacritics. Use special characters (e.g. comma, dash, = / and others) should be limited to the minimum. It is recommended use these characters in agreement with CA Disig. Otherwise, the CA Disig has right to refuse such a request for a certificate.
In the field Organization name shall not use the comma character!!!

Important! Certificate request in the form of PKCS # 10 shall include a valid **e-mail address** of the certificate holder (physical person).

3.1.3 Uniqueness of names

CA Disig not enforced uniqueness of names within the community of holders of certificates, but of course, guarantees uniqueness of the serial number for each certificate issued by it, i.e. guarantees that there is never there two issued certificates, which would have the same serial number.

Furthermore, it is also enforce uniqueness of a key pairs certified by the certificate - in practice this means that it refuses to issue a public key certificate on the certificate request containing the public key, for which has been issued certificate by CA Disig.

3.1.4 Name claim dispute resolution procedure

In case of disputes relating to the collision of names and names in general will follow the provisions of Section 2.4.

3.1.5 Recognition, authentication and role of trademarks

Any entity has no guarantee that its name in the certificate will include the brand name (trademark), and even at his express request.

The certificate may be used only brand names, which the ownership or lease applicant for a certificate supports with evidence. CMA does not carry other authentication of trademarks.

CMA has not issue a certificate containing the name deliberately, which the competent court arbiters that violates another trademark. CMA is not obliged to examine the trade mark or to resolve disputes relating to trade marks.

3.1.6 Method to prove possession of private key

RA will require the applicant for the certificate confirmed 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) certificate on the newly generated cryptographic key pair is acceptable, that the applicant for a certificate will prove ownership of private key that way that he/she sends certificate request to RA via signed e-mail and this e-mail is signed with previous certificate.

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.

CMA does not generate key pairs for foreign entities. Exceptions may only be generating the keys and request directly in SSCD equipment on RA.

CA Disig or part of its, in any case, does not archiving the private key belonging to the applicant (a foreign entity).

3.1.7 Authentication of organization identity

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).

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.

3.1.8 Authentication of individual identity

CMA must ensure that the identity of the applicant for a certificate and its public key are linked in tandem. Each CMA has to specify in its CPS procedures for authenticate the identity of the applicant for a certificate. CA will record the process for each certificate in written or electronic form. Documentation of the identification must include at least:

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

The identification documentation must be personally signed by the applicant, in the presence of the person conducting the authentication of identity and shall including identification details of the applicant for a certificate.

If the case of issuing subsequent certificate from the CA Disig, written signature of applicant can be replaced by his/her electronic signature on condition specified in CPS.

Applicants for a certificate may be a citizen of Slovak Republic or a foreign national. Verification of identity is performed by CMA on the base of presentation of these data:

- full name and surname,
- permanent residence (if it is listed in the document),
- birth registration number (applicants who have it assigned),
- date of birth (applicants without birth registration number),
- identity card number,
- identity card issuer,
- identity card expiration date,

If the certificate is issued for a natural person and it is designated to sign e-mail (extension of Secure Email - OID 1.3.6.1.5.5.7.3.4) CMA shall verify ownership of the selected e-mail account, the procedure is given in Chapter 4.1.2.

If the certificate is issued for a natural person and it is designated to sign the software code (extension Code Signing - OID1.3.6.1.5.5.7.3.3), the contract must contain a request for the certificate holder that the information provided to third parties together with him signed applications will be true, accurate and not

misleading (the application name, URL and informative description of the application).

Other requirements for the initial registration of the applicant (holder) are described in detail in chapter 3.1.10 and 3.1.11.

3.1.9 Authentication of the component identity

CMA (Certificate Management Authority) has to guarantee that the certificate issued for hardware or software component (code signing) that is able to use the certificate, that the component identity and the public key are bonded together.

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 5.2).

Person is obliged to provide following information to CMA, as described in sections 3.1.10 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,

CMA 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 section 3.1.8,
- 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.

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

In the case of using the domain name is the condition that the second level domain is owned by an entity which is an applicant for a certificate for the server. Subject has to demonstrate to RA operator that it is the holder of the domain for which calls for issuance of the certificate.

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.).

Full domain name 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 certificate for the domain shall send back verification information as proof of ownership of the domain within specified period of time.

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, CA Disig refuses to issue a certificate to that request.

The same validation rules will be applied to "wildcard" SSL certificates, which contain the asterisk (*) in the third and higher position of domain level.

The CA Disig implements a process that prevents an OU attribute from including a name, DBA, tradename, trademark, address, location, or other text that refers to a specific natural person or Legal Entity unless the CA Disig has verified this information.

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

3.1.11.1 General

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 point 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

3.1.11.2 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

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 contractual partner shall meet other conditions for issuing of this type of certificate determined by the contractual 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.

3.1.11.3 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 3.1.11.2. It must also submit consent to the issuance of a certificate from the employer. This requirement does not apply to an employee of contractual partner, which is contractually agreed upon a different authentication mechanism.

3.1.11.4 Legal person

In this case, the applicant shall submit the certificate documents referred to in Chapter 3.1.11.2 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.

3.1.11.5 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

RA staff checked on the submitted documents the following:

Personal documents of physical persons:

a) data consistency in the request and the data referred in personal documents, particularly the name, surname and residence,

b) the validity of the document,

c) legal age (i.e. age 18 years),

d) consistency between the photograph and personal view of the proprietor of identity documents,

e) 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:

a) validity of extract – there must be not older than 3 months,

b) acting as a legal entity – i.e. whether it has/have physical(s) person(s), who submitted a statement power to act (sign) for the legal person

c) the form of extract - original or official (notary / registry) a certified copy of an extract.

Consent to the issuance of the certificate:

a) the authority to act for the company - the person signing the consent must be authorized to represent the employer. Eligibility is checked by an extract from OR respectively another designated register. As the person signing is not registered in this extract, he/she must submit other evidence on which it can act as a company (usually a notary authenticated power).

b) validity - as far as in the agreement is written the validity of consent, is also controlled.

Power of attorney:

a) verification of power of attorney (notary/registry)

b) consistency of the data listed in the power of attorney, which defines the physical and/or representative of legal person, with the data provided on the personal identification card of representative respectively with those set out in the extract or another register representing a legal person,

c) the scope of the power of attorney - that is 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,

d) any time limit or other conditions specified in power of attorney

Statutory declaration:

a) the authority to sign - the person signing the declaration must be 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 credentials)

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.)

3.2 Subsequent issue of certificate

In a subsequent issue of certificate, there is a change in key pair - a new certificate will create and will have identical mandatory values of distinctive name, a different public key (corresponding to a new, different private key), and different serial number and may have different validity time.

The holder of a valid certificate may request a subsequent issue of certificate only during the last 30 days of its validity.

The subsequent issue of certificate (personal certificate, certificate of legal person) may apply as follows:

a) Applicant for a certificate creates a new request for issuance of a subsequent certificate electronically signed by the private key associated with the previous valid certificate. This process is implemented through a web interface accessible at the web site CA Disig.

b) Applicant for the certificate requests for issuance of a subsequent certificate, so that he will send his request to RA via e-mail. For signing of e-mail he shall use a private key corresponding to the previous valid certificate.

c) Applicant for the certificate shall be subjected to the initial registration requirements - by visiting a branch of the RA.

The holder of a valid personal certificate issued for the purpose of the contractual partner may apply for subsequent certification through the mechanism agreed with the CA Disig. To sign the electronic request, the applicant must use the private key belonging to the still valid certificate.

In the case of certificates for the server, the domain controller and code signing the subsequent certificates are not issued.

All CA Disig certificates are issued with the validity period maximum of 36 month e.g. 3 years.

3.3 Issue of subsequent certificate after revocation of the previous one

CA Disig does not support this service. In the event that after the revocation of the certificate applicant wants to have a new valid certificate issued by CA Disig, he/she must apply for a new certificate in accordance with Chapter 4.1. During this act is subjected to the same authentication as specified in Chapter 3.1.7 - 3.1.9.

3.4 Revocation Request

Certificate revocation request shall be authenticated, see section 4.4.1.3. In the case of revocation request for personal certificate 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

The purpose of this CP is:

- identify the minimum requirements and procedures that are necessary to promote trust in the certificates,
- minimize the specific implementation requirements for the CMA, the applicants, for the certificate holders and the party relying on the certificates.

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 shall demonstrate that the public key create a pair with the private key and is in his/her ownership (according Section 3.1.6),
- applicant shall provide sufficient documentation to verify any particulars data to be given to the certificate.

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.

These steps can be performed in any order, to the satisfaction of the CMA and applicants and is not in conflict with security.

CA Disig implementing this CP shall certify another CA (also applies to the cross-certification) only under the authorization of PMA.

Request on CA for issuing certificate for another CA will be presented to PMA through a contact listed in Section 0 and will be complemented by CPS on the basis of Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework (RFC 3647).[6]

PMA evaluate the acceptability of the delivered CPS. PMA may require an initial audit to be conducted by an entity chosen by the PMA, to make sure that the CMA is prepared to implement all aspects of delivered CPS, before PMA authorize CMA to issue and manage certificates under this CP.

CA will only issue certificates under this CP on the basis of a written authorization issued by PMA, and may do so only within the limits imposed by the PMA.

Procedure for subCA issuing is described in detail in actual version of “Certificate Practice Statement – Part: Certification Authority”).

4.1.1 The detailed procedure for obtaining a personal certificate (physical person, legal person), SSL certificate for and code-signing certificate

The personal certificate can be applied only on the basis of electronically-generated requests. The applicant for a certificate is required generate a new personal certificate request through the Disig web site (see URL section 0) using compliant browser on his computer and save it on the appropriate medium (HD, USB drive, floppy disc, etc.).

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

Request for a certificate for signing and encryption of electronic mail shall be send to the relevant RA in advance electronically from e-mail address which is included in the request for certificate in the field „E-mail“. E-mail addresses of RA CA Disig are available on the Disig web site (see 0).

When requesting a certificate for the server the client using their software (usually, for example. Microsoft IIS or Apache/OpenSSL) generates a new request for a certificate and save it on a suitable medium.

An applicant for a subsequent certificate creates a request according the procedure in chapter 3.2.

Application for a certificate respectively a public key located inside, for which the certificate was already issued, cannot be used for safety reasons repeatedly, and such request will be rejected by the RA!

When entering the items into a certificate request by the applicant it necessary to have in mind that on the RA should prove all the data that were entered.

Request for a personal certificate issued to the individual who is employer of contractual partner, can be generated by other means than through the Disig web site e.g. own web portal contractual partner and so forth. This method is agreed in advance with the contractual partner and the individual applicants are informed about process of generating and transmitting requests from the contractor side as well as from the CA Disig.

4.1.2 Procedure for registration of an applicant on the RA

6. RA staff checked the completeness and accuracy of the data received in the certificate request. RA staff considering meaningfulness of all items taken into accounts (please see section 3.1.2) - violation of the principle of meaningfulness may be a reason for refusing to issue the certificate. Request for issuance of personal certificates for signing and encryption of electronic mail must be send electronically to the appropriate RA from addresses, which is included in the request in the field E-mail.
7. The applicant for a certificate shall satisfactorily demonstrate to the RA all the elements which entered into certificate request.

8. RA must verify whether electronically transmitted certificate request was sent by the applicant from the same e-mail address, which is located in the certificate request. In the case of the differences observed may refuse to issue the certificate. This is no case while certificate which will be issued doesn't contain "Secure Email (1.3.6.1.5.5.7.3.4)" extension.
9. In connection with the verification of an e-mail address in the request for certificate which is used to sign electronic messages (extension "Secure Email (1.3.6.1.5.5.7.3.4)") perform RA worker verification checks of e-mail addresses in the certificate request, via the responds to the e-mail, from which request was send. 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. In case that the verification of e-mail address runs unsuccessfully, CA Disig refuses to issue the certificate. If the certificate request for issuing subsequent certificate is sent via e-mail and that e-mail is signed with the valid electronic signature and certificate was issued by CA Disig and e-mail in the request is identical with the sender e-mail, verifying od e-mail address is not required.
10. Information system of CA Disig automatically verifies that on the public key contained in the certificate request has not been previously issued certificate. If it was, certificate request is rejected by RA for security reasons. The reason is that once certified public key can be used again for issuing another certificate.
11. RA staffs familiarize the applicant with the text of contract called „Agreement about issue and use a certificate and services of CA Disig". Consent by the applicant with this contract is a condition for issuing the certificate.
12. RA staff insert certificate request into CA Disig information system and the other required information. In the event that on certificate request cannot be issued certificate for some reason, the CA shall notify the appropriate RA, including giving the reason. RA then notifies the applicant for the certificate. The applicant for a certificate in this case must submit a new certificate request.
13. In the case of a subsequent certificate proceed in accordance with Chapter 3.2.

4.1.3 Certificates for internal use of contractual partner

In cases of personal certificate issued for the purpose of contractual partner, a personal certificate for a domain user and certificate for the domain controller, which serve solely for internal needs of the contractual partner, the detailed procedures for these types of certification and registration procedures for the RA to the contractual partner are written in the contractual partner CPS document or his in-house documents.

4.1.4 Delivery of the applicant's public key to the CA Disig

In order to guarantee a bond of applicant's verified identity to the public key a certificate public key (contained in the certificate request) must be delivered to CA through the RA. May be served either personally by the applicant (or via plenipotentiary, whom the applicant is allowed to represent at the RA), or on the basis of agreements with RA may be sent by e-mail.

If the certificate is for signing electronic mail (extension "Secure Email (1.3.6.1.5.5.7.3.4)") application shall send request for certificate to the appropriate RA in advance that RA can carried out verification checks of validity of email account of the applicant.

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.

4.2.1 Service of a private key to the certificate holder

The private key is generated by the applicant itself.

In the event that the storage of private key is intended SSCD facility under contract with the holder, the SSCD must be delivered to the holder in reliable manner, preferably by hand to the hands of the holder on RA. In the event of submitting SSCD via another way, SSCD activation data (e.g. password, PIN) has to be delivered to the holder separately from the SSCD and only after the holder confirms that received SSCD. Responsibility for the imposition and state of SSCD, until this has been delivered to the holder, has CMA.

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 0),
- 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

Certificates are created and issued automatically and continuously. Immediately after issuing the certificate the applicant may download its certificate. After issuing a certificate RA staff will sign with the applicant the appropriate documentation:

- Personal certificate, certificate for a legal person, a certificate for the server, code-signing certificate (commercial RA):
  - Contract on the issuing certificate and using CA Disig services
  - Acknowledge receipt of issue personal certificate and its submitting to the applicant (in the case of personal certificate)
- Server certificate (commercial RA):
  - Contract on the issuing certificate and using CA Disig services
  - Acknowledge receipt of issue certificate and its submitting to the applicant
- The personal certificate for the contract parties, the domain user certificate and certificate for the domain controller
  - Acknowledge receipt of issue certificate and its submitting to the applicant

All documents shall be made in two copies - one original is for the applicant, and the second one for the RA.

The applicant for a certificate respectively another authorized person may take the certificate via following ways:

- RA staff submit certificate to the applicant on the supported medium (except where the request was previously sent by mail),
- immediately after issuing the certificate e-mail is send to the holder with the link for downloading certificate from Disig web site,
- certificate is available for download through the service "Certificate search" provided on the CA Disig web site,
- another procedure - only according to the specific contract.

In the event of a subsequent application for a certificate electronically via web site, the applicant will receive a certificate to the e-mail address specified in the certificate.

Upon receipt of the certificate, the customer is obliged to pay for the service provided under the rates of CA Disig by the previously agreed manner.

In the event of a subsequent certificate, the payment is done electronically on the basis of an electronic invoice, unless otherwise agreed in the contract.

4.4 Certificate Revocation and Suspension

4.4.1 Circumstances for revocation

4.4.1.1 Background of revocation certificate

The certificate should be 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 will be presented into 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 CRL issuance frequency

CRL is:

- issued without delay after the revocation of the certificate,
- issued automatically every 24 hours (even though in the last 24 hours is no certificate revoked),
- publishes through repository.

CA Disig:

- revoke the certificate immediately after receipt of proper certificate revocation request at the RA, at the latest within 24 hours of receipt of the revocation request,
- publish to the addition to the current CRL, all of the latest issued CRL, from the beginning of its activities,
- keeps all the CRL, which issued.

RA will send to the current CRL via secure email to the agreed email address as soon as possible upon request on sending.

4.4.3.1 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 available forms of revocation advertisements

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 Z. z.

Full view of the archived records will allow to PMA and to the persons performing the audit

Modification or removal of archived information is not acceptable.

Audit records are archived at least 7 years from their making out.

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 private key is the corresponding certificate issued on public key revoked and also the privet key is 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 provable ensures that CA Disig signature date (private key) cannot be reused.

Details are described in the paragraph 4.9 of CPS_CA Disig CA.

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 CA key must be at least 2 048 bits.

6.2 Private Key Protection

6.2.1 CA private keys

CA Disig private keys (root, subCA) are 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 keys (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 keys.

The private keys are used solely for signing certificates and CRLs issued by CA Disig.

Before any operation with the CA Disig private keys, 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 keys are stored. The backup of CA Disig private keys 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 keys are 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.

7.1.1 CA Disig root certificates

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

Signature Algorithm
sha1RSA[1)] resp. **sha256RSA**
Public key
RSA, length 2 048 bit or 4096 bit
Validity
maximum 30 years

[1)] - SHA-1 may be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide

Table 5: The contents of the items in the CA Disig root certificates

Abbreviation	OID	Field name	Value
C	2.5.4.6	countryName	**SK**
L	2.5.4.7	localityName	**Bratislava**
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*It depends on CA type*[1)]

[1)] - trade name "CA Disig" shall be part of the common name field together with the additional specification e.g. Root R1, Root R2 etc.

Table 6: Certificate extension in the CA Disig root certificates

Extension/ Extension type	Value
basicConstraints / 2.5.29.19 Critical extension	CA:TRUE
keyUsage / 2.5.29.15 Critical extension	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
subjectKeyIdentifier / 2.5.29.14 Non-critical extension	*generated by the CA system*
subjectAltName / 2.5.29.17 Non-critical extension	RFC822 Name=caoperator@disig.sk URL=http://www.disig.sk/ca
crlDistributionPoints / 2.5.29.31[1)] Non-critical extension	Distribution Point Name: Full Name: URL=http://www.disig.sk/ca/crl/ca_disig.crl Distribution Point Name: Full Name: URL=http://ca.disig.sk/ca/crl/ca_disig.crl
certificatePolicies / 2.5.29.32* Non-critical extension	Policy Identifier=1.3.158.35975946.0.0.0.1.1.1

[1)] - these extension are not part of root CA Disig created after July 1, 2012

7.1.2 Subordinate Certification authorities (subCA)

Algorithms and key lengths applied in the SubCA CA Disig certificates:

Signature Algorithm
sha1RSA[1)] resp. **sha256RSA**
Public key
RSA, length 2 048 bit
Validity
maximum 15 years

[1)] - SHA-1 MAY be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.

Table 7: The contents of the items in the SubCA CA Disig certificates

Abbreviation	OID	Field name	Value
C	2.5.4.6	countryName	**SK**
L	2.5.4.7	localityName	**Bratislava**
O	2.5.4.10	organizationName	**Disig a.s.**
CN	2.5.4.3	commonName	*It depends on CA type*[1)]

[1)] - trade name "CA Disig" shall be part of the common name field together with the additional specification of subCA e.g. I1 Certification Service, R1I1 Certification Service etc.

Table 8: Certificate extension in the SubCA CA Disig certificates

Extension/ Extension type	Value
authorityInfoAccess / 1.3.6.1.5.5.7.1.1	[1]Authority Info Access Access Method=On-line Certificate Status Protocol (1.3.6.1.5.5.7.48.1) Alternative Name: URL=http://ca-ocsp.disig.sk [2]Authority Info Access Access Method=Certification Authority Issuer (1.3.6.1.5.5.7.48.2) Alternative Name: URL=http://www.disig.sk/.....[1)]
basicConstraints / 2.5.29.19 Critical extension	CA:TRUE Path Length Constraint=0
keyUsage / 2.5.29.15 Critical extension	Certificate Signing, Off-line CRL Signing, CRL Signing (06)
subjectKeyIdentifier / 2.5.29.14 Non-critical extension	*generated by the CA system*
subjectAltName / 2.5.29.17 Non-critical extension	RFC822 Name=caoperator@disig.sk
crlDistributionPoints / 2.5.29.31 Non-critical extension	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/.....[2)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/.....[2)]

certificatePolicies / 2.5.29.32 Non-critical extension	Policy Identifier=2.5.29.32.0

[1] - path to the issued CA is specific for each RootCA e.g. "../ca/cert/ca_disig.der"; "…/rootcar1/cert/rootcar1.der"

[2] - path to the CRL is specific for each subCA e.g. /subcar0i1/crl/subcar0i1.crl

Details concerning issuing subCA certificates are written in current version of document "Certificate Practice Statement of Certification Authority CA Disig Part – Certification Authority".

7.1.3 Certificate issued by CA Disig to the end entity

7.1.3.1 Personal certificate

Algorithms and key lengths applied in the personal certificate issued by CA Disig:

Signature Algorithm
sha1RSA[1] respectively sha256RSA
Public key
RSA, minimal length 2 048 bit
Personal certificate validity period
maximum 3 years (36 month e.g. 3x365 days)

[1] - SHA-1 may be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.

Table 9: The contents of the standard fields in the personal certificate

Abbreviation	OID	Field name	Value
C	**2.5.4.6**	countryName	**SK** **Mandatory value!!!**
L	2.5.4.7	localityName	Locality name Optional value
O	2.5.4.10	organizationName	Organization name Optional value
OU	2.5.4.11	organizationUnitName	Organization unit name Optional value
CN	**2.5.4.3**	commonName	Name and surname **Mandatory value!!!**

Personal certificate can be extending with other fields according of RFC 5280 article 4.1.2.6.

Table 10: Certificate extensions in personal certificate

Extension/ OID	Value

Extension type	
Subject Key Identifier / 2.5.29.14 Non-critical extension	*Value is created automatically by CA Disig*
Authority Key Identifier / 2.5.29.35 Non-critical extension	KeyID= *Value is added automatically by CA Disig*
Key Usage / 2.5.29.15 Non-critical extension	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
CRL Distribution Points / 2.5.29.31 Non-critical extension	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/…[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/...[1)]
Extended Key Usage / 2.5.29.37 Non-critical extension	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)
Certificate Policies / 2.5.29.32 Non-critical extension	Policy Identifier=1.3.158.35975946.0.0.0.1.1
nsCertType / 2.16.840.1.113730.1.1 Non-critical extension	SSL Client Authentication, SMIME (a0)
subjectAltName / 2.5.29.17 Non-critical extension	E-mail address of certificate holder (rfc822Name)

[1)] - path to the CRL is specific for each subCA e.g. /subcar0i1/crl/subcar0i1.crl

7.1.3.2 Certificate of legal person

Algorithms and key lengths in the certificate applied for a legal person are the same as in the case of personal certificate (see 7.1.2.1).

Table 11: The contents of the standard fields in the legal person certificate

Abbreviation	OID	Field name	Value
C	**2.5.4.6**	countryName	**SK** **Mandatory value!!!**
L	2.5.4.7	localityName	Locality name Optional value
O	2.5.4.10	organizationName	Organization name Optional value
OU	2.5.4.11	organizationUnitName	Organization unit name Optional value
CN	**2.5.4.3**	commonName	Organization name **Mandatory value!!!**

Certificate for the legal person can be extending with other fields according of RFC 5280 article 4.1.2.6.

Table 12: Certificate extensions in legal person certificate

Extension / OID Extension type	Value
Subject Key Identifier / 2.5.29.14 Non-critical extension	*Value is created automatically by CA Disig*
Authority Key Identifier / 2.5.29.35 Non-critical extension	KeyID= *Value is added automatically by CA Disig*
Key Usage / 2.5.29.15 Non-critical extension	Digital Signature, Non-Repudiation, Key Encipherment, Data Encipherment (f0)
CRL Distribution Points / 2.5.29.31 Non-critical extension	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/...[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/...[1)]
Extended Key Usage / 2.5.29.37 Non-critical extension	Client Authentication (1.3.6.1.5.5.7.3.2) Secure Email (1.3.6.1.5.5.7.3.4)[2)]
Certificate Policies / 2.5.29.32 Non-critical extension	Policy Identifier=1.3.158.35975946.0.0.0.1.1
subjectAltName / 2.5.29.17 Non-critical extension	E-mail address of certificate holder (rfc822Name)(2.5.29.17)

[1)] - path to the CRL is specific for each subCA e.g. /subcar0i1/crl/subcar0i1.crl
[2)] - CA Disig can issue certificate for legal person without this extension

7.1.3.3 SSL certificates and domain controller certificates

Algorithms and key lengths applied in the SSL certificates issued by CA Disig:

Signature Algorithm
sha1RSA[1)] respectively sha256RSA
Public key
RSA, minimal length 2 048 bit
Server certificate validity period
maximum 3 years (36 month e.g. 3x365 days)

[1)] - SHA-1 may be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.

Table 13: The contents of the standard fields in the SSL certificates

Abbreviation	OID	Field name	Value
C	**2.5.4.6**	countryName	**SK** **Mandatory value!!!**
ST	2.5.4.8	stateOrProvinceName	Province Name Optional value
L*	2.5.4.7	localityName	Locality name Optional value[1)]
O*	2.5.4.10	organizationName	Organization name Optional value[1)]
OU	2.5.4.11	organizationUnitName	Organization unit name Optional value
CN	**2.5.4.3**	commonName	Component name (full domain name) **Mandatory value!!!**

[1)] - If organizationName is present, then localityName is required. If organizationName is absent, then the certificate must not contain a localityName.

SSL certificates can be extending with other fields according of RFC 5280 article 4.1.2.6.

Table 14: Certificate extensions in the SSL certificates

Extension / OID Extension type	Value
Subject Key Identifier / 2.5.29.14 Non-critical extension	*Value is created automatically by CA Disig*
Authority Key Identifier / 2.5.29.35 Non-critical extension	KeyID= *Value is added automatically by CA Disig*
Key Usage / 2.5.29.15 Non-critical extension	Digital Signature, Key Encipherment, Data Encipherment (b0)
CRL Distribution Points / 2.5.29.31 Non-critical extension	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/...[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/...[1)]
Extended Key Usage / 2.5.29.37 Non-critical extension	Server Authentication (1.3.6.1.5.5.7.3.1) eventually Client Authentication ((1.3.6.1.5.5.7.3.2)
Certificate Policies / 2.5.29.32 Non-critical extension	[1]Certificate Policy: Policy Identifier=1.3.158.35975946.0.0.0.1.1 [2]Certificate Policy: Policy Identifier=2.23.140.1.2.1[2)] resp. 2.23.140.2.2[3)]

nsCertType / 2.16.840.1.113730.1.1 Non-critical extension	SSL Server Authentication (40) eventually SSL Client Authentication
subjectAltName[4] **/ 2.5.29.17** Non-critical extension	E-mail address of certificate holder (rfc822Name) DNS Name[4]

[1] - path to the CRL is specific for each subCA e.g. /subcar0i1/crl/subcar0i1.crl
[2] - when used it MUST NOT include organizationName, streetAddress, localityName, stateOrProvinceName, or postalCode in the Subject field.
[3] - when used it MUST also include organizationName, localityName, stateOrProvinceName (if applicable), and countryName in the Subject field.
[4] - there could be another DNS alternative name in this extension

7.1.3.4 Code signing certificate

Algorithms and key lengths applied in the code signing certificate issued by CA Disig::

Signature Algorithm
sha1RSA[1] **respectively sha256RSA**
Public key
RSA, minimal length 2 048 bit
Server certificate validity period
maximum 3 years (36 month e.g. 3x365 days)

[1] - SHA-1 may be used until SHA-256 is supported widely by browsers used by a substantial portion of relying parties worldwide.

Table 15: The contents of the standard fields in the code signing certificate

Abbreviation	OID	Field name	Value
C	**2.5.4.6**	countryName	**SK** **Mandatory value!!!**
L	2.5.4.7	localityName	Locality name Optional value
O	2.5.4.10	organizationName	Organization name Optional value
OU	2.5.4.11	organizationUnitName	Organization unit name Optional value
CN	**2.5.4.3**	commonName	Organization name or holder name and surname **Mandatory value!!!**

Code signing certificate can be extending with other fields according of RFC 5280 article 4.1.2.6.

Table 16: Basic certificate extensions in the code signing certificate

Extension / OID Extension type	Value
Subject Key Identifier / 2.5.29.14 Non-critical extension	*Value is created automatically by CA Disig*
Authority Key Identifier / 2.5.29.35 Non-critical extension	KeyID= *Value is added automatically by CA Disig*
Key Usage / 2.5.29.15 Non-critical extension	Digital Signature
CRL Distribution Points / 2.5.29.31 Non-critical extension	[1]CRL Distribution Point Distribution Point Name: Full Name: URL=http://www.disig.sk/...[1)] [2]CRL Distribution Point Distribution Point Name: Full Name: URL=http://ca.disig.sk/...[1)]
Extended Key Usage / 2.5.29.37 Non-critical extension	Code Signing (1.3.6.1.5.5.7.3.3)
Certificate Policies / 2.5.29.32 Non-critical extension	Policy Identifier=1.3.158.35975946.0.0.0.1.1.
subjectAltName / 2.5.29.17 Non-critical extension	E-mail address of certificate holder (rfc822Name)

[1)] - path to the CRL is specific for each subCA e.g. /subcar0i1/crl/subcar0i1.crl

7.1.4 Other designation

Structure (profile) for other certificates issued by CA Disig, which are intended solely for internal use by the contracting partners is described in detail in the CPS, including the use of extension certificates (certificate extensions).

The structure of the certificates issued by CA Disig may be changed only according the decision of PMA and in the case of contracting partner's certificates on the mutual agreement.

Basic extension (certificate extensions) used for the different types of certificates may be extended according to current needs on the basis of the PMA decision. Such extension shall not be considered as a change in the certificate profile as is defined in the paragraph 7.1

7.2 CRL profile

Certificate Revocation Lists (CRL) profiles issued according this CP is version 2 CRL.

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.

CP and the CPS must be reviewed at regular intervals of at least one time per year, irrespective of whether at the time are proposed changes or not. Management of CP Authority (PMA) is responsible for reviewing of these documents - see 1.3.1.1.

8.2 Publication and Notification Procedures

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

PMA will maintain a list of CA, which implements this CP. Proposed changes to this CP and CP updates should be sent to this CA.

CMA shall notify the holders of certificates via the mechanism described in the relevant CPS of any change in this CP.

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.