NIIF Certification Authority

Certification Practice Statement (CPS)

Version 1.4

Document OID: 1.3.6.1.4.1.11914.1.1.1.1.4

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 Certification Practice Statement of the NIIF Certification Authority and describes the practice employed by the NIIF CA in issuing digital certificates.
The NIIF CA supports the creation and use of key pairs and of Public Key certificates. Key pairs and Public Key certificates are used according to the provisions of NIIF CA's certificate services, including but not limited to:

- authentication services (authentication, integrity and non-repudiation);
- confidentiality services.

This CPS provides factual information that describes the:

- practices employed within the NIIF CA to support certificate services;
- attendant use of technologies and processes to support the underlying operational infrastructure.

The practices described in this CPS together with the technologies and processes referred to in other specific operational documentation serve to illustrate the trustworthiness and integrity of NIIF CA's certificate operations from certificate generation and signing to expiry.
A number of Certificate Policies may be operated under this CPS.
A relying party may use this CPS to determine the level of trust associated with the given Certificate Policy.

1.1.1 Revisions

This CPS 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 RFC 3280. This CPS differs from the RFC 2527 and RFC 3280 standards 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	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 indicate 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.
End Entity	A person or device for whom/which requests a certificate from the NIIF CA.
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.

1.1.4 PKI operational infrastructure

1.1.4.1 CA domain

The NIIF CA is responsible for issuing certificates.

1.1.4.2 RA domain

The RA domain consists of all RAs that are operated under the NIIF CA hierarchy. These RAs are responsible for supplying user registration and revocation services to End Entities.

1.1.4.3 End Entities domain

This domain includes End Entities, which use or rely on certificates for authentication, integrity, non-repudiation and confidentiality.

1.1.5 Security Philosophy

The security philosophy governing the operational management of the NIIF PKI is:
"Prevention, Detection and Response based on risk assessment".

This philosophy means that the first aim of the NIIF CA is:

- to assess the risk of unauthorised action taking place arising from technology, human resources and operational procedures;
- to build preventive and detective countermeasures to reduce the likelihood of relevant risks; and
- to respond to unauthorised events or actions in a considered and positive manner.

In all cases, NIIF CA operates to:

- securely generate their Private Keys and take adequate precautions to protect against their compromise, modification, disclosure, loss or unauthorised use;
- be able to detect and record unauthorised events and actions.

1.1.6 Staffing Arrangements

The NIIF CA PKI has adopted and employs personnel and management practices to ensure the trustworthiness, integrity and professional conduct of its staff.
The following personnel standards are applied:

- all NIIF Institute operations staff enter into non-disclosure agreements to protect against the unauthorised disclosure of confidential information;
- all NIIF Institute operations staff are trained in:
    a. basic PKI concepts;
    b. the use and operation of CA or RA software;
    c. documented CA and RA procedures;
    d. computer security awareness and procedures;
    e. for pertinent RA staff, how to explain to End Entity certificate applicants the responsibilities adhering to the possession, use and operation of their key pairs;
    f. the meaning and effect of relevant CP, this CPS.

1.2. Identification

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

IANA	1.3.6.1.4.1
NIIF	.11914
Services	.1
Policy	.1
CPS	.1
Major Version	.1
Minor Version	.4

1.3. Community and Applicability

The practices in this CPS must adhere to the primary purpose of the CPS, of ensuring the uniformity and efficiency of practices throughout the PKI.

In keeping with their primary purpose, the practices in this document:

- are the minimum requirements necessary to ensure that subscribers and relying parties have the highest possible level of assurance, and that critical functions are provided at appropriate levels of trust;

- apply to all stakeholders, for the generation, issue, use and management of all certificates and key pairs.

1.3.1 Certification authorities

The NIIF CA established a Root Certification Authority, which provides PKI services for the Hungarian Academic Community. The NIIF CA self-signs its own certificate. The specific applicability of the certificates issued by the NIIF CA is stated in the relevant CPs.
The NIIF CA does not issue certificates to subordinate Certification Authorities.

1.3.2 Registration authorities

The NIIF Institute manages the functions of the Registration Authority. Partners subscribed to the Hungarian Academic Community may operate other RAs, but this requires that the RAs must sign an agreement with the NIIF CA stating the obligation to adhere to this CPS and the relevant CPs.
RAs must not issue certificates under this CPS and the relevant CPs. The list of RAs associated with the operation they have permission to perform is available from the NIIF CA website.

1.3.3 End entities

The targeted End Entities are 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 the corresponding CP, subscribers that are subjects of the issued certificates may be:

- any natural person which can be uniquely identified;
- any legal person which can be uniquely identified;
- any IT resources including servers, SSL based services and VPN devices which are managed by NIIF or the Hungarian Academic Community.

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).
Certificates issued by the NIIF CA can facilitate:

- Authentication
- Authorization
- Confidentiality
- Integrity
- Non-repudiation

Applicable key usage is indicated in the X.509 v3 keyUsage extension of the certificate. Any usage other than the one(s) indicated in this extension is at the risk of the relying party. The specific applicability requirements may be stated in the relevant CP.

1.4. Contact Details

1.4.1 Specification administration organization

The Security Officer of the NIIF Institute is responsible for the management of the NIIF CA including the maintenance of this CPS [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
URL: 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 the 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;
- operate according to this CPS and the Hungarian laws;
- verify that any CA with which it cross-certifies itself complies with the according CP.

The NIIF CA is obliged to

- create global certificate policy, which is applied on all certificates issued by NIIF CA;
- make reasonable efforts to ensure they conduct an efficient and trustworthy operation. "Reasonable efforts" includes but does not limit the CA to operate in compliance with:
  - a contractual agreement;
  - documented internal operational procedures;
  - applicable CP;
  - this CPS;
  - within applicable law;
- handle certificate requests and issue new certificates, including:
  - accepting certification requests from End Entities requesting a certificate according to the procedures described in this CPS and in the relevant 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 this CPS and the relevant CP;
  - authenticating entities requesting revocation of a certificate;
  - issuing certificate revocation list and make CRL publicly available;
  - operating OCSP responder.

NIIF CA is obliged to protect its private key in accordance with this CPS, including restrictions. The NIIF CA's private key used for issuing certificates in accordance with this CPS and the relevant CP may be used only for signing certificates, CRLs, and other adequate information consistent with the certificate management.

2.1.2 RA obligations

The RAs must sign an agreement to adhere to the procedures described in this document. RA must operate in accordance with its CPS and the law of Hungary.

The RA is obliged to

- 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 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 CPS;
- protect its private key in accordance with this CPS;

- advise End Entities about their obligations under the relevant CP, this CPS and the appropriate subscriber agreement and relying party agreement, and providing End Entities with copies of the relevant CP and this CPS 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 issued to facilitate routine secure communication between RA and CA.

2.1.3 Subscriber obligations

To request a certificate, the subscriber must:

- understand and, if necessary, receive proper education in the use of Public-Key cryptography and certificates;
- accept the conditions and adhere to the procedures described in this document;
- voluntary 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 CPS;
- 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 this CPS and the relevant 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.

2.1.4 Relying party obligations

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

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

2.1.5 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

The NIIF Institute has introduced a number of measures to reduce or limit its liabilities in the event that the safeguards in place to protect its resources fail to:

- inhibit misuse of those resources by authorized personnel;
- prohibit access to those resources by unauthorized individuals.

2.2.1 CA liability

The NIIF CA warrants that all certificates issued were issued in accordance with this CPS and the relevant CP.
Although it aims to achieve a reasonable level of security, the NIIF CA provides no warranties, express or implied, including in respect of security and confidentiality, and of fitness for a particular purpose. NIIF accepts no liability for or in connection with the certification services and the parties using or relying on them shall hold NIIF free and harmless from liability resulting from such use or reliance.

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 no financial responsibility for certificates issued under this CPS.

2.3.1 Indemnification by relying parties

The NIIF CA assumes no financial responsibility for improperly used certificates.

2.3.2 Fiduciary relationships

Issuing certificates in accordance with this CPS and the corresponding CP does not make the NIIF CA, or any RA within the NIIF CA infrastructure an agent, fiduciary, trustee, or other representative of any End Entity or relying parties.

2.3.3 Administrative processes

Not applicable.

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:

- Cross-certification agreement, if applicable, which describes contractual arrangements which defines the functional and assurance requirements is included in the relevant CP which is the liability of the NIIF representative, who signs the contract;
- 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, who recline upon the End Entity certificate.

2.4.1.2 Force Majeure

Neither NIIF CA nor any related RAs operating under this CPS shall be in default hereunder or liable for any losses, costs, expenses, liabilities, damages, claims, or settlement amounts arising out of or related to delays in performance or from failure to perform or comply with the terms this document and related agreement due to any causes beyond its reasonable control, which causes include acts of the public enemy, riots and insurrections, war, accidents, fire, strikes, embargoes, judicial action, acts of civil or military authorities.

2.4.2 Severability, survival, merger, notice

Should it be determined that one section of this CPS is incorrect or invalid, the other sections shall remain in effect until the CPS is updated as indicated in Section 8.
In the event that any one or more of the provisions of the CPS or related CPs shall for any reason be held to be invalid, illegal, or unenforceable at law, such unenforceability shall not affect any other provision, but that document shall then be construed as if such unenforceable provision or provisions had never been contained herein, and insofar as possible, construed to maintain the original intent of that document.
If the certification services provided by the NIIF CA and the related CPS and CPs terminate all certificates issued by the NIIF CA will be revoked no later than the time of termination. Regulations related to revocation and the procedures to handle revocation data will be valid without constraints.
The NIIF CA will make all reasonable efforts to notify all its subscribers, all cross-certifying CAs, and any relying parties known to the NIIF CA to be currently and actively relying on certificates issued by the NIIF CA on such termination.

2.4.3 Dispute resolution procedures

In case a dispute is not successfully resolved by negotiations, the parties involved may appoint an independent third party arbitrator. If arbitration proves impossible, the parties can take legal actions based on Hungarian laws.

2.5. Fees

2.5.1 Certificate issuance or renewal fees

No fees are charged for issuing certificates.

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

No fees are charged for allowing policy and CPS information access.

2.5.5 Refund policy

Not applicable.

2.6. Publication and Repository

2.6.1 Publication of CA information

The NIIF CA must make publicly available, in its repositories:

- The NIIF CA's certificate for its signing key;
- The current and previous versions of the NIIF CA certificate Practice Statement;
- The current and previous versions of the applicable certificate Policies and related user guide explaining how End Entities should request a certificate;
- All issued certificates including CA-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 the CPS are published according to section 8.

2.6.3 Access controls

There is no access control on reading the CPS and related CPs.
There is no access control on reading the certificates and certificate revocation list, but the access is limited to a single name search enquiry in the NIIF certificate repository. This repository does not

- provide access to End Entities in any manner other than that stated in this CPS;
- provide any information or services to End Entities other than that information and those services listed in this CPS;
- alter any certificate details or notices that it receives.

NIIF provides OCSP functionality which is publicly accessible to other repositories for certificate status checking purposes. Beside OCSP functionality other repositories are freely available, and access only to the OCSP.
Appropriate access controls are used to restrict to authorized personnel the ability to write to or modify these items.

2.6.4 Repositories

The NIIF CA maintains repositories with different availabilities. The consistency of data contained in the different repositories is ensured by NIIF CA.

2.6.4.1 Web based repository

The NIIF CA maintains a website, which contains all the information listed in section 2.6.1 such as the following:

Availability	Content
http://www.ca.niif.hu/rootkey.htm	The NIIF CA's certificate for its signing key
http://www.ca.niif.hu/policies/NIIF_CA_CPS_v<version>.pdf	The current and previous versions of the NIIF CA Certificate Practice Statement in English, in PDF format
http://www.ca.niif.hu/en/policies/NIIF_CA_CPS_v<version>.pdf	The current and previous versions of the NIIF CA Certificate Practice Statement in English, in PDF format
http://www.ca.niif.hu/policies/NIIF_CA_CP_<function>_v<version>.pdf	The current and previous versions of the applicable Certificate Policies and related user guide explaining how End Entities should request a certificate in English, in PDF format
http://www.ca.niif.hu/en/policies/NIIF_CA_CP_<function>_v<version>.pdf	The current and previous versions of the applicable Certificate Policies and related user guide explaining how End Entities should request a certificate in English, in PDF format
http://www.ca.niif.hu/crl/niif-ca-crl.crl	Signed Certificate Revocation List
http://ocsp.ca.niif.hu:2560/	OCSP responder function

The English version of the above mentioned documents are the official reference.

2.6.4.2 LDAP based certificate repository

The NIIF CA maintains an LDAP based repository, which contains all the information listed in section 2.6.1 such as the following:

Availability	Content

ldap://directory.iif.hu O=NIIF CA,C=HU	All issued certificates including CA-certificates, which perform the following functions: ▪ allow a name search enquiry on master directories or copies thereof to determine within the span of the directory structure: ○ if agreed with the Subscriber, the number of certificates held by the nominated person, ○ the type or grade of each certificate, ○ the status of each certificate; ▪ provide access to Public Keys via certificate download; This repository shall not publish information about any information pertaining to an End Entity not contained in the certificate.
ldap:///cn=NIIF Root CA,ou=Certificate Authorities,o=NIIF,c=HU rootkey	The NIIF CA's certificate for its signing key

2.6.4.3 Other availability

Printed versions of the NIIF CA CPS and CP documents are available in the NIIF Institute for fee. The contact person receives the requests.

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 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

2.8.1.1 Certificate information

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 NIIF 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 are 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.

2.8.1.2 NIIF CA documentation

The following documents are considered to be confidential information of NIIF CA:

- Protective Security Risk Review;
- System Security Plan;
- Contingency & Disaster Recovery Plan;
- Operating Procedures.

2.8.2 Types of information not considered confidential

2.8.2.1 Certificate information

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

2.8.2.2 NIIF CA documentation

The following NIIF CA documents are public documents and are not considered to be confidential information:

- CPs;
- this CPS;

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 does 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;
- a properly constituted instrument that has emanated from a court having jurisdiction or an authority having legal jurisdiction requiring production of the information is produced; and
- the person requiring production is a person authorised to do so.

2.8.5 Disclosure upon owner's request

The subscriber shall have full access to its personal data, and shall be empowered to authorise 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 authorisation may take two forms:

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

No release of information is permitted without a formal authorisation in accordance with this section.

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 CPS and related CPs is acknowledged.
The NIIF CA claims no intellectual property rights on issued certificates, this CPS or related CPs.

3 IDENTIFICATION AND AUTHENTICATION

3.1. Initial Registration

3.1.1 Types of names

The NIIF CA assigns each End Entity a distinguished name – irrespectively of type - that is in compliance with the X.500 standard and serves as a unique identifier of the End Entity.
All End Entity DNs in certificates issued under this CPS shall start with invariable part identifying the CA (C=HU,O=NIIF). The following variable part can consist of the optional RDN which is defined by the relevant CP.
The RA proposes and approves distinguished names for subscriber, and as a minimum check it verifies that the proposed distinguished name is unique, ie. the name is not listed already in the NIIF CA repository.

3.1.2 Need for names to be meaningful

The Subject and Issuer names contained in a certificate, are meaningful in the sense that the issuing CA has proper evidence of the existent association between these names and the entities to which they belong.
In case of natural persons, RAs are not to accept pseudonymous names, which they believe may cause offence.
In case of legal entities, the RA accepts only names contained in documents relating to legal personality or their official abbreviation.
In case of IT resources, the RA accepts only names listed in the Internet public DNS registry (www.nic.hu) directory and where the owner of the DNS domain name corresponds with certificate requesting natural or legal person, or a requester must provide a legal document, which states that the requester is allowed to use the specific DNS domain name for a minimum of 1 year and 1 month from the time of the request.
The NIIF CA supports the use of certificates as a form of identification within a particular community of interest. Anonymous certificates are not supported by the NIIF CA.

3.1.3 Rules for interpreting various name forms

See section 3.1.1.

3.1.4 Uniqueness of names

Distinguished names is unambiguous and unique, certificates must apply to unique individuals or resources. Individuals must not share certificates.

3.1.5 Name claim dispute resolution procedure

The person named in 1.4.2 responsible to manage name dispute.

3.1.6 Recognition, authentication and role of trademarks

Recognition, authentication and the role of trademarks is a commercial issue. Nothing in this CPS shall prevent the use of a trademark in a Distinguished Name.

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 certificate request of the subscriber. The method to be employed to do this is detailed in the RA operating procedures, but should, as the minimum involve signing and verifying a message. This may typically be accomplished by exchanging digitally signed and encrypted email messages or web form with the subscriber.
This should be done for both the Authentication keys and the Confidentiality keys.
The RA is to also take reasonable steps to ensure the subscriber is the true owner of the key pairs. Reasonable steps consist of:

- the RA validates the signature using the public key from the subscriber's certificate request;
- additionally, if deemed appropriate, obtaining a statutory declaration from the subscriber that they are the true owner of the key pairs, which could be verified with the unique Request password (which is provided via the Certificate Request interface) of the certificate requester.

If any doubt exists, the registrar is not to request certification. If the subscriber's right to use or possession of self-generated keys cannot be shown or proven, or reasonable doubt exists the certificate must not be issued.

3.1.8 Authentication of organization identity

Every time a 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 procedures of initial authentication of individual identity must comply with the CP applicable to the certificates. In case where the CP requires personal photo-id authentication, the RA must meet the holder in person to compare the photograph in the officially issued identity card of the subscriber and register the type and number of the identification document. The relevant CP must not specify other acceptable identity documents but may detail the procedure described.
Additionally, the RA may consider that the user is correctly identified if the RA has previously identified the user using the procedure described above. In this case the RA must check by using the information provided during the initial request that this new request originated at the known user.
The subscriber asking for a certificate for a service or server component must prove that he has the necessary authorization by providing a signed statement made by the representatives of the organization operating the resource. The statement may be in electronic form in which case it is digitally signed by a valid certificate issued by the NIIF CA.
If authentication is not completed within 30 days of receipt of the certificate request by the RA the request will be deemed to have expired and any authentication of identity must then be preceded by a new certificate request.

3.2. Routine Renewal

Renewal of certificates will follow the same procedure as an initial registration or subscriber may use digitally signed new certificate requests signed with the previous certificate sent to the RA

before certificate expiration for renewal. In case of renewal subscriber must create a new key pair but the personal authentication of individual entity is not required.
In case where the certificate to be renewed 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 must not be re-certified, routine rekey is not supported.

3.4. Revocation Request

A request to revoke keys and certificates, if initiated by an EndEntity and signed by a valid key and certificate under the relevant CP and this CPS, regardless of the document version, shall constitute a valid and enforceable revocation request. Furthermore 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. Certificate preprocessing request

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.

Signature: .....

4.2. Certificate Application

It is the responsibility of the subscriber requiring a certificate to send that request to an approved RA.
In all cases the subscriber is responsible to generate his/her own key pair and submit the public key and other data required by relevant CP to the RA.
The subscriber is obliged to choose a pass phrase during the certificate application process, which allows of the initiation of certificate suspension and revocation. The subscriber is obliged to choose a Request pass phrase during the certificate application process, which allows the request identification verification.

4.3. Certificate Issuance

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

- RA verifies whether the subscriber qualifies for the certificate;
- RA verifies the identity of the subscriber as indicated in Section 3.1
- RA validates the prove of possession of private key using procedures indicated in Section 3.1.7, including the Request password;
- When the certificate request does not contain an email address, RA registers the email address to which the subscriber wants the certificate issuance notification to be sent;
- 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 or to the address registered by the RA;
- The subscriber
    - downloads the certificate from the site given in the notification;
    - accesses its keys and certificates in a secure format;
    - installs the received certificates;

4.3.1 Relying parties

Relying parties may need to access nominated certificates. They may obtain the certificates they require directly from subscriber, or by requesting certificates from the NIIF 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. If a certificate request is rejected, the requesting RA is to promptly inform the subscriber. CA is under no obligation to disclose the reason for the rejection of any certificate request, except where required by the CP under which the certificate was to have been issued, or by Hungarian laws.

4.3.3 Operational periods

All certificates begin their operational period on the date of issue. The operational period of a certificate is governed by:

- the Certificate Profile;
- the CP;
- this CPS.

The expiry date of issued certificates must not result in an operational period greater than that permitted by the above instruments. In the event that a certificate is issued with a greater than permitted operational period, the certificate is to be revoked.

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 the associated CP and this CPS;
- warrants that according to his/her knowledge no unauthorised 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. Each certificate issued by this CA has a maximum lifetime of 386 days.

4.6. Certificate Suspension and Revocation

Each revocation/suspension request must be initiated at the RA where certificate request submitted. If it is not possible for some reasons, then the revocation/suspension request must be submitted directly to NIIF RA office.

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 subscriber of the certificate;
- an authorised third party.

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

The practices involved in processing of a revocation request will vary depending on the identity of the originator. This section describes the practices where revocation is:
- requested by the End Entity;
- verified by an RA;
- processed by a CA.

Where a revocation request is originated by a party other than the subscriber:
- the practices employed in processing the request will comply to the fullest extent possible with the practices that are described below;
- the reason for the request is documented and documents is handled according to this CPS.

4.6.3.1 CA processing

To process a revocation request initiated by RA, the NIIF CA:
- receives and authenticates the digitally signed request from the RA;
- prioritizes the request according to the revocation response times contained within the relevant CP;
- revokes the certificate;
- adds the certificate to its CRL in the repository and issues notices of revoked certificates and the reason for revocation via OCSP;
- revoked certificates are stored in the CRL for ever;
- revoked certificates are deleted from the online certificate repository.

In case of the revocation of NIIF CA certificate the CA first revokes all the issued certificates under the affected CA certificate and shall in addition inform the subscribers and cross-certifying CAs and it shall terminate the certificate, CRLs distribution service and OCSP for certificates/CRLs issued using the compromised private key.

4.6.3.2 RA processing

To process a revocation request initiated by a subscriber, an RA:
- receives and authenticates the request;

- ensures the certificate and Public Key are current;
- prioritizes the request according to the processing times indicated in the relevant 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 is delivered to the RA either in the form of digitally signed file, printed document signed by the subscriber or in person.

4.6.3.3 Subscriber processing

If allowed by the relevant CP, the subscriber gives 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.
Subscribers can issue a revocation request to the RA, if

- personally request the RA to revoke the certificate;
- send a signed Certificate Revocation Request Form in letter to the RA;
- fax a signed Certificate Revocation Request Form to the RA, including the pass phrase selected during certification request procedure.

4.6.3.4 Certificate Revocation Request

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

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. ** Suspension of device certificates not applicable.

Section 4 – Reason for revocation/suspension *** .... *** This section is optional for certificate owners requesting revocation of their own certificates.
Section 5 – Authorization Authorized by: ❑ certificate owner ❑ Authorized third party (Original documentation verifying authorization is sighted.) Signature: ....

4.6.3.5 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 private key associated with the revoked certificate.

4.6.4 Revocation request grace period

The NIIF CA responds within one working day 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.
- Suspension of NIIF CA certificates is not applicable.

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

4.6.7.1 CA processing

To process a suspension request initiated by RA, the NIIF CA:

- receives and authenticates the digitally signed request from the RA;
- suspend the certificate;
- adds the certificate to its CRL in the repository and issues notices of suspended certificates via OCSP;

4.6.7.2 RA processing

To process a suspension request initiated by a subscriber, an RA:

- receives and authenticates the request;
- ensures the certificate and Public Key are current;
- sends a digitally signed suspension request to the CA.

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

4.6.7.3 Subscriber processing

The procedure to be followed is the same as in case of revocation (see section 4.6.3.3).

4.6.7.4 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 4.6.3.4.

4.6.7.5 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)

CRLs are issued by NIIF CA after every certificate revocation, periodical revocation list update being valid for 8 days occurring daily. The most up to date CRL is published into the NIIF certificate repository and into the NIIF CA Web Site.

4.6.10 CRL checking requirements

Before using of a certificate, a relying party must

- validate it against the most recently issued CRL
- or 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 (OCSP, see section 2.6.4) for verifying the status of certificates issued within 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 is 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

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, including CRLs;
- audit records
    - Boots of the equipment,
    - Login and logouts to the RA/CA system,
    - Use of the RA/CA software,
    - Unauthorized attempts to access the RA/CA system;
- revocation records.

4.7.2 Frequency of processing log

Audit logs are processed on a weekly, monthly and annual basis.

4.7.3 Retention period for audit log

Audit logs are retained as archive records. The audit logs are kept on CA equipment for a minimum period of 3 month and a maximum period of six month after which they are moved to the archive.

4.7.4 Protection of audit log

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

4.7.5 Audit log backup procedures

A backup of the audit logs shall be performed at least weekly on physical removable media. The backup media is kept in safe storage.

4.7.6 Audit collection system (internal vs. external)

The audit collection system shall be running separately form the CA software in a secure environment.
The NIIF CA audit collection system is a combination of automated and manual processes performed by the CA or RA operating system, the CA or RA application, and by operational personnel.

Type of event Collection	System	Recorded by
Successful and failed attempts to changes operating system security parameters.	Automatic	Operating system
Application startup and shutdown.	Automatic	Operating system
Successful and failed log-in and log-off attempts.	Automatic	Operating system
Successful and failed attempts to create, modify, or delete system accounts.	Automatic	Operating system
Successful and failed attempts to create, modify or delete authorized system users.	Automatic	Operating system
Successful and failed attempts to request, generate, sign, issue or revoke keys and certificates.	Automatic	CA or RA software
Successful and failed attempts to create, modify or delete certificate holder information.	Automatic	RA software
Backup, archiving and restoration.	Automatic and manual	Operating system and operation personnel
System configuration changes.	Manual	Operations personnel
Software and hardware updates.	Manual	Operations personnel
System maintenance.	Manual	Operations personnel
Personnel changes	Manual	Operations personnel

4.7.7 Notification to event-causing subject

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

4.7.8 Vulnerability assessments

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

4.8. 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.

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 5 years.

4.8.3 Protection of archive

Digitally stored archive records are stored in a safe place on permanent removable media.

4.8.4 Archive backup procedures

Archive records are weekly moved from the CA and RA equipments to the removable media. The copies are stored in different locations which enables complete restoration of current service in the event of a disaster situation. See Section 4.8.3.

4.8.5 Requirements for time-stamping of records

All archive records are time stamped, but Trusted Time source is not available.

4.8.6 Archive collection system (internal or external)

The archive collection system is internal to the NIIF CA.

4.8.7 Procedures to obtain and verify archive information

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

- at the time the archive is prepared;
- annually at the time of a programmed Security Audit ordered by security officer;
- at any other time when a full security audit is required.

4.9. Key Changeover

The NIIF CA's keys should be changed while sufficient validity time – 13 months - remains on the existing keys to allow uninterrupted validity of all subordinate keys. The following procedure should be undertaken when changing the NIIF CA's keys:

- a new NIIF CA key is generated and self signed certificate issued.
- the old key is signed by the new one.
- the new key is signed by the old one.
- all the newly issued certificates are published.

4.10. Compromise and Disaster Recovery

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

If the CA resources are damaged or rendered inoperative, but the CA private key is not destroyed, CA operation will be reestablished as quickly as possible as described in NIIF Institute Contingency and Disaster Recovery Plan, including:

- starting the backup repository and services systems when needed;
- notifying users via the NIIF CA home page (http://www.ca.niif.hu);
- notifying cross-certifying CAs personally;
- diagnosing the cause of the corruption, and in that case the extent of the corruption cannot be exactly specified, the entire system is rebuilt;
- repairing and replacing corrupted parts of the system;
- starting the data recovery procedure;

If the private key is destroyed the case will be treated as described in section 4.10.2.2.

4.10.2 Entity public key is revoked

4.10.2.1 CA Key

The NIIF CA has established a key and user compromise plan that addresses the actions to be taken in the event that the CA Public Key is revoked, which contains the following steps

- all the issued certificates under the affected key revoked;
- the key is revoked;
- the CRL is updated and published;
- the PKI system is terminated;
- new CA keys pair is generated as indicated in section 6.1in accordance with the entity identification procedure defined in section 3.1;
- users are notified via NIIF CA home page (http://www.ca.niif.hu) or personally.

4.10.2.2 Subscriber's Key

See section 3.2, 3.3 and 3.4

4.10.3 Entity key is compromised

4.10.3.1 CA Key

The NIIF CA has established a key and user compromise plan that addresses the actions to be taken in the event that the NIIF CA Private Key is compromised. This procedure is the same as section 4.10.2.

4.10.3.2 Subscriber's Key

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.

4.10.4 Secure facility after a natural or other type of disaster

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

4.10.5 Contingency & Disaster Recovery Plan

The purpose of this plan is to restore core services as quickly as practicable when systems operations have been significantly and adversely impacted by catastrophic event. The plan primary goal of reinstating the NIIF CA platform in order to make accessible the logical records kept within the software. Recovery actions approved within the plan should be given a priority.

4.11. CA Termination

4.11.1 Transfer of CA services

If the NIIF CA decides to transfer its PKI services to another organization, the NIIF CA must:

- make all reasonable efforts to inform subscribers and cross-certifying CAs and relying parties at least 6 month before the transfer;
- ensure that the new organization complies with this CPS and with the corresponding CP;
- take the procedures described in section 4.11.2.

4.11.2 Cessation of CA services

If the NIIF CA decides to cease its services or third party requires from NIIF CA to cease the services, the following steps are undertaken:

- the CA must inform all subscribers, cross certifying CAs, and relying parties about the decision at least 6 month before the termination date;
- any certificates issued after the announcement of the termination must have the expiration date not exceeding the termination date;
- at the termination date all the certificates issued by the CA is revoked;
- the CA stops distributing certificates and CRLs at the date of termination.

5 PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1. Physical Controls

5.1.1 Site location and construction

The NIIF CA operates within a secure physical zone within the office area, to which the access is strictly controlled.

5.1.2 Physical access

The physical access to the NIIF CA security zone is restricted. This means that only authorized personnel, after successful identification, can enter to the security zone and has access to the CA hardware. Regarding to the recommendations of Hungarian Insurance Association (MABISZ recommendations - http://www.pluto.hu/), different kind of physical security devices are installed including

- card based intrusion system,
- cameras,
- guards,

and log is maintained of all accesses.
Unauthorized personnel and visitors who require access to the secure zone are escorted by authorized personnel at all times. The number of personnel authorized to enter the zone is kept to a minimum.

5.1.3 Power and air conditioning

To ensure the continuity of services all critical hardware components of the NIIF CA system are connected to uninterrupted power supply and the environmental conditions (temperature and humidity) of the security zone are controlled by air conditioning.

5.1.4 Water exposures

The secure zone of NIIF CA is protected against water exposure by being located on above the ground floor of the office building that is not in a flood zone.

5.1.5 Fire prevention and protection

Suitable fire extinguishers are maintained in the secure zone of NIIF CA, to guard against the possibility of fire. There is a smoke detection and fire alarm system installed in the secure zone, which are supervised online on a 7x24 basis.
Regular auditing of the prevention and protection system is accomplished by the official fire department.

5.1.6 Media storage

All magnetic media containing NIIF CA information, including backup media, are stored in fire proof safes which are located either within the NIIF CA office area or in a secure off-site storage area.

5.1.7 Waste disposal

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

5.1.8 Off-site backup

Endorsed off site storage agents are used for the storage and retention of backup software and data. The off site storage:

- is available to authorised personnel non-stop for the purpose of retrieving software and data;
- has appropriate levels of physical security in place.

Weekly backups of NIIF CA IT resources, CA install software and NIIF CA private keys are stored on this site.

5.2. Procedural Controls

5.2.1 Trusted roles

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

- system administrator;
- registrar;
- certification authority;
- security officer.

5.2.1.1 Responsibilities of system administrator

- The NIIF CA equipment supervision, maintenance and management.
- The security of the NIIF CA equipment.
- The execution of regular backups.

5.2.1.2 Responsibilities of certification authority

- Issuing certificates and CRLs.
- Compliance with the CPS.

5.2.1.3 Responsibilities of security officer

- Audit logs monitoring.
- Execution of Security Audit.

5.2.1.4 Responsibilities of registrar

- Authentication of identities.

Different roles is occupied by different individual, system administrator can be contracting personnel.

5.2.2 Number of persons required per task

Separate individuals fill each of the four roles described above. This provides the maximum security and affords the opportunity for the greatest degree of checks and balances over system operation. However:

- a single individual may assume the roles of the System Administrator and Registrar;
- the Security Administrator must always remain separate from the System Administrator in order to provide an independent review of the audit log;
- any task requiring the creation, backup or importation into a database of the NIIF CA Private Key must involve two trusted persons, one performing the function and the second fulfilling a security monitoring role.

5.2.3 Identification and authentication for each role

Persons filling trusted roles must undergo a formal checking process conducted by the NIIF Institute Security Officer.

5.3. Personnel Controls

5.3.1 Background, qualifications, experience, and clearance requirements

The recruitment and selection practices for NIIF CA services personnel take into account the background, qualifications, experience and clearance requirements of each position, which are compared against the profiles of potential candidates.

5.3.2 Background check procedures

Background and clearance check requires an official document that the person has not criminal record.

5.3.3 Training requirements

The NIIF CA personnel is trained in:

- basic PKI Concepts;
- the use and operation of the PKI software;
- the relevant CPs and CPS;
- the documented internal procedures;
- computer security awareness and procedures.

5.3.4 Retraining frequency and requirements

NIIF CA services personnel staff receive a security briefing update at least once a year.
Training in the use and operation of the PKI software is provided when new version of the software is installed.
Any changes in CPs and/or CPS is communicated to the NIIF CA personnel as soon as possible.

5.3.5 Job rotation frequency and sequence

No job rotation has been defined.

5.3.6 Sanctions for unauthorized actions

Unauthorized actions by NIIF CA services personnel staff are submitted to staff members with the appropriate authority including, but not limited to, the Security Officer.
Security officer must check that the action is punished by Hungarian laws, and has the right to start legal procedures against the personnel.

5.3.7 Contracting personnel requirements

NIIF CA services personnel may be contractors who are appointed in writing and given written notification of the terms and conditions of their position. They are normally assigned full-time to their responsibilities.

5.3.8 Documentation supplied to personnel

NIIF CA services personnel have access to all relevant:

- hardware and software documentation;
- this CPS;
- all applicable CPs.

6 TECHNICAL SECURITY CONTROLS

6.1. Key Pair Generation and Installation

6.1.1 Key pair generation

Key pairs for the NIIF CA are generated exclusively by authorized NIIF CA personnel acting in the role of CA following the procedure defined in the Key Management Plan. The private key of the NIIF CA is stored on a FIPS 140-1 Level 3 certified tamper proof device.
End entities' key pairs are always generated by their application during the requesting process. They are never generated or stored by the NIIF CA.

6.1.2 Private key delivery to entity

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

6.1.3 Public key delivery to certificate issuer

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

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

The preferred transport method for certification requests is the SSL protected HTTP End Entity certification request service provided by the RA.

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.

6.1.5 Key sizes

The NIIF CA uses RSA public key algorithm.
The CA private key is a minimum length of 2048 bits.
The RA private key is a minimum length of 2048 bits.
All other private keys is a minimum length of 1024 bits.

6.1.6 Public key parameters generation

The parameters used to create Public Keys are generated by the NIIF CA.

6.1.7 Parameter quality checking

The quality of Public Key parameters is automatically checked by the NIIF CA software.

6.1.8 Hardware/software key generation

The NIIF CA keys are generated in hardware, see above.
The subscribers' keys may be generated in software or hardware.

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, applicable key usage extensions are defined in section 7.1.2 of the relevant CP.
NIIF CA key usage purposes are:

- digitalSignature
- nonRepudiation
- keyCertSign
- cRLSign

The keyUsage extension in the CA certificate marked as critical.

6.2. Private Key Protection

6.2.1 Standards for cryptographic module

The NIIF CA does claim that the used cryptographic module is compliant with the FIPS 140-1 Level 3 standard.
The NIIF CA private key is generated in the cryptographic module, and remains there in encrypted form, and is activated only at the time at which it is being used by the NIIF CA software.
Cryptographic modules used by subscribers must comply with industry standards.

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

The NIIF CA Root key is under multi-person control. There is 4 activation keys available distributed among different persons, and a minimum of 2 keys necessary to be able to activate the cryptographic engine. The keys are physical keys and a PIN is required for them, which means the officers authenticated using a two factor authentication mechanism.

6.2.3 Private key escrow

Private Key escrow is not supported.

6.2.4 Private key backup

The NIIF CA private key and its backup are stored on FIPS 140-1 Level 3 certified tamper proof devices, and the backup copy is maintained on a secure off site storage. Backup copy can only be made by the software component included in the cryptographic module. The software requires the backup activation physical key and a PIN code, and the PIN length must be at least 16 characters.

6.2.5 Private key archival

In accordance with international guidelines and Hungarian law, only confidentiality keys should be archived. The NIIF CA uses the backup copy for archiving purposes.
The NIIF CA does not issue confidentiality keys, that's why it does not maintain key recovery agent for issued confidentiality keys.

6.2.6 Private key entry into cryptographic module

See section 6.2.1.

6.2.7 Method of activating private key

The NIIF CA software at startup requires a minimum of 2 activation keys from the four available. Each key is owned by different officers, which means that the CA activation requires a minimum of 2 officer's attendance.

6.2.8 Method of deactivating private key

If the NIIF CA software closes the activated session, the NIIF CA private key is deactivated.

6.2.9 Method of destroying private key

The NIIF CA private key can be destroyed by a new initialization. The initialization must be done by a physical key protected application of the cryptographic module. The password length attached to each physical key is at least 16 characters.

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

The NIIF CA root certificate have a validity of 10 years. The validity period for issued certificates is set according to the requirements stated in the relevant CP.

6.4. Activation Data

6.4.1 Activation data generation and installation

During the initialization of the cryptographic module it is required to assign activation data with each physical key which length must be at least 16 characters.

6.4.2 Activation data protection

The Root Key activation data is stored in the physical activation keys, each protected with a password of minimum 16 characters. The NIIF CA's other activation data (e.g. Internal Database password, LDAP bind password) is stored in software strong encrypted database, please refer to section 6.2.7.

6.4.3 Other aspects of activation data

None.

6.5. Computer Security Controls

6.5.1 Specific computer security technical requirements

The NIIF CA computer system satisfies the following requirements:

- The NIIF CA runs on a dedicated computer system;
- Only the software needed to perform CA/RA operations are installed on the system;
- The system is connected to a secured network, and access to the operating system and the CA software is allowed only to the authorized NIIF CA personnel;
- Physical access to the system is allowed only to the authorized NIIF CA personnel;
- All operational personnel that are authorized to have access to the system are required to use hardware tokens to gain access to the physical room and hardware tokens in conjunction with a PIN to gain access to the system;
- All security related events are audited and the audit records are maintained on a dedicated logging device.

The desired functionality is provided by the operating system, the cryptographic module, the CA software, physical protection and by the combination of those.

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

System security management is controlled by the privileges assigned to operating system accounts, and by the trusted roles described in section 5.2.1.

6.6.3 Life cycle security ratings

The NIIF Institute has established a risk assessment methodology that identifies and addresses all high or significant life cycle security threats.

6.7. Network Security Controls

The CA system is connected to a highly secured internal network which separated from other networks by firewalls. Remote access to CA system via the administration software interface – which is connected to the internal network with the same security requirements - is secured using the security features of the authentication and encryption features of the Secure Socket Layer Protocol and the installed firewalls.
The NIIF Institute has established a risk assessment methodology that identifies and addresses all high or significant network security threats.

6.8. Cryptographic Module Engineering Controls

The cryptographic module used by NIIF CA is designed to conform to FIPS 140-1 level 3 requirements. Optional hardware tokens may be used to generate Key Pairs that may conform with other levels of FIPS validation, but which must at least conform to level 1.

7 CERTIFICATE AND CRL PROFILES

7.1. Certificate Profile

7.1.1 Version number(s)

The NIIF CA supports and uses X.509 Version 3 Certificates, which contain v.3 in the version field.

7.1.2 Certificate extensions

The NIIF CA supports and uses X.509 Version 3 Certificate extensions.

7.1.3 Algorithm object identifiers

The following hash/digest algorithms are supported:

- Secure Hash Algorithm-1 – (x500 oid:1.3.14.3.2.26)
- Message Digest 5 - (x500 oid: 1.2.840.113549.2.5)

The following signature algorithms are supported:

- RSA - (x500 oid: 1.2.840.113549.1.1.1)

The use of multiple algorithms within the same hierarchy is supported.

7.1.4 Name forms

See section 3.1.1.

7.1.5 Name constraints

See section 3.1.2.

7.1.6 Certificate policy Object Identifier

OIDs are carried in the standard extension field of X.509 Certificates and are published in the CP.

7.1.7 Usage of Policy Constraints extension

Not stipulation.

7.1.8 Usage of Basic Constraints extension

Each issued End Entity certificate must contain the basicConstraints extension, which must be critical and must contain: CA False value.

7.1.9 Policy qualifiers syntax and semantics

The NIIF CA supports the use of syntax and semantics policy qualifiers.

7.1.10 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 supports and uses X.509 Version 2 CRLs.

7.2.2 CRL and CRL entry extensions

The NIIF CA supports and uses X.509 Version 2 CRL entry extensions.

8 SPECIFICATION ADMINISTRATION

8.1. Specification change procedures

Suggested changes to this CPS is communicated to the contact person (see section Contact Details).
There are two possible types of policy change depending on the significance of the change had evaluated by the NIIF CA:

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

If an existing policy requires re-issue, the change process employed 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,
- publishes, in the repository (see section Repositories).

Minor editorial or typographical changes to this CPS 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 given in section 2.6.4.

8.3. CPS approval procedures

All the CPS 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.

9 Appendix A – CP Supported under this CPS

The following CPs are supported under this CPS:

- NIIF GRID User CP, OID 1.3.6.1.4.1.11914.1.1.2.1.4.;
- NIIF GRID Server CP, OID 1.3.6.1.4.1.11914.1.1.3.1.4.;