SiGNET CA CP/CPS

Jan Jona Javorsek, Borut Paul Kersevan

25 September 2004
1.0

1 INTRODUCTION

1.1 Overview

SiGNET CA functions as part of the Experimental Particle Physics Department (F9-IJS) of the "Jozef Stefan" Institute in Ljubljana, Slovenia (IJS), the leading Slovenian non-profit research organization.

SiGNET CA is the top level Certification Authority for Slovenia. SiGNET CA provides public key infrastructure (PKI) to Slovenian research and educational organisations and users, and Slovenian participants in grid projects and EGEE collaboration.

This document describes the set of rules, operational procedures and obligations for the issuance and management of certificates used by the Slovenian Grid Net Certification Authority (SiGNET CA).

This document is a draft Certification Policy and Certification Practice Statement written according to the structure suggested by the RFC 2527.

1.1.1 General Definitions

The following definitions and associated abbreviations are used in this document.

Activation data Data values, other than keys, that are required to operate cryptographic modules and that need to be protected (e.g., a PIN, a passphrase, or a manually-held key share).

CERN The European Organisation for Nuclear Research, an intergovernmental organisation having its seat in Geneva, Switzerland.

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 Authority Request Gateway (CA-GATE) A computer configured with appropriate software to support the procedures described in this CPS.

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

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.

F9-IJS Experimental Particle Physics Department of the "Jozef Stefan" Institute in Ljubljana, Slovenia. F9-IJS is leading SiGNET and actively participating in grid infrastructure deployment in Slovenia. (More info on F9-IJS: `http://www-f9.ijs.si/`.)

Fully Qualified Domain Name (FQDN) A fully qualified domain name consists of a host name and all domain names up to and including the top-level domain. FQDN is sufficient for unique identification of a host (multihomed IP non withstanding) or service.

IJS, "Jozef Stefan" Institute in Ljubljana "Jozef Stefan" Institute in Ljubljana, Slovenia (IJS), is the leading Slovenian research organisation. This non-profit organisation is responsible for a broad spectrum of basic and applied research in the fields of natural sciences and technology. (More info on IJS: `http://www.ijs.si/`.)

Issuing Certification Authority (Issuing CA) In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

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.

Public Key Infrastructure (PKI) Organisations, policies and computing facilities required for operating a public key security, encryption and authentication scheme.

Policy Qualifier Policy-dependent information that accompanies a certificate policy identifier in an X.509 certificate.

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).

Relying party 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.

Repository A storage area, usually online, which contains published materials, such as lists of issued certificates, CRLs, policy documents, etc.

Set of Provisions A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a certificate policy definition or CPS employing the approach described in this framework.

Slovenian Grid Network (SiGNET) Slovenian Grid Network is the root organisation providing grid and computational network services to Slovenian scientific, educational and research communities.

Slovenian Grid Network Certification Authority (SiGNET CA) SiGNET CA is the top level Certification Authority for Slovenia. SiGNET CA provides public key infrastructure (PKI) to Slovenian research and educational organisations and users, and Slovenian participants in grid projects and EGEE collaboration. (More info on SiGNET CA: `http://signet-ca.ijs.si/`.)

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

Within this document the words *must*, *must not*, *required*, *shall*, *shall not*, *should*, *should not*, *recommended*, *may*, *optional* are to be interpreted as in RFC 2119.

Any other terms are to be understood as in RFC 2527.

1.2 Identification

Document title	Slovenian Grid Net Certification Authority Certificate Policy and Certification Policy Statement
Short title	SiGNET CA CP/CPS
Document version	Document version 1.0
Document date	September 2004
Document validity	Valid until further notice.
ASN.1 Object Identifier for Document (OID)	1.3.6.1.4.1.15312.3.1.1.0

ASN.1 OID is constructed in the following way:

IANA	1.3.6.1.4.1
IJS	.15312

SiGNET CA .3
CP/CPS .1
Major Version .1
Minor Version .0

1.3 Community and Applicability

1.3.1 Certification authorities

SiGNET certificates are signed by SiGNET CA. SiGNET CA does not issue certificates to subordinate certification authorities.

SiGNET CA certificate is signed by itself.

1.3.2 Registration authorities

SiGNET CA manages the functions of its Registration Authority.

Additional registration authorities may be created by SiGNET CA as required. Such trusted intermediaries are formally assigned by SiGNET CA and their identities and contact details are published in an on-line accessible repository at the following URL: `http://signet-ca.ijs.si/signet-ralist.txt`.

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

1.3.3 End entities

SiGNET CA will issue certificates to entities formally based or having offices in Slovenia, or participating in projects based in Slovenia, and are intended for cross-organisational sharing of resources in the fields of research and/or education.

Certificates can be issued to persons and computer entities (services or hosts). Organisations 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:

(a) personal certificates: authorised for document-signing, personal authentication, non-repudiation and encryption of communications

(b) host certificates: authorised for object-signing, host authentication, non-repudiation and encryption of communications

(c) service certificates: authorised for object-signing, service authentication, non-repudiation and encryption of communications

The certificates issued by SiGNET CA may not be used for financial transactions or for any commercial usage, including gifts.

1.4 Contact Details

1.4.1 Specification administration organisation

SiGNET CA is managed by the F9 - Experimental Particle Physics Department of the "Jozef Stefan" Institute in Ljubljana, Slovenia.

F9 IJS general web address is: `http://www-f9.ijs.si/`.
SiGNET CA general web address is: `http://signet-ca.ijs.si/`.
SiGNET CA policy documents are at: `http://signet-ca.ijs.si/policy/`.
SiGNET CA Certificate Repository is at: `http://signet-ca.ijs.si/cert/`.
SiGNET CA CRL Repository is at: `http://signet-ca.ijs.si/crl/`.
SiGNET CA address for operational issues is:

SiGNET CA
F9 Experimental Particle Physics Department
"Jozef Stefan" Institute
Jamova 39
P.O. BOX 3000
SI-1001 Ljubljana
Slovenia

email: signet-ca@ijs.si
phone: +386 1 477 3742
fax: +386 1 425 7074

1.4.2 Contact person

The contact person for questions related with this document is:

Jan Jona Javorsek
F9 Experimental Particle Physics Department
"Jozef Stefan" Institute
Jamova 39
P.O. BOX 3000
SI-1001 Ljubljana
Slovenia

email: jona.javorsek@ijs.si
phone: +386 1 477 3742
fax: +386 1 425 7074

The contact person for questions related with SiGNET CA operations is:

Borut Kersevan
F9 Experimental Particle Physics Department
"Jozef Stefan" Institute
Jamova 39
P.O. BOX 3000
SI-1001 Ljubljana
Slovenia

email: borut.kersevan@ijs.si
phone: +386 1 477 3454
fax: +386 1 425 7074

1.4.3 Person determining CPS suitability for the policy

The second person named under *section 1.4.2*.

2 GENERAL PROVISIONS

2.1 Obligations

2.1.1 CA obligations

SiGNET CA is solely responsible for the issuance and management of certificates referencing this document. SiGNET CA shall:

1. Ensure that all services, operations and infrastructure conform to this CP/CPS at all times;
2. Handle certificate requests and issue new certificates:
    - Accept and confirm certification request from entitled entities and approved certification requests from RAs;

- Authenticate entities requesting a certificate, where applicable with the assistance of the designated RAs listed at the location specified in *section 1.3.2*;
- Issue certificates based on approved certificate requests from authenticated entities;
- Send notification of the issuing of the certificate to the subscriber;
- Make issued certificates publicly available;

3. Handle certificate revocation requests and certificate revocation:

   - Accept and confirm revocation requests from entitled entities and RAs requesting that a certificate be revoked according to procedures described in this document;
   - Authenticate entities requesting that a certificate should be revoked;
   - Revoke certificates based on approved revocation requests from authenticated entities;
   - Issue a Certificate Revocation List (CRL) according to the procedures outlined in this document;
   - Make certificate revocation information publicly available in the form of published CRL.

2.1.2 RA obligations

A SiGNET RA must sign an agreement to adhere to the procedures described in this document. Each SiGNET RA shall:

1. Authenticate entities requesting a certificate according to the procedures outlined in this document;
2. Approve certificate requests according to the procedures outlined in this document;
3. Validate the connection between a public key and the requester identity including a suitable proof of possession method;
4. Confirm such validation to the CA;
5. Send the approved certificate requests to SiGNET CA;
6. Check that the subscriber knows and agrees to subscriber obligations concerning safeguarding their private key - for a personal key, this means that the key is protected by a pass-phrase of at least 15 characters in length; for a server key it means that the key is at least readable only by root or a restricted user account;
7. Check that the information provided in the certificate request is correct and check that the email address provided by the subscriber is correct;
8. Approve revocation requests according to the procedures outlined in this document;
9. Send the approved revocation requests to SiGNET CA;
10. Sign each request before sending it to SiGNET CA;
11. Request revocation of a certificate in the event that it becomes aware of circumstances justifying such revocation;
12. inform the CA and request the revocation of the RA's certificate if the RA's private key is destroyed, lost, compromised or suspected to be compromised;
13. Log all transactions and requests;
14. Follow the policies and procedures described in this document.

2.1.3 Subscriber obligations

Subscribers must:

1. Accept conditions and adhere to the procedures described in this document;
2. Represent correct information on the certificate application and only such information as he/she is entitled to submit for the purposes of this document.
3. Authorise the treatment and conservation of personal data;
4. Generate a key pair using a trustworthy method;
5. Take reasonable precautions to prevent any loss, disclosure or unauthorised use of the private key associated with the certificate, including
   - selecting a strong passphrase with a minimum of 15 characters and
   - protecting the passphrase from others;
6. Use the certificate exclusively for authorised and legal purposes, consistent with this document;
7. Notify SiGNET CA when the certificate is no longer required;
8. Notify SiGNET CA when the information in the certificate becomes wrong or inaccurate;
9. Notify SiGNET CA immediately if the private key associated with the certificate is destroyed, lost, compromised or suspected to be compromised;
10. Notify SiGNET CA when they no longer fulfill the conditions for use of a SiGNET CA certificate, and cease usage immediately;
11. By using the authentication procedures described in this document subscribers accept the restrictions to liability described in *section 2.2*.

2.1.4 Relying party obligations

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

1. Accept conditions and adhere to the policies and procedures described in this document;
2. Verify the certificate revocation information before validating a certificate;
3. Use the certificate exclusively for authorised and legal purposes, consistent with this document;

2.1.5 Repository obligations

1. SiGNET CA will will publish all information described in *section 2.6.1* on its public web server at the following URL: `http://signet-ca.ijs.si/`.
2. SiGNET CA will publish its public key on its public web server;
3. SiGNET CA will publish its certificate revocation information, CRLs on its public web server as soon as issued.
4. The repository is operated at a best-effort basis, where the intended availability is continuous.

2.2 Liability

2.2.1 CA liability

1. SiGNET CA only guarantees to control the identity of the subjects requesting a certificate according to the practices described in this document;
2. SiGNET CA will not give any guarantees about the security or suitability of the service;
3. SiGNET CA aims to achieve a reasonable level of security, but its certification services are provided on a best-effort basis only;
4. SiGNET CA provides no warranties, express or implied, including in respect of security and confidentiality, and of fitness for a particular purpose, for its procedures, repositories, databases and certificates, and will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides;
5. IJS, F9 IJS and SiGNET CA accept no liability for or in connection with the certification services and the parties using or relying on them shall hold IJS, F9 department and SiGNET CA free and harmless from liability resulting from such use or reliance;
6. IJS, F9 IJS and SiGNET CA deny any financial or any other kind of responsibilities for damages or impairments resulting from SiGNET CA's operation.

2.2.2 RA liability

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

It is the RA's responsibility to authenticate the identity of subscribers requesting certificates, according to the practices described in this document. It is the RA's responsibility to request revocation of a certificate if the RA is aware that circumstances for revocation are satisfied.

2.3 Financial Responsibility

No financial responsibility is accepted.

2.3.1 Indemnification by relying parties

No stipulation.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

No stipulation.

2.4 Interpretation and Enforcement

2.4.1 Governing law

This document is subject to all applicable laws of the Republic of Slovenia.

2.4.2 Severability, survival, merger, notice

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

2.4.3 Dispute resolution procedures

SiGNET CA will resolve naming disputes according to best current practice.

2.5 Fees

No fees are charged for any service provided by SiGNET 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

SiGNET CA will publish the following information:

1. SiGNET CA's root certificate;
2. A Certificate Revocation List signed by SiGNET CA;
3. All past and current versions of this document;
4. Other relevant information.

2.6.2 Frequency of publication

The frequency of CRL publication is specified in section *4.4.9*.

New versions of CP-CPS will be published as soon as they have been approved.

2.6.3 Access controls

SiGNET CA imposes no any access control on its Policy, its Certificate and CRLs.

SiGNET Grid CA may at any time impose a more restricted access control policy to the repository at its discretion.

SiGNET CA public web site, online repository and certificate request submission web interface are operated at a best-effort basis, where the intended availability is continuous.

2.6.4 Repositories

SiGNET CA publishes the above mentioned information through its online repository at `http://signet-ca.ijs.si/`.

2.7 Compliance Audit

No external audit will be required, only a self-assessment by the SiGNET CA that its operation is according to this document.

Requests for external audit from other trusted CA may be considered at the discretion of IJS 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

SiGNET CA collects personal information about the subscribers (e.g. full name, organisation, organisation unit, e-mail address, phone number public key, certificate request file).

These data will be protected according to law of Republic of Slovenia.

By making an application for a certificate a subscriber is deemed to have consented to their personal data being stored and processed, subject to the Personal Data Protection Act of the Republic of Slovenia (ZVOP, 210-01/89-3/20, 1999 art. 3).

The full name is included in the certificate. Any info on organisation and organisational unit is included in the certificate. E-mail address and phone number are *not* included in the certificate.

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 SiGNET CA.

Record of the e-mail messages sent and received by SiGNET CA is considered confidential.

Under no circumstances will SiGNET CA have access to the private keys of the subscribers to whom it issues a certificate.

2.8.2 Types of information not considered confidential

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

2.8.3 Disclosure of certificate revocation/suspension information

SiGNET CA will notify and inform the following entities:

1. The subject of the personal certificate;
2. The requester of the server certificate;
3. The IJS Networking Center security officer in case of security compromise.

No information about the reason for a revocation is published.

2.8.4 Release to law enforcement officials

SiGNET CA will not disclose certificate or any certificate-related information to any third party, aside from information publicly available, except when so required by a legal authority of competent jurisdiction.

2.8.5 Release as part of civil discovery

As per *section 2.8.4* .

2.8.6 Disclosure upon owner's request

As per *section 2.8.4* .

2.8.7 Other information release circumstances

As per *section 2.8.4* .

2.9 Intellectual Property Rights

This document is based on the following sources:

- RFC 2527;
- EuroPKI Certificate Policy;
- Global Grid Forum Certificate Policy Model, version 7 October 2002;
- CERN Certificate Policy and Certificate Practice Statement;
- Grid-Ireland CA Certificate Policy and Certificate Practice Statement;
- IUCC CA Certificate Policy and Certificate Practice Statement;
- PK-GRID-CA Certificate Policy and Certificate Practice Statement;
- Polish Grid CA Certificate Policy and Certificate Practice Statement.

3 IDENTIFICATION AND AUTHENTICATION

3.1 Initial Registration

3.1.1 Types of names

The Subject Name is an X.500 distinguished name. Name forms are further defined in *section 7.1.5*.

Any name under this CP/CPS starts with `C=SI, O=SiGNET`. If the subject is part of an organisation, an `O=`*organisation*. An optional `OU=`*organisational_unit* must be appended if the organisation consists of multiple administrative divisions. (Changes in division name that do not change the organisational layout of an organisation do not constitute a reason to invalidate the current unit name.) The last part is the CN, which takes one of the following forms:

For a Person: CN is the full name of the subject.The name must include at least one given name in full and the full surname. Only ASCII alphanumeric letters, space and dash may be used.

Example of a full subject name for a person from IJS:

```
C=SI, O=SiGNET, O=IJS, OU=F9 CN=Janez Kranjski
```

A change in the name of the person does not invalidate the certificate and does not necessitate immediate change of the distinguished name.

For a Host: CN is the host fully qualified domain name DNS name (FQDN). In case the host entity is not an internetwork entity or no such FQDN is assigned for other reasons, the entity is not eligible for certification under this policy.

FQDN domains may be different from organisation and `organisational_unit` fields since assigned FQDN does not always follow the structural layout of an organisation or network.

Example of a full subject name for a server:

```
C=SI, O=SiGNET, O=IJS, OU=F9, CN=host.ijs.si
```

For a Service: CN is constructed in the same way and under the same conditions as for hosts, but with a service identifier related to the service appended to the front.

Example of a full subject name for a service:

```
C=SI, O=SiGNET, O=IJS, OU=F9, CN=ldap/host.ijs.si
```

3.1.2 Need for names to be meaningful

The subject name in a certificate must have a reasonable association with the authenticated name of the subscriber.

The common name CN in the certificate subject name must be obtainable from the real subject name. For persons it must be obtainable from a name of the person. For host certificates, the CN must be formed from the registered fully qualified domain name (DNS FQDN). For a service certificate, the CN must be related to the type of service the certificate is identifying.

The Organisation Name in the certificate subject name must be one of the organisations involved in SiGNET activities. Current list of values available for Organisation Names in the in the certificate subject name can be obtained from the URL mentioned in *section 1.3.2*.

3.1.3 Rules for interpreting various name forms

See *section 3.1.1*.

3.1.4 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.

Certificates must apply to unique individuals or resources. Users must not share certificates.

3.1.5 Name claim dispute resolution procedure

Name claim disputes are resolved by discretion of the first person named under *section 1.4.2*.

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 organisation identity

No certificates are issued directly to organisations. Certificate requests for entities such as hosts and services must be made by a secure online submission to SiGNET CA Public Server, signed with a valid personal SiGNET certificate. Alternatively, an e-mail message signed with a valid personal personal SiGNET certificate may be used.

SiGNET CA may take steps to ascertain that the user is indeed entitled to represent the organisation or entity which has the rights over the host or service on behalf of which the certificate request has been made.

If the name of an organisation is requested to be part of a subject name, SiGNET CA may take steps to ascertain that the organisation consents to such use.

In the certificate request, the generic e-mail for the host or service must be specified in the *Certificate data* part and the e-mail of the user requesting the certificate in the *User data*.

3.1.9 Authentication of individual identity

A user requesting a certificate must either meet in person with the RA and show their IJS access card, acceptable Slovenian photo ID or acceptable foreign photo ID recognised in Slovenia, such as a passport.

If the identification document is valid and the photo image corresponds to the bearer, the RA shall consider that the user is correctly identified.

The RA must forward a photocopy of the document for safekeeping in the CA.

Additionally, the RA may consider that the user is correctly identified if the RA has previously identified the user using the procedure described above and the user can prove possession of his/her secret key of an existing certificate issued by SiGNET CA. In this case the RA must check by telephone or personal conversation that the request originated at the known user.

If authentication is not completed within fifteen days of receipt of the certificate request by the RA, the request will be deemed to have expired. The process of submitting a certificate request and complying with the authentication procedure as per sections *3.1.8* and *3.1.9* shall have to be repeated.

3.2 Routine Rekey

Rekeying of certificates will follow the same procedure as an initial registration.

Additionally, rekeying of certificates of persons before their expiration can be requested by submitting a rekey request to the SiGNET CA Public Server, signed by the subscriber's current personal SiGNET CA certificate.

3.3 Rekey After Revocation

A public key whose certificate has been revoked shall not be re-certified.

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

3.4 Revocation Request

Unless SiGNET CA can independently verify that a key compromise has occurred, a revocation request must be authenticated before being accepted. Anyone can make certificate revocation requests by sending email to the CA. However, the CA will not revoke a certificate unless the request is authenticated, or it can be verified independently that there is reason to revoke the certificate. See *section 4.4*.

Authenticated certificate revocation requests may be made by

- The RA using:
  - Digitally signed email to **signet-ca@ijs.si**;
  - Other secure method, as specified in the RA Operator's procedure;
  - The method for authentication of individual entity, as described in *section 3.1.9*.
- The subscriber by:

– Mailing the SiGNET CA directly by email to **signet-ca@ijs.si**, digitally signed with a certificate which has not expired or been revoked and was issued under this CP/CPS, regardless of the document version, where the e-mail address in the request must belong to the person that owns the certificate;
– The method for authentication of individual entity, as described in *section 3.1.9*.

4 OPERATIONAL REQUIREMENTS

4.1 Certificate Application

Any certificate application request to SiGNET must follow the following provisions:

- The subject must be an acceptable end user entity, as defined by this policy.
- Personal certificates must not be shared; server certificates must be linked to a single network entity.
- The applicant must register with a SiGNET RA as per *section 3*.
- The request must obey SiGNET CA distinguished name scheme.
- The distinguished name must be as per *section 3.1.1*; see also *section 7*.
- The distinguished name must be unambiguous and unique.
- The applicant must generate a their key pair as per *section 6*.
- The applicant must guard their private key and not reveal it to SiGNET CA. SiGNET CA must not generate the key pair for the applicant.

Maximal lifetime of a certificate is one year. The default validity period is one year.

Certificate requests are made via SiGNET CA's public web interface at `http://signet-ca.ijs.si/`. Alternatively, if the web interface can not be used, certificate requests can be made via e-mail with the attached public key in PEM-format at **signet-ca.user@ijs.si**.

Certificate requests are submitted also through any additional approved RA's as per *section 1.3.2*.

4.2 Certificate Issuance

The first step in the issuance process is the approval of the request by an RA (including SiGNET CA's own RA). The following requirements must be fulfilled:

- RA must authenticate the applicant according to the procedures described in *section 3.1.9*;
- RA must check if the request sender can apply for a certificate according to *section 1.3.3*
- RA is recognised by SiGNET CA as a RA for the applicant, as specified in *section 1.3.2*

If all the above requirements are fulfilled, then RA approves the request and passes on the request to the CA for issuance of a certificate.

The subject will be notified by e-mail. If the subject is a person, the e-mail will be sent to the address accompanying the request. Otherwise the e-mail will be sent to the address specified in the request. In the case of rejection, the e-mail will state the reason.

If the e-mail fails to be delivered in a period of 5 days, the certificate is revoked without further notice.

Once a certificate request has been approved by the RA, the certificate is normally issued by the CA within seven working days.

4.3 Certificate Acceptance

No stipulation.

4.4 Certificate Suspension and Revocation

4.4.1 Circumstances for revocation

A certificate will be revoked when the information it contains is suspected to be incorrect or compromised. This includes situations where:

1. The subscriber's private key is lost, destroyed or suspected to be compromised;
2. The information in the subscriber's certificate is suspected or confirmed to be inaccurate;
3. The subscriber no longer needs the certificate to access Relying Parties' resources;
4. The subscriber no longer fulfills the conditions for participation in SiGNET;
5. The subscriber violated his/her obligations;
6. The system or service to which the certificate has been issued has been retired.

In addition, the CA will revoke all certificates in the event that its key has been compromised (as per *section 4.8.3*) or in the event that the CA has been terminated (as per *section 4.9*).

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 circumstances for revocation, as described in *section 4.4.1*.

4.4.3 Procedure for revocation request

The entity requesting the revocation must send the revocation request with an authenticated deposition via the public web interface at SiGNET or by a signed e-mail to SiGNET CA or a SiGNET RA. If this is not possible the CA/RA must be contacted directly. Authentication can be performed as per *section 3.1.9*.

In both cases above, the requesting entity must specify the reason for the revocation request and provide evidence of circumstances as described in *section 4.4.1*.

4.4.4 Revocation request grace period

There will be no grace period associated with certificate revocation. SiGNET CA handles revocation requests with priority and a certificate will be revoked as soon as possible after circumstances for revocation, as described in *section 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)

CRLs are issued after every certificate revocation or at least 7 days before the current CRL expires. The usual validity of a 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

No stipulation.

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 regarding key compromise

No stipulation.

4.5 Security Audit Procedures

4.5.1 Types of event audited

The following events are recorded and audited:

- Certification requests;
- Issued certificates;
- Issued CRLs;
- Requests for revocation;
- Boots and shutdowns of the CA equipment;
- Interactive system logins at the CA equipment.

4.5.2 Frequency of processing log

Audit logs will be analysed at least once per month.

4.5.3 Retention period for audit log

Logs will be kept for a minimum of 3 years.

4.5.4 Protection of audit log

Only authorised CA personnel and authorised external auditors are allowed to view and process audit logs. Audit logs are copied to an off-line non-magnetic medium.

4.5.5 Audit log backup procedures

Audit logs backups are copied to an off-line medium, which is stored at a dislocated room with physically restricted access.

4.5.6 Audit collection system (internal vs external)

The audit log collection system is internal to SiGNET CA.

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 event recorded

The following events are recorded and archived:

1. Certification requests;
2. Approved Certification requests;
3. Issued certificates;
4. Requests for revocation;
5. Issued CRLs;
6. System logs for startups and shutdowns of the CA equipment;
7. System logs for interactive system logins at the CA equipment.
8. All e-mail messages received by SiGNET CA;
9. All e-mail messages sent by SiGNET CA.

4.6.2 Retention period for archive

Logs will be kept for a minimum of 3 years.

4.6.3 Protection of archive

Only authorised CA personnel and authorised external auditors are allowed to view and process audit logs. Audit logs are copied to an off-line medium.

4.6.4 Archive backup procedures

Audit log backups are copied to an off-line medium, which is stored at a dislocated room with physically restricted access.

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 SiGNET CA.

4.6.7 Procedures to obtain and verify archive information

No stipulation.

4.7 Key Changeover

The private signing key for SiGNET CA is changed periodically. To avoid interruption of validity of subordinate keys the new SiGNET CA private key should be generated one year before the expiration of the old key. From that point on new certificates are signed by the newly generated signing key. The new SiGNET CA public key is posted in the on-line repository.

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. If the private key is destroyed the case will be treated as in *section 4.8.3*.

4.8.2 Entity public key is revoked

Same procedure as in *section 4.8.3*.

4.8.3 Entity key is compromised

If the CA's private key is destroyed, lost, compromised or suspected to be compromised, the CA will:

- Make all reasonable efforts to notify subscribers, RAs and cross-certifying CAs of which the CA is aware;
- Terminate the certificates and CRL 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;
- Notify relevant security contacts at IJS.

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

If an RA's private key is compromised or suspected to be compromised, the RA will inform the CA and request the 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.

4.8.4 Secure facility after a natural or other type of disaster

In the case of a disaster whereby the CA installation is physically damaged and all copies of the CA signature key are destroyed as a result, SiGNET CA will take whatever action it deems appropriate.

4.9 CA Termination

Before SiGNET CA terminates its services, SiGNET CA shall:

- Make all reasonable efforts to inform subscribers, RAs and cross-certifying CAs;
- Make knowledge of its termination widely available;
- Cease issuing certificates and CRLs;
- Destroy all copies of private keys.
- Notify relevant security contacts at IJS.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1 Physical Controls

5.1.1 Site location and construction

SiGNET CA operates in the computer centre of the F9 department at IJS, building C. The access to the building and the computer centre room is controlled.

5.1.2 Physical access

The private keys of the SiGNET CA are only available in encrypted format on media in a secure location. Physical access to the hardware is restricted to personnel authorised to operate SiGNET CA.

5.1.3 Power and air conditioning

The computer centre room is environmentally controlled, has suitable air conditioning system and the repository machines are connected to an UPS system and any available building backup power.

5.1.4 Water exposures

No stipulation.

5.1.5 Fire prevention and protection

No stipulation.

5.1.6 Media storage

SiGNET CA key and back-up copies of SiGNET CA related data are kept on several removable storage media in a secure location. Backups are kept in an off-site secure location.

5.1.7 Waste disposal

Waste carrying potential confidential information, such as old media and storage devices, are physically destroyed before being trashed.

5.1.8 Off-site backup

Off-site backup is stored at a dislocated room with physically restricted access.

5.2 Procedural Controls

5.2.1 Trusted roles

No stipulation.

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

5.3.1 Background, qualifications, experience, and clearance requirements

SiGNET CA personnel must be staff members of the F9 IJS, Experimental Particle Physics Department of the "Jozef Stefan" Institute in Ljubljana, Slovenia.

SiGNET CA personnel must pass F9 IJS computer room clearance.

SiGNET CA personnel must be appointed by the manager of F9 IJS who can revoke the appointment at his/hers discretion any time without any notice.

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 unauthorised actions

No stipulation.

5.3.7 Contracting personnel requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

6 TECHNICAL SECURITY CONTROLS

6.1 Key Pair Generation and Installation

6.1.1 Key pair generation

Each subscriber must generate his/her own key pair. SiGNET CA does not generate private keys for subjects. The private key should not be known by other than the authorised user of the key pair.

Applicants are recommended to use tools available from SiGNET CA public web server to create their key 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 *section 6.1.5*.

Key pairs for the SiGNET CA are generated exclusively by SiGNET CA staff members on a dedicated, disconnected system, using a recent, trustworthy version of required operating system software and software package.

6.1.2 Private key delivery to entity

Each applicant must generate their own key pair.

6.1.3 Public key delivery to certificate issuer

Applicants public keys are delivered to the issuing CA by the HTTP protocol via the CA's public web interface.

Alternatively, applicants public keys are delivered to the RA or directly to SiGNET CA in in PEM-format in an email containing the certificate request. The RA must send the public key to SiGNET CA in an email signed by the RA.

6.1.4 CA public key delivery to users

SiGNET CA certificate and public key can be downloaded from SiGNET CA public repository at the following URL: `http://signet.ijs.si/pub/`.

6.1.5 Key sizes

- The minimum key length for a personnel, server or service certificate is 1024 bits;
- The CA key minimum 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 (as per X.509 v3 key usage field)

Keys may be used for authentication, non-repudiation, data enchipherment, message integrity and session key establishment. The SiGNET CA private key is the only key that can be used for signing SiGNET certificates and CRLs.

For the certificates issued by SiGNET CA under this policy, `keyUsage` field must be used in accordance with RFC 2459. The `keyUsage` extension is defined in *subsection 7.1.2*.

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

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

6.2.4 Private key backup

SiGNET CA private key is kept encrypted in multiple copies on removable devices media in safe places, including off-site storage. The passphrase is in a sealed envelope kept in a safe.

6.2.5 Private key archival

See *section 6.2.4*.

6.2.6 Private key entry into cryptographic module

No stipulation.

6.2.7 Method of activating private key

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

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 (including those specified in *section 6.2.4*) 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

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

6.4 Activation Data

6.4.1 Activation data generation and installation

SiGNET CA private key is protected by a passphrase with a minimum length of 15 characters. All passphrases used by the SiGENT CA have a length of at least 15 characters, consist of both letters, numbers and signs and does not contain consecutive or repetitive keystrokes.

6.4.2 Activation data protection

A copy of the passphrase is kept in a safe. The passphrase is known to current staff members of SiGNET CA on a need to know basis. Change of staff will imply a change in the passphrases.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer Security Controls

6.5.1 Specific computer security technical requirements

- The operating systems of CA/RA computers are maintained at a high level of security by applying all the relevant patches;
- CA systems configuration is reduced to the bare minimum;
- The machine used for signing certificates is not connected to any network and is kept powered off when not in use;
- The machines used to hold online repositories and run web site interfaces is protected by a suitable firewall;
- Unauthorised physical access is prohibited.

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

- The CA signing machine is not connected to any kind of network;
- 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 PROFILES

7.1 Certificate Profile

7.1.1 Version number(s)

X.509 v3 (0x2).

All certificates that reference this CPS will include a reference to the AIN.1 O.I.D. of this document as per *section 1.2* within the appropriate field.

7.1.2 Certificate extensions

The following extensions are set in user certificates:

- X509v3 Basic Constraints: CRITICAL CA:FALSE
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier
- X509v3 Key Usage: CRITICAL Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
- X509v3 CRL Distribution Points
- X509v3 Issuer Alternative Name
- X509v3 Certificate Policies
- Netscape Cert Type: SSL Client, S/MIME
- Netscape Base URL

The following extensions are set in host certificates:

- X509v3 Basic Constraints: CRITICAL, CA:FALSE
- X509v3 Subject Key Identifier
- X509v3 Authority Key Identifier
- X509v3 Key Usage: CRITICAL Digital Signature, Non Repudiation, Key Encipherment, Data Encipherment, Key Agreement
- X509v3 CRL Distribution Points
- X509v3 Issuer Alternative Name
- X509v3 Certificate Policies
- Netscape Cert Type: SSL Server, SSL Client, S/MIME
- Netscape Base URL

The following extensions are set in the SiGNET CA self-signed certificate:

- X509v3 Basic Constraints: CRITICAL CA:TRUE

- X509v3 Subject Key Identifier:
- X509v3 Authority Key Identifier:
- X509v3 Key Usage: CRITICAL Certificate Sign, CRL Sign
- X509v3 CRL Distribution Points
- X509v3 Issuer Alternative Name
- X509v3 Subject Alternative Name
- Netscape Cert Type: SSL CA, S/MIME CA
- Netscape Base URL

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

See *section 3.1.1*.

7.1.5 Name constraints

`countryName`	must be `SI`.
`organisationName`	must be `SiGNET`.
`organisationName(2)`	If set, must be the Slovenian scientific or educational organisation involved in SiGNET activities. Current list of values available for `organisationalUnitName` can be obtained at the location specified in *section 1.3.2*.
`commonName`	must be name and surname or FQDN of the subject.

See also sections *3.1.2*, *3.1.3* and *3.1.4*.

7.1.6 Certificate policy Object Identifier

SiGNET Grid CA identifies this policy with the object identifier (OID) as specified in *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)

X.509 v1 (0x0).

Version 1 is required for compatibility with Netscape Communicator.

7.2.2 CRL and CRL entry extensions

No stipulation.

8 SPECIFICATION ADMINISTRATION

8.1 Specification change procedures

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

8.2 Publication and notification policies

This document and any older versions are available from the on-line repository given in *section 2.1.5*.

8.3 CPS approval procedures

No stipulation.

9 Appendix A.

9.1 Registration Authority Agreement

```
This forms part of the operating procedures of the SiGNET Certification
Authority (CA).

1. In acting as a Registration Authority (RA) for SiGNET CA I have
read and understood and accepted the responsibilities and tasks
assigned to an RA laid out in SiGNET CA Certification Policy and
Practice Statement (CP/CPS) document available on SiGNET CA web site -
http://signet-ca.ijs.si/.

2. I understand that SiGNET CA will notify me by email of changes to
CP/CPS and I will immediately notify SiGNET CA if I am no longer willing
to act as an RA under any new CP/CPS.

3. I understand that failure to fulfill my responsibilities and tasks
under this agreement may result in the termination of my appointment
as an RA.

4. In the event of resignation, I will inform the SiGNET CA at least
90 days prior to my resignation.

Signed by  ..................................... on ..............



Email:     ....................................



Signature:                                        ......................
```

10 Appendix B.

10.1 Bibliography

- 7.S. Bradner, Key words for use in RFCs to Indicate Requirement Levels, RFC 2119, March 1997 - `http://www.ietf.org/rfc/rfc2119.txt`
- CA Certificate Revocation List. `http://ca.grid-support.ac.uk/cgi-bin/importCRL`.
- CA web site. `http://ca.grid-support.ac.uk/`.

- R. Cecchini. INFN CA CP/CPS. http://security.fi.infn.it/CA-CPS/CPS-1.0.pdf, December 2001. Version 1.0.
- CERN Administrative Procedures manual - http://as.cern.ch/AdminMan/.
- CERN CA Security Group http://service-grid-ca.web.cern.ch/service-grid-ca - Email: **service-grid-ca@cern.ch**.
- CERN Certificate Policy and Certificate Practice Statement v2.2 - http://service-grid-ca.web.cern.ch/service-grid-ca/cp_cps/cp_cps.html.
- CERN IT Division Grid Deployment Group - http://it-div-gd.web.cern.ch/it-div-gd/.
- S. Chokani and W. Ford, Internet X.509 Infrastructure Certificate Policy and Certification Practices Framework, RFC 2527, March 1999 - http://www.ietf.org/rfc/rfc2527.txt.
- The European DataGrid Project http://eu-datagrid.web.cern.ch.
- EuroPKI Certificate Policy. http://www.europki.org/ca/root/cps/en_index.html, October 2000. Version 1.1.
- Tony Genovese. DOE Science Grid CA CP/CPS. http://www.doegrids.org/Docs/CP-CPS.pdf, December 2001. Version 1.1.
- Global Grid Forum Certificate Policy Model, version 7, October 2002 - http://caops.es.net.
- Grid-Ireland CA Certificate Policy and Certificate Practice Statement v0.4 - https://www.cs.tcd.ie/grid-ireland/gi-ca/gi-ca0v4.pdf.
- R. Housley, W. Ford, W. Polk, and D. Solo. Internet X.509 Public Key Infrastructure Certificate and CRL Profile. AKA RFC 2459. http://www.rfc-editor.org/rfc/rfc2459.txt, January 1999.
- IUCC CA Certificate Policy and Certificate Practice Statement v1.5 - http://certificate.iucc.ac.il/ca/.
- National Computational Science Alliance Certificate Policy. http://archive.ncsa.uiuc.edu/SCD/Alliance/GridSecurity/Certificates/AllianceCP9.1.html, June 1999.
- Nystrom & Kaliski, Certification Request Syntax Specification, RFC 2986, November 2000 - http://www.ietf.org/rfc/rfc2986.txt.
- The OpenSSL Project - http://www.openssl.org/.
- PK-GRID-CA Certificate Policy and Certificate Practice Statement v1.1.1.3 - http://www.ncp.edu.pk/pk-grid-ca.
- Polish Grid CA Certificate Policy and Certificate Practice Statement v0.4 - http://www.man.poznan.pl/plgrid-ca/ca-policy.html.
- Port numbers. http://www.iana.org/assignments/port-numbers.
- TrustID Certificate Policy. http://www.digsigtrust.com/certificates/policy/tsindex.html.
- UK Grid Support Centre. http://www.grid-support.ac.uk/.
- X.509 Certificate Policy For The Federal Bridge Certification Authority. Available from http://www.cio.gov/fbca/lib/index.htm, December 1999. Version 1.0.

11 Appendix C.

11.1 Changelog

1.0 (public document) 25-Sept-2004

- ASN OID Changed.
- Minor typos corrected.

0.3 (public draft implementing `dg-eur-ca` list comments) - 18-Sept-2004

- 1.3.3 - Last statement changed: certificates are not issued directly to organisations and organisations are not end entities, as per 3.1.8.
- 3.1.1 - Deleted reference to empty section 7.1.4.
- 3.1.9 - Addition: CA will keep copies of documents used for identification. Clarification: it is not possible to use telephone conversation for identification, but it is used for confirmation when a user identifies by the possession of a secret key for an existing certificate.
- 4.1. item 5 - Added reference to section 3.1 where forms of names are defined.
- 2.1.2 item 6 - Reformulated to not force RA to check the safeguarding of subscriber's private keys, but merely assure they are informed about their obligations.
- 2.1.5 item 1 - Reformulated.
- 2.4.3 - Replaced unclear name dispute resolution policy with "according to best current practice".
- 3.1.1 - Deleted reference to emtpy section 7.1.4.
- 3.1.1 - Reference to name changes for persons is now clearer.
- 3.1.8 - Requirement for both generic host/service e-mail and personal e-mail in host and service certificate request added.
- 3.1.9 - Addition: CA will keep copies of documents used for identification. Clarification: it is not possible to use telephone converstation for identification, but it is used for confimation when a user identifies by the possession of a secret key for an existing certificate.
- 4.1. item 5 - Added reference to section 3.1 where forms of names are defined.
- The SiGNET CA contact email changed to **signet-ca@ijs.si**.
- A number of typos and grammatical errors.

0.2 (first public draft) - 30-April-2004 Name changes and internal revisions.

A number of changes based on the IUCC Certification Authority CA/CPS document and others.

0.1 (internal draft)- April-2004 Initial revision.

Contents