NIIF Certification Authority

Certificate Policy and
Certificate Practice Statement

Version 2.0

Document OID: 1.3.6.1.4.1.11914.1.1.1.2.0

3 February 2015

Table of Contents

1 INTRODUCTION

This document is based on the framework outlined by IETF RFC 3647 and structured as proposed therein.

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

1.1 Overview

The National Information Infrastructure Development Institute (NIIF Institute, NIIFI) is the Hungarian National Research and Education Network (NREN). This document is the Certification Practice Statement of the NIIF Certification Authority (NIIF CA) and describes the set of rules and procedures used by NIIF CA, and applies to all NIIF CA PKI Participants, including Assurers, Customers, Resellers, Subscribers, Relying Parties and NIIF CA itself.

A number of Certificate Policies may be operated under this CPS.

1.2 Document name and identification

NIIF Certification Authority Certificate Practice Statement (CPS)

Version:	2.0	
Date:	3 February 2015	
OID assigned:	1.3.6.1.4.1.11914.1.1.1.2.0	
	IANA	1.3.6.1.4.1
	NIIF	.11914
	Services	.1
	Policy	.1
	CPS	.1
	Major version	.2
	Minor version	.0

1.3 PKI participants

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 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.

The list of RAs associated with the operation they have permission to perform is available from the NIIF CA website.

1.3.3 Subscribers

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 Relying parties

Relying parties may be:

- natural persons receiving signed e-mails, or accessing hosts or services;
- hosts to which certificate owners login or send processes or jobs;
- services called by owners of a certificate associated with Grid or e-Science related research and development activities.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

CA certificates and their associated private keys may only be used to issue certificates and for checking certificates that claim to be issued by the NIIF CA.

RA certificates and their associated private keys may only be used by the RA agent for RA related activities.

The end-entity certificate may be used for any application that is suitable for X.509 certificates, in particular:

- authentication of users, hosts and services;
- authentication and encryption of communications;
- authentication of signed e-mails;
- authentication of signed objects;

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 are defined in 7.1.2.

1.4.2 Prohibited certificate uses

The certificates issued by NIIF CA must not be used for commercial or financial transactions.

1.5 Policy administration

1.5.1 Organization administering the document

NIIF Institute
H-1132 Budapest
Victor Hugo u. 18-22.
Hungary
Phone: +36 (1) 450-3060
e-mail: ca@niif.hu

1.5.2 Contact person

The manager of the NIIF CA:

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

1.5.3 Person determining CPS suitability for the policy

The manager of the NIIF CA (see 1.5.2) is responsible for determining the CPS suitability for the policy.

1.5.4 CPS approval procedures

The document shall be submitted to EUGridPMA for acceptance and accreditation.

1.6 Definitions and acronyms

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

NIIF	National Information Infrastructure Development (NIIF) Institute having its seat in Budapest, Hungary.
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.

2 PUBLICATION AND REPOSITORY RESPONSIBILITIES

2.1 Repositories

The online repository of information from the NIIF CA is accessible at the URI https://www.ca.niif.hu

2.2 Publication of certification information

The NIIF CA shall maintain a public World Wide Web server with unlimited access. The information made available on this site shall include:

- the NIIF CA root certificate, and all previous ones necessary to check still valid certificates;
- the list of revoked NIIF CA certificates (CRL);
- all valid NIIF CA certificates;
- the CP/CPS document in effect as well as all previous versions;
- if available, documentation to support subscribers who want to use the services of the NIIF CA.

2.3 Time or frequency of publication

The certificates shall be made available as soon as they are issued. The certificate revocation list (CRL) shall have a lifetime of at most 8 days. The NIIF CA must issue a new CRL daily or immediately after having processed a revocation, whichever comes first. A new CRL must be published immediately after its issuance.

2.4 Access controls on repositories

- Certificates, CRL, CP/CPS for NIIF CA are available to the public as read-only information from the NIIF CA web site;
- CRL updates are fully automated and under the control of NIIF CA;
- Modification of website content is only allowed to NIIF employees with proper authorization by NIIF CA Manager (see 1.5.2).

3 IDENTIFICATION AND AUTHENTICATION

3.1 Naming

3.1.1 Types of names

The subject name in certificates issued by this CA is a X.501 distinguished name (DN). A DN has one of the following forms:

- For a person: **C=HU,O=NIIF CA,OU=GRID,[O=<organisation>, [OU=<organisationalunit>,]]CN=<fullname>**, where:
  - *organisation* (optional) is either the official name or one of the well-known abbreviations of the name of the institution the subscriber is affiliated with;
  - *organisationalunit* (optional) is an abbreviation or name referring to the department or other organisational unit the subscriber is affiliated with;

    - *fullname* is the common name of the subscriber;
- For a host or a service: **C=HU,O=NIIF CA,OU=GRID, [O=<organization>,]CN=[servicename/]<fqdn>**, where:
    - *organisation* (optional) is either the official name or one of the well-known abbreviations of name of the institution the subscriber is affiliated with;
    - *fqdn* is the fully qualified domain name of the host;
    - *servicename* is an optional service name

For natural persons, a subject alternative name extension of the type `rfc822Name` must be present with a value that is a valid e-mail address according to RFC822.

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.

E-mail addresses that appear in the alternative name entries must be real addresses to which messages can be sent in order to reach the subject.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers must not be anonymous or pseudonymous. The NIIF CA validates identity of subscribers.

3.1.4 Rules for interpreting various name forms

All characters in the DN components must be mapped to PrintableString (RFC1778).

The CN component of the subject name in a certificate for a natural personal should contain the first and the family name as it appears in the authentication document proving the name of the subscriber. The Hungarian name order is: family name(s) first name(s). It is allowed to leave out any middle names or additional last names, at the discretion of the subscriber. It is also allowed to use the name at birth (maiden name) as the CN component, provided that the information can be verified based on the authentication document.

The CN entry for a host shall be the fully qualified domain name (FQDN) that can be universally used to access that host.

The CN entry for a service shall be the name of the application followed by a slash (“/”) followed by the FQDN of the host on which the application is executed.

3.1.5 Uniqueness of names

The Distinguished Name must be unique for each entity. Individuals must not share certificates.

Two names for a natural person or a service/application are considered identical if they differ only in case or punctuation or whitespace; in other words case, punctuation or whitespace must not be used to make the difference.

The RA must ensure that the DN of a new request does not match the DN of a valid certificate of another entity. In case of a collision of personal names, the common name part of DN of the certificate request may be changed as long as it matches the requirements of section 3.1.4 and is agreed by the subscriber. If the uniqueness of the distinguished names can not be provided in this way, the certificate request must be rejected.

3.1.6 Recognition, authentication, and role of trademarks

No stipulation.

3.2 Initial identity validation

3.2.1 Method to prove possession of private key

The possession of the private key by the requestor is considered proven when the signature of the certificate signing request (CSR) is verified using the public key present in the request.

The subscriber must supply a PIN code along with the certificate request. During the personal authentication (as described in 3.2.3) an RA may request the subscriber enter the PIN into a trusted terminal for verification.

3.2.2 Authentication of organization identity

The RA must have evidence that the requesting person is legally authorised by one of the member institutions of NIIF Institute. If an organisation name is present in the certificate, then this name must refer to the authorising institution. The authorisation document must either assert a legal affiliation between the subscriber and the member institution or provide a permission for the subscriber for obtaining certificates.

The subscriber asking for a certificate for a service or server component must prove that he has the necessary authorisation by providing a legally binding statement made by the representatives of the organisation operating the resource.

If the organisation name is not present in the certificate, the organisational unit name must also be absent.

3.2.3 Authentication of individual identity

The RA personally authenticates any subscriber asking for a certificate, using an officially recognised photo-id card. The RA must store a copy of the identification document.

If a requesting party fails to meet the authentication requirements within 30 days after the request has been received by the RA, the request is void, and a new one has to be submitted.

3.2.4 Non-verified subscriber information

The subject's affiliation to an organisational unit is not verified by the RA. However, the RA shall take steps to verify that the organisational unit exists within the institution by using public resources if the affiliation is not present in the authorisation document (see 3.2.2).

3.2.5 Validation of authority

The authorisation statement of the authorising organisation must be signed by one of its representatives. The RA may use public resources to validate the document.

For host and service certificate requests, the RA must ensure that the authorisation is made by the representatives of the owner of the domain of the FQDN of the host or service. Public resources (such as WHOIS service) and private records might be used for validating the domain ownership.

3.2.6 Criteria for interoperation

No stipulation.

3.3 Identification and authentication for re-key requests

3.3.1 Identification and authentication for routine re-key

Re-key requests either follow the same procedure as an initial registration or the subscriber may use a digitally signed new certificate request signed with the previous certificate sent to the RA before the certificate expiration. 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 contains the name of a certain organization, new legal documents as indicated in Section 3.2.2 must be presented.

3.3.2 Identification and authentication for re-key after revocation

After revocation of a key, no re-key is possible. Initial registration procedures apply (see 3.2).

3.4 Identification and authentication for revocation request

Unless the revocation request originates from the NIIF CA because it has independently verified that a key compromise has occurred, the revocation request has to be verified and the requesting party has to be authenticated.

If the revocation is initiated by the subscriber, the request must be authenticated by

- an e-mail sent to the CA signed with the private key of the (still not expired) certificate;
- using the certificate serial number and the revocation PIN code received on the issuance of the certificate.

If the revocation is initiated by the organisation that consented to the certificate, the request must be made by using an officially signed document or e-mail that is recognised by law.

If the revocation is initiated by an RA, it must be made by e-mail signed by the corresponding RA private key.

In case of emergency if no other methods can be reasonably used, the revocation may be initiated via oral communication with the an RA or the NIIF CA. The RA or the NIIF CA must make their best effort to authenticate the request.

4 CERTIFICATE LIFE-CYCLE OPERATIONAL REQUIREMENTS

4.1 Certificate Application

4.1.1 Who can submit a certificate application

In case of a personal certificate, the application must be submitted by the subject.

In case of a host or service certificate, the application must be submitted by a person who has appropriate administrative rights on the host or service.

4.1.2 Enrollment process and responsibilities

For host and service certificates, the key pair and the PKCS#10 (RFC2986) certificate request must be generated by using appropriate software (i.e. OpenSSL), and the certificate request must be submitted on the enrollment web page of NIIF CA in base64-encoded PEM (RFC1421) format.

In addition to PKCS#10 requests, for personal certificates, the subscriber may generate the key pair and submit the certificate request in his browser by using a designated web interface of the NIIF CA site.

If PKCS#10 format is used, the DN of the request should comply to section 3.1.1.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Rules defined in 3.2 and 3.3 apply.

The RA verifies the documents presented by the subscriber with due diligence.

4.2.2 Approval or rejection of certificate applications

Upon successful authentication of the request, the RA submits the certificate request to the CA signed by its own private key.

If the authentication information proves to be inaccurate or if the requesting party fails to meet the requirements of section 3.2.3, the certificate must be rejected.

4.2.3 Time to process certificate applications

The turn-around time from request to issuance is typically up to 11 days, depending mostly on the authentication process.

Section 3.2.3 specifies the maximum time for the authentication to be performed.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

The CA machine can not be accessed from the network, therefore every CA action is initiated as a scheduled batch job.

As a scheduled job the CA software connects to the designated RA machine and checks if there is any certificate request that is exported for CA signing. The CA downloads the request and verifies that the certificate request was signed by an authorised and valid RA key. If the request is verified, it is signed by the CA private key using the capabilities of its hardware token. The certificate is transferred back to the RA machine for further processing.

4.3.2 Notification to subscriber by the CA of issuance of certificate

As a scheduled batch job, the RA machine checks if there is any new certificate uploaded by the CA. If a new certificate is found, the RA notifies the subscriber via e-mail. The notification e-mail contains the signed certificate and a machine-generated revocation PIN and is signed by the RA agent's certified private key.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

The certificate is assumed to be accepted by the subscriber unless the subscriber explicitly rejects it via authenticated communication with the RA. The subscriber must reject the certificate if it is not associated with the keypair he/she intended to certify.

By accepting a certificate, the subscriber warrants that according to his/her knowledge no unauthorised person has had access to the private key associated with the certificate.

4.4.2 Publication of the certificate by the CA

The RA agent copies the certificate to the public CA repository (see 2.1).

4.4.3 Notification of certificate issuance by the CA to other entities

The RA agent sends a copy of the certificate to the RA.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

Certificates issued by the NIIF CA and their associated private keys must only be used according to the permissions and prohibition stated in section 1.4. They must only be used according to the key usage fields of the certificate.

When a certificate is revoked or has expired the associated private key shall not be used any more.

4.5.2 Relying party public key and certificate usage

A relying party must, upon being presented with a certificate issued by the NIIF CA, check

- its validity by
    - checking that it trusts the CA that issued the certificate;
    - checking that the certificate hasn't expired;
    - consulting the NIIF CA CRL in effect at the time of use of the certificate or querying the certificate's validity using the OCSP facility, after its planned installation;
- the appropriate usage according to the usage keys included in the certificate.

4.6 Certificate renewal

Certificate renewal is not supported by the NIIF CA.

4.6.1 Circumstance for certificate renewal

Not applicable.

4.6.2 Who may request renewal

Not applicable.

4.6.3 Processing certificate renewal requests

Not applicable.

4.6.4 Notification of new certificate issuance to subscriber

Not applicable.

4.6.5 Conduct constituting acceptance of a renewal certificate

Not applicable.

4.6.6 Publication of the renewal certificate by the CA

Not applicable.

4.6.7 Notification of certificate issuance by the CA to other entities

Not applicable.

4.7 Certificate re-key

4.7.1 Circumstance for certificate re-key

Re-key of a certificate is allowed for a revoked certificate, an expired certificate and a valid certificate.

4.7.2 Who may request certification of a new public key

The owner of a valid certificate may request the certification of a new public key in a CSR also signed with his/her still valid private key.

If the certificate has already expired a certificate request procedure as described for an initial certification request must be followed.

4.7.3 Processing certificate re-keying requests

See 4.2.

4.7.4 Notification of new certificate issuance to subscriber

See 4.3.2

4.7.5 Conduct constituting acceptance of a re-keyed certificate

See 4.4.1

4.7.6 Publication of the re-keyed certificate by the CA

See 4.4.2

4.7.7 Notification of certificate issuance by the CA to other entities

See 4.4.3

Certificate modification

4.7.8 Circumstance for certificate modification

Certificates must not be modified. The old certificate must be revoked, and a new key pair must be generated and a request for the modified certificate contents submitted with the new public key. The revocation may be conditional on the issuance and acceptance of the new certificate, and thus the old certificate will only be revoked after the new one is accepted.

4.7.9 Who may request certificate modification

The owner of the original certificate may submit the requests for re-key and revocation as per 4.7.2 and 4.8.3 respectively.

4.7.10 Processing certificate modification requests

Not applicable.

4.7.11 Notification of new certificate issuance to subscriber

Not applicable.

4.7.12 Conduct constituting acceptance of modified certificate

Not applicable.

4.7.13 Publication of the modified certificate by the CA

Not applicable.

4.7.14 Notification of certificate issuance by the CA to other entities

Not applicable.

4.8 Certificate revocation and suspension

4.8.1 Circumstances for revocation

A certificate must be revoked if:

- its associated private key has been (or is suspected to be) compromised or lost;
- its contents have become or proved to be inaccurate;
- it is not needed any more;
- the consenting organisation/unit withdraws its consent.

Should the private key of the NIIF CA be compromised or lost, all certificates signed with it shall be revoked.

4.8.2 Who can request revocation

The revocation request can be issued by

- the owner of the certified key
- the NIIF CA or any RA that has proof of a compromise
- the organisation/unit that wants to revoke its consent to its inclusion in the certificate

4.8.3 Procedure for revocation request

The revocation request must be authenticated as described in 3.4.

4.8.4 Revocation request grace period

No grace period shall be defined for a revocation request. The NIIF CA shall process the authenticated request with priority and publish the revocation as fast as possible.

4.8.5 Time within which CA must process the revocation request

The NIIF CA will process the revocation request within one working day.

4.8.6 Revocation checking requirement for relying parties

Relying parties must check the revocation status of a certificate before its validation.

4.8.7 CRL issuance frequency

CRLs are issued immediately after each revocation and at least once in a day.

4.8.8 Maximum latency for CRLs

The posting of the CRL to the repository is within one hour from its generation.

4.8.9 On-line revocation/status checking availability

The NIIF CA provides an on line repository (OCSP, see section 2.1) for verifying the status of certificates issued within the NIIF CA.

4.8.10 On-line revocation checking requirements

Relying Parties must confirm the validity of a certificate via the CRL and/or OCSP prior to relying on the Certificate.

4.8.11 Other forms of revocation advertisements available

No stipulation.

4.8.12 Special requirements re key compromise

No stipulation.

4.8.13 Circumstances for suspension

Certificate suspension is not supported by NIIF CA.

4.8.14 Who can request suspension

Not applicable.

4.8.15 Procedure for suspension request

Not applicable.

4.8.16 Limits on suspension period

Not applicable.

4.9 Certificate status services

4.9.1 Operational characteristics

NIIF CA offers its CRL and OCSP service publicly available to allow Relying Parties to verify the validity of the certificates signed by NIIF CA. Both the CRL and the OCSP Responder contain information for all NIIF CA's non-expired revoked certificates.

The CRL is archived as described in section 5.5.

4.9.2 Service availability

Both the CRL and the OCSP Responder services operate 24x7. The services are operated by the system administrators of NIIF Institute.

4.9.3 Optional features

No stipulation.

4.10 End of subscription

The subscription ends with the expiry of the certificate if it is not renewed before that date.

The subscription may end earlier if the certificate is revoked for any reason.

4.11 Key escrow and recovery

Not supported.

4.11.1 Key escrow and recovery policy and practices

Not applicable.

4.11.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 FACILITY, MANAGEMENT, AND OPERATIONAL CONTROLS

5.1 Physical controls

The NIIF CA makes every reasonable effort to detect and prevent material breaches, loss, damage or compromise of assets and interruption to business activities.

5.1.1 Site location and construction

The NIIF CA performs its CA operations in a the NIIF data centre located in Hungary, in the same building as NIIF Institute is based.

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. Different kinds of physical security devices are installed including

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

Every access to the security zone is logged. Unauthorized personnel and visitors must be 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

Removable media shall be stored in locked safe places to which only authorised personnel have access.

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

The on-line servers implementing NIIF CA service are backed up by using the regular backup procedures of NIIF servers, which may or may not be off-site. Because the machine hosting the CA private key is not accessible from the backup server, it is not backed up but the server image is archived.

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* who is responsible for the continuous secure operation of NIIF CA equipment;
- *RA* who is responsible for authenticating subscribers and delivering the trusted certification and revocation requests to the CA;
- *CA Administrator* who configures and manages the CA agent in compliance with this CPS;
- *Security Officer* who is responsible for security audit and monitoring logs;
- *Security Trustee* who is responsible for activating CA private key.

5.2.2 Number of persons required per task

At least one person per role is required. Section 6.2.2 contains additional information on key activation.

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.

5.2.4 Roles requiring separation of duties

An individual having Security Officer role must not have other trusted roles defined in 5.2.1.

5.3 Personnel controls

5.3.1 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 are trained in:

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

5.3.4 Retraining frequency and requirements

Retraining shall be mandatory when new software or features, as well as new organisational procedures are introduced.

Any changes in CPS is communicated to the NIIF CA personnel as soon as possible.

5.3.5 Job rotation frequency and sequence

Not 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 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

All NIIF CA personnel shall be provided with all documentation required for successfully performing their task.

5.4 Audit logging procedures

5.4.1 Types of events recorded

At a minimum, the following events must be recorded on all NIIF CA equipment:

- boot and shutdown;
- logins and logouts;
- incoming and outgoing certification requests and revocation requests;
- certificate issuance;
- scheduled job information, including CRL generation and publication.

5.4.2 Frequency of processing log

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

5.4.3 Retention period for audit log

Audit logs are retained as archive records. The audit logs are kept on NIIF's central log server for a minimum period of 6 months.

5.4.4 Protection of audit log

Only authorised system administrators of NIIF can access the audit logs.

Log messages of the signing operations are chained (contain a cryptographic checksum of the previous message) in order to detect tampering with log messages.

5.4.5 Audit log backup procedures

Backup of the audit logs shall be performed at least once a week.

5.4.6 Audit collection system (internal vs. external)

Audit event records are collected on NIIF's central log server, external to the CA equipment.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

NIIF CA is constantly (24x7) monitored and all attempts to gain unauthorized access to any of the services are logged and analyzed.

5.5 Records archival

5.5.1 Types of records archived

The following data files must be archived:

- audit logs (see 5.4.1);
- every issued certificate;
- every issued certificate revocation list;
- documents attached to certification or revocation requests.

5.5.2 Retention period for archive

Audit logs are archived from the log server and kept on read-only media for a minimum period of 1 year.

Other archived records are kept for a minimum period of 3 years.

5.5.3 Protection of archive

Only authorised system administrators of NIIF can access the archive records.

Only authorised RAs and individuals performing CA audit can access archived documents attached to certification and revocation requests.

5.5.4 Archive backup procedures

Backup of the archive is performed on a daily basis.

5.5.5 Requirements for time-stamping of records

All event records shall have a timestamp.

5.5.6 Archive collection system (internal or external)

Archive data is collected in external systems.

5.5.7 Procedures to obtain and verify archive information

Not defined.

5.6 Key changeover

The NIIF CA's keys should be changed while sufficient validity time (see 6.3.2) remains on the existing keys to allow uninterrupted validity of all subordinate keys. The following procedure should be followed 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.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

Online nodes of the NIIF CA infrastructure is actively monitored in order to detect problems of the infrastructure. The CA Administrator periodically examines the logs of the restricted CA node for the signs of intrusion or hardware errors.

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

Installation steps for bootstrapping the NIIF CA infrastructure are recorded and backed up. The private key is backed up as described in 6.2.4. Internal databases containing the state of the CA software is backed up via the online RA node.

In case of a corruption, the NIIF CA infrastructure can be rebuilt based on the backups if the private key (or its backup) remains accessible. Subscribers and relying parties are notified about the service disruption via the NIIF CA website.

5.7.3 Entity private key compromise procedures

- If the keys of an end entity are lost or compromised, a NIIF RA must be informed immediately in order to revoke the certificate. The owner of the certificate can do this by himself using the NIIF CA website
- If NIIF CA's private key is (or suspected to be) compromised, the CA will:
  - inform the Registration Authorities, subscribers and relying parties of which the CA is aware;
  - revoke all issued certificates issued using the compromised key;
  - revoke the compromised key;
  - subscribers are notified via the NIIF CA website or personally.
- If one of the RA's private key is (or suspected to be) compromised, the CA must be informed without delay. The certificate must be revoked immediately. The CA together with the RA shall start without delay investigating the damage to and loss of information stored at the RA in order to minimise the impact on all end entities and relying parties concerned.

5.7.4 Business continuity capabilities after a disaster

Not defined.

5.8 CA or RA termination

In case of termination of its services NIIF CA will:

- make all reasonable efforts to inform subscribers and RAs as soon as possible,
- announce the termination as widely as possible,
- cease issuing certificates,
- revoke all certificates, and
- destroy all copies of private keys of NIIF CA.

6 TECHNICAL SECURITY CONTROLS

6.1 Key pair generation and installation

6.1.1 Key pair generation

RAs must generate their key pairs by using hardware tokens.

Other subscribers may use hardware tokens or software for key pair generation.

The key pair for the NIIF CA is generated as a ceremony supervised in person by:

- the manager of the NIIF CA (see 1.5.2);
- at least one person with *CA Administrator* role;
- at least one person with *Security Officer* role (see 5.2.1).

The key pair for the NIIF CA is generated on a computer which is not connected to the network. The private key is generated on volatile storage protected by a passphrase. The key is backed up as described in 6.2.4 and then loaded into an initialised FIPS 140-2 Level 3 certified tamper proof device before signing any certificate but the CA itself. The private key is removed immediately after being loaded into the HSM.

6.1.2 Private key delivery to subscriber

Each requesting party (including RA's) must generate its own key pair.

6.1.3 Public key delivery to certificate issuer

The RA authenticating the request delivers the public key of the subject to the CA in a signed certification request by using a web application.

6.1.4 CA public key delivery to relying parties

The NIIF CA public key is published on the NIIF CA public repository (see 2.1).

6.1.5 Key sizes

The NIIF CA uses RSA public key algorithm. The CA private key must be a length of 2048 bits.

The RA private key must have a minimum length of 2048 bits.

All other private keys must have a minimum length of 1024 bits.

6.1.6 Public key parameters generation and quality checking

No stipulation.

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

The keys may be used according to the type of certificate:

- With an end-entity certificate for
    - authentication
    - data and key encipherment
    - message integrity
    - session establishment
    - proxy creation and signing (RFC3820)
- With an RA certificate (certificate issued to Registration Authority) for all activities needed for the work of an RA agent
- With the CA certificate
    - certificate signing
    - CRL signing

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

All copies on NIIF CA private key is stored on FIPS140-2 Level 3 Hardware Security Modules, operated on FIPS140-2 Level 3 mode. The Hardware Security Module is locked in the chassis of the CA machine.

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

End entities must not use multi-person control to their private keys.

NIIF CA uses multi-person control for accessing the private key backup. At least two people is required for restoring the NIIF CA private key.

6.2.3 Private key escrow

Not available.

6.2.4 Private key backup

For the NIIF CA, the private key is backed up during the key generation ceremony (see 6.1.1) in the following way:

1. the encrypted private key is saved in an offline media, which is stored in well protected safe;
2. the encryption passphrase is distributed using n out of m multi-person control (see 6.2.2);
3. parts of the encryption passphrase must be stored in different locked safes that must not be the same as the one that stores the encrypted private key.

Subscribers are responsible for the backup of their encrypted private keys.

6.2.5 Private key archival

NIIF CA private key is stored in encrypted form.

6.2.6 Private key transfer into or from a cryptographic module

NIIF CA private key is never exposed from the HSM in any form. NIIF CA private key is loaded into the the Hardware Sercurity Module during key generation (see 6.1.1) on a machine that is not connected to any network.

6.2.7 Private key storage on cryptographic module

The HSM must not allow exporting the private key and must require activation data for key operations.

6.2.8 Method of activating private key

The activation data of NIIF CA signing key is stored on volatile media on the CA machine. Before starting the CA, the activation data must be entered on a local console by at least two authorized personnel using n out of m multi-person control.

6.2.9 Method of deactivating private key

The activation data of NIIF CA is removed whenever the CA machine is powered down or rebooted, or when the Hardware Security Module containing the private key is detached from the machine.

6.2.10 Method of destroying private key

Keys can be destroyed by erasure of appropriate key container or using user initiated tamper which causes all data on the HSM to be erased. Backups of the private key must to be destroyed by appropriate means.

6.2.11 Cryptographic Module Rating

The HSM of the NIIF CA is FIPS140-2 Level 3 certified.

6.3 Other aspects of key pair management

6.3.1 Public key archival

No public key archiving service is available. Instead, all issued certificates are archived.

6.3.2 Certificate operational periods and key pair usage periods

The self-signed certificate of NIIF CA is valid for 20 years. Certificates for other entities shall be valid for at most 395 days.

6.4 Activation data

6.4.1 Activation data generation and installation

For NIIF CA private key, the activation data is the user PIN on the HSM hosting the private key, which is generated during the key generation ceremony (see 6.1.1). The private key must not be activated without the user PIN.

6.4.2 Activation data protection

NIIF CA activation data is shared using n out of m multi-person control. Parts of the activation data must be securely protected by its holders. See 6.2.9 for details about deactivating the key.

6.4.3 Other aspects of activation data

After multiple unlocking failures, the HSM must lock out the user PIN, in which case the private key hosted by the HSM becomes inaccessible.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

All nodes of the CA equipment (see 6.7) are running Linux with OpenCA software. The RA node receives regular software patches in at least weekly manner. The CA image is updated only if absolutely necessary.

Administrator access to the RA node is restricted to SSH by using public key authentication. Only certified NIIF CA personnel can access the RA node.

Administrator access to the CA node is restricted to console login by using secure passphrases. Every person having CA Administrator role has his/her own user and passphrase on the CA node.

6.5.2 Computer security rating

No stipulation.

6.6 Life cycle technical controls

6.6.1 System development controls

No stipulation.

6.6.2 Security management controls

No stipulation.

6.6.3 Life cycle security controls

No stipulation.

6.7 Network security controls

NIIF CA equipment comprises of two lightweight computers hard-wired in a single chassis: the *RA node* and the *CA node*. The chassis has one network connection that is connected to a stateful packet filtering firewall and is terminated by the RA node.

Only the following kinds of traffic is allowed in the direction of the RA node:

- accessing the RA web interface from known static IP addresses of RA workstations;
- backup the RA node;
- actively monitor the RA node;
- secure remote access from known static administrator IP adresses.

The RA node can only initiate network traffic for the following purposes:

- accessing certification and revocation request that are submitted on a public web interface;

- publishing certificates and CRLs on the NIIF CA public repository;
- sending out notification e-mails through a smarthost;
- feeding log information to the external log server;
- synchronising its clock using NTP servers;
- accessing the domain name system.

The RA node and the CA node are directly cabled together inside the chassis. The CA node has no other network connections. The CA node implements its own stateful packet filtering firewall, configured in a way that it can not be accessed from any host, including the RA node. The RA node does not route traffic to and from the CA node.

The CA node can only initiate network traffic to the RA node for the following purposes:

- (as a scheduled batch job) accessing certification and revocation requests that are signed by an RA and submitted to the CA for signing;
- (as a scheduled batch job) publishing certificates and CRLs on a defined location of the RA node for further processing (publication and notification);
- providing audit log information using the RA node as an intermediate log server;
- synchornising its clock using the RA node as an NTP server.

The CA node is not connected to any routed network nor to any IP gateway.

6.8 Time-stamping

All online servers synchronise their clocks to public and private time sources using NTP protocol.

The CA node synchronises its clock using the RA node as a single NTP server.

7 CERTIFICATE, CRL, AND OCSP PROFILES

7.1 Certificate profile

NIIF CA issues certificates conforming to Internet PKI Profile for X.509 Certificates as defined in RFC3280.

7.1.1 Version number(s)

Only X.509 version 3 certificates are issued by NIIF CA.

7.1.2 Certificate extensions

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

The following extensions shall be present in certificates issued by NIIF CA

- *for natural persons*
  - Basic Constraints: **CRITICAL**, `CA: FALSE`
  - Key Usage: **CRITICAL**
    - `digitalSignature`
    - `keyEncipherment`
    - `dataEncipherment`
  - Extended Key Usage:
    - `clientAuth` (1.3.6.1.5.5.7.3.2)
    - `emailProtection` (1.3.6.1.5.5.7.3.4)
  - Subject Alternative Name
    - `rfc822Name`: alternative e-mail address of the entity
  - Certificate Policies: the OID of this document (see 1.2)
  - Authority Key Identifier: composed of the 160 bit SHA-1 hash of the issuer's public key
  - Subject Key Identifier: composed of the 160 bit SHA-1 hash of the subject's public key
  - CRL Distribution Points: `URI: http://crl2.ca.niif.hu`
  - Authority Access Info:
    - CA Issuers: `URI: http://crt.ca.niif.hu/niif-ca-root.crt`
    - OCSP: `URI: http://ocsp2.ca.niif.hu`
- *for hosts and services*
  - Basic Constraints: **CRITICAL**, `CA: FALSE`
  - Key Usage: **CRITICAL**
    - `digitalSignature`
    - `keyEncipherment`
    - `dataEncipherment`
  - Extended Key Usage:
    - `serverAuth` (1.3.6.1.5.5.7.3.1)
    - `clientAuth` (1.3.6.1.5.5.7.3.2)
  - Subject Alternative Name
    - `dNSName`: alternative fully qualified domain name(s) of the entity
  - Certificate Policies: the OID of this document (see 1.2)
  - Authority Key Identifier: composed of the 160 bit SHA-1 hash of the issuer's public key
  - Subject Key Identifier: composed of the 160 bit SHA-1 hash of the subject's public key
  - CRL Distribution Points: `URI: http://crl2.ca.niif.hu`
  - Authority Access Info:
    - CA Issuers: `URI: http://crt.ca.niif.hu/niif-ca-root.crt`

        - OCSP: `URI: http://ocsp2.ca.niif.hu`
- *for an OCSP server*:
    - Basic Constraints: **CRITICAL**, `CA: FALSE`
    - Key Usage:
        - `digitalSignature`
    - Extended Key Usage
        - `OCSPSigning`
    - Subject Alternative Name
        - `dNSName`: alternative fully qualified domain name(s) of the entity
    - Certificate Policies: the OID of this document (see 1.2)
    - Authority Key Identifier: composed of the 160 bit SHA-1 hash of the issuer's public key
    - Subject Key Identifier: composed of the 160 bit SHA-1 hash of the subject's public key
    - CRL Distribution Points: `URI: http://crl2.ca.niif.hu`
    - Authority Access Info:
        - CA Issuers: `URI: http://crt.ca.niif.hu/niif-ca-root.crt`
- *for the NIIF CA* (root CA certificate)
    - Basic Constraints: **CRITICAL**, `CA: TRUE`
    - Key Usage: **CRITICAL**
        - `CertSign`
        - `CRLSign`
    - Authority Key Identifier: composed of the 160 bit SHA-1 hash of the public key of the NIIF CA
    - Subject Key Identifier: composed of the 160 bit SHA-1 hash of the public key of the NIIF CA
    - CRL Distribution Points: `URI: http://crl2.ca.niif.hu`
    - Authority Access Info:
        - CA Issuers: `URI: http://crt.ca.niif.hu/niif-ca-root.crt`
        - OCSP: `URI: http://ocsp2.ca.niif.hu`

7.1.3 Algorithm object identifiers

The NIIF CA issues certificates using the following algorithms:

- rsaEncryption (OID 1.2.840.113549.1.1.1)
- sha256WithRSAEncryption (OID 1.2.840.113549.1.1.11)

7.1.4 Name forms

The distinguished name of the NIIF CA issuer is `C=HU, O=NIIF, OU=Certificate Authorities, CN=NIIF Root CA 2`.

For distinguished names of other entities see section 3.1.

7.1.5 Name constraints

Constraints are defined in 3.1.

The NIIF CA does not use the nameConstraints extension.

7.1.6 Certificate policy object identifier

Certificate policy extension is set according to 7.1.2.

7.1.7 Usage of Policy Constraints extension

Not used.

7.1.8 Policy qualifiers syntax and semantics

Not used.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

The NIIF CA issues CRLs in accordance with CRL version 2 format as defined in the international standard X.509 version 3.

7.2.2 CRL and CRL entry extensions

The NIIF CA uses the following CRL extensions:

- AuthorityKeyIdentifier: composed of the 160 bit SHA-1 hash of the public key of the NIIF CA
- CRL Number: sequence number of the issued CRL

7.3 OCSP profile

The NIIF CA operates an OCSP responder supporting OCSP protocol (RFC 2560). A response is signed every 24 hours or immediately after a certificate revocation. The `nextUpdate` field of a response is set to the time of its `thisUpdate` field increased by 96 hours.

7.3.1 Version number(s)

The NIIF CA OCSP responder uses the OCSP protocol version 1.

7.3.2 OCSP extensions

The NIIF CA OCSP responder does not support any OCSP extensions. In particular, the NIIF CA does not use a cryptographic nonce in connection with its OCSP services. Instead, local time should be used by participants to ensure the freshness of the OCSP response.

8 COMPLIANCE AUDIT AND OTHER ASSESSMENTS

8.1 Frequency or circumstances of assessment

NIIF CA shall make at least once a year a self-assessment to check the compliance of the operation with the CP/CPS document in effect.

The CA shall at least once a year assess the compliance of the procedures of each RA with the CP/CPS document in effect.

8.2 Identity/qualifications of assessor

No stipulation.

8.3 Assessor's relationship to assessed entity

No stipulation.

8.4 Topics covered by assessment

No stipulation.

8.5 Actions taken as a result of deficiency

In case of a deficiency, the NIIF CA responsible will announce the steps that will be taken to remedy the deficiency, including a timetable. If a discovered deficiency has direct consequences on the reliability of the certification process, the certificates (suspected to be) issued under the influence of this problem shall be revoked immediately.

8.6 Communication of results

The NIIF CA staff will make the result publicly available on the NIIF CA web site with all relevant details.

9 OTHER BUSINESS AND LEGAL MATTERS

9.1 Fees

9.1.1 Certificate issuance or renewal fees

No fees are charged for issuing certificates.

9.1.2 Certificate access fees

None.

9.1.3 Revocation or status information access fees

None.

9.1.4 Fees for other services

None.

9.1.5 Refund policy

Not available.

9.2 Financial responsibility

No financial responsibility is accepted.

9.2.1 Insurance coverage

Not available.

9.2.2 Other assets

Not available.

9.2.3 Insurance or warranty coverage for end-entities

No stipulation.

9.3 Confidentiality of business information

9.3.1 Scope of confidential information

No stipulation.

9.3.2 Information not within the scope of confidential information

No stipulation.

9.3.3 Responsibility to protect confidential information

No stipulation.

9.4 Privacy of personal information

9.4.1 Privacy plan

The privacy policy of the NIIF CA service is defined in this CPS.

9.4.2 Information treated as private

Any information about Subscribers and their Requesters that is not publicly accessible or available through the content of the issued certificate, a CRL, or an OCSP response is treated as private information.

Private information shall not be released to outside the NIIF CA and the RA performing the registration.

9.4.3 Information not deemed private

Certificates, CRLs, the OCSP, and the information appearing in them are not considered private. By requesting a certificate, the Subscriber consents that the personal data within the certificates and the content of the revocation request will be published without restriction.

9.4.4 Responsibility to protect private information

The responsibility to protect private information rests with the NIIF CA and all its accredited RAs.

9.4.5 Notice and consent to use private information

The subscriber is notified about the privacy plan in electronic form.

9.4.6 Disclosure pursuant to judicial or administrative process

Persuant to a judicial or administrative process private information shall only be released upon presentation of a regular warrant issued according to the Hungarian law.

9.4.7 Other information disclosure circumstances

No stipulation.

9.5 Intellectual property rights

Parts of this document are inspired or even copied from the CP/CPS documents of AustrianGrid CA, CERN CA, CESNET CA, GARR CA, Terena eScience Personal CA, Terena eScience Server CA and maybe indirectly from documents they draw from.

Anybody may freely copy any parts of this CP/CPS document provided they include an acknowledgement of the source.

9.6 Representations and warranties

9.6.1 CA representations and warranties

The information published in the certificates, CRLs and OCSP responses are accurate to the best of NIIF CA's knowledge. No other warranties are accepted.

9.6.2 RA representations and warranties

All accredited RAs shall perform their task of identification of the requesting parties as described in 3.2.2 and 3.2.3 to the best of their knowledge. No other warranties are accepted.

9.6.3 Subscriber representations and warranties

No stipulation.

9.6.4 Relying party representations and warranties

No stipulation.

9.6.5 Representations and warranties of other participants

No stipulation.

9.7 Disclaimers of warranties

See 9.6.1.

9.8 Limitations of liability

Except if dictated otherwise by the Hungarian law the NIIF CA declines any liability for damages incurred by a relying party accepting one of its certificates, or by a subscriber whose valid certificate is refused or whose revoked certificate is unduly accepted by a relying party.

It also declines any liability for damages arising from the non-issuance of a requested certificate, or for the revocation of a certificate initiated by the CA or the appropriate RA acting in conformance with this CP/CPS.

9.9 Indemnities

The NIIF CA declines any payment of indemnities for damages arising from the use or rejection of certificates it issues. End entities shall idemnify and hold harmless the NIIF CA and all appropriate RAs operating under this CP/CPS against all claims and settlements resulting from fraudulent information provided with the certificate application, and the use and acceptance of a certificate which violates the provisions of this CP/CPS document.

9.10 Term and termination

9.10.1 Term

This document becomes effective after its publication on the Web site of the NIIF CA starting at the date announced there.

No term is set for its expiration.

9.10.2 Termination

This CP/CPS remains effective until it is superseeded by a newer version.

9.10.3 Effect of termination and survival

Its text shall remain available for at least 5 years after the last certificate issued under this CP/CPS expires or is revoked.

9.11 Individual notices and communications with participants

All communications between CA and RAs must happen in a secure way.

9.12 Amendments

9.12.1 Procedure for amendment

Amendments to this CP/CPS must undergo the same procedures as for the initial approval (see 1.5.4). Rephrasing provisions to improve their understandability as well as pure spelling corrections are not considered amendments.

9.12.2 Notification mechanism and period

Planned changes will be advertised on the CA web site and sent to all the RAs at least 15 days in advance.

9.12.3 Circumstances under which OID must be changed

Each non trivial change will require a change of the OID.

9.13 Dispute resolution provisions

Disputes arising out of the CP/CPS shall be resolved by the manager of the NIIF CA (see 1.5.2).

9.14 Governing law

The NIIF CA and its operation are subject to the Hungarian law. All legal disputes arising from the content of this CP/CPS document, the operation of the NIIF CA and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by NIIF CA shall be treated according to Hungarian law.

9.15 Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of a NIIF CA certificate must comply with the Hungarian law. Activities initiated from or destined for another country than Hungary must also comply with that country’s law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS document superseeds any prior agreements, written or oral, between the parties covered by this present document.

9.16.2 Assignment

No provisions.

9.16.3 Severability

Should a clause of the present CP/CPS document become void because it is conflicting with the governing law (see 9.14) or because it has been declared invalid or unenforceable by a court or other law-enforcing entity, this clause shall become void (and should be replaced as soon as possible by a conforming clause), but the remainder of this document shall remain in force.

9.16.4 Enforcement (attorneys' fees and waiver of rights)

No stipulation.

9.16.5 Force Majeure

Events that are outside the control of NIIF CA will be dealt with immediately by the EUGridPMA.

9.17 Other provisions

No stipulation.