UNIVERSITY OF ZAGREB

UNIVERSITY COMPUTING CENTRE

SRCE CERTIFICATION AUTHORITY

Certificate Policy and Certification Practice Statement

Document OID: 1.2.840.113612.5.4.2.4.1.1.1

November 20, 2009.

http://www.srce.hr/

SRCE Certification Authority Certificate Policy and Certification Practice Statement was written by:

- ***Dobriša Dobrenić,*** *University Computing Centre (Srce);*
- ***Emir Imamagić,*** *University Computing Centre (Srce);*
- ***Joško Ivankov,*** *University Computing Centre (Srce).*

In Zagreb November 20, 2009.
Ref. no: 03-307-8260/001-09

CONTENTS

1 INTRODUCTION 7

1.1 OVERVIEW 7
1.1.1 General Definitions 7
1.2 IDENTIFICATION 8
1.3 COMMUNITY AND APPLICABILITY 8
1.3.1 Certification authorities 8
1.3.2 Registration authorities 8
1.3.3 End entities 8
1.3.4 Applicability 8
1.3.5 User restrictions 9
1.4 CONTACT DETAILS 9
1.4.1 Specification administration organization 9
1.4.2 Contact person 9
1.4.3 Person determining CPS suitability for the policy 9

2 GENERAL PROVISIONS 10

2.1 OBLIGATIONS 10
2.1.1 CA obligations 10
2.1.2 RA obligations 10
2.1.3 Subscriber obligations 10
2.1.4 Relying party obligations 11
2.1.5 Repository obligations 11
2.2 LIABILITY 11
2.2.1 CA liability 11
2.2.2 RA liability 11
2.3 FINANCIAL RESPONSIBILITY 11
2.3.1 Indemnification by relying parties 11
2.3.2 Fiduciary relationships 11
2.3.3 Administrative processes 11
2.4 INTERPRETATION AND ENFORCEMENT 12
2.4.1 Governing law 12
2.4.2 Severability, survival, merger, notice 12
2.4.3 Dispute resolution procedures 12
2.5 FEES 12
2.5.1 Certificate issuance or renewal fees 12
2.5.2 Certificate access fees 12
2.5.3 Revocation or status information access fees 12
2.5.4 Fees for other services such as policy information 12
2.5.5 Refund policy 12
2.6 PUBLICATION AND REPOSITORY 12
2.6.1 Publication of CA information 12
2.6.2 Frequency of publication 13
2.6.3 Access controls 13
2.6.4 Repositories 13
2.7 COMPLIANCE AUDIT 13
2.7.1 Frequency of entity compliance audit 13
2.7.2 Identity/qualifications of auditor 13
2.7.3 Auditor's relationship to audited party 13
2.7.4 Topics covered by audit 13
2.7.5 Actions taken as a result of deficiency 13
2.7.6 Communication of results 13
2.8 CONFIDENTIALITY 13
2.8.1 Types of information to be kept confidential 14

2.8.2 Types of information not considered confidential 14
2.8.3 Disclosure of certificate revocation/suspension information 14
2.8.4 Release to law enforcement officials 14
2.8.5 Release as part of civil discovery 14
2.8.6 Disclosure upon owner's request 14
2.8.7 Other information release circumstances 14
2.9 INTELLECTUAL PROPERTY RIGHTS 14

3 IDENTIFICATION AND AUTHENTICATION 15

3.1 INITIAL REGISTRATION 15
3.1.1 Types of names 15
3.1.2 Need for names to be meaningful 15
3.1.3 Rules for interpreting various name forms 15
3.1.4 Uniqueness of names 16
3.1.5 Name claim dispute resolution procedure 16
3.1.6 Recognition, authentication and role of trademarks 16
3.1.7 Method to prove possession of private key 16
3.1.8 Authentication of organization identity 16
3.1.9 Authentication of individual identity 16
3.2 ROUTINE REKEY 16
3.3 REKEY AFTER REVOCATION 17
3.4 REVOCATION REQUEST 17

4 OPERATIONAL REQUIREMENTS 18

4.1 CERTIFICATE APPLICATION 18
4.1.1 User certificate 18
4.1.2 Host and service certificate 18
4.2 CERTIFICATE ISSUANCE 18
4.3 CERTIFICATE ACCEPTANCE 18
4.4 CERTIFICATE SUSPENSION AND REVOCATION 18
4.4.1 Circumstances for revocation 18
4.4.2 Who can request revocation 18
4.4.3 Procedure for revocation request 18
4.4.4 Revocation request grace period 19
4.4.5 Circumstances for suspension 19
4.4.6 Who can request suspension 19
4.4.7 Procedure for suspension request 19
4.4.8 Limits on suspension period 19
4.4.9 CRL issuance frequency (if applicable) 19
4.4.10 CRL checking requirements 19
4.4.11 On-line revocation/status checking availability 19
4.4.12 On-line revocation checking requirements 19
4.4.13 Other forms of revocation advertisements available 19
4.4.14 Checking requirements for other forms of revocation advertisements 19
4.4.15 Special requirements re key compromise 19
4.5 SECURITY AUDIT PROCEDURES 19
4.5.1 Types of event audited 19
4.5.2 Frequency of processing log 20
4.5.3 Retention period for audit log 20
4.5.4 Protection of audit log 20
4.5.5 Audit log backup procedures 20
4.5.6 Audit collection system (internal vs external) 20
4.5.7 Notification to event-causing subject 20
4.5.8 Vulnerability assessments 20
4.6 RECORDS ARCHIVAL 20
4.6.1 Types of event recorded 20

4.6.2 Retention period for archive 20
4.6.3 Protection of archive 20
4.6.4 Archive backup procedures 20
4.6.5 Requirements for time-stamping of records 20
4.6.6 Archive collection system (internal or external) 21
4.6.7 Procedures to obtain and verify archive information 21
4.7 KEY CHANGEOVER 21
4.8 COMPROMISE AND DISASTER RECOVERY 21
4.8.1 Computing resources, software, and/or data are corrupted 21
4.8.2 Entity public key is revoked 21
4.8.3 Entity key is compromised 21
4.8.4 Secure facility after a natural or other type of disaster 21
4.9 CA TERMINATION 22

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS 23

5.1 PHYSICAL CONTROLS 23
5.1.1 Site location and construction 23
5.1.2 Physical access 23
5.1.3 Power and air conditioning 23
5.1.4 Water exposures 23
5.1.5 Fire prevention and protection 23
5.1.6 Media storage 23
5.1.7 Waste disposal 23
5.1.8 Off-site backup 23
5.2 PROCEDURAL CONTROLS 23
5.2.1 Trusted roles 23
5.2.2 Number of persons required per task 24
5.2.3 Identification and authentication for each role 24
5.3 PERSONNEL CONTROLS 24
5.3.1 Background, qualifications, experience, and clearance requirements 24
5.3.2 Background check procedures 24
5.3.3 Training requirements 24
5.3.4 Retraining frequency and requirements 25
5.3.5 Job rotation frequency and sequence 25
5.3.6 Sanctions for unauthorized actions 25
5.3.7 Contracting personnel requirements 25
5.3.8 Documentation supplied to personnel 25

6 TECHNICAL SECURITY CONTROLS 26

6.1 KEY PAIR GENERATION AND INSTALLATION 26
6.1.1 Key pair generation 26
6.1.2 Private key delivery to entity 26
6.1.3 Public key delivery to certificate issuer 26
6.1.4 CA public key delivery to users 26
6.1.5 Key sizes 26
6.1.6 Public key parameters generation 26
6.1.7 Parameter quality checking 26
6.1.8 Hardware/software key generation 26
6.1.9 Key usage purposes (as per X.509 v3 key usage field) 26
6.2 PRIVATE KEY PROTECTION 26
6.2.1 Standards for cryptographic module 26
6.2.2 Private key (n out of m) multi-person control 26
6.2.3 Private key escrow 27
6.2.4 Private key backup 27
6.2.5 Private key archival 27
6.2.6 Private key entry into cryptographic module 27

6.2.7 Method of activating private key *27*
6.2.8 Method of deactivating private key *27*
6.2.9 Method of destroying private key *27*
6.3 OTHER ASPECTS OF KEY PAIR MANAGEMENT 27
6.3.1 Public key archival *27*
6.3.2 Usage periods for the public and private keys *27*
6.4 ACTIVATION DATA 27
6.4.1 Activation data generation and installation *27*
6.4.2 Activation data protection *27*
6.4.3 Other aspects of activation data *27*
6.5 COMPUTER SECURITY CONTROLS 28
6.5.1 Specific computer security technical requirements *28*
6.5.2 Computer security rating *28*
6.6 LIFE CYCLE TECHNICAL CONTROLS 28
6.6.1 System development controls *28*
6.6.2 Security management controls *28*
6.6.3 Life cycle security ratings *28*
6.7 NETWORK SECURITY CONTROLS 28
6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS 28

7 CERTIFICATE AND CRL PROFILES 29

7.1 CERTIFICATE PROFILE 29
7.1.1 Version number(s) *29*
7.1.2 Certificate extensions *29*
7.1.3 Algorithm object identifiers *30*
7.1.4 Name forms *30*
7.1.5 Name constraints *30*
7.1.6 Certificate policy Object Identifier *30*
7.1.7 Usage of Policy Constraints extension *30*
7.1.8 Policy qualifiers syntax and semantics *30*
7.1.9 Processing semantics for the critical certificate policy extension *30*
7.2 CRL PROFILE 30
7.2.1 Version number(s) *30*
7.2.2 CRL and CRL entry extensions *30*

8 SPECIFICATION ADMINISTRATION 31

8.1 SPECIFICATION CHANGE PROCEDURES 31
8.2 PUBLICATION AND NOTIFICATION POLICIES 31
8.3 CPS APPROVAL PROCEDURES 31

1 INTRODUCTION

1.1 OVERVIEW

The University Computing Centre (SRCE) was founded in 1971. As the oldest infrastructure institution of the academic community in the field of establishing and using information and communication technologies (ICT), it is today one of the foundations of the planning, designing, establishing, maintenance and use system of ICT in the academic community, in other words it is part of a broader similar system which is being developed on a national scale. The founder of SRCE is the University of Zagreb, Croatia.

This document is the combined Certificate Policy and Certification Practice Statement of the SRCE Certification Authority. It describes the set of procedures followed by the SRCE Certification Authority and is structured according to RFC 2527 (http://www.ietf.org/rfc/rfc2527.txt). The latter does not form part of this document and only the information provided in this document may be relied on.

1.1.1 General Definitions

The following definitions and associated abbreviations are used in this CP/CPS.

SRCE	See section 1.1.
Certificate	Synonymous with Public Key Certificate.
Certification Authority (CA)	An entity trusted by one or more users to create and assign public key certificates and be responsible for them during their whole lifetime.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification Practice Statement (CPS)	A statement of the practices which a certification authority employs in issuing certificates.
CA equipment	A highly secured computer on which public key certificates are signed. For further security technical requirements for this machine see subsection 6.5.1.
Public web interface	A computer configured with appropriate software to support the procedures described in this CP/CPS.
Certificate Revocation List (CRL)	A time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.
Public Key Certificate	A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.
Registration Authority (RA)	An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA). In this

	CP/CPS the term “team leader” is synonymous with RA.
Relying party	A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this CP/CPS, the terms "certificate user" and "relying party" are used interchangeably.

Within this CP/CPS the words “MUST”, “MUST NOT”, “REQUIRED”, “SHALL”, “SHALL NOT”, “SHOULD”, “SHOULD NOT”, “RECOMMENDED”, “MAY”, “OPTIONAL” are to be interpreted as in RFC 2119.

1.2 IDENTIFICATION

This document is named *SRCE Certification Authority Certificate Policy and Certification Practice Statement*. The version is *1.1*, dated November 20, 2009. The following ASN.1 Object Identifier (OID) has been assigned to this CP/CPS: ***1.2.840.113612.5.4.2.4.1.1.1.*** This OID is constructed as shown below.

International Grid Trust Federation	1.2.840.113612.5
Members	.4
Issuing Authorities	.2
SRCE CA	.4
CP/CPS	.1
Major Version	.1
Minor Version	.1

1.3 COMMUNITY AND APPLICABILITY

SRCE CA provides PKI services for the Croatian academic and research community.

1.3.1 Certification authorities

The SRCE CA does not issue certificates to subordinate Certification Authorities.

1.3.2 Registration authorities

SRCE CA manages the functions of its Registration Authority.

Additional registration authorities may be created by SRCE CA as required. Such trusted intermediaries are formally assigned by SRCE CA and their identities and contact details are published in a public repository described in subsection 2.6.4.

RAs must sign an agreement with the SRCE CA, stating their adherence to the procedures described in this CP/CPS. RAs are not allowed to issue certificates under this CP/CPS.

1.3.3 End entities

Certificates can be issued to a natural person (user certificate), a computer (host certificate) or a service (service certificate) involved in activities described in section 1.3. Organizations employing the person or owning the computer entity are not the end entities themselves.

1.3.4 Applicability

Certificates issued are of the following types:

- User certificates: authorized for authentication and encryption of data and communication.
- Host certificates: authorized for authentication and encryption of data and communication.
- Service certificates: authorized for authentication and encryption of data and communication.

1.3.5 User restrictions

Certificates issued by the SRCE CA are only valid for purposes described in section 1.3. Any other usage is forbidden.

The certificates issued by the SRCE CA must not be used for financial transactions.

Ownership of any kind of issued SRCE CA certificate does not imply automatic access to any kind of computing resources.

1.4 CONTACT DETAILS

1.4.1 Specification administration organization

The Head of Computer System Department is responsible for the management of the SRCE CA.

SRCE general web address is: http://www.srce.hr.

SRCE CA general web address is: http://ra.srce.hr.

SRCE CA address for operational issues is:

SRCE CA
University Computing Centre
Josipa Marohnića 5.
10000 Zagreb
Croatia
Email: srce-ca@srce.hr
Phone: +385 1 616 55 41
Fax: +385 1 616 55 59

1.4.2 Contact person

Dobriša Dobrenić
Head of Computer System Department
University Computing Centre
Josipa Marohnića 5.
10000 Zagreb
Croatia
Email: dobrisa.dobrenic@srce.hr
Phone: +385 1 616 55 41
Fax: +385 1 616 55 59

1.4.3 Person determining CPS suitability for the policy

The person named in subsection 1.4.2 determines CPS suitability for the policy.

2 GENERAL PROVISIONS

2.1 OBLIGATIONS

2.1.1 CA obligations

The SRCE CA is solely responsible for the issuance and management of certificates referencing this CP/CPS. The SRCE CA shall:

- handle certificate requests and issue new certificates:
  - confirm certification requests from entities requesting a certificate according to the procedures described in this CP/CPS
  - issue certificates based on requests from authenticated entities
  - send notification of issued certificates to requesting entities
  - make issued certificates publicly available
- handle certificate revocation requests and certificate revocation:
  - confirm revocation requests from entities requesting that a certificate be revoked according to the procedures described in this CP/CPS
  - issue CRLs
  - make certificate revocation information publicly available
- publish SRCE CA's root of trust to a trust anchor repository defined by accrediting Policy Management Authority (PMA).

2.1.2 RA obligations

Each RA shall:

- accept conditions and adhere to the procedures described in this CP/CPS
- handle certificate requests
  - verify that the information provided in the certificate request is correct and check that the email address provided by the subscriber is correct
  - authenticate the identity of the person requesting a certificate
  - check that the subscriber knows and agrees to subscriber obligations as defined in 2.1.3
  - approve and sign certificate requests
  - notify the SRCE CA that a certificate request is authenticated and approved
- handle certificate revocation requests
  - verify that the information provided in the certificate revocation request is correct
  - approve and sign revocation revocation requests
  - notify the SRCE CA that the certificate revocation request is authenticated and approved

2.1.3 Subscriber obligations

In requesting a certificate, subscribers agree to:

- accept conditions and adhere to the procedures described in this CP/CPS
- provide true and accurate information to the SRCE CA and only such information as he/she is entitled to submit for the purposes of this CP/CPS
- use the certificate exclusively for authorized and legal purposes, consistent with this CP/CPS
- by using the authentication procedures described in this CP/CPS subscribers accept the restrictions to liability described in section 2.2
- by using the authentication procedures described in this CP/CPS subscribers accept the statements relating to confidentiality of information in section 2.8

- generate a key pair using a trustworthy method
- use at least 12 characters long passphrase, consisting of letters, number and signs, to protect private key of user certificate
- ensure that private key of host or service certificate is readable only by root or a restricted user account
- take reasonable precautions to prevent any loss, disclosure or unauthorized use of the private key associated with the certificate
- notify the SRCE CA immediately in case a private key is lost or compromised.

2.1.4 Relying party obligations

In using a certificate issued by the SRCE CA relying parties agree to:

- accept conditions and adhere to the procedures described in this CP/CPS
- verify the certificate revocation information before using a certificate
- use the certificate exclusively for authorized and legal purposes, consistent with this CP/CPS.

2.1.5 Repository obligations

The SRCE CA maintains an online accessible repository with information described in subsection 2.6.1. The repository is operated at a best-effort basis, where the intended availability is continuous. Online repository can be reached at the following address: http://ra.srce.hr.

2.2 LIABILITY

2.2.1 CA liability

The SRCE CA shall verify the identity of the subjects requesting a certificate in accordance with the procedures described in this CP/CPS. Although it aims to achieve a reasonable level of security, the SRCE CA provides its certification services on a best effort basis only and provides no warranties, express or implied, including in respect of security and confidentiality, and of fitness for a particular purpose. SRCE accepts no liability for or in connection with the certification services and the parties using or relying on them shall hold SRCE free and harmless from liability resulting from such use or reliance.

2.2.2 RA liability

Subsection 2.2.1 applies *mutatis mutandis* to the liability of the RA.

2.3 FINANCIAL RESPONSIBILITY

The SRCE CA accepts no financial responsibility for certificates issued under this CPS.

2.3.1 Indemnification by relying parties

The SRCE CA accepts no financial responsibility for improperly used certificates.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

No stipulation.

2.4 INTERPRETATION AND ENFORCEMENT

2.4.1 Governing law

Insofar as any of the conditions stipulated in this CP/CPS are ambiguous or unclear, exclusive reference shall be had to Croatian law.

2.4.2 Severability, survival, merger, notice

SRCE shall be entitled to terminate the certification services at any time. The SRCE CA will make all reasonable efforts to notify all its subscribers, all cross-certifying CAs, and any relying parties known to the SRCE CA to be currently and actively relying on certificates issued by the SRCE CA on such termination. All certificates issued by the SRCE CA that reference this CP/CPS will be revoked no later than the time of termination.

2.4.3 Dispute resolution procedures

The Head of Computer System Department resolves all disputes related to interpretation and enforcement of conditions and rules described in this CP/CPS.

2.5 FEES

No fees are charged for any service provided by the SRCE CA.

2.5.1 Certificate issuance or renewal fees

See section 2.5.

2.5.2 Certificate access fees

See section 2.5.

2.5.3 Revocation or status information access fees

See section 2.5.

2.5.4 Fees for other services such as policy information

See section 2.5.

2.5.5 Refund policy

See section 2.5.

2.6 PUBLICATION AND REPOSITORY

2.6.1 Publication of CA information

The SRCE CA operates a secure online repository that contains:

- the SRCE CA's certificate for its signing key
- the latest CRL signed by the SRCE CA
- all past and current versions of this CP/CPS
- links to all trust anchor repositories where the SRCE CA’s root of trust is published
- SRCE CA’s contact information described in subsection 1.4.1
- a user guide explaining how end entities should request a certificate
- a team leader guide explaining how RA should approve certificate requests
- a manager guide giving an overview of the SRCE CA architecture and explaining how to process certificate requests and issue CRLs.

2.6.2 Frequency of publication

Certificates are published as soon as issued. The frequency of CRL publication is specified in subsection 4.4.9. New versions of CP/CPSs are published as soon as they have been approved.

2.6.3 Access controls

The SRCE CA does not impose reading control on its CP/CPSs, CRLs and guides. Appropriate access controls are used to restrict to authorized personnel the ability to write to or modify these items.

2.6.4 Repositories

A website is maintained by the SRCE CA. It contains all the information published by the SRCE CA specified in subsection 2.6.1. The website also contains public web interface for requesting certificates and certificate revocations. The website can be reached at the following address: http://ra.srce.hr.

SRCE CA certificate can be reached at the following address: http://ra.srce.hr/cacert.pem. The most recent SRCE CA CRL can be found at the following address: http://ra.srce.hr/cacrl.crl. The most recent version of this CP/CPS can be found at the following address: http://ra.srce.hr/policy.pdf.

2.7 COMPLIANCE AUDIT

No external audit will be required, only a self-assessment by the SRCE CA that its operation is according to this CP/CPS.

Requests for external audit from other trusted CAs must be considered at the discretion of SRCE with the consideration that all costs and accommodations associated with such an audit will be borne by the requesting party.

2.7.1 Frequency of entity compliance audit

No stipulation.

2.7.2 Identity/qualifications of auditor

No stipulation.

2.7.3 Auditor's relationship to audited party

No stipulation.

2.7.4 Topics covered by audit

No stipulation.

2.7.5 Actions taken as a result of deficiency

No stipulation.

2.7.6 Communication of results

No stipulation.

2.8 CONFIDENTIALITY

The SRCE CA collects each subscriber’s full name, organization, address, phone number and email address. No other information is collected from subscribers.

2.8.1 Types of information to be kept confidential

Any information about subscriber that is not present in the certificate and CRL is considered confidential and will not be released outside of SRCE CA. Record of the email messages sent and received by SRCE CA is considered confidential. Under no circumstances does the SRCE CA have access to the private keys of any subscriber to whom it issues a certificate.

2.8.2 Types of information not considered confidential

Data contained in CRLs and the subscriber's certificate shall not be considered confidential and will be published in a publicly accessible location.

2.8.3 Disclosure of certificate revocation/suspension information

No information about the reason for a revocation is published.

2.8.4 Release to law enforcement officials

SRCE CA will not disclose certificate or any certificate-related information to any third party, aside from information listed in subsection 2.8.2, except when so required by a legal authority of competent jurisdiction.

2.8.5 Release as part of civil discovery

See subsection 2.8.4.

2.8.6 Disclosure upon owner's request

See subsection 2.8.4

2.8.7 Other information release circumstances

See subsection 2.8.4.

2.9 INTELLECTUAL PROPERTY RIGHTS

The use of following documents for drafting this CP/CPS is acknowledged:

- RFC 2527
- RFC 3280
- Profile for Traditional X.509 Public Key Certification Authorities with secured infrastructure (version 4.0)
- NIIF Certification Authority Certification Practice Statement
- Slovenian Grid Net Certification Authority Certificate Policy and Certification Policy Statement
- CERN Certification Authority Certificate Policy and Certification Practice Statement (version 2.4)
- CESNET CA Certificate Practice Statement (version 2.0)
- UK e-Science Certification Authority Certificate Policy and Certification Practices Statement (version 1.2)
- Grid-Ireland Certification Authority Certificate Policy and Certification Practice Statement
- GridKa-CA Certificate Policy and Certification Practice Statement (version 1.2).

The SRCE CA claims no intellectual property rights on issued certificates, this CP/CPS or related material.

3 IDENTIFICATION AND AUTHENTICATION

3.1 INITIAL REGISTRATION

3.1.1 Types of names

The subject name is an X.500 distinguished name (DN). The DN must be a non-empty and encoded as printableString. All names under this CP/CPS must have form:

- Name must start with *"C=HR, O=edu, OU=<organization name>"*. Following this a *CN* part takes one of the following forms:
  - for a person: full name of the person. Example of a full subject name for a person:
    C=HR, O=edu, OU=srce, CN=Pero Peric
  - for a host: the host DNS name (FQDN). Example of a full subject name for a host:
    C=HR, O=edu, OU=srce, CN=host1.srce.hr
  - special case of host certificate is grid host certificate: "host/" prefix, followed by the server DNS name (FQDN). Example of a full subject name for a host:
    C=HR, O=edu, OU=srce, CN=host/host1.srce.hr
  - for a service: an identifier related to the service. Example of a full subject name for a service:
    C=HR, O=edu, OU=srce, CN=ldap/host1.srce.hr.

In case of person, the CN part of DN can contain only letters, numbers and following special characters: left round bracket ('('), right round bracket (')'), space (' ') and hyphen ('-'). In case of host and service, the CN part of DN can contain only letters, numbers and following special characters: dot ('.') and hyphen ('-'). Additionally, in case of grid host certificate and service certificate character '/' can be used. The maximal length of the CN is 128 characters for all types of certificates.

The Subject field of CA certificate has following value:

- *C=HR, O=edu, OU=srce, CN=SRCE CA*

The Issuer field of each certificate including CA certificate has following value:

- *C=HR, O=edu, OU=srce, CN=SRCE CA*

3.1.2 Need for names to be meaningful

The Subject and Issuer names contained in a certificate, are meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong.

In case of persons, RAs are not to accept any pseudonymous names. In case of hosts, the RA accepts only names listed in the Internet public DNS registry. In case of services, the RA accepts only names related to the type of service.

Organization name in certificate subject name is part of realm name without "hr" suffix as defined within AAI@EduHr project. Organizations that do not have realm name within AAI@EduHr project can contact SRCE CA in order to define appropriate organization name.

The SRCE CA supports the use of certificates as a form of identification within a particular community of interest. Anonymous certificates are not supported by the SRCE CA.

3.1.3 Rules for interpreting various name forms

See subsections 3.1.1 and 3.1.2.

3.1.4 Uniqueness of names

Distinguished names for each certificate must be unambiguous and unique. In case of real subject name duplication, additional numbers and/or letters will be appended to the distinguished name to guarantee uniqueness.

Entities must not share certificates.

Distinguished name can not be recycled.

3.1.5 Name claim dispute resolution procedure

The person named in subsection 1.4.2 will resolve any name claim dispute.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

No stipulation.

3.1.8 Authentication of organization identity

SRCE CA does not issue certificates directly to organizations.

3.1.9 Authentication of individual identity

A person requesting a user certificate must meet in person with the appropriate RA, show a valid official identification document, i.e. identity card or passport, and provide its official email address (email form must show association with person's name and organization, e.g. pero.peric@srce.hr).

A person requesting a host or service certificate must be an official administrator of a machine certificate is being issued to and provide the same information as in case of user certificate. Exceptionally, if a person posses valid SRCE CA user certificate, authentication can be achieved via email signed with person's certificate.

SRCE CA must take steps to ascertain that the organization, which name is requested to be the part of a subject name, consents to such use. In case of host or service certificate, SRCE CA must take steps to ascertain that the person requesting a certificate is an official administrator of a machine certificate is being issued to.

If authentication is not completed within seven days of receipt of the certificate request by the RA the request will be deemed to have expired and any authentication of identity must then be preceded by a new certificate request.

Once the person requesting certificate obtains the certificate he/she must send signed email stating that he/she accepts conditions and adhere to the procedures described in this CP/CPS. If the person fails to send the email within seven days of certificate receipt, the certificate will be revoked.

3.2 ROUTINE REKEY

Expiration warning will be issued to subscribers within 31 days before certificate expiration. Rekeying before expiration follows the same procedure as an initial registration with the exception that the authentication is achieved via email signed with the user's current valid certificate. Authentication of person requesting rekeying must be performed by meeting RA in person at least every 5 years.

After certificate expiration, rekeying of certificate follows the same rules as an initial registration.

SRCE CA does not support certificate renewal.

3.3 REKEY AFTER REVOCATION

Rekeying of certificate after revocation follows the same rules as an initial registration.

3.4 REVOCATION REQUEST

See subsection 4.4.2.

4 OPERATIONAL REQUIREMENTS

4.1 CERTIFICATE APPLICATION

4.1.1 User certificate

User certificate requests should be submitted to the appropriate RA through the public web interface.

4.1.2 Host and service certificate

Host and service certificate requests should be submitted to the appropriate RA through the public web interface.

4.2 CERTIFICATE ISSUANCE

When the applicant submits the request through the public web interface, appropriate RA performs identity vetting as described in subsection 3.1.9.

If the request is valid, RA uses public web interface to approve and sign the request. Web interface uses https protocol and RA is authenticated by providing its certificate and login/password.

SRCE CA issues the certificate if, and only if, the authentication of the subject is successful according to subsection 3.1.9. When the appropriate RA approves and signs the request, CA transfers the request to the CA equipment by using removable media. When accessing the request, CA uses the same interface and security mechanisms as RA. Certificate is signed on CA equipment and then transferred back to the public web interface by using removable media. CA then publishes certificate and notifies the applicant and the RA.

4.3 CERTIFICATE ACCEPTANCE

No stipulation.

4.4 CERTIFICATE SUSPENSION AND REVOCATION

4.4.1 Circumstances for revocation

A certificate is revoked on the request of the subscriber or under any of the following circumstances

- the subscriber's private key is lost or suspected to be compromised
- the information in the subscriber's certificate is inaccurate
- the subscriber no longer needs the certificate
- the subscriber has violated his/her obligations under this policy.

4.4.2 Who can request revocation

A certificate revocation can be requested by the holder of the certificate concerned, by the issuing RA or by any other entity presenting evidence of circumstances as described in subsection 4.4.1.

4.4.3 Procedure for revocation request

Requests for revocation should be submitted through public web interface. The requesting entity must specify the reason for the revocation request and provide evidence of circumstances as described in subsection 4.4.1 if appropriate. Additionally, revocation requests can be brought to the RA personally.

4.4.4 Revocation request grace period

There will be no grace period associated with certificate revocation. The SRCE CA handles revocation requests with priority and a certificate will be revoked as soon as possible, but within one working day, after circumstances for revocation, as described in subsection 4.4.1, are established.

4.4.5 Circumstances for suspension

There is no provision for certificate suspension.

4.4.6 Who can request suspension

No stipulation.

4.4.7 Procedure for suspension request

No stipulation.

4.4.8 Limits on suspension period

No stipulation.

4.4.9 CRL issuance frequency (if applicable)

New CRL is issued immediately after every certificate revocation and at least 7 days before expiration. Validity of CRL is 30 days.

4.4.10 CRL checking requirements

Before use of a certificate, a relying party must validate it against the most recently issued CRL.

4.4.11 On-line revocation/status checking availability

The SRCE CA provides a public repository (see subsection 2.6.4) for verifying the status of certificates issued within the SRCE CA.

4.4.12 On-line revocation checking requirements

No stipulation.

4.4.13 Other forms of revocation advertisements available

No stipulation.

4.4.14 Checking requirements for other forms of revocation advertisements

No stipulation.

4.4.15 Special requirements re key compromise

No stipulation.

4.5 SECURITY AUDIT PROCEDURES

4.5.1 Types of event audited

The minimum audit records to be kept include all:

- Types of registration record, including records relating to rejected applications
- Certificate generation requests, whether or not certificate generation was successful
- Certificate issuance records, including CRLs
- Revocation records
- Audit records:
    - Boots and shutdowns of the CA equipment

- Login and logouts to the CA equipment
- Use of the CA software.

4.5.2 Frequency of processing log

Audit logs are processed on a weekly basis.

4.5.3 Retention period for audit log

Audit logs are retained as archive records. The audit logs are kept on the CA and public web interface equipment for a minimum period of three years.

4.5.4 Protection of audit log

Only authorized SRCE CA personnel is allowed to view and process audit log files. Audit log files stored on the CA and public web interface equipment will not be open for modification by any human, or by any automated process other than those that perform audit and archival.

4.5.5 Audit log backup procedures

A backup of the audit logs shall be performed on removable media at the time of audit log processing (see subsection 4.5.2). The minimal retention period for backup copies of the audit logs is defined in subsection 4.5.3. The backup media is kept in a safe. Safe's technical details are described in subsection 5.1.2.

4.5.6 Audit collection system (internal vs external)

The audit collection system shall be running separately from the CA software in a secure environment. The audit collection system is internal to the SRCE CA.

4.5.7 Notification to event-causing subject

Operations personnel notify their security administrator when a process or action causes a critical security event or discrepancy.

4.5.8 Vulnerability assessments

A security risk assessment has been completed and regularly repeated for the entire SRCE CA hierarchy. This assessment covers the overarching risks and threats that may impact the Public Key Infrastructure (PKI). The SRCE CA personnel must pay attention to any sign of an attempt to violate the integrity of the PKI system. Any deficiency is followed by a vulnerability assessment revision.

4.6 RECORDS ARCHIVAL

4.6.1 Types of event recorded

All events listed in subsection 4.5.1 are archived.

4.6.2 Retention period for archive

See subsection 4.5.3.

4.6.3 Protection of archive

See subsection 4.5.4.

4.6.4 Archive backup procedures

See subsection 4.5.5.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

See subsection 4.5.6.

4.6.7 Procedures to obtain and verify archive information

All certificate data published by SRCE CA are publicly available. Data used for the registration and identification of subscribers are for internal use only. The integrity of SRCE CA archives is verified:

- at the time the archive is prepared
- annually at the time of a programmed security audit
- at any other time when a full security audit is required.

4.7 KEY CHANGEOVER

CA's private signing key is changed periodically. To avoid interruption of validity of all subordinate keys the new CA key is generated at least one year plus one month before the old one looses validity and, from that point onwards, new certificates are signed with the new key. The new CA certificate is posted in the public repository (see subsection 2.6.4).

4.8 COMPROMISE AND DISASTER RECOVERY

4.8.1 Computing resources, software, and/or data are corrupted

If the CA equipment is damaged or rendered inoperative, but the CA private key is not destroyed, CA operation will be reestablished as quickly as possible by using backup of private key.

If the CA private key is destroyed, the case will be treated as in subsection 4.8.3.

4.8.2 Entity public key is revoked

See subsection 4.8.3.

4.8.3 Entity key is compromised

If the private key of the SRCE CA is, or is suspected to be, compromised, the SRCE CA shall:

- make all reasonable effort to inform subscribers, cross-certifying CAs, PMAs that have accredited SRCE CA and any known relying parties
- terminate distribution services for certificates and CRLs issued using the compromised key
- generate a new CA key pair and certificate and make the latter available in the public repository.

In the case of such a CA key compromise, new certificates will be issued only in accordance with the entity identification procedures defined in section 3.1.

If an RA's private key is compromised, or is suspected to be compromised, the RA informs the SRCE CA and requests a revocation of the RA's certificate.

If an entity private key is compromised or suspected to be compromised, the entity or its administrator must request a revocation of the certificate and make all reasonable efforts to inform any known relying parties. SRCE CA will inform subscribers, cross-certifying CAs and any known relying parties.

4.8.4 Secure facility after a natural or other type of disaster

In the case of a disaster SRCE CA personnel will take every possible action to secure CA and public web interface equipment located in SRCE CA’s premises. SRCE CA will inform subscribers, cross-certifying CAs and any known relying parties about the disaster as soon as possible.

If the backup data and the CA private key are not destroyed the case will be treated as in subsection 4.8.1.

In the case of a disaster whereby all copies of the CA private key are destroyed as a result, the case will be treated as in subsection 4.8.1.

4.9 CA TERMINATION

Before the SRCE CA terminates its services, the SRCE CA shall:

- make all reasonable efforts to inform subscribers, cross-certifying CAs and relying parties
- make knowledge of its termination widely available
- revoke all the issued certificates
- cease issuing certificates and CRLs
- destroy all copies of private keys
- keep audit logs archive for at least period defined in subsection 4.6.2.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 PHYSICAL CONTROLS

5.1.1 Site location and construction

See subsection 5.1.2.

5.1.2 Physical access

The CA and public web interface equipment is situated in a room with restricted and audited access and installed cameras. The building entrance has a security desk with the guard.

The SRCE CA private key is not stored on the CA equipment but it is kept locked in a safe.

All safes used by SRCE CA are equipped with electronic lock. Lock codes are known only to all current SRCE CA staff. Change of staff will imply a change of all codes. Codes are changed every three months. All safes are situated in a room with restricted and audited access and installed cameras.

5.1.3 Power and air conditioning

The CA and public web interface equipment is connected to uninterruptible power supply.

The environmental conditions (temperature and humidity) of the room with the CA and public web interface equipment are controlled by air conditioning.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

Suitable fire extinguishers are maintained in and near the room with the CA and public web interface equipment, to guard against the possibility of fire.

5.1.6 Media storage

All removable media containing SRCE CA information, including backup media, is stored in a safe. Safe's technical details are described in subsection 5.1.2.

5.1.7 Waste disposal

All SRCE CA related paper waste is shredded. Magnetic media is physically/mechanically destroyed before disposal.

5.1.8 Off-site backup

No off-site backups are currently performed. All removable media containing SRCE CA information are stored in safes located in SRCE’s premises.

5.2 PROCEDURAL CONTROLS

5.2.1 Trusted roles

In order to prevent any one person from circumventing the entire system, responsibilities at the SRCE CA are divided among different trusted roles and individuals:

- system administrator
- registrar
- certification authority

- security officer.

5.2.1.1 Responsibilities of system administrator

Responsibilities of system administrator are following:

- The SRCE CA equipment supervision, maintenance and management
- The security of the SRCE CA equipment
- The execution of regular backups
- Installation of security updates
- Compliance with this CP/CPS.

5.2.1.2 Responsibilities of registrar

Responsibilities of registrar are following:

- Authentication of identities
- Compliance with this CP/CPS.

5.2.1.3 Responsibilities of certification authority

Responsibilities of certification authority are following:

- Issuing certificates and CRLs
- Performing CA/RA staff audit
- Compliance with this CP/CPS.

5.2.1.4 Responsibilities of security officer

Responsibilities of security officer are following:

- Performing actions when an intrusion is detected
- Audit logs monitoring
- Execution of Security Audit
- Compliance with this CP/CPS.

5.2.2 Number of persons required per task

No stipulation.

5.2.3 Identification and authentication for each role

No stipulation.

5.3 PERSONNEL CONTROLS

SRCE CA will maintain list of CA and RA staff. Certification authority person (described in subsection 5.2.1.3) will perform staff audit at least once per year.

5.3.1 Background, qualifications, experience, and clearance requirements

SRCE CA personnel must be staff members of the University Computing Centre, SRCE, Zagreb, Croatia. SRCE CA personnel must pass SRCE computer room clearance.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Contracting personnel requirements

No stipulation.

5.3.8 Documentation supplied to personnel

SRCE CA guides are available at public repository (see subsection 2.6.4).

6 TECHNICAL SECURITY CONTROLS

6.1 KEY PAIR GENERATION AND INSTALLATION

6.1.1 Key pair generation

SRCE CA does not generate private keys for applicants. The private key should not be known by other than the authorized user of the key pair. Applicants are recommended to use public web interface to create their pair as part of the request generation process. If key pairs are generated by some other means, the applicant must ensure that key lengths conform to those given in subsection 6.1.5.

6.1.2 Private key delivery to entity

See subsection 6.1.1.

6.1.3 Public key delivery to certificate issuer

Applicant must submit a certificate request with the public key according to the procedures defined in section 4.1.

6.1.4 CA public key delivery to users

The SRCE CA certificate is available from the public repository (see subsection 2.6.4).

6.1.5 Key sizes

The CA private key is a minimum length of 2048 bits. The RA private key is a minimum length of 2048 bits. All other private keys are a minimum length of 1024 bits.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

No stipulation.

6.1.9 Key usage purposes (as per X.509 v3 key usage field)

Keys may be used for digital signature, data and key enchipherment, message integrity and session key establishment. The SRCE CA private key is the only key that can be used for signing SRCE certificates and CRLs.

For certificates issued by the SRCE CA under this policy, the *key Usage* extension is defined in subsection 7.1.2.

6.2 PRIVATE KEY PROTECTION

6.2.1 Standards for cryptographic module

The SRCE CA does not use any cryptographic module.

6.2.2 Private key (n out of m) multi-person control

No stipulation.

6.2.3 Private key escrow

The SRCE CA keys are not given in escrow. The SRCE CA is not available for accepting escrow copies of keys of other parties.

6.2.4 Private key backup

A backup of the SRCE CA private key is kept on removable media in a safe. The passphrase for activating the backup is kept in a different safe from the one containing the private key. Safe's technical details are described in subsection 5.1.2.

6.2.5 Private key archival

See subsection 6.2.4.

6.2.6 Private key entry into cryptographic module

See subsection 6.2.1.

6.2.7 Method of activating private key

The activation of the CA private key is done by providing the passphrase.

The SRCE CA private key passphrase is kept in a sealed envelope in a safe. The safe which contains the passphrase does not contain any copy of the private key. Safe's technical details are described in subsection 5.1.2.

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

After termination of the CA, all media that contain the private key of the CA will be securely and permanently destroyed, according to then best current practice.

6.3 Other Aspects of Key Pair Management

6.3.1 Public key archival

The public key is archived as part of the certificate archival.

6.3.2 Usage periods for the public and private keys

SRCE CA certificate have a validity of five years. For other entity certificates, the maximum validity period for a certificate is one year plus one month.

6.4 Activation Data

6.4.1 Activation data generation and installation

The minimal length of the CA private key passphrase is 18 characters and it consists of letters, numbers and signs. All other passphrases and passwords used for the operation of SRCE CA must have a length of at least 12 characters and must consist of letters, numbers and signs.

6.4.2 Activation data protection

All passphrases and passwords are known to all current staff members of the SRCE CA. Change of staff will imply a change of all passphrases and passwords.

6.4.3 Other aspects of activation data

No stipulation.

6.5 COMPUTER SECURITY CONTROLS

6.5.1 Specific computer security technical requirements

The CA equipment satisfies the following requirements:

- Physical access to the system is as described in subsection 5.1.2
- The SRCE CA runs on a dedicated computer system
- Only the software needed to perform CA operations are installed on system
- The CA equipment is not connected to network
- All security related events are audited.

6.5.2 Computer security rating

No stipulation.

6.6 LIFE CYCLE TECHNICAL CONTROLS

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security ratings

No stipulation.

6.7 NETWORK SECURITY CONTROLS

Certificates are signed on the CA equipment which is not connected to any kind of network.

The public web interface equipment is protected by SRCE firewalls.

6.8 CRYPTOGRAPHIC MODULE ENGINEERING CONTROLS

No stipulation.

7 CERTIFICATE AND CRL PROFILES

7.1 CERTIFICATE PROFILE

7.1.1 Version number(s)

SRCE CA issues X.509 Version 3 certificates.

7.1.2 Certificate extensions

Extension X509v3 Subject Alternative Name in the host and service certificates is set to the FQDN of the machine. In case of user certificate this extension is set to user's email address.

In extension X509v3 Certificates Policies, Policy identifier is set to the OID of the CP/CPS that is in effect at the time of the certificate signing.

The values of extensions in case of CA certificate are following:

- X509v3 Basic Constraints: critical CA:TRUE
- X509v3 Key Usage: critical Certificate Sign, CRL Sign
- X509v3 Subject Key Identifier: <CA key ID>
- X509v3 Authority Key Identifier:
  - keyid:<CA key ID>
- X509v3 Subject Alternative Name: email:srce-ca@srce.hr
- X509v3 Certificates Policies:
  - Policy: <OID of the effective CP/CPS>
  - CPS: http://ra.srce.hr/policy/.

The values of extensions in case of user certificates are following:

- X509v3 Basic Constraints: critical CA:FALSE
- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
- X509v3 Extended Key Usage: TLS Web Client Authentication, E-mail Protection, Microsoft Smartcardlogin
- X509v3 Subject Key Identifier: <subject key ID>
- X509v3 Subject Alternative Name: email:<user's email address>
- X509v3 Certificates Policies:
  - Policy: <OID of the effective CP/CPS>
  - CPS: http://ra.srce.hr/policy/
- X509v3 CRL Distribution Points: URI:http://ra.srce.hr/cacrl.crl.

The values of extensions in case of host and service certificates are following:

- X509v3 Basic Constraints: critical CA:FALSE
- X509v3 Key Usage: critical Digital Signature, Key Encipherment, Data Encipherment, Key Agreement
- X509v3 Extended Key Usage: TLS Web Client Authentication, TLS Web Server Authentication
- X509v3 Subject Key Identifier: <subject key ID>
- X509v3 Subject Alternative Name: DNS:<host DNS address>
- X509v3 Certificates Policies:
  - Policy: <OID of the effective CP/CPS>
  - CPS: http://ra.srce.hr/policy/
- X509v3 CRL Distribution Points: URI:http://ra.srce.hr/cacrl.crl.

7.1.3 Algorithm object identifiers

The following hash/digest algorithm is supported:

- SHA-1

The following signature algorithm is supported:

- RSA

7.1.4 Name forms

See subsection 3.1.1.

7.1.5 Name constraints

See subsection 3.1.2.

7.1.6 Certificate policy Object Identifier

See section 1.2.

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical certificate policy extension

No stipulation.

7.2 CRL PROFILE

7.2.1 Version number(s)

SRCE CA issues X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

Digest and signature algorithms used for CRLs are the same as for certificates (see subsection 7.1.3).

8 SPECIFICATION ADMINISTRATION

8.1 SPECIFICATION CHANGE PROCEDURES

Users will not be advised in advance of changes to the SRCE CA's CP and CPSs. Changes are made available as defined in section 2.6.

8.2 PUBLICATION AND NOTIFICATION POLICIES

This CP/CPS and any older versions are available from the public repository given in subsection 2.6.4.

8.3 CPS APPROVAL PROCEDURES

No stipulation