NIIF Certification Authority

Grid Server Certificate Policy (Grid Server CP)

Version 1.4

Document OID: 1.3.6.1.4.1.11914.1.1.3.1.4

January 30, 2009

Contents

1 INTRODUCTION

1.1. Overview

The Hungarian National Information Infrastructure (NIIF) Program serves as a framework for the development and operation of the research network and related services in Hungary for the Hungarian Academic Community. This document is the NIIF Grid Server Certificate Policy of the NIIF Certification Authority and describes the practice employed by NIIF CA in issuing digital certificates for users regarding to specific grid project requirements.

This CP may be used by relying parties to determine the level of trust associated with this policy. The issued X.509 Version 3 certificates should contain a reference to this certificate policy.

More detailed information about the practices what the NIIF CA employs in its operations in issuing certificates can be found in the NIIF Certification Authority Certification Practice Statements (CPS).

1.1.1 Revisions

This CP undergoes a regular review process as prescribed by the NIIF internal policies. Revisions of this document are identified through a configuration baseline schema and numbering convention.

1.1.2 Standards

The structure of this document is based on RFC 2527 and on RFC 3280. This CP differs from the RFC 2527 standard only to the degree necessary to adequately describe the operational practices used within the NIIF CA.

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.

1.1.3 Glossary

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

NIIF Institute
National Information Infrastructure Development (NIIF) Institute having its seat in Budapest, Hungary [www.niif.hu].

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.

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. In the context of a particular certificate, the issuing CA is the CA that issued the certificate.

Certificate Policy (CP)
A named set of rules, that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.

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

certificates.

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.

Registration Authority (RA)

An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e. an RA is delegated certain tasks on behalf of a CA). In this document the term “team leader” is synonymous with RA.

Relying party

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

In this CP relying party is the specific grid project.

End Entity

A person who requests a certificate for a device from the NIIF CA.

Specific grid project

Each project which is registered by NIIF as a grid project. The currently registered projects are listed on NIIF CA web site.

For the registration of a specific project the following data is required to be provided:

- Project name
- Project Manager name and contact details
- Project home page
- Institute which coordinates the project
- Project timeframe

Authorized Project Leader

Those projects, which have a necessary number of Hungarian project members, might have a project responsible authorized by NIIF to simplify the Certification registration procedure.

The project leader signs an agreement with NIIF, which covers the roles and responsibilities for the Certificate request registration process.

The Authorized Project Leader is liable for the decision, that the subscriber has the right to request certificate from NIIF or not.

Online Certificate Status Protocol (OCSP)

An Internet protocol used for obtaining the revocation status of an X.509 digital certificate. It is described in RFC 2560 and is on the Internet standards track.

1.2. Identification

This certificate policy is identified by the following unique registered Object Identifier (OID):

IANA	1.3.6.1.4.1
NIIF	.11914
Services	.1
Policies	.1

Grid Server CP	.3
Major Version	.1
Minor Version	.4

1.3. Community and Applicability

Certificates issued under this CP are issued to devices used in a specific grid project.

1.3.1 Certification authorities

The NIIF CA has the permission to operate as a Root Certification Authority for grid-related activities in Hungary.

1.3.2 Registration authorities

The NIIF Institute and its RA Partner Institutes manage the functions of the Registration Authority regarding to grid projects. RA is needed for physical identification/authentication of entities. RA must not issue certificates under this CP.

1.3.3 End entities

Only a predetermined subset of the employees and students of the whole Hungarian Academic Community and those of any contracted organizations cooperating with these entities in the practice of research, educational and administrative functions as well as computers and application services operated by these organizations.
In accordance with this CP, devices that are subjects of the issued certificates may be any device whose authorization is predetermined and which can be uniquely identified with the association of the End Entities.

1.3.4 Applicability

Certificates issued by the NIIF CA must not be used for financial transactions, any business, including e-business related activity or activities covered by Hungarian laws (e.g. contract signing).

1.4. Contact Details

1.4.1 Specification administration organization

The CP is maintained by NIIF Institute [www.niif.hu].

1.4.2 Contact person

Tamás Máray
NIIF Institute
Victor Hugo u. 18-22
H-1132 Budapest
Hungary

Phone: +36 (1) 450-3070
Facsimile: +36 (1) 350-6750
email: ca@niif.hu
URI: www.niif.hu

1.4.3 Person determining CPS suitability for the policy

The organization responsible for the policies across the member countries is the EU Grid PMA, which determines CPS suitability for the policy and for the EU Grid PMA minimum CA requirements.

2 GENERAL PROVISIONS

2.1. Obligations

2.1.1 CA obligations

The NIIF CA is solely responsible for the issuance and management of certificates referencing this document. The NIIF CA must:

- publish a CPS describing the practices employed in issuing the certificates, and ensure that the CPS is conform with this CP;
- operate according to the CPS, this CP and the Hungarian laws;
- verify that any CA with which it cross-certifies itself complies with the EUGridPMA CP requirements.

The NIIF CA is obliged to

- make reasonable efforts to ensure they conduct an efficient and trustworthy operation. “Reasonable efforts” includes but does not limit the CA to operating in compliance with:
  - this CP;
  - a contractual agreement;
  - documented internal operational procedures;
  - the CPS;
  - within applicable law;
- handle certificate requests and issue new certificates, including:
  - accepting certification requests from NIIF partner organization’s End Entities requesting a certificate according to the procedures described in the CPS and in this CP;
  - authenticating entities requesting a certificate, where applicable with the assistance of the designated RAs;
  - issuing certificates based on requests from authenticated End Entities;
  - the sending of notification of issued certificates to requesting entities;
  - making issued certificates publicly available;
- handle certificate revocation requests and certificate revocation, including:
  - accepting revocation requests from entities requesting that a certificate be revoked according to the procedures described in the CPS and this CP;
  - authenticating entities requesting revocation of a certificate;
  - issuing certificate revocation list and make CRL publicly available;
  - operating OCSP responder.

2.1.2 RA obligations

RA must operate in accordance with this CP and the law of the Hungary and is obliged to

- verify with the project manager in the pre-authorization phase that the subscriber is authorised to access grid project services, and ensure that only authorised subscribers are able to create certification requests. If the subscriber has no right to use grid project services, the RA must close the procedure;
- authenticate the identity of the subject to be certified using procedures specified in section 3.1;
- validate the connection between a public key and the requester identity with the unique Request Password including a suitable proof of possession method of the corresponding private key;
- confirm such validation to the CA;

- keep supporting evidence for any certificate request made to a CA in accordance with this CP;
- protect its private key in accordance with this CP;
- advise End Entities of their obligations under this CP, the CPS and the appropriate subscriber agreement and relying party agreement, and providing End Entities with copies of this CP or advising them how these documents may be accessed;
- revoke certificates in terms of section 4.6.1;
- maintain a list of compromised keys. The compromised list is to include relevant information regarding the identity of the individual(s) concerned, reasons and causes for inclusion on the list and such other information as might be required to minimize damage or liability to all NIIF CA End Entities. This information is to be protected in accordance with the Hungarian Data Protection Act.

The private key used by a RA for signing certificate signing requests (CSRs), certificate suspensions, and certificate revocations as part of its RA function must not be used for any other purpose. Separate certificates will be issued to facilitate routine secure communication between RA and CA.

2.1.3 Authorized Project Leader obligation

The Authorized Project Leader must operate in accordance with this CP, and must ensure during the pre-authorization phase that the requester has an employment or contractual relationship with one of the NIIF member Organizations.

The Authorized Project Leader must provide a statement to RA, which explicitly states, the subscriber has permission to request certificate or not.

The Authorized Project Leader has the permission

- to suggest changes on this CP;
- to initiate the revocation of certificate issued under this CP.

2.1.4 Subscriber obligations

To request a certificate, the subscriber must:

- initiate the authorization request;
- understand and, if necessary, receive proper education in the use of Public-Key cryptography and certificates;
- accept conditions and adhere to the procedures described in this document;
- voluntarily provide true and accurate information, and only such information as he/she is entitled to submit for, required in the certification request and accept the data protection rules of the CP;
- use the certificate exclusively for authorized and legal purposes, consistent with this document;
- generate a key pair using a trustworthy method;
- take reasonable precautions to prevent any loss, disclosure, modification or unauthorized use of the private key associated with the certificate in accordance with the CPS and this CP. 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, i.e. every usage of their private key is assumed to be the act of its owner;
- notify the CA immediately by sending a certificate revocation request in case of suspicion that their private keys are compromised;
- notify the CA immediately by sending a certificate revocation request in case of change in the content of their certificates;
- accept the restrictions to liability described in section 2.2

By following the authentication procedures described in this document, the subscriber accepts the statements relating to confidentiality of information in section 2.8.

2.1.5 Relying party obligations

In using a certificate issued by the NIIF CA under this CP, relying parties must:

- be familiar with the CPS and this CP before drawing any conclusion on how much trust he can put in the use of a certificate issued from the CA;
- accept conditions and adhere to the procedures described in the CPS and this CP;
- verify the certificate revocation information when validating a certificate;
- use the certificates only for the permitted purposes as defined in the CPS and this CP and must not use for purposes explicitly not defined in the relevant documents.

2.1.6 Repository obligations

The NIIF CA shall maintain an online, publicly accessible repository of certificates and certificate revocation information. The repository shall be available as much as practically possible.

2.2. Liability

2.2.1 CA liability

The NIIF CA must define the liability accepted. The complete list of accepted liabilities are specified in the CPS.

2.2.2 RA liability

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

2.3. Financial Responsibility

The NIIF CA accepts responsibility as specified in the CPS.

2.3.1 Indemnification by relying parties

The NIIF CA accepts responsibility as specified in the CPS.

2.3.2 Fiduciary relationships

No stipulation.

2.3.3 Administrative processes

Not stipulation.

2.4. Interpretation and Enforcement

2.4.1 Governing law

In so far as any of the conditions stipulated in this document are ambiguous or unclear, exclusive reference shall be had to the Act No XXXV of 2001 on THE USE OF CERTIFICATES and related Hungarian laws.

2.4.1.1 Applicable contract structure

The contractual structure that underpins the policies and practices described in this document includes the:

- Authorized Project Leader Agreement, which establishes a relationship between NIIF and the specific grid project leader.
- End Entity Subscriber Agreement, which establishes an arrangement relationship between RA's and End Entities for the provision of services by the RA and between an End Entity and other End Entities.

2.4.2 Severability, survival, merger, notice

The conditions must be clearly defined in NIIF CA CPS.

2.4.3 Dispute resolution procedures

In case a dispute is not successfully resolved by negotiations between End Entity and Authorized Project Leader, then it is the NIIF RA's or NIIF CA's responsibility to clarify the situation and make a decision.

2.5. Fees

2.5.1 Certificate issuance or renewal fees

The issuing of certificates is free of charge.

2.5.2 Certificate access fees

Access to certificates on the NIIF CA certificate Registry is free of charge.

2.5.3 Revocation or status information access fees

Access to certificate Revocation Lists on the NIIF CA certificate repository is free of charge.

2.5.4 Fees for other services such as policy information

Policy and CPS information access is free of charge.

2.5.5 Refund policy

Not applicable.

2.6. Publication and Repository

2.6.1 Publication of CA information

In its repositories, the NIIF CA makes publicly available:

- The NIIF CA's certificate for its signing key;
- The current and all previous versions of the NIIF CA Certificate Practice Statement;
- The current and all previous versions of this CP and related user guide explaining how End Entities should request and handle certificates;
- All issued certificates;
- Signed certificate Revocation Lists.

2.6.2 Frequency of publication

Certificates are published promptly following their issue.
The frequency of CRL publication is specified in section 4.6.9.
New versions of CPS are published according to section 8.

2.6.3 Access controls

The CPS, the CP, CRL, OCSP functionality and issued certificates are publicly available for reading without access control.
Appropriate access controls are implemented to restrict to authorized personnel only the ability to write or modify these items.

2.6.4 Repositories

The NIIF CA maintains a public repository which contains all the information referred in section 2.6.1. The availability of all this information is described in the NIIF CA CPS. The English versions of all documents are the official references.

2.7. Compliance Audit

No external audit will be required, only a self-assessment by the NIIF CA that its operation is according to this document. Each RA partner must accept being audited by the NIIF CA Auditor to verify its compliance with the rules and procedures specified in its CP/CPS document.
The NIIF Auditor performs operational audits of the CA and RA staff at least once per year.

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

2.8.1 Types of information to be kept confidential

All subscribers' information that is not present in the certificate and CRL issued by the NIIF CA is considered confidential and shall not be disclosed to any third party without explicit written permission of the subscriber.

The RA is authorized to collect personal data (e.g. full name, organization, address, and e-mail address), provided voluntary by subscribers, that is necessary to perform its services, but this operation must conform with Hungarian Act No LXIII of 1992 on PROTECTION OF PERSONAL DATA AND DISCLOSURE OF DATA OF PUBLIC INTEREST and these activities must be registered in the Hungarian Data Protection Register maintained by Parliamentary Commissioner for Data Protection and Freedom of Information Hungary.

Both the full name and the email address are included in the issued certificate. NIIF RA must ensure that the collected personal data can only be used in the context of the certification services provision, and must keep it up to 5 years according to the Hungarian laws. The subscriber has the right to access and request correction of these data.

The NIIF CA may have other confidential documentation, but these documents must be listed in the NIIF CA CPS.

2.8.2 Types of information not considered confidential

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

2.8.3 Disclosure of certificate revocation/suspension information

When a certificate is revoked/suspended, the reason code must be shared with all other users and relying parties, this code is not considered confidential. However, no other information regarding to the revocation are normally disclosed.

2.8.4 Release to law enforcement officials

The NIIF CA will not disclose confidential information to law enforcement agencies or officials except

- a properly constituted warrant is produced or the information is otherwise legally, according to Hungarian laws, required to be disclosed; and
- the law enforcement official is properly identified.

2.8.5 Disclosure upon owner's request

The subscriber shall have full access to its personal data, and shall be empowered to authorize release of that record to another party. The subscriber will not have access to any other subscriber’s registration record unless proper authorisation is given by the relevant person.
Formal authorization may take two forms:

- a properly constituted electronic request providing that the request is digitally signed by a valid digital signature under a recognized CP; or
- by application in writing.

No release of information is permitted without a formal authorization in accordance with this CP.

2.8.6 Other information release circumstances

Not applicable.

2.9. Intellectual Property Rights

The use of RFC 2527 and RFC 3280 for drafting this CP and the CPS is acknowledged.
The NIIF CA must not claim intellectual property rights on issued certificates or this CP.

3 IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1 Types of names

The NIIF CA assigns each End Entity Device a distinguished name that is in compliance with the X.500 standard and serves as a unique identifier of the End Entity Device. The DN must be constructed using the following naming convention:

- country, which is “HU”;
- organizationName, which is “NIIF CA”;
- organizationUnitName, which is “GRID”;
- organizationName, which is the official name or one of the official abbreviations of the institution the subscriber is affiliated with;

commonName, which is the fully qualified domain name (FQDN) of the device.

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.

3.1.3 Rules for interpreting various name forms

See section 3.1.1.

3.1.4 Uniqueness of names

Distinguished names must be unambiguous and unique, so certificates must apply to unique individuals or resources. Individuals must not share certificates. The fulfillment of these requirements are checked by the RA or, in case of doubt, by the NIIF CA.

3.1.5 Name claim dispute resolution procedure

No stipulation.

3.1.6 Recognition, authentication and role of trademarks

No stipulation.

3.1.7 Method to prove possession of private key

The RA must ascertain that the Private Key in the possession of the subscriber does in fact correspond to the Public Key in the possession of the subscriber. According to the method the subscriber generates its own key pair and submits the public key, and the information required by the forms on the End Entity interface will be signed by his private key. The RA must validate the Request password provided by the subscriber via the RA EndEntity interface.
This methodology is accomplished by the technology provided by NIIF CA End Entity interface.

3.1.8 Authentication of organization identity

If the subscriber requires the inclusion of the name of a certain organization in a certificate, the RA must have evidence that the organization has full knowledge about this fact. In order to obtain this result the RA must require written legally binding documents.

3.1.9 Authentication of individual identity

The RA personally authenticates any subscriber asking a certificate, using officially recognized identity personal photo-id card. The detailed procedure is defined in the NIIF CA CPS.

3.2. Routine Renewal

After certificate expiration, the CA will not issue a new certificate for the same key. The CA may issue a new certificate for a new key. Renewal of certificates will follow the same procedure as an initial registration.
In case of renewal subscriber must create a new key pair using the same procedure as described in section 3.1, but the personal authentication of individual entity is not required.
In case where the certificate to be reissued contains the name of a certain organization, new legal documents as indicated in Section 3.1.8 must be presented before renewal.

3.3. Routine Rekey and Rekey After Revocation

A public key whose certificate has been revoked will not be re-certified, routine rekey is not supported.

3.4. Revocation Request

A request to revoke keys and certificates, if initiated by an authorized party and signed by a valid key and certificate under this CP, regardless of the document version, shall constitute a valid and enforceable revocation request. Revocation request

- may be made in writing in the form described at 4.6.3;
- may be initiated by using the pass phrase subscriber had chosen during initial registration;

4 OPERATIONAL REQUIREMENTS

4.1. Pre-authorization

A requester must indicate to the RA that he/she would be request a device certificate to a specific grid project.
Two different pre-authorization procedures are defined, the requester may follow any of the following by his/her own decision:

- without Authorized Project Leader approval
- with Authorized Project Leader approval.

4.1.1 Pre-Authorization without Authorized Project Leader Control

If the subscriber does not wish to provide an approval from the Authorized Project Leader, or there is no authorized project leader assigned to the specific grid project, then the initial pre-authorization request must contain

- subscriber's name;
- the name of the specific grid project;
- if the specific grid project is not listed among the specific grid projects, then the requester must provide some details on the project registration request form;
- legal statement about the employment status or contractual relationship with the NIIF member organization;
- a document about the requested device's domain name are under the control of his/her organization;
- if the domain name controlled by others, then a legally binding statement about that the organization is allowed to use the domain name in the following one year at least;
- subscriber's email address.

Based on the provided information the RA has the right to authorize the subscriber to access the NIIF CA End Entity interface, which requires an account/password authentication for certificate request submittal.

4.1.2 Pre-Authorization with Authorized Project Leader Control

The Authorized Project Leader controlled initial pre-authorization request must contain

- subscriber's name;
- the name of the project;
- the name of the Authorized Project Leader;
- name of the organization subscriber works for;
- a document about the requested device's domain name are under the control of his/her organization;
- if the domain name controlled by others, then a legally binding statement about that the organization is allowed to use the domain name in the following minimum of one year;
- subscriber's email address.

RA sends the request for validation to the Authorized Project Leader. After the receipt of the Authorized Project Leader’s written approval the RA has the right to authorize the subscriber to access the NIIF CA End Entity interface, which requires an account/password authentication.
The RA has the responsibility to notify the subscriber how he/she can send his/her certification request to RA. This notification must contain the date of the authentication process of the individual entity.

4.1.3 Pre-Authorization Request form

A certificate preprocessing request, whether in paper or electronic (e.g. e-mail) form, is to contain the information illustrated in the example form below:

Certification Request Date : ....

To: **NIIF CA RA**
Victor Hugo u. 18-22., H-1132, Budapest, HUNGARY

Section 1 – Requestor's details
Requestor's name: ....
E-Mail Address: ....
Phone Number: ....
Organisation (O): ....
Department (OU): ....
Common Name (CN)*: ....
* For personal certificates: given name + family name (without accented letters)
For server/device certificates: fully qualified domain name

Type of requested certificate:
□ - Grid □ - HBONE □ - General purpose

Requested certificate is an (check only one):
□ - End User Certificate □ - Server/Device Certificate

Section 2 – Reason for request:
....
....
....
....

Section 3 – Attached documents:
□ Copy of the Photo – ID
□ Statement about the employment status at the organisation. (For general purpose certificates)
□ Statement about the domain name ownership (For server certificates)
□ Statement about the domain name usability (For server certificate)
□ NIIF Partners' IdP Privacy Statement Form (For users without an HREF Home Organisation)
□ Other: ....

I know and accept all the rules and obligations described in the NIIF CA CP/CPS documents under which authority the requested certificate is going to be issued.

4.2. Certificate Application

It is the responsibility of the subscriber to submit the request through the NIIF CA End Entity interface. Additionally, the subscriber's responsibility is to generate the key pair and to submit the public key, and the information required by the forms on the End Entity interface. The requester's public key must be signed by his/her private key.

The subscriber is obliged to choose a pass phrase during the certificate application process, which allows of the initiation of certificate suspension and revocation. It is the subscriber's interest to protect the pass phrase. Without the pass phrase it is not possible to initiate certificate suspension or revocation on the End Entity interface of the NIIF CA.

The subscriber is also obliged to choose a Registration Password during the certificate application process, to be able to identify itself as the initiator of the request to the RA.

4.3. Certificate Issuance

In order to issue a certificate, the following general process must be implemented in each case:

- RA verifies whether the subscriber qualifies/pre-authorized for the certificate;
- RA verifies the identity of the subscriber as indicated in Section 3.1
- RA validates the proof of possession of private key using procedures indicated in Section 3.1.7;
- RA sends the digitally signed certificate request to the CA;
- On receipt of a certificate request, the CA will verify the RA's signature and issue a certificate;
- The subscriber is notified via email to the address included in the certificate request form or to the address registered by the RA, the sender address is ca@niif.hu;
- The subscriber
  - downloads the certificate(s) from the site given in the notification;
  - installs a recognised subscriber application on their PC;
  - accesses its keys and certificate(s) in a secure format;
  - installs the received certificate(s).

4.3.1 Relying parties

Relying parties need to access nominated certificates for the authentication of digital signatures and/or encryption of secured files. They may obtain the certificates what they require directly from the subscriber, or by retrieving the certificates from the NIIF CA certificate repository.

4.3.2 CA's right to reject certificate requests

Certificates are issued at the discretion of the NIIF CA receiving a certificate request. NIIF CA has the right to reject a certificate request according to NIIF CA CPS.

4.4. Certificate Acceptance

The certificate is assumed to be accepted by the subscriber, unless the subscriber explicitly rejects it via an authenticated communication with the RA.

By accepting a certificate, the subscriber:

- agrees to be bound by the continuing responsibilities, obligations and duties imposed on him/her by his/her Subscriber agreement, according to this CP and the CPS;
- warrants that according to his/her knowledge no unauthorized person has had access to the Private Key associated with the certificate;
- asserts that the certificate information he/she has supplied during the registration interview is truthful and has been accurately and fully published within the certificate.

4.5. Certificate Expiry

The time limit for the use of certificates is noted in the certificate.

4.6. Certificate Suspension and Revocation

4.6.1 Circumstances for revocation

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

- the subscriber's private key is lost, known to be or suspected to be compromised or misused;
- the information in the subscriber's certificate is suspected to be inaccurate;
- the subscriber no longer needs the certificate to access Relying Parties' resources;
- the subscriber has violated his/her obligations;
- the subscriber initiate a properly formatted certificate revocation;
- an subscriber generates the keys associated with a certificate and those keys are found to be weak;
- a validated request is received from an authorised third party, for example:
  - a court order;
  - a request made by a person with power of attorney;
- the certificate of the NIIF CA is compromised;
- NIIF CA in the future does not maintain its certificate services.

4.6.2 Who can request revocation

Certificate revocation can be initiated by:

- NIIF CA;
- the owner of the certificate;
- the project leader.

Subscribers may request revocation of their certificates for any reason, or for no reason, and must request revocation under the conditions specified in 4.6.1.

4.6.3 Procedure for revocation request

4.6.3.1 RA applied revocation

To process a revocation request initiated by a subscriber, the RA:

- receives and authenticates the request;
- ensures the certificate and Public Key are current;
- prioritizes the request according to the processing times indicated in this CP;
- if applicable:

  - adds the user's keys to its list of compromised keys;
- sends a digitally signed revocation request to the CA.

The RA verification requirements for revocation requests are the same as for certificate renewal, and because of these requirements such requests must be delivered to the RA either in the form of digitally signed file, printed document signed by the subscriber or in person.

4.6.3.2 End Entity applied revocation

The End Entity enters the pass phrase (chosen during the certificate application process) on the End Entity interface of the NIIF CA and initiates certificate revocation, in which case revocation is automatically carried out without the involvement of the RA.

The End Entity can issue a revocation request to the RA, if

- its certificate is valid and issue a request on the NIIF CA End Entity interface;
- it knows the one time password selected during the certificate application phase and authenticates itself with this pass phrase before trying to request revocation on NIIF CA End Entity interface;
- it sends a signed Certificate Revocation Request Form in letter to the RA;
- it faxes a signed Certificate Revocation Request Form to the RA, including the pass phrase selected during certification request procedure.

4.6.3.3 Certificate Revocation Request Form

A certificate revocation request, whether in paper or electronic (e.g. e-mail) form, must contain the following information:

Certificate Revocation/suspension Request Date : ____________________

To: < RA NAME>
< RA ADDRESS>

Section 1 – Certificate details (if known)
certificate
SUBJECT: ....
certificate serial
number: ....

Section 2 – Certificate owner details
Full
Name: ....
(For private individuals, show family name last.)
Organizational users only:
Organization: ....
Department: ....

Section 3 – requested operation*
The requested operation with the above described certificate (Check only one):
❑ - Revocation of the Certificate ❑ - Suspension of the Certificate
* This section is obligatory for certificate every request.

Section 4 – Reason for revocation ***
....
....
....
....
*** This section is optional for certificate owners requesting revocation of their own certificates.

Section 4 – Authorization
Authorized by: ❑ certificate owner
❑ Authorized third party
(Original documentation verifying authorization must be sighted.)
Signature: ....

4.6.3.4 Certificate owner duties

The owner of a revoked certificate is to:

- continue to safeguard the Private Key associated with the revoked certificate, until the date of certificate expiry; or
- securely destroy the Authentication Private Key associated with the revoked certificate.

4.6.4 Revocation request grace period

The NIIF CA responds within one day (excluding weekends and public holidays) to revocation requests. It shall however handle revocation requests with priority as soon as the request is recognized as such.

4.6.5 Circumstances for suspension

A certificate is suspended when the subscriber would like to suspend the use of the certificate for the following reasons:

- The service for which the certificate is used is suspended for unspecified time;
- Subscriber is not going to use the certificate for an amount of time.

4.6.6 Who can request suspension

The owner of the certificate can initiate certificate suspension. Subscribers may request suspension of their certificates for any reason, or for no reason, and must request suspension under the same conditions as described in section 4.6.5

4.6.7 Procedure for suspension request

The CA and RA follow the suspension procedure defined in the CPS. The procedure to be followed is the same as in case of revocation (see section 4.6.3.1).

4.6.7.1 Certificate Suspension Request

A certificate suspension request, whether in paper or electronic (e.g. e-mail) form, is to contain the information illustrated in section 4.6.3.3. Certificate owner duties
The owner of a suspended certificate is to:

- continue to safeguard the Private Key associated with the suspended certificate;
- request for resuming the certificate using the same procedure as described in certificate renewal (see section 3.2).

4.6.8 Limits on suspension period

No stipulation.

4.6.9 CRL issuance frequency (if applicable)

If a certificate revocation occurred, then the CA system immediately issues a new CRL. The CRL lifetime must be at least 8 days and must not be longer than 15 days. CRLs must be reissued at least 8 days before expiration, even if no additional revocations have been occurred.

4.6.10 CRL checking requirements

Before using of a certificate, a relying party

- must validate it against the most recently issued CRL;
- or it must validate it through an available OCSP responder.

If the preferred method is not available, then the other one must be used.
If the OCSP response contains “Status Unknown” value, then the certificate must be identified as a revoked one.

4.6.11 On-line revocation/status checking availability

The NIIF CA provides an on-line repository for verifying the status of certificates issued by the NIIF CA.

4.6.12 On-line revocation checking requirements

Refer to 4.6.10.

4.6.13 Other forms of revocation advertisements available

The subscriber will be notified of the revocation of his certificate by email.

4.6.14 Checking requirements for other forms of revocation advertisements

Not applicable.

4.6.15 Special requirements re key compromise

Not applicable.

4.7. Security Audit Procedures

NIIF CA documents security audit procedures applied in the CPS.

4.7.1 Types of event audited

The minimum audit records to be kept include all:

- types of registration records, including records relating to rejected applications;
- key generation requests, whether or not key generation was successful;
- certificate generation requests, whether or not certificate generation was successful;
- certificate issuance records;
- revocation records;
- CRL issuance.

4.7.2 Frequency of processing log

Audit logs are processed on a monthly and annual basis.

4.7.3 Retention period for audit log

Audit logs are retained as archive records.

4.7.4 Protection of audit log

Only authorized NIIF CA personnel is allowed to view and process audit log files.

4.7.5 Audit log backup procedures

The backup of the audit logs must be performed regularly on physical removable media.

4.7.6 Audit collection system (internal vs. external)

The audit collection system runs separately form the CA software in a secure environment.
The NIIF CA documents in the CPS the type of event audited.

4.7.7 Notification to event-causing subject

Operations personnel notifies either the CA or the RA when a process or action causes a critical security event or discrepancy.

4.7.8 Vulnerability assessments

A security risk assessment, including network security risk assessment is accomplished annually.

4.8. Records Archival

4.8.1 Types of event recorded

The NIIF CA maintains an archive of relevant records as follows:

- audit logs;
- certificate request information including certificate requests and related messages exchanged between the subscriber and the RA and CA;
- certificates, including CRLs generated;
- revocation requests and related messages exchanged with the requester and/or the subscriber;
- complete back up records;
- records on cross-certification;
- copies of e-mail logs;
- formal correspondence;
- Policy and Practice documentation.

The RA archives

- all validation information, legal documents collected from the subscriber;
- all relevant messages exchanged with the CA.

4.8.2 Retention period for archive

Digital signature certificates stored by the NIIF CA and issued CRLs shall be archived for at least five years after key expiration. Private signature keys should not be archived after key expiration. All other archive records shall be archived for at least 2 years.

4.8.3 Protection of archive

The NIIF CA has an archive procedure described in CPS.

4.8.4 Archive backup procedures

The NIIF CA has an archive backup procedure described in CPS.

4.8.5 Requirements for time-stamping of records

No stipulation.

4.8.6 Archive collection system (internal or external)

The NIIF CA must implement an archive backup system specified in CPS.

4.8.7 Procedures to obtain and verify archive information

No stipulation.

4.9. Key Changeover

No stipulation.

4.10. Compromise and Disaster Recovery

If the CA s private key is compromised or suspected to be compromised, the CA shall at least:

- notify users via NIIF CA home page (http://www.ca.niif.hu);
- notify Authorised Project Leaders if there is any;
- terminate the certificates and CRLs distribution service for certificates/CRLs issued using the compromised private key;
- revoke the CA certificate.

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

The NIIF CA has a written disaster recovery plan.

4.10.2 Entity public key is revoked

See section 3.2, 3.3 and 3.4, NIIF CA certificate procedure is defined in CPS.

4.10.3 Entity key is compromised

Whenever the subscriber's key, including RA's key, is compromised, the subscriber is obliged to notify NIIF CA as soon as possible. The revocation procedure will follow according to section 3.3 and section 3.4.
NIIF CA certificate procedure is defined in CPS.

4.10.4 Secure facility after a natural or other type of disaster

In case of a natural or other type of disaster the NIIF CA will start the recovery as soon as possible using off-site stored backups.

4.11. CA Termination

Termination of the NIIF CA services is described in the CPS in detail.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

Security requirements are indicated in the NIIF CA CPS. The CA system runs on a dedicated server which is physically secured.

5.1. Physical Controls

5.1.1 Site location and construction

No stipulation.

5.1.2 Physical access

Physical access control is required, which is conform to the recommendations of Hungarian Insurance Association (MABISZ recommendations - http://www.pluto.hu).

5.1.3 Power and air conditioning

No stipulation.

5.1.4 Water exposures

No stipulation

5.1.5 Fire prevention and protection

Fire prevention and protection system meet the requirements of Hungarian laws, no special stipulation

5.1.6 Media storage

All magnetic media containing NIIF CA information, including backup media, is stored in fire proof safe.

5.1.7 Waste disposal

All related paper waste must be shredded. Magnetic media is physically/mechanically destroyed before disposal.

5.1.8 Off-site backup

No stipulation.

5.2. Procedural Controls

All the issues related to procedural control, like the definition of trusted roles, are specified in the CPS.

5.2.1 Trusted roles

No other stipulation.

5.2.1.1 Responsibilities of system administrator

No other stipulation.

5.2.1.2 Responsibilities of certification authority

No other stipulation.

5.2.1.3 Responsibilities of security officer

No other stipulation.

5.2.1.4 Responsibilities of registrar

No other stipulation.

5.2.2 Number of persons required per task

Any task requiring the creation, backup or importation data into a database of the NIIF CA Private Key must involve two trusted persons, one performing the function and the second fulfilling the security monitoring role.

5.2.3 Identification and authentication for each role

No other stipulation.

5.3. Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

All the issues related to personnel controls are specified in the CPS.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

No stipulation.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Contracting personnel requirements

No stipulation.

5.3.8 Documentation supplied to personnel

No stipulation.

6 TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1 Key pair generation

The NIIF CA key pair generation must meet the procedures defined in the NIIF CA CPS. Subscriber's key pairs must be generated by their client application during the requesting process. They are never generated or stored by the NIIF CA. The application used must be compliant with industry standards, but the subscriber is responsible for the integrity and suitability of this application. The NIIF CA lists some of the suitable applications on its public web pages.

6.1.2 Private key delivery to entity

Subscriber's private keys are never delivered. The subscriber must generate his/her own key pair.

6.1.3 Public key delivery to certificate issuer

Subscriber's public keys are delivered to the RA in the certification request via the End Entity certification request service provided by the RA to End Entities.
The NIIF CA shall accept certificate requests in any of the following forms:

- PEM encoded certificate request (See RFC 1424).
- Netscape Signed Public Key And Challenge (SPKAC) format
- PKCS#10 request format.(See RFC 2314).

6.1.4 CA public key delivery to users

The NIIF CA public key is published on the NIIF CA public repository: http://www.ca.niif.hu/rootkey.html (see section 2.6.4).

6.1.5 Key sizes

The NIIF CA uses RSA public key algorithm.
The CA private key must have a length of 2048 bits.
The RA private key must have a length of 2048 bits.
All other private keys must be of at least 1024 bit key size.

6.1.6 Public key parameters generation

No stipulation.

6.1.7 Parameter quality checking

No stipulation.

6.1.8 Hardware/software key generation

The subscriber's keys can be generated by different applications depending on what is available on the device.

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

Keys may be used for the purposes and in the manner described in section 1.3.4, applied key usage field for issued user certificates:

- digitalSignature
- nonRepudiation
- keyEncipherment
- keyAgreement
- dataEncipherment

The NIIF CA key usage purposes are defined in the CPS.

6.2. Private Key Protection

6.2.1 Standards for cryptographic module

The policy does not mandate the use of cryptographic module compliant with pre-determined standards. The CPS details the cryptographic module used, and its compliance with industry standards.
Cryptographic module usage is not required for the subscriber, but in case of use it must comply with industry standards and the private key should be stored in an encrypted form.

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

Private Keys of subscribers must not be under multi-person control. NIIF CA multi-person control is defined in the NIIF CA CPS.

6.2.3 Private key escrow

Private Key escrow is not supported.

6.2.4 Private key backup

The NIIF CA private key backup is defined in the CPS, and it ensures that the key will not be lost. This policy suggests for end entities that they should maintain a backup copy of the private key in order to be able to reconstitute it in case of destruction of the key. This backup must be carefully protected.

6.2.5 Private key archival

The NIIF CA private key backup is defined in the CPS. End Entity keys are not archived. However, End Entities are allowed to back up their own keys.

6.2.6 Private key entry into cryptographic module

See section 6.2.1.

6.2.7 Method of activating private key

As a general rule for the activation of a private key some specific activation data must be entered in the cryptographic module:

- If the private key is stored on a cryptographic token, the PIN length must be a minimum of 4 characters.
- If the private key is stored on the host computer in a file, the file's pass phrase length must be a minimum of 12 characters.

The NIIF CA private key activation is defined in the CPS.

6.2.8 Method of deactivating private key

The NIIF CA private key deactivation is defined in the CPS.

6.2.9 Method of destroying private key

The NIIF CA private key destruction is defined in the CPS.

6.3. Other Aspects of Key Pair Management

6.3.1 Public key archival

The public key archiving is part of the certificate archival, and the NIIF CA accomplishes this functionality. The procedure of archiving is defined in the CPS.

6.3.2 Usage periods for the public and private keys

6.3.2.1 CA key pair

Described in the CPS.

6.3.2.2 End entity key pair

The validity period of an End Entity key pair must not extend one year.

6.4. Activation Data

6.4.1 Activation data generation and installation

NIIF CA activation practice must be defined in the CPS.
The minimum length of the End Entity pass phrase or PIN is described in 6.2.7.
In case of file store the activation data must contain:

- a lowercase character,
- an uppercase character,
- a number and
- minimum one non alphanumeric character.

In case of cryptographic tokens, the activation data must contain numbers and should contain alphanumeric characters.

6.4.2 Activation data protection

Pass phrases or PINs protecting the private keys must be accessible only to the authorised person.

6.4.3 Other aspects of activation data

No activation data other than access control mechanisms is required to operate cryptographic modules.

6.5. Computer Security Controls

6.5.1 Specific computer security technical requirements

Described in the CPS.

6.5.2 Computer security rating

No formal computer security rating is required.

6.6. Life Cycle Technical Controls

6.6.1 System development controls

The NIIF CA operational software is developed in a controlled environment employing appropriate quality controls. Production and development environments are totally separated.

6.6.2 Security management controls

Separation of the roles is required and the practice is specified in the NIIF CA CPS.

6.6.3 Life cycle security ratings

No stipulation.

6.7. Network Security Controls

Remote access to the CA software via the administration software interface is secured. Only the End Entities module of the RA component can be accessed from the network, which has a different security rating. This connection is protected by dedicated firewall which requires authentication and authorization and communication via Secure Socket Layer.
Regular network security testing is undertaken.

6.8. Cryptographic Module Engineering Controls

No stipulation.

7 CERTIFICATE AND CRL PROFILES

7.1. Certificate Profile

To ensure the interoperability the NIIF CA issues certificates profiling them accordingly to RFC 2459.

7.1.1 Version number(s)

The version field in the certificate shall state 2, indicating X.509v3 certificates.

7.1.2 Certificate extensions

Certificates issued under this CP contain the following certification extensions:

Extension:	Details:	Criticality
Key Usage	¤ digitalSignature ¤ nonRepudiation ¤ keyEncipherment ¤ keyAgreement ¤ dataEncipherment	Critical
CertificatePolicies	Policy Identifier OID:	Non critical
subjectAltName	¤ dnsName	Non critical
CRLDistributionPoints	¤ uri: http://www.ca.niif.hu/crl/niif-ca-crl.crl ¤ directoryString: ldap:///cn=NIIF Root CA,ou=Certificate Authorities,o=NIIF,c=HU	Non critical
AuthorityAccessInfo	URI: http://ocsp.ca.niif.hu:2560/	Non critical
ExtendedKeyUsage	¤ (varies on the targeted usage)	Non critical
BasicConstraints	¤ CA=False	Critical

7.1.3 Algorithm object identifiers

No stipulation.

7.1.4 Name forms

Please see section 3.1

7.1.5 Name constraints

See section 3.1.2. NIIF certificate directory ensures that the names are unique.

7.1.6 Certificate policy Object Identifier

The policy requires including only the policy object identifier in the issued certificate.

7.1.7 Usage of Policy Constraints extension

Not stipulation.

7.1.8 Policy qualifiers syntax and semantics

The certificates issued under this CP use the policy qualifiers.

7.1.9 Processing semantics for the critical certificate policy extension

See section 7.1.2.

7.2. CRL Profile

7.2.1 Version number(s)

The NIIF CA provides X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

The NIIF CA provides X.509 Version 2 CRL entry extensions as it is defined in RFC 2459.
The issued certificate revocation list contains the following CRL extensions:

Extension:	**Details**	**Criticality**
CRL Number		Non critical
CRL Reason		Non critical
HoldInstruction	Reject	Non critical

8 SPECIFICATION ADMINISTRATION

8.1. Specification change procedures

Suggested changes to this CP must be communicated to the contact person (see section Contact Details).
There are two possible types of policy changing depending on the significance of the change:

- issuing a new CP, if the change is determined to influence the trust procedures of relying parties and/or cooperating CAs;
- change or alteration of the existing policy.

If an existing policy requires re-issuing, the changing process applied is the same as for initial publication, which means

- the NIIF CA will assign a new OID to the modified CPS, which differs from the previous OID only in the policy version number,
- the NIIF CA will publish the document in the repository (see section Repositories).

Minor editorial or typographical changes to this CP may be made without approval.
All changes will be communicated to the interested parties. See section Publication and notification policies.

8.2. Publication and notification policies

This document and any older versions are available from the on-line repository specified in section 2.6.4.

8.3. CP approval procedures

It is the responsibility of the NIIF Institute's Security Officer to validate that the statements and requirements of this CP are met with the procedures described in the CPS, every time when this CP or the CPS is modified.
All the CP modifications must be approved by the EU Grid PMA before coming in force. All the planned modifications are reported to the EU Grid PMA, and applied only after approval received from the EU Grid PMA Policy Board.
The CP is valid, if and only if the CPS requirements are satisfied.