Institute of Informatics Slovak Academy of Sciences

SlovakGrid CA

Certificate Policy and Certification Practice Statement

Version 1.2
June 2003

Contents

1 Introduction

1.1 Overview

This is a document based on the structure suggested by the RFC 2527.
This document describes:

a) Applicability of certificates signed by the SlovakGrid CA;

b) Operational practices used by the SlovakGrid CA.

SlovakGrid CA is the Certification Authority at Institute of Informatics, Slovak Academy of Sciences. (http://ups.savba.sk/ca).

1.2 Identification

Title: SlovakGrid CA Certificate Policy and Certification Practice Statement.
Version: Version 1.2.
Date: June 16, 2003
Expiration: This document is valid until further notice.
OID: 1.3.6.1.4.1.13496.1.2.1.1.2

1.3 Community and Applicability

1.3.1 Certification Authorities

SlovakGrid certificates are signed by the SlovakGrid CA.

1.3.2 Registration Authorities

The SlovakGrid CA also performs the role of RA. Further registration authorities may be created by the SlovakGrid CA as required.

1.3.3 End entities

Certificates can be issues to natural persons and to computer entities. The entities that are eligible for certification by the SlovakGrid Certification Authority are all those entities related to organizations, formally based in and/or having offices inside Slovakia, that are involved in the research or deployment of multi-domain distributed computing infrastructure, intended for cross organizational sharing of resources.
Current list of organizations eligible for certification by SlovakGrid CA can be obtained from the following URL: http://ups.savba.sk/ca/ra-list.html

1.3.4 Applicability

The issue certificate types and suitability is as follows:

a) Server certificates: authentication and communication encryption;

b) Personnel certificates: authentication and communication encryption.

c) Services certificates: authentication and communication encryption;

The certificates issued by the SlovakGrid Certification Authority may not be used for financial transactions and for any commercial usage.
The ownership of a SlovakGrid certificate does not imply automatic access to any kind of computing resources.

1.4 Contact Details

The SlovakGrid CA is managed by the II SAS.

The CA address for operational issues is:

SlovakGrid Certification Authority
Institute of Informatics
Dubravska cesta 9
845 07 Bratislava
Slovakia

Phone:	+421 2 59411289
Fax:	+421 2 54771004
Email:	ca.ui@savba.sk

The contact person for questions related with document or any other SlovakGrid CA related issues is:

Jan Astalos
Institute of Informatics SAS
Dubravska cesta 9
845 07 Bratislava
Slovakia

Phone:	+421 55 6025123
Fax:	+421 2 54771004
E-mail:	astalos.ui@savba.sk

2 General Provisions

2.1 Obligations

2.1.1 CA and RA Obligations

SlovakGrid CA will:

a) Accept certification requests for entitled entities;

b) Issue certificates based on requests from authenticated entities;

c) Notify the subscriber about the certificate issuance;

d) Publish the issued certificates;

e) Accept revocation requests from RAs or entitled entities;

f) Authenticate revocation requests before performing revocations;

g) Issue CRLs according with the rules described in this document;

h) Publish the issued CRLs;

i) Follow the policies and procedures described in this document.

Authorized RAs will:

a) Accept certification requests for entitled entities;

b) Accept revocation requests according to the procedures described in this document;

c) Authenticate entities according to the procedures described in this document;

d) Send validated certification requests to the SlovakGrid CA;

e) Create and send validated revocation requests to the SlovakGrid CA;

f) Follow the policies and procedures described in this document.

2.1.2 Subscriber Obligations

a) Read and accept the policies and procedures published in this document;

b) Generate a key pair using a trustworthy method;

c) Keep the private key safe and protected;

d) Use a strong passphrase with a minimum of 8 characters to protect the private key of personal certificates;

e) Notify the CA in case of possible private key compromise;

f) Notify the CA in case of key destruction and loss;

g) Notify the CA when the certificate is no longer required;

h) Notify the CA when the information in the certificate becomes wrong or inaccurate.

2.1.3 Relying Party Obligations

a) Read and accept the policies and procedures published in this document;

b) Verify the CRL before validating a certificate;

c) Use the certificates for permitted uses only.

2.1.4 Repository Obligations

a) SlovakGrid CA will keep a web server page at http://ups.savba.sk/ca

b) SlovakGrid CA will publish its public key on its web server.

c) SlovakGrid CA will publish on its web server the CRLs as soon as issued.

2.2 Liability

a) SlovakGrid CA guarantees to control the identity of the certification requests according to the procedures described in this document;

b) SlovakGrid CA guarantees to control the identity of the revocation requests according to the procedures described in this document;

c) SlovakGrid CA is run on a best effort basis and does not give any guarantees about the service security or suitability;

d) SlovakGrid CA will not be held liable for any problems arising from its operation or use made of certificates it issues;

e) SlovakGrid CA denies any kind of responsibilities for damages or impairments resulting from its operation.

2.3 Financial responsibility

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

2.4 Interpretation and Enforcement

2.4.1 Governing Law

The law governing the interpretation of this document is the Slovak law.

2.4.2 Dispute Resolution Procedures

Legal disputes arising from the operation of the SlovakGrid CA will be resolved according with the Slovak law.

2.5 Fees

No fees are charged.

2.6 Publication and Repositories

2.6.1 Publication of CA Information

SlovakGrid CA publishes the following information through its online repository:

a) The CA certificate;

b) The latest CRL;

c) A copy of this document containing the CP and CPS;

d) Other relevant information.

2.6.2 Frequency of Publication

New information will be published as soon as available.
CRLs will be published as soon as issued and at least every 23 days.

2.6.3 Access Controls

SlovakGrid CA does not impose any access control restrictions to the information available at its web site, which includes the CA certificate, latest CRL, LDAP repository with public keys and a copy of this document containing the CP and CPS.

SlovakGrid CA may impose a more restricted access control policy to the repository at its discretion.

The SlovakGrid CA web site is maintained in a best effort basis. Excluding maintenance shutdowns and unforeseen failures the site should be available most of the time.

2.6.4 Repositories

The SlovakGrid CA online repository is available at http://ups.savba.sk/ca.

2.7 Compliance Audit

The SlovakGrid CA may be audited by other trusted CAs to verify its compliance with the rules and procedures specified in this document.

2.8 Confidentiality

The SlovakGrid CA collects personal information about subscribers (e.g.. full name, organization and e-mail address). These data will be protected according to the Slovak law.

2.8.1 Confidential Information kept by the CA/RA

All information about subscriber that is not present in the certificate and CRL is considered confidential and will not be released outside.

2.8.2 Types of Information not Considered Confidential

Information included in issued certificates and CRLs is not considered confidential.

2.8.3 Disclosure of certificate Revocation/Suspension information

The CA will notify and inform the following entities:

a) The subject of the personal certificate;

b) The requester of the server certificate;

c) The II SAS security officer in case of security compromise.

2.8.4 Release of Information to Law Enforcement Officials

Any confidential information collected by the CA will be subject to Slovak law.

2.8.5 Information that can be revealed as Part of Civil Discovery

Any confidential information collected by the CA will be subject to Slovak law.

2.8.6 Conditions for Disclosure Upon Owner's Request

Any confidential information collected by the CA will be subject to Slovak law.

2.8.7 Other Circumstances for Disclosure of Confidential Information

Any confidential information collected by the CA will be subject to Slovak law.

2.9 Intellectual Property Rights

This document is based on the following sources:

a) RFC 2527;

b) EuroPKI Certificate Policy;

c) TrustID Certificate Policy;

d) NCSA Certificate Policy;

e) FBCA Certificate Policy;

f) INFN Certificate Policy and Certificate Practice Statement;

g) NIKHEF Certificate Policy and Certificate Practice Statement.

h) LIP certificate Policy and Certificate Practice Statement.

3 Identification and Authentication

3.1 Initial Registration

3.1.1 Types of Names

The subject names obey to the X.500 standard:

a) For persons the name includes the person name;

b) For servers the subject includes the server DNS FQDN name. It may be prefixed with "host/".

c) For services the subject includes the server DNS FQDN name, prefixed with the service name.

3.1.2 Name Meanings

The format of a SlovakGrid distinguish name is:
"C=SK, O=SlovakGrid, O=organisation, CN=subject-name"
The common name in the certificate subject must be obtainable from the real subject name. Current list of values available for distinguished name O can be obtained from the following URL:
http://ups.savba.sk/ca/ra-list.html.

3.1.3 Uniqueness of Names

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

3.1.4 Method to Prove Possession of Private Key

No stipulation.

3.1.5 Authentication of Organization Identity

No stipulation.

3.1.6 Authentication of Individual Identity

Procedures differ if the subject is a person or a server:
Person requesting a certificate:

a) The certificate request must be sent to ca.ui@savba.sk from an e-mail address in a persons organization domain;

b) The requesting person must contact indicated RA personally;

c) The subject authentication is performed through the presentation of a valid official identification document (Passport or Identity card) or by firm personal acquaintance by RA.

Server or service certificate:

a) Requests must be send by e-mail and be signed by the valid personal SlovakGrid CA certificate of the corresponding system administrator;

b) The requesting person must contact RA personally and prove that he has necessary authorisation.

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

Certificate revocation requests should be submitted by:

a) E-mail sent to ca.ui@savba.sk signed with a valid SlovakGrid CA certificate.

b) When E-mail is not an option the request will be authenticated using the procedure described in section 3.1.6 (Authentication of individual identity).

4 Operational Requirements

4.1 Certification Application

Applicants must generate their own key pair. The minimum key length for all applications is at least 1024 bits. The maximum validity period for a certificate is 1 year. The requests must obey to the SlovakGrid CA distinguished name scheme. Certificate requests in PEM-format are sent by e-mail to ca.ui@savba.sk or to the corresponding RA. Depending on if the requester is a person or a machine or a service the procedures outlined in 3.1.6 are applied

4.2 Certificate Issuance

The following requirements must be meet for a certificate to be issued:

a) The subject authentication must be successful.

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

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for Revocation

A certificate will be revoked in the following circumstances;

a) The subject does not want the certificate any more;

b) The private key has been lost or compromised;

c) The information in the certificate is wrong or inaccurate;

d) The subject has failed to comply with the rules in this policy;

e) The system to which the certificate has been issued has been retired.

4.4.2 Who can request revocation

The revocation of the certificate can be requested by:

a) The certificate subscriber;

b) Any other entity presenting proof of knowledge of the private key compromise or of the modification of the subscriber's data.

4.4.3 Procedure for Revocation Request

The entity requesting the certificate revocation is authenticated by:

a) Signing the revocation request with a valid SlovakGrid CA certificate.

Otherwise authentication is to be performed with the same procedure used to authenticate the identity of a person requesting a certificate.

4.4.4 Circumstances for Suspension

No stipulation.

4.4.5 Who can request suspension

The certificate subscriber can request the suspension of the certificate.

4.4.6 Procedure for suspension request

The suspension requester is authenticated by:

a) Signing the suspension request with the corresponding SlovakGrid CA certificate.

4.4.7 Limits on Suspension Period

Not specified.

4.4.8 CRL Issuance Frequency

a) CRLs are issued whenever a certificate issued by SlovakGrid CA is revocated;

b) CRLs are reissued and at least 7 days before expiration. Maximum lifetime of CRL is 30 days;

a) CRLs will be published as soon as issued .

4.4.9 CRL Checking Requirements for Relying Parties

Download the CRL at least once a day and implement its restrictions while validating certificates.

4.4.10 Online Revocation/status Checking Availability

Not Implemented.

4.4.11 Online Revocation Checking Requirements

Not Implemented.

4.4.12 Other Forms of Revocation Advertisement

None.

4.4.13 Requirements for Relying Parties on Other Forms of Revocation Advertisement

None.

4.4.14 Variations of the Above in Case of Private Key Compromise

If a major security problem may be generated from a compromised certificate the SlovakGrid CA may choose to warn the known relying parties using any means seem fit.

4.5 Security Audit Procedures

4.5.1 Types of Events Recorded

a) Boot of CA machine

b) Interactive logins to CA machine

c) Certification requests;

d) Revocation requests;

e) Issued certificates;

f) Suspension requests;

g) Issued CRLs.

4.5.2 Processing Frequency of Audit Logs

No stipulation.

4.5.3 Retention Period for Audit Logs

Logs will be kept for a minimum of 3 years.

4.5.4 Protection of Audit Logs

Only authorized CA personnel and authorized external auditors are allowed to view and process audit logs. Audit logs are copied to an off-line medium stored in safe storage.

4.6 Records Archival

4.6.1 Types of Events Recorded

a) Certification requests;

b) Revocation requests;

c) Issued certificates;

d) Suspension requests;

e) Issued CRLs;

f) E-mail messages sent and received by the CA/RA.

4.6.2 Processing Frequency of Records

No stipulation.

4.6.3 Retention Period for Records

Logs will be kept for a minimum of 3 years.

4.6.4 Protection of Records

Only authorized CA personnel and authorized external auditors are allowed to view and process records. Records are copied to an off-line medium stored in safe storage.

4.7 Key Changeover

No stipulation.

4.8 Compromise and Disaster Recover

If the CA private key is compromised the CA will:

a) Notify subscribers, RAs and cross-certifying CAs;

b) Terminate the issuance and distribution of certificates and CRLs;

c) Notify relevant security contacts.

4.9 CA Termination

Upon termination the SlovakGrid CA will:

a) Notify subscribers, RAs and cross-certifying CAs;

b) Terminate the issuance and distribution of certificates and CRLs;

c) Notify relevant security contacts;

d) Notify widely as possible the end of the service.

5 Physical, Procedural, and Personnel Security Controls

5.1 Physical Security Controls

5.1.1 Site Location

The SlovakGrid CA is located at the II SAS.

5.1.2 Physical Access

Physical access to the SlovakGrid CA is restricted to authorized personnel.

5.1.3 Power and Air Conditioning

CA machine is powered off between uses.

5.1.4 Water Exposures

Due to the location of the SlovakGrid CA facilities floods are not expected.

5.1.5 Fire Prevention and Protection

SlovakGrid CA facilities obey to the Slovak law regarding fire prevention and protection in buildings.

5.1.6 Media Storage

a) The SlovakGrid CA key is kept in several removable storage media;

b) Backup copies of CA related information is kept in floppies and CDROM.

5.1.7 Waste Disposal

Waste carrying potential confidential information such as old floppy disks are physically destroyed before being trashed.

5.1.8 Off-site Backup

No off-site backups are currently performed.

5.2 Procedural Controls

Not defined.

5.3 Personnel Security Controls

5.3.1 Background Checks and Clearance Procedures for CA Personnel

CA personnel are recruited from the II SAS staff.

5.3.2 Background Checks and Security Procedures for Other Personnel

No other personnel are authorized to access CA facilities without the physical presence of CA personnel.

5.3.3 Training Requirements and Procedures

Internal training is given to CA operators.

5.3.4 Training Period and Retraining Procedures

No stipulation.

5.3.5 Frequency and Sequence of Job Rotation

Job rotation is not performed.

5.3.6 Sanctions Against Personnel

No stipulation.

5.3.7 Controls on Contracting Personnel

No stipulation.

5.3.8 Documentation Supplied to Personnel

a) Copies of this document;

b) SlovakGrid CA Operations Manual;

6 Technical Security Controls

6.1 Key Pair Generation and Installation

6.1.1 Key Pair Generation

Each subscriber must generate his own key pair. The SlovakGrid CA does not generate private keys for subjects.

6.1.2 Private Key Delivery to Entity

No stipulation.

6.1.3 Public Key Delivery to Certificate Issuer

Public keys are delivered by encrypted E-mail, SSL over http or floppy disk.

6.1.4 CA Public Key Delivery to Users

CA certificate can be downloaded from the SlovakGrid CA web site (http://ups.savba.sk/ca).

6.1.5 Key Sizes

a) The minimum key length for a personnel or server certificate is 1024 bits;

b) The CA key length is 2048 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

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 Private Key (n out of m) Multi-person Control

No stipulation.

6.2.2 Private Key Escrow

No stipulation.

6.2.3 Private Key Archival and Backup

The SlovakGrid CA private key is kept encrypted in multiple copies in floppy disks and CDROMs in safe places. The passphrase is in a sealed envelope kept in a safe.

6.3 Other Aspects of Key Pair Management

The SlovakGrid CA private key has currently a validity of five years.

6.4 Activation Data

The SlovakGrid CA private key is protected by a passphrase with minimum of 15 characters.

6.5 Computer Security Controls

6.5.1 Specific Security Technical Requirements

a) The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;

b) Monitoring is performed to detect unauthorized software changes;

c) CA systems configuration is reduced to the base minimum;

d) The signing machine is kept powered off between uses.

6.5.2 Computer Security Rating

No stipulation.

6.6 Life Cycle Security Controls

No stipulation.

6.7 Network Security Controls

a) The CA signing machine is kept off-line;

b) CA/RA machines other than the signing machine are protected by a firewall.

6.8 Cryptographic Module Engineering Controls

No stipulation.

7 Certificate and CRL Profile

7.1 Certificate Profile

7.1.1 Version Number

X.509 v3.

7.1.2 Certificate Extensions

CA certificate extensions:
Basic constraints: critical
    CA
Key usage: critical
    Digital Signature, Non Repudiation, Certificate Sign, CRL Sign
Subject key identifier
Authority key identifier
Issuer alternative name
CRL distribution points
Netscape cert type
Netscape comment
Netscape base URL
Netscape revocation URL
Netscape CA policy URL

Subsriber certificate extensions:
Basic constraints: critical
    Not a CA
Key usage: critical
    Digital Signature, Non Repudiation, Key Encipherment
Subject key identifier
Authority key identifier
Subject alternative name
Issuer alternative name
CRL distribution points
Netscape cert type
Netscape comment
Netscape base URL
Netscape revocation URL
Netscape CA policy URL

7.1.3 Algorithm Object Identifiers

No stipulation.

7.1.4 Name Forms

Issuer: C=SK, O=SlovakGrid, CN=SlovakGrid CA
Subject: C=*countryName*, O=SlovakGrid, O=o*rganizationName*, CN=*commonName*

7.1.5 Name Constraints

Subject attribute constraints:
countryName: (mandatory)
Must be "SK".
organizationName: (mandatory)
Must be the organization with which the subject is related. Current list of possible values of *organizationName* can be obtained from the following URL: http://ups.savba.sk/ca/ra-list.html
commonName: (mandatory)
Name and surname or DNS FQDN of the subject. For hosts and services, FQDN may be prefixed with service name.

7.1.6 Certificate Policy Object Identifier

OID: as specified in 1.2

7.1.7 Usage of Policy Constraints Extensions

No stipulation.

7.1.8 Policy Qualifier Syntax and Semantics

No stipulation.

7.2 CRL Profile

7.2.1 Version

x.509 v1.

7.2.2 CRL and CRL Entry Extensions

No stipulation.

8 Specification Administration

8.1 Specification Change Procedures

Only the subscribers will be warned of changes to SlovakGrid CA's policy and CPS.

8.2 Publication and Notification Procedures

The SlovakGrid CA policy is available at http://ups.savba.sk/ca/ca-policy.html

8.3 CPS Approval Procedures

No stipulation.