Estonian Grid Certification Authority

Certificate Policy and Certification Practice Statement

Version 1.3

Document OID: 1.3.6.1.4.1.19974.10.1.1.3

September 2004

Table of Contents

1. INTRODUCTION

1.1 Overview

Estonian Educational and Research Network (EENet) is a governmental nonprofit organization with the task of managing, coordinating and developing the computer network of science, education and culture in Estonia.

Estonian Grid is a nationwide project aimed at administering, coordinating and developing Grid resources in Estonia.

EENet manages, coordinates and developes the Estonian Grid Certification Authority (EGCA).

This document is the combined Certificate Policy and Certification Practice Statement of the EGCA. It describes the set of procedures followed by the EGCA and is structured according to RFC 2527. The latter does not form part of this document and only the information provided in this document may be relied on.

1.2 Identification

1. Document title: "Estonian Grid Certification Authority Certification Policy and Certificate Practice Statement"
2. Version: 1.3.
3. Document Date: 17.09.2004
4. OID: 1.3.6.1.4.1.19974.10.1.1.3

IANA	1.3.6.1.4.1
EENet	.19974
EGCA	.10
CP/CPS	.1
Major Version	.1
Minor Version	.3

5. Expiration: This document is valid until further notice.

1.3 Community and Applicability

1.3.1 Certification authorities

Estonian Grid certificates are signed by the EGCA, which is defined as a medium security CA.

1.3.2 Registration authorities

The EGCA manages the functions of its Registration Authority (RA). There is an addidtional RA managed by National Institute of Chemical Physics and Biophysics. Additional registration authorities may be created by the EGCA as required.

1.3.3 End entities

The EGCA will issue certificates to natural persons, computer and service entities. Entities eligible for certification from the EGCA are: all those entities formally based and/or having offices in Estonia, that are involved in research or education. The focus of these organizations should also be in research and/or education.

1.3.4 Applicability

There will be three categories of certificates:

1. Server certificates: authentication, non-repudiation and communication encryption;
2. User certificates: authentication, non-repudiation, data encryption and communication encryption.
3. Services certificates: authentication, non-repudiation, data encryption and communication encryption.

The ownership of a EGCA certificate does not imply automatic access to any kind of resources.

Certificates issued by EGCA MUST NOT be used for financial transactions.

1.4 Contact Details

1.4.1 Specification administration organization

The EGCA is created and managed by the Estonian Educational and Research Network.

The EGCA address for operational issues is:

Estonian Grid Certification Authority
EENet
Raekoja pl 14
Tartu 51004
Estonia
Tel: +372 730 2110
Fax: +372 730 2111
Email: ca@grid.eenet.ee

1.4.2 Contact person

Lauri Anton
EENet
Raekoja pl 14
Tartu 51004
Estonia

Tel: +372 730 2110
Fax: +372 730 2111
Email: lauri.anton@eenet.ee

1.4.3 Person determining CPS suitability for the policy

See Section 1.4.2

2. GENERAL PROVISIONS

2.1 Obligations

2.1.1 EGCA obligations

The EGCA is responsible for all aspects of the issuance and management of a certificate referencing this policy, including:

1. Development of a detailed statement of practices and procedures (the CPS) by which the EGCA implements the requirements of this policy.
2. Publication of EGCA contact information.
3. Certificate application/enrollment process.
4. Verification of the identity of the applicant.
5. Certificate signing process.
6. Posting of the signed certificate in a public repository.
7. Revocation of the certificate.
8. Certificate renewals.
9. Issuing and
10. Ensuring that all aspects of the CA services and CA operations and CA infrastructure related to certificates issued under this policy are performed in accordance with the requirements, representations, and warranties of this policy.
11. Define and publish a dispute resolution procedure.

By issuing a certificate that references this policy, the CA certifies to the subscriber, and to all relying parties who reasonably and in good faith rely on the information contained in the certificate during its operational period, that:

1. The CA has issued, and will manage, the certificate in accordance with this policy.
2. There are no misrepresentations of fact in the certificate known to the CA, and the CA has taken reasonable steps to verify additional information in the certificate unless otherwise noted in its CPS.
3. The certificate meets all material requirements of this policy and the CA's CPS.

2.1.2 RA obligations

The RA is responsible for the following aspects:

1. authenticate entities requesting a certificate according to the procedures described in this document;
2. send validated certificate requests to EGCA;
3. create and send validated revocation requests to the EGCA;
4. communicate with EGCA using secure channels and methods;

5. follow the policies and procedures described in this document;

2.1.3 Subscriber obligations

In all cases, the EGCA SHALL require the subscriber to:

1. Subscribers MUST accurately represent the information required of them in a certificate request.
2. Subscribers MUST properly protect their private key at all times, against loss, disclosure to any other party, modification and unauthorized use, in accordance with this CP /CPS. From the creation of their private and public key pair, subscribers are personally and solely responsible of the confidentiality and integrity of their private keys. Every usage of their private key is assumed to be the act of its owner. The private key MUST NOT be shared to other parties.
3. Upon suspicion that their private keys are compromised subscribers MUST notify the CA that issued their certificates by sending a certificate revocation request.
4. Upon any change of information in their certificates subscribers MUST notify the CA that issued their certificates by sending a certificate revocation request.
5. Subscribers MUST use the keys and certificates only for the purposes authorized by the CA.
6. Subscribers MUST authorize the treatment and conservation of their personal data.
7. The passphrase used for protection of subscribers private key MUST be at least 12 characters long.

2.1.4 Relying party obligations

A relying party MUST be familiar with the this CP/CPS before drawing any conclusion on how much trust he can put in the use of a certificate issued from the CA.

The relying party MUST only use the certificate for the prescribed applications and MUST NOT use the certificates for forbidden applications.

Relying parties MUST verify the digital signature of a received digitally signed message and to verify the digital signature of the CA who issued the certificate used for the verification purpose.

When validating a certificate a relying party MUST check it for its validity, revocation, or suspension.

2.1.5 Repository obligations

The EGCA is responsible for providing a public repository, accessible through the World Wide Web at http://grid.eenet.ee/CA/.

1. EGCA will publish it s public key on the above website;
2. EGCA will publish on the above website the CRLs as soon as they are issued.

2.2 Liability

1. EGCA guarantees to control the identity of the certification requests according to the procedures described in this document;
2. EGCA guarantees to control the identity of the revocation requests according to the procedures described in this document;
3. EGCA is run on a best effort basis and does not give any guarantees about the service security or suitability;
4. EGCA SHALL NOT be held liable for any problems arising from its operation or inproper use of the issued certificates or CRLs;
5. EGCA denies any kind of responsibilities for damages or impairments resulting from its operation.

2.3 Financial responsibility

EGCA denies any financial responsibilities for damages or impairments resulting from its operation.

2.4 Interpretation and Enforcement

2.4.1 Governing law

The enforceability, construction, interpretation and validity of this policy shall be governed by the Laws of the Republic of Estonia.

2.4.2 Severability, survival, merger, notice

No stipulation.

2.4.3 Dispute resolution procedures

No stipulation.

2.5 Fees

No fees SHALL be charged.

2.6 Publication and Repository

2.6.1 Publication of CA information

The EGCA is obligated to maintain a secure on-line repository that is available through a web interface at http://grid.eenet.ee/CA and which contains:

1. the EGCA certificate for its signing key;
2. the latest CRL;

3. a copy of this document which specifies the CP and CPS;
4. other relevant information relating to certificates that refer to this Policy.

2.6.2 Frequency of publication

All information to be published in the repository SHALL be published promptly after such information is available to the CA. CRLs issued by EGCA are renewed whenever any certificate is revoked, and at least 7 days before expiration of the previously issued CRL.

2.6.3 Access controls

EGCA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL and a copy of this document containing the CP and CPS. EGCA may impose a more restricted access control policy to the repository at its discretion. The EGCA web site is maintained in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available most of the time.

2.7 Compliance audit

The EGCA may be audited by other trusted CAs to verify its compliance with the rules and procedures specified in this document. Any costs associated with such an audit MUST be covered by the requesting party.

2.8 Confidentiality

2.8.1 Types of information to be kept confidential

All subscribers' information that is not present in the certificate and CRLs issued by EGCA is considered confidential and SHALL not be released outside without explicit subscriber's authorization.

2.8.2 Types of information not considered confidential

Information included in public certificates and CRLs issued by a conforming CA are not considered confidential.

2.8.3 Disclosure of certificate revocation/suspension information

When a certificate is revoked/suspended, a reason code is not considered confidential and MAY be shared with all other users and relying parties. However, no other details concerning the revocation are normally disclosed.

2.8.4 Release to law enforcement officials

EGCA MUST NOT disclose confidential information to any third party, except when required by law enforcement officials that exhibit regular warrant.

2.8.5 Release as part of civil discovery

No stipulation.

2.8.6 Disclosure upon owner's request

The CA SHALL release information if authorized by the subscriber.

2.8.7 Other information release circumstances

No stipulation.

2.9 Intellectual Property Rights

No stipulation.

3. IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

The subject names for the certificate applicants SHALL follow the X.509 standard. Any name under this CP/CPS starts with C=EE, O=Grid.

1. In case of **personal** certificate:
   - Common Name MUST include the person's full name and MAY the person's e-mail address.
   - Organizational Unit MAY include the organization domain name.
2. In case of **server** certificate
   - Common Name MUST include the server DNS name (FQDN).
   - Organizational Unit MAY include the organization domain name.
3. In case of **grid service** certificate
   - Common Name MUST include the "*servicename*/" prefix, followed by the server DNS name (FQDN).
   - Organizational Unit MAY include the organization domain name.

3.1.2 Need for names to be meaningful

The Subject and Issuer names contained in a certificate MUST be 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.

For personal certificates, the CN DN attribute contains the legal name as presented in a government issued photo-identification.

For server certificates, the CN DN attribute contains the fully qualified domain name of the server.

For service certificates, the CN MUST be related to the type of service the certificate is identifying.

3.1.3 Rules for interpreting various name forms

See Section 3.1.1 and Section 3.1.2.

3.1.4 Uniqueness of names

The *Common Name* MUST be unique for each subject entity certified by the EGCA. In case of name collision when more than one person uses the same name, a random string is appended to the *Common Name* to make the name unique.

3.1.5 Name claim dispute resolution procedure

Name disputes are managed according to the law of Estonia.

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

RA MUST verify the authentication of organization by checking if:

1. The organization is known to be part of a grid-computing project or related partner.
2. The organization is registered and operate in Estonia. Registration in Estonia will be validated through proper public authorities.

The person who issues a request MUST demonstrate the relation between him/her and the organization he/she represents.

3.1.9 Authentication of individual identity

1. Person requesting a certificate:
   - A request sent to RA SHALL be considered authenticated when it is cryptographically signed by requestors valid Estonian ID-card certificate or by valid certificate issued for the requestor by the EGCA.
2. Otherwise, a user requesting a certificate MUST meet in person with the RA and show his/her personal photo-id (passport, Estonian ID-card or Estonian Driver License). If the photo-id is valid and the photo image corresponds to the bearer, the RA SHALL consider that the user is correctly identified.
3. Server or service certificate:
   - Requests MUST be signed by the personal certificate of the corresponding system administrator issued by EGCA or by Estonian ID-card.
4. Person not requesting a certificate (revocation):
   - Individual identity may be authenticated by personal acquaintance with RA staff;
   - By physical presence and proof of identity through a photo-id (passport, Estonian ID-card or Estonian Driver License);
   - By consulting a public directory and verifying whether that person made a request.

RA SHALL send authenticated requests to the EGCA. Any information exchanged between the requestor, the RA and the CA shall be either signed by strong cryptographic means, or shall be verifed by out-of-band methods in a phone conversation with firm positive identifcation by parties involved.

3.2 Routine Rekey

Expiration warnings will be issued to subscribers when rekey time arrives. Rekey before expiration can be accomplished by sending a rekey request signed with the current user certificate. Rekey after expiration follows the same authentication procedure as new certificate.

3.3 Rekey after Revocation

Rekey after revocation follows the same rules as an initial registration.

3.4 Revocation Request

A proper authentication method is required in order to accept revocation request. EGCA MUST accept as a revocation request a message digitally signed with a not expired and not previously revoked certificate issued under this policy. The same procedures adopted for the authentication during initial registration are also considered suitable.

4. OPERATIONAL REQUIREMENTS

4.1 Certificate Application

The necessary provisions that MUST be followed in any certificate application request to the EGCA are:

1. the subject MUST be an acceptable end user entity, as defined by this Policy;
2. the request MUST obey the EGCA distinguished name scheme;
3. the distinguished name MUST be unambiguous and unique;
4. the key MUST have at least 1024 bits.

4.2 Certificate Issuance

The following requirements MUST be met for a certificate to be issued:

1. the subject authentication MUST be successful;
2. the maximum validity period for a certificate MUST be 1 year.

The subject will be notified by E-mail about the certificate issuance or rejection. In the case of rejection the E-mail will state the reason.

4.3 Certificate Acceptance

The certificate is assumed to be accepted unless its requester explicitly rejects it in an authenticated communication with the CA.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A certificate will be revoked when the information in the certificate is known to be suspected or compromised or at the request of the authorized entity. It includes following situations:

1. The associated private key is known to be compromised or misused.
2. The associated private key is suspected to be compromised or misused.
3. The subscriber's information in the certificate has changed.
4. The subscriber is known to have violated his obligations.
5. The authenticated requester requested the certificate revocation.

4.4.2 Who can request revocation

A certificate revocation can be requested by the holder of the certificate to be revoked or by any other entity presenting proof of knowledge of the private key compromise or of the variation of the subscriber's data.

4.4.3 Procedure for revocation request

In case where the CA can independently confirm that the certificate has been compromised or misused, the CA SHALL revoke the certificate, even if the request to do so comes from an unauthenticated source and/or the holder of the certificate is unreachable.

In all other cases the CA SHALL authenticate the revocation request and try to contact the subscriber before revoking the certificate.

If the revoked certificate is a CA certificate the CA SHALL in addition inform the subscribers and cross-certifying CAs and it SHALL terminate the certificate and CRLs distribution service for certificates/CRLs issued using the compromised private key.

4.4.4 Revocation request grace period

The EGCA has a maximum response time of two days (excluding weekends and public holidays in the Estonia) for revocations; it will however handle revocation requests with priority as soon as the request is recognised as such.

4.4.5 Circumstances for suspension

No stipulation.

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)

CRLs issued by EGCA are renewed whenever any certificate is revoked, and at least 7 days before expiration of the previously issued CRL. The maximum CRL lifetime MUST be at most 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 on-line revocation/status checking service is not currently available.

4.4.12 On-line revocation checking requirements

No stipulation.

4.4.13 Other forms of revocation advertisements available

The subscriber is notified of the revocation of his certificate by email.

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 recorded

1. boot and shutdown of CA machine;
2. Certification requests;
3. Revocation requests;
4. Issued certificates;
5. Issued CRLs.

4.5.2 Frequency of processing log

No stipulation.

4.5.3 Retention period for audit log

Logs will be kept for a minimum of three years. After termination of EGCA or a RA, the logs will be kept for a minimum of three years by EGCAs host organization.

4.5.4 Protection of audit log

Audit logs may be consulted by:

1. CA personnel;
2. Authorized external auditors.

4.5.5 Audit log backup procedures

No stipulation.

4.5.6 Audit collection system (internal vs external)

No stipulation.

4.5.7 Notification to event-causing subject

No stipulation.

4.5.8 Vulnerability assessments

No stipulation.

4.6 Records Archival

4.6.1 Types of events recorded

The following events are recorded and archived:

1. certificate requests
2. approved certificate requests
3. issued certificates
4. CRLs

4.6.2 Retention period for archive

The minimum retention period is three years. After termination of EGCA or a RA, the archive will be kept for a minimum of three years by EGCAs host organization.

4.6.3 Protection of archive

Records are backed up on removable media, which are stored in a room with restricted access.

4.6.4 Archive backup procedures

See section 4.6.3.

4.6.5 Requirements for time-stamping of records

No stipulation.

4.6.6 Archive collection system (internal or external)

The archive collection system is internal to the EGCA.

4.6.7 Procedures to obtain and verify archive information

No stipulation.

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 one year before the old one looses validity and, from that point onwards, new certificates are signed with the new key. The new key is posted in the repository.

4.8 Compromise and Disaster Recovery

If the private key of the EGCA is compromised or suspected to be compromised, the EGCA will:

1. inform subscribers, relevant relying parties and all cross-certifying CAs,
2. terminate the certificate and CRL distribution for the certificates or CRL's issued using the compromised private key.

If a RA's private key is compromised or suspected to be compromised, the RA shall inform the EGCA and request revocation of the RA's certificate. If an entities private key is compromised or suspected to be compromised, the entity or its administrator or responsible MUST request revocation of the certificate and inform any relevant relying parties.

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

The private keys of the EGCA are only available in encrypted form on media stored in a secure location. The machine used to activate the private key is not accessible via any network. If the machine and/or the media are lost, this will be handled as a major compromise that implies generating a new key pair and terminating all services associated with the lost key pair.

If the hardware or software of the CA activation machine become corrupt, the status will be diagnosed and suitably repaired. If there is any doubt about the extent of the damage involved, this will imply rebuilding the machine from scratch, using original supplied parts and software distributions.

If data becomes corrupted, the cause will be diagnosed and the data restored from the latest back-up.

4.8.2 Entity public key is revoked

See section 4.8.

4.8.3 Entity key is compromised

See section 4.8.

4.8.4 Secure facility after a natural or other type of disaster

In case of (natural) disaster, the EGCA administrator(s) will as soon as physically possible confrm that all CA activation materials are at the intended locations. Depending on the situation, disaster recovery will start.

4.9 CA Termination

Before the EGCA terminates its services, the EGCA shall:

1. make all reasonable efforts to inform subscribers, RAs and cross-certifying CAs
2. make knowledge of its termination widely available
3. cease issuing certificates and CRLs
4. destroy all copies of private keys

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

The EGCA is located at the EENet office.

5.1.2 Physical access

Physical access to the EGCA is restricted to authorized personnel.

5.1.3 Power and air conditioning

The critical EGCA equipment is connected to uninterrupted power supply units.

5.1.4 Water exposures

The EGCA secure operating room is located on the first floor of the building. No floods are expected.

5.1.5 Fire prevention and protection

The EGCA secure operating room is provided with smoke detectors.

5.1.6 Media storage

1. The EGCA key is kept in several removable storage media;
2. Backup copies of CA related information are kept in USB storage devices and CDROM.

5.1.7 Waste disposal

All EGCA paper waste MUST be shredded. Magnetic media MUST be physically/mechanically destroyed before disposal.

5.1.8 Off-site backup

No off-site backups are currently performed.

5.2 Procedural Controls

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

There is no requirement within the EGCA to act within any role in the presence of more then one person.

5.2.3 Identification and authentication for each role

No stipulation.

5.3 Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The role of the CA requires a suitably trained person that is familiar with the importance of a PKI, and who is technically and professionally competent. There are no background checks of clearance procedures for trusted or other roles.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to CA and RA operators.

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

Copies of this document MUST be given to personnel of CA and RAs.

6. TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Key pairs for the EGCA are generated exclusively by authorized EGCA personnel acting in the role of CA.

End entities' key pairs are always generated by their application during the requesting process. They are never generated or stored by the EGCA.

6.1.2 Private key delivery to entity

Private keys are never delivered. End entities are required to generate their own key pairs.

6.1.3 Public key delivery to certificate issuer

1. The entity MUST submit a certificate request with the public key according to the requirements detailed in section 4.1.
2. The entity MUST be authenticated according to the procedures described in 3.1.9 and 3.1.8.
3. The entity SHOULD submit a cryptographically signed certification request via e-mail to ca@grid.eenet.ee or SHOULD deliver a certification request to the RA during face-to-face meeting.

6.1.4 CA public key delivery to users

CA-s root certificate can be downloaded from EGCA website.

6.1.5 Key sizes

The RSA key length for the EGCA is 2048 bits. Keys submitted for certification MUST be at least 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 authentication, non-repudiation, data encipherment, message integrity and session establishment.Certificates and CRLs are signed by the CA private key.

6.2 Private Key Protection

6.2.1 Standards for cryptographic module

No stipulation.

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

No stipulation.

6.2.3 Private key escrow

No stipulation.

6.2.4 Private key backup

The EGCA private key is kept encrypted in multiple copies on USB storage devices and CDROMs in safe places. The passphrase is in a sealed envelope kept in a safe.

6.2.5 Private key archival

No stipulation.

6.2.6 Private key entry into cryptographic module

No stipulation.

6.2.7 Method of activating private key

Every activation of a EGCA private key MUST require entering of passphrase. Passphrase MUST meet conditions described in 6.4.

6.2.8 Method of deactivating private key

No stipulation.

6.2.9 Method of destroying private key

After termination of the CA and after the archival period for archives has expired, 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

The EGCA private key has currently a validity of five years.

6.4 Activation Data

6.4.1 Activation data generation and installation

All pass phrases used by the CA have a length of at least 15 characters, and are suitably strong according to current best practice.

6.4.2 Activation data protection

All pass phrases are known to all current staff members of the CA. Change of staff will imply change of pass phrases.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

The secure environment for CA operations are provided by bootable Knoppix Linux CDROM, which is used for CA machines working environment. Unauthorized access to that Knoppix Linux CDROM and USB storage devices are prohibited.

The CA machine is a computer with no network connection. Keys and necessary scripts are kept on USB storage device, which is held in safe. Unauthorised physical access to CA machine or USB storage device is prohibited.

Copy of keys are printed out and held also in a safe.

The systems used by the CA to hold on-line repositories are maintained at a high level of security by applying all recommended and applicable security patches. The machine(s) are protected by a suitable firewall.

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

Software installed on the ca signing system is periodically checked for integrity by comparing strong cryptographic message digests. Firmware and hardware are not explicitly checked for correct operations.

6.6.3 Life cycle security ratings

No stipulation.

6.7 Network Security Controls

Certificates are issued on a machine that is not connected to any kind of network.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7. CERTIFICATE AND CRL PROFILES

7.1 Certificate Profile

The certificates issued in accordance with this CPS SHOULD follow the RFC 2459 [3] and the PKIX profiles.

7.1.1 Version number

X.509 v3.

7.1.2 Certificate extensions

The following extensions are set in user certificates:

1. X509v3 Basic Constraints: CRITICAL CA:FALSE
2. X509v3 Key Usage: CRITICAL
3. X509v3 Subject Key Identifier
4. X509v3 Authority Key Identifier
5. X509v3 Certificate Policies Identifier

The following extensions are set in root certificates:

1. X509v3 Basic Constraints: CRITICAL CA:TRUE
2. X509v3 Subject Key Identifier
3. X509v3 Authority Key Identifier
4. Netscape Cert Type: SSL CA, S/MIME CA, Object Signing CA

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

Issuer: C=EE, O=Grid, CN=Estonian Grid Certification Authority

7.1.5 Name constraints

See section 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

X.509 v1.

7.2.2 CRL and CRL entry extensions

No stipulation.

8. SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

The significance of the change is evaluated by the EGCA. If the change is determined to influence the trust procedures of relying parties and/or cooperating CAs, the EGCA MUST assign a new OID to the modified CPS.

Minor editorial or typographical changes to the policy and CPS MAY be made without approval.

All changes MUST be communicated to the interested parties.

8.2 Publication and notification policies

The policy is available on http://grid.eenet.ee/CA/.

8.3 CPS approval procedures

No stipulation.

APPENDIX 1: Glossary

Certification Authority (CA) - An authority trusted by one or more users to create and assign public key certificates. Optionally the CA may create the user's keys. It is important to note that the CA is responsible for the public key certificates during their whole lifetime, not just for issuing them.

CA-certificate - A certificate for one CA's public key issued by another CA.

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. For example, a particular certificate policy might indicate applicability of a type of certificate to the authentication of electronic data interchange transactions for the trading of goods within a given price range.

Certification path - An ordered sequence of certificates which, together with the public key of the initial object in the path, can be processed to obtain that of the final object in the path.

Certification Practice Statement (CPS) - A statement of the practices which a certification authority employs in issuing certificates.

Certificate revocation list (CRL) - A CRL is a time stamped list identifying revoked certificates which is signed by a CA and made freely available in a public repository.

EENet - Estonian Educational and Research Network

Estonian ID card - ID card is mandatory for all Estonian residents, including Estonian citizens and resident aliens. The ID card functions as an electronic identity, enabling you to use services online conveniently and securely. You can also use your ID card to give digital signatures. According to Estonian law, digital signatures are equivalent to handwritten ones if the systems used to give and process it meet certain regulations.

IPR - Intellectual Property Rights

Issuing certification authority (issuing CA) - In the context of a particular certificate, the issuing CA is the CA that issued the certificate (see also Subject certification authority).

Public Key Certificate (PKC) - 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.

Public Key Infrastructure (PKI) - The set of hardware, software, people, policies and procedures needed to create, manage, store, distribute, and revoke PKCs based on public-key cryptography.

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). [Note: The term Local Registration Authority (LRA) is used elsewhere for the same concept.]

Relying party (RP) - A recipient of a certificate who acts in reliance on that certificate and/or digital signatures verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

Subject certification authority (subject CA) - In the context of a particular CAcertificate, the subject CA is the CA whose public key is certified in the certificate

APPENDIX 2: Key words for use in RFCs to Indicate Requirement Levels

According to RFC 2119 [2] Key words for use in RFCs to Indicate Requirement Levels , we specify how the main keywords used in RFCs should be interpreted.

Authors who follow these guidelines should incorporate this phrase near the beginning of their document:

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHAL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119.

1. **MUST** This word, or the terms "REQUIRED" or "SHALL", mean that the definition is an absolute requirement of the specification.
2. **MUST NOT** This phrase, or the phrase "SHALL NOT", mean that the definition is an absolute prohibition of the specification.
3. **SHOULD** This word, or the adjective "RECOMMENDED", mean that there may exist valid reasons in particular circumstances to ignore a particular item, but the full implications must be understood and carefully weighed before choosing a different course.
4. **SHOULD NOT** This phrase, or the phrase "NOT RECOMMENDED" mean that there may exist valid reasons in particular circumstances when the particular behavior is acceptable or even useful, but the full implications should be understood and the case carefully weighed before implementing any behaviour described with this label.
5. **MAY** This word, or the adjective "OPTIONAL", mean that an item is truly optional. One vendor may choose to include the item because a particular marketplace requires it or because the vendor feels that it enhances the product while another vendor may omit the same item. An implementation which does not include a particular option MUST be prepared to interoperate with another implementation which does include the option, though perhaps with reduced functionality. In the same vein an implementation which does include a particular option MUST be prepared to interoperate with another implementation which does not include the option (except, of course, for the feature the option provides.)

REFERENCES

[1] EuroPKI Certificate Policy : VERSION 1.1 January 2004 [http://www.europki.org/ca/root/]

[2] RFC 2119 Key words for use in RFCs to Indicate Requirement Levels March 1997 [ftp://ftp.isi.edu/in-notes/rfc2119.txt]

[3] RFC 2459 Internet X.509 Public Key Infrastructure: Certificate and CRL Profile January 1999 [ftp://ftp.isi.edu/in-notes/rfc2459.txt]