CERN

European Organization for Nuclear Research

Category: CP/CPS

Status: published

Document: CERN LCG IOTA Certification Authority Certificate Policy and Certificate Practice Statement

Editors: Paolo Tedesco, Emmanuel Ormancey

Date created: September 28, 2015 14:13

Last updated: January 28, 2016 11:18

Number of pages: 40

CERN LCG IOTA Certification Authority Certificate Policy and Certificate Practice Statement

Paolo Tedesco, Emmanuel Ormancey

CERN IT/OIS

Version 1.0, Revision 1

Document OID: 1.3.6.1.4.1.96.10.7.2.1.1.0

Table of contents

1 Introduction

1.1 Overview

The European Organization for Nuclear Research (CERN) is an intergovernmental organization having its seat in Geneva, Switzerland[1].

This document is the combined Certificate Policy and Certification Practice Statement of the CERN certification authority infrastructure capable of issuing Security Token Service certificates for e-Science authentication.

The infrastructure will be referred to as "CERN LCG IOTA Certification Authority" in the rest of this document, and it comprises both the actual PKI services and all the other services (web services, APIs) involved in the certificates enrollment process.

This document describes the set of procedures followed by the CERN LCG IOTA Certification Authority.

This document is structured according to RFC 3647[2]. The latter does not form part of this document and only the information provided in this document may be relied on.

1.2 Document name and identification

This document is named *CERN LCG IOTA Certification Authority Certificate Policy and Certificate Practice Statement*. The following ASN.1 Object Identifier (OID) has been assigned to this document: 1.3.6.1.4.1.96.10.7.2.1.1.0

This OID is constructed as shown in the table below:

IANA	1.3.6.1.4.1
CERN	.96
CERN CA	.10
CERN Certification Authority 2	.7
Documents	.2
CP-CPS	.1
Major Version	.1
Minor Version	.0

1.3 PKI participants

1.3.1 Certification authorities

The CERN LCG IOTA Certification Authority provides PKI services to identity federation users; it does not issue certificates to subordinate Certification Authorities.

Its certification relies on CERN Root Certification Authority 2 (CP/CPS document 1.3.6.1.4.1.96.10.4.2.1.1.1, available on web site http://cafiles.cern.ch/cafiles).

1.3.2 Registration authorities

The CERN LCG IOTA Certification Authority ensures the authentication of individual identities combining the data provided by:

- The Registration Authorities of the institutions participating to the identity federation
- The LHC VO Management Service (VOMS), which in turn relies on information stored in the CERN HR database

Depending on the nature of a person's association with CERN, personal information is gathered by the appropriate CERN Registration Authority:

- For members of personnel, as defined in Administrative Circular 11[3], except for Unpaid Associates and USERs, registration is carried out by the HR Department.
- For Unpaid Associates and USERs it is carried out by the CERN Users Office.
- For the staff of CERN contractors it is carried out by the Registration Service.

These services complete and validate the data in the CERN HR database after various identity checks. Each person is assigned a status, classifying his relationship with CERN.

1.3.3 Subscribers

The CERN LCG IOTA Certification Authority issues only Security Token Service certificates for persons (user certificates) to applications registered as clients of the STS service.

1.3.4 Relying parties

Relying parties are individuals or organizations using the certificates to verify the identity of subscribers and to secure communication with this subscriber. Relying parties may or may not be subscribers within this CA.

1.3.5 Other participants

No stipulation.

1.4 Certificate usage

1.4.1 Appropriate certificate uses

Certificates issued within the scope of this CP may be used by subscribers for purposes of Grid authentication.

1.4.2 Prohibited certificate uses

Any certificate use is permissible only if the limitations in the registration process and therefore the restrictions on the liability are accepted for the intended purpose.

1.5 Policy administration

1.5.1 Organization administering the document

CERN - European Organization for Nuclear Research
Policy Management Authority (PMA)

CH-1211 Geneva
Switzerland

Tel: +41 22 767 6111
http://www.cern.ch , https://www.cern.ch/ca

1.5.2 Contact persons

Paolo Tedesco

CERN - European Organization for Nuclear Research
CH-1211 Geneva
Switzerland

Tel: +41 22 767 0898
Paolo.Tedesco@cern.ch

Emmanuel Ormancey

CERN - European Organization for Nuclear Research
CH-1211 Geneva
Switzerland

Tel: +41 22 767 1057
Emmanuel.Ormancey@cern.ch

A **mailing list** containing CERN CA Managers has been setup to ensure quick response:

cern-ca-managers@cern.ch

1.5.3 Person determining CPS suitability for the policy

CERN CA Managers (see 1.5.2) determine 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:

CERN status	Classification of a person's relationship with CERN. Examples are STAFF, USER, UPAS (unpaid associate), ENTC (employee of a CERN contractor)
CERN user	A person registered in the CERN HR database with an active status.
CERN USER	(**Note the uppercase USER**). A CERN user registered with the status "USER" in the CERN HR database. This status corresponds to people employed by an external institute who are participating in a CERN experiment.

Certificate	Equivalent to Public Key Certificate.
Certification Authority (CA)	An entity trusted by one or more users to create and assign public key certificates and be responsible for them during their whole lifetime.
Certificate Policy (CP)	A named set of rules that indicates the applicability of a certificate to a particular community and/or class of application with common security requirements.
Certification 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.
Public Key Certificate	A data structure containing the public key of an end entity and some other information, which is digitally signed with the private key of the CA which issued it.
Policy Management Authority (PMA)	An entity establishing requirements and best practices for Public Key Infrastructures.
Registration Authority (RA)	An entity that is responsible for identification of the end entity, 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 “CERN RA” is equivalent to RA.
Security Token Service (STS)	Service providing short-duration user certificates to a requesting application.

2 Publication and repository responsibilities

2.1 Repositories

The CERN LCG IOTA Certification Authority is only accessible programmatically, through the Security Token Service online application, which is a soap service available at the address https://sts.cern.ch:8443/sts/wstrust.

2.2 Publication of certification information

The files and information required to use the services provided by the CERN LCG IOTA Certification Authority are provided through a website at the following address: http://cafiles.cern.ch/cafiles

The files distributed through this site include:

Certificates of the root and intermediate certification authorities

Certificate revocation lists (CRLs) of the root and intermediate certification authorities

All past and current versions of the CP-CPS documents of the root and intermediate certification authorities

2.3 Time or frequency of publication

- Full CRL is published every 24 hours, and after each request of revocation of a certificate for security reasons.
- New versions of CP/CPS are published as soon as they have been approved.

2.4 Access controls on repositories

- CRL, CP and CPS for the CERN LCG IOTA Certification Authority are available to the public as read-only information from the web site: http://cafiles.cern.ch/cafiles.
- CRL updates are fully automated and under the control of the CERN LCG IOTA Certification Authority.
- Modification of CP and CPS is only allowed to CERN employees with proper authorization by CERN CA Managers.

3 Identification and authentication

3.1 Naming

3.1.1 Types of names

The subject name of **user certificates** issued by this CA is a X.500 distinguished name (DN) in the following form:

CN=*Unique ID*, O=*Federation*, DC=STS, DC=CERN, DC=CH

- *Unique ID* is a federation-wide unique identifier for the user.
- *Federation* is the name of the identity provider that issued the credentials that the user authenticated with when the certificate request was performed.

The subject name of **proxy certificates** issued by this CA is a X.500 distinguished name (DN) in the following form:

CN=*Proxy ID*, CN=*Unique ID*, O=*Federation*, DC=STS, DC=CERN, DC=CH

- *Proxy ID* is a random identifier for the certificate.
- *Unique ID* and *Federation* are the same values of the user certificate used to sign the proxy certificate.

3.1.2 Need for names to be meaningful

The Subject Name in a certificate must have a reasonable association with the authenticated name of the subscriber: it contains a unique ID of the user to ensure uniqueness.

While the unique ID does not need to contain information about the identity of the user, it must be possible to associate it to the identity of a user. This association is ensured by the VOMS registration process.

3.1.3 Anonymity or pseudonymity of subscribers

Subscribers must not be anonymous or pseudonymous. The CERN RA, implied in the VOMS registration process, validates the identity of subscribers.

3.1.4 Rules for interpreting various name forms

Many languages have special characters that are not supported by the ASCII character set used to define the subject or the organization name in the certificate. To work around this problem local substitution rules can be used:

- In general national characters are represented by their ASCII equivalent. E.g. é, è, à, ç are represented by e, e, a, c.
- The German “umlaut” characters may receive special treatment: ä, ö, ü are represented by either ae, oe, ue or a, o, u.

3.1.5 Uniqueness of names

The Subject Name included in the CN part of a certificate must be unique for all certificates issued by the CERN LCG IOTA Certification Authority.

This unique ID provided by identity providers must be reserved and cannot be reused after user account closure or deletion.

Only accounts belonging to IdPs capable of providing a unique and not reusable ID are eligible to obtain a certificate from the CERN LCG IOTA Certification Authority.

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 client application requesting a certificate proves the possession of the private key by signing the certificate request with the private key before submitting it to the CERN LCG IOTA Certification Authority.

The CERN LCG IOTA Certification Authority verifies the possession of the private key by accepting only signed certificate requests.

3.2.2 Authentication of organization identity

No stipulation.

3.2.3 Authentication of individual identity

Certificates are issued only to selected users of the EduGAIN identity federation, who are fully registered in the VOMS service as members of one of the LHC VOs.

In order to be registered as a member of an LHC VO, the user is requested to be physically present at the appropriate registration service, and to present his national ID card or passport.

Additionally, a user must be authenticated by an EduGAIN identity provider capable of providing a unique and persistent (non-reassigned) identifier for the user in the SAML assertions of the authentication token, typically through the "eduPersonPrincipalName" attribute (ePPN).

3.2.4 Non-verified subscriber information

None.

3.2.5 Validation of authority

No stipulation.

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

Certificate re-key is not supported, and the user has to request a new certificate.

3.3.2 Identification and authentication for re-key after revocation

A revoked certificate cannot be renewed; user has to request a new certificate.

3.4 Identification and authentication for revocation request

Revocation requests must be submitted to the CERN CA Managers by opening a support ticket with the CERN Service Desk (service-desk@cern.ch).

Given the short validity period of certificates issued by the CERN LCG IOTA Certification Authority, certificate revocation can only be requested for security reasons or by anyone who can prove possession of a private key by an unauthorized party.

4 Certificate life-cycle operational requirements

4.1 Certificate Application

4.1.1 Who can submit a certificate application

To request a certificate a user must:

- be authenticated by an Identity Provider belonging to the EduGAIN federation, capable of providing a unique and persistent identifier for the user in the SAML assertions of the authentication token (typically through the "eduPersonPrincipalName" attribute)
- be fully registered in the VOMS service as members of one of the LHC VOs

4.1.2 Enrolment process and responsibilities

Certificates are generated by one of the Security Token Services (STS) of the CERN LCG IOTA Certification Authority, upon request by a client application.

Each STS service is dedicated to a single client application, and accepts requests only from that application. Additionally, the STS service is restricted to issue certificates only for a set of allowed VOs. Currently, the following STS service endpoints are defined:

STS endpoint	Client application	Allowed VOs
https://sts.cern.ch:8443/sts/wstrust	WebFTS	Atlas

Client applications authenticate to the service with the user's federated credentials, and request the creation of an STS certificate for the user in the context a virtual organization.

The client application starts the process by generating a public / private key pair couple, and submitting a request to the STS service, containing:

- The public key of a key pair generated by the client application
- The user's SAML authentication token, which must include an attribute with a federation-wide unique and persistent identifier for the user
- The name of a Virtual Organization to which the user belongs, and for which the STS service instance is allowed to release certificates

The Security Token Service will query user's data in the LCG VOMS service for the specified VO, using the value of the eduPersonPrincipalName SAML attribute to uniquely identify the user.

If the query is successful, meaning that the user has a valid registration in VOMS for the given VO, then the STS service will request a user certificate to the internal PKI service.

The STS service generates a new private/public key pair, and uses it to sign a Certificate Signing Request for the user certificate. The CSR is then submitted to the internal PKI service through a SOAP application, accessible only from inside CERN.

The STS service authenticates to the internal PKI service with a robot certificate issued by the CERN Grid Certification Authority. Only the STS service account is authorized to request certificates to the internal PKI service.

The user certificate obtained from the internal PKI service has a lifetime of one week. The user certificate could be cached by the STS service to be reused for future requests.

The user certificate, once obtained, will in turn be used to sign a proxy certificate for the user in the context of that VO. The proxy certificate will contain the VOMS extensions for the user and the public key that was sent in the initial request from the client application.

Finally, the proxy certificate will be returned to the client application from the STS service.

4.2 Certificate application processing

4.2.1 Performing identification and authentication functions

Users must have a computer account belonging to an EduGAIN service provider with valid credentials in order to authenticate to the CERN LCG IOTA Certification Authority Security Token Service and request a certificate.

Additionally, the Identity Provider must issue a claim in the user's SAML token with a federation-wide unique and persistent identifier for the user.

Users' authentication is performed using the CERN Single Sign On infrastructure, using any available authentication method.

4.2.2 Approval or rejection of certificate applications

Certificate requests are automatically approved or rejected by the CERN LCG IOTA Certification Authority infrastructure by verifying that all the issuance conditions are met (see the requirements expressed in 4.1.1).

4.2.3 Time to process certificate applications

Certificate issuing and processing is done immediately: identity verification has been made previously by the federated identity providers and the CERN RA, and is mandatory to proceed with the request for a certificate.

4.3 Certificate issuance

4.3.1 CA actions during certificate issuance

No stipulation.

4.3.2 Notification to subscriber by the CA of issuance of certificate

The Security Token Service delivers the issued certificate to the client application that made the request. No other notification mechanism is provided.

4.4 Certificate acceptance

4.4.1 Conduct constituting certificate acceptance

No stipulation.

4.4.2 Publication of the certificate by the CA

The CERN LCG IOTA Certification Authority does not publish end entity certificates.

4.4.3 Notification of certificate issuance by the CA to other entities

No stipulation.

4.5 Key pair and certificate usage

4.5.1 Subscriber private key and certificate usage

By accepting the certificate the subscriber assures all participants of the CERN LCG IOTA Certification Authority and all parties relying on the trustworthiness of the information contained in the certificate that:

- All data and statements given by the subscriber in relation to the information contained in the certificate are truthful and accurate.
- The private key will be maintained in a safe and secure manner.
- No unauthorized person has or will ever have access to the private key.
- The certificate will solely and exclusively be used in accordance with this Certificate Policy.
- Immediate action will be undertaken on the subscriber's part to revoke the certificate if the private key is missing, stolen, or is in any other way compromised.

4.5.2 Relying party public key and certificate usage

Every person using a certificate issued within the framework of this CP for purposes of authentication

- must verify the validity of the certificate before using it.
- must use the certificate solely and exclusively for authorized and legal purposes in accordance with this CP.
- should have a basic understanding of the use and purpose of certificates.

4.6 Certificate renewal

Certificate renewal is not supported. A new key pair is generated for every request.

4.7 Certificate re-key

Certificate re-key follows the same procedures of an initial certificate request. See sections 4.1, 4.2 and 4.3.

4.8 Certificate modification

Certificates must not be modified. In case of changes, a new certificate must be requested.

4.9 Certificate revocation and suspension

This section explains the circumstances under which a certificate should be revoked. No provision is made for the suspension (temporary invalidity) of certificates. Once a certificate has been revoked, it may not be renewed or extended.

4.9.1 Circumstances for revocation

Certificates must be revoked by the CERN LCG IOTA Certification Authority should at least one of the following circumstances be known:

- The private key of a subscriber has been stolen, published or compromised and/or misused in any other manner.
- The subscriber does not comply with the terms and conditions of the CP.
- The CERN LCG IOTA Certification Authority or RA does not comply with the terms and conditions of the CP or the CPS.
- The certification service is discontinued.
- The CERN LCG IOTA Certification Authority private key is compromised.

4.9.2 Who can request revocation

Any subscriber may request the CERN LCG IOTA Certification Authority to revoke his certificate for security reasons, i.e. if the certificate is known or suspected to be compromised.

The requester will also need to provide a brief description of the security incident, which will be submitted to the CERN Computer Security Team to evaluate the security risk for the CERN computing infrastructure.

Acceptance of a revocation request of a certificate is conditional on the successful identification and authentication of the subscriber in accordance with section 3.4.

The CERN RA is also allowed to ask a certificate revocation from CERN CA Staff, in case of compromise of a key.

The CERN CA staff can revoke any certificate for security reasons.

4.9.3 Procedure for revocation request

If the conditions to acceptance of the request (see section 4.9.2) are met, the certificate will be revoked.

4.9.4 Revocation request grace period

Should circumstances for revocation of a certificate exist (see section 4.9.1), the subscriber is obliged to notify the CERN LCG IOTA Certification Authority immediately of the same, and to initiate revocation of the certificate.

4.9.5 Time within which CA must process the revocation request

The CERN LCG IOTA Certification Authority will process a request for revocation of a certificate as soon as possible if the conditions to acceptance of the request (see section 4.9.2) are met.

4.9.6 Revocation checking requirement for relying parties

The provisions of section 3.4 apply.

4.9.7 CRL issuance frequency (if applicable)

The provisions of section 2.3 apply.

4.9.8 Maximum latency for CRLs (if applicable)

The provisions of section 2.3 apply.

4.9.9 On-line revocation/status checking availability

CRLs are available from the URL given in the associated CPS section 2.2.

4.9.10 On-line revocation checking requirements

Prior to every usage of the certificate, its validity should be checked. The relevant standards are given in section 7.2 (CRL Profile) and section 7.3 (OCSP Profile) of the CPS.

4.9.11 Other forms of revocation advertisements available

Currently no other forms of revocation advertisements are available.

4.9.12 Special requirements regarding re-key compromise

Should a private key become compromised, the certificate so affected shall immediately be revoked. Should the private key of the CERN LCG IOTA Certification Authority become compromised, all certificates issued by the CERN LCG IOTA Certification Authority shall be revoked.

4.9.13 Circumstances for suspension

Suspension of certificates is not supported.

4.9.14 Who can request suspension

Not applicable.

4.9.15 Procedure for suspension request

Not applicable.

4.9.16 Limits on suspension period

Not applicable.

4.10 Certificate status services

No Online Certificate Status Protocol service is provided.

4.10.1 Operational characteristics

Not applicable.

4.10.2 Service availability

Not applicable.

4.10.3 Optional features

Not applicable.

4.11 End of subscription

The term of the contractual relationship is given by the period of validity as indicated in the certificate.

The minimum period for the archiving of documents and certificates corresponds to the period of validity of the certificate of the CERN LCG IOTA Certification Authority with the addition of a further period of one year.

4.12 Key escrow and recovery

The CERN LCG IOTA Certification Authority does not support key escrow and recovery.

4.12.1 Key escrow and recovery policy and practices

Not applicable.

4.12.2 Session key encapsulation and recovery policy and practices

Not applicable.

5 Facility, management and operational controls

5.1 Physical controls

5.1.1 Site location and construction

The CERN LCG IOTA Certification Authority is hosted in CERN Computer Center.

5.1.2 Physical access

Physical access to CERN LCG IOTA Certification Authority is restricted to authorized personnel of the CERN CA.

5.1.3 Power and air conditioning

The critical CERN LCG IOTA Certification Authority equipment is connected to uninterrupted power supply units, and CERN Computer Center is running uninterrupted air conditioners.

5.1.4 Water exposures

No floods are expected in CERN Computer Center.

5.1.5 Fire prevention and protection

CERN Computer Center is equipped with various smoke and fire detectors.

5.1.6 Media storage

The CERN LCG IOTA Certification Authority key is kept in several removable storage media. Backup copies of CA related information are kept on CD-Roms or DVD-Roms. Removable media are stored in a secure location.

5.1.7 Waste disposal

All CERN LCG IOTA Certification Authority paper waste MUST be shredded. Electronic media MUST be physically/mechanically destroyed before disposal.

5.1.8 Off-site backup

No off-site backups are currently performed.

5.2 Procedural controls

5.2.1 Trusted roles

No stipulation.

5.2.2 Number of persons required per task

One CERN CA staff only is required.

5.2.3 Identification and authentication for each role

No stipulation.

5.2.4 Roles requiring separation of duties

No stipulation.

5.3 Personnel controls

5.3.1 Qualifications, experience, and clearance requirements

The role of the CA requires a suitably trained person that is familiar with the importance of a PKI, and who is technically and professionally competent. There are no background checks or clearance procedures for trusted or other roles.

5.3.2 Background check procedures

No stipulation.

5.3.3 Training requirements

Internal training is given to CERN CA and RA operators.

5.3.4 Retraining frequency and requirements

No stipulation.

5.3.5 Job rotation frequency and sequence

No stipulation.

5.3.6 Sanctions for unauthorized actions

No stipulation.

5.3.7 Independent contractor requirements

No stipulation.

5.3.8 Documentation supplied to personnel

Personnel assigned to the CA operation have access to a restricted website were all operational procedures can be found, as well as this document.

5.4 Audit logging procedures

5.4.1 Types of events recorded

The following events are recorded in the CA log:

- Backup and restore the CA database
- Change CA configuration
- Change CA security settings
- Issue and manage certificate requests
- Revoke certificates and publish CRLs
- Store and retrieve archives keys

The following events are recorded in the server log:

- Login/Logout
- Reboot

5.4.2 Frequency of processing log

Log is 300MB size, and is automatically archived to a file when 100% full.

5.4.3 Retention period for audit log

Logs are kept on CD-Rom/DVD-Rom for at least 3 years.

5.4.4 Protection of audit log

Audit logs are only accessible to the administrators of the CERN LCG IOTA Certification Authority and to authorized audit personnel.

5.4.5 Audit log backup procedures

Every archive log file is burned on a CD-Rom or a DVD-Rom.

5.4.6 Audit collection system (internal vs. external)

Audit collection is internal to the CERN LCG IOTA Certification Authority service.

5.4.7 Notification to event-causing subject

No stipulation.

5.4.8 Vulnerability assessments

The CERN LCG IOTA Signing Certification Authority 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 archives

The CERN LCG IOTA Certification Authority keeps record of:

- All certificate requests
- All issued certificates
- All revoked certificates
- Certificate Revocation Lists
- Login and reboot information of the servers operating the infrastructure

5.5.2 Retention period for archive

The minimum retention period is 3 years.

5.5.3 Protection of archive

The records archived is accessible to CERN CA personnel only.

5.5.4 Archive backup procedures

Records are archives on removal media (CD-Rom, DVD-Rom) and are stored in a restricted access area.

5.5.5 Requirements for time-stamping of records

All records are saved with an automatically generated time stamp.

5.5.6 Archive collection system (internal or external)

Archiving system is CERN internal.

5.5.7 Procedures to obtain and verify archive information

No stipulation.

5.6 Key changeover

The rekeying of the CERN LCG IOTA Certification Authority certificate shall be performed 6 months in advance of the certificate expiration date, to ensure that the new certificate can be distributed before it starts being used to sign certificates.

After the rekey, all newly issued end-entity certificates will be signed by the new certificate.

The old CA certificate will be available for its normal validity period, and will be used only to sign the CRL containing the revocation information for the certificates signed with the old CA certificate.

In parallel, a new CRL will be distributed, signed with the new CA certificate. The new CRL will contain revocation information for the certificates signed with the new CA certificate.

5.7 Compromise and disaster recovery

5.7.1 Incident and compromise handling procedures

If the keys of an end entity are lost or compromised, the CERN RA must be informed immediately in order to revoke the certificate.

In case the CERN LCG IOTA Certification Authority private key is compromised, provisions in 5.7.3 apply.

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

The CERN CA operators will ensure that recovery procedures are functional and up to date.

All CERN LCG IOTA Certification Authority software and system will be backed up (encrypted backup) on a daily basis. In case of corruption or hardware failure, a new functioning hardware will be installed and the latest working and not-corrupted state of the CERN LCG IOTA Certification Authority software and data will be restored.

If needed, the CERN LCG IOTA Certification Authority issuing Private Key stored in the Hardware Security Module will be restored according HSM's restore procedures (see 6.2.4), therefore operations should restart without any certificate revocation.

5.7.3 Entity private key compromise procedures

In case the private key of the CERN LCG IOTA Certification Authority is compromised, the CERN CA will:

- Inform the Registration Authorities, subscribers and relying parties of which the CA is aware.
- Make a reasonable effort to notify the responsible of the STS services client applications.
- Terminate the certificates and CRL distribution services for certificates and CRLs issued using the compromised key.

- Request revocation of the compromised certificate.
- Generate a new CERN LCG IOTA Certification Authority key pair and certificate and publish the certificate in the repository.
- Revoke all certificates signed using the compromised key.
- Publish the new CRL on the CERN LCG IOTA Certification Authority repository.

5.7.4 Business continuity capabilities after a disaster

Provisions for data backup and hardware/software failures detailed in sections 5.7.1, 5.7.2 and 5.7.3 apply.

5.8 CA or RA termination

Before CERN LCG IOTA Certification Authority terminates its services, it will:

- Inform the relying parties (STS service clients) the CA is aware of;
- Make information of its termination widely available;
- Stop issuing certificates
- Revoke all certificates
- Generate and publish CRL
- Destroy its private keys and all copies

An advance notice of at least 60 days will be given in the case of scheduled termination. The CERN CA Manager at the time of termination will be responsible for the subsequent archival of all records as required in section 5.5.2.

6 Technical security controls

6.1 Key pair generation and installation

6.1.1 Key pair generation

- The private key of the CERN LCG IOTA Certification Authority is generated by the HSM module, following HSM instructions and using the HSM Administrator toolkit. A strong password is also required to generate the key pair.
- The Security Token Service generates the key pairs used to request user certificates (which are in turn used for proxy signing).
- Clients of the Security Token Service generate the key pairs used to request proxy certificates.

6.1.2 Private key delivery to subscriber

The CA does not generate private keys for its subscribers and therefore does not deliver private keys to subscribers.

6.1.3 Public key delivery to certificate issuer

Subscribers' public keys are delivered to the CA by the Security Token Service, as part of the Certificate Signing Request submitted through the internal SOAP service.

6.1.4 CA public key delivery to relying parties

The CERN LCG IOTA Certification Authority public key is delivered to subscribers through the secure website http://cafiles.cern.ch/cafiles (see chapter 2).

6.1.5 Key sizes

Keys of length less than 2048 bits are not accepted. The CERN LCG IOTA Certification Authority key is 4096 bits long.

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 proxy certificate for
  - authentication
  - session establishment
- With a user certificate for
  - proxy certificate signing
- With the CA certificate
  - certificate signing
  - CRL signing

The CA's private key is the only key that can be used for signing CRLs.

6.2 Private Key Protection and Cryptographic Module Engineering Controls

6.2.1 Cryptographic module standards and controls

The CERN LCG IOTA Certification Authority private key is protected by a Safenet ProtectServer External Hardware Security Module (HSM), FIPS140-2 Level 3 certified.

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

No stipulation.

6.2.3 Private key escrow

Private keys must not be escrowed.

6.2.4 Private key backup

The private key is backed up from the HSM module using the 'multiple custodians method': the key is split into multiple shares and then distributed to multiple custodians. The shares are encrypted (wrapped) by a second key called the wrapping key which is selected at random.

The scheme to split the key into multiple shares is done in such a way that the original key will only be recovered with the co-operation of all the custodians.

Each custodian is a smart card secured by a password PIN. Smart Card reader is connected to the parallel port on the back of the HSM. All PIN and Key exchange sessions between the smart card and the HSM are encrypted.

Each smart card has its own PIN number and user name and belongs to one CERN CA Staff who is responsible for it.

The restore procedure is the same as backup. All custodians (smart cards) are read one by one by the HSM.

6.2.5 Private key archival

Private key archival is not supported.

6.2.6 Private key transfer into or from a cryptographic module

Keys are never exposed from the HSM in clear form. All key transfers are encrypted, and occur only during backup and restore procedures (see 6.2.4).

6.2.7 Private key storage on cryptographic module

Keys are stored in a battery-backed secure key storage. A battery provides back-up power to the tamper-sensing electronics when no system power is available. Any detected tamper event, including battery removal or disconnection of the secure key storage from HSM, will immediately activate key memory erasure.

6.2.8 Method of activating private key

No stipulation.

6.2.9 Method of deactivating private key

No stipulation.

6.2.10 Method of destroying private key

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

6.2.11 Cryptographic Module Rating

The HSM is FIPS140-2 Level 3 certified.

6.3 Other aspects of key pair management

6.3.1 Public key archival

Public key archival is not supported.

6.3.2 Certificate operational periods and key pair usage periods

The CERN LCG IOTA Certification Authority Certificate has a validity period of 10 years.

The user certificates used by the STS service for proxy signing have a validity period of 1 week. The STS service may cache these certificates to sign multiple proxy certificates with the same user certificate.

The issued proxy certificates have a lifetime of 24 hours.

6.4 Activation data

6.4.1 Activation data generation and installation

The private key is generated by the HSM module, following HSM instructions and using the HSM Administrator toolkit. A strong password is also required to generate the key pair.

6.4.2 Activation data protection

Only CERN CA Staff are allowed and can activate the CA private key.

6.4.3 Other aspects of activation data

No stipulation.

6.5 Computer security controls

6.5.1 Specific computer security technical requirements

The server hosting the CERN LCG IOTA Certification Authority PKI service is based on Microsoft Certificate Services. The server is currently running Microsoft Windows 2008 Enterprise Edition.

The Security Token Service is a soap service running on Scientific Linux servers. The current version of the operating system is Scientific Linux 6.

No other services or software are loaded or operated on these servers. Servers are regularly kept up to date with security patches by the CERN CA Managers or authorized CERN Staff. When appropriate, the operating system versions will be updated, and the existing services migrated to the new operating system.

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

The CERN Root Certification Authority 2 is offline, and must not be connected to any computer network under any circumstances (see CERN Root CA CP/CPS document).

The PKI service issuing user certificates and the Security Token Service are connected to the CERN network, and are protected by the CERN firewall, configured and maintained according to the recommendations of the CERN Security team, for protection from off-site sources.

6.8 Time-stamping

All time stamping of entries created on the online servers at the CERN LCG IOTA Certification Authority is based on the network time provided by the time servers of CERN, which are synchronized with *Navstar Global Positioning System* (GPS).

7 Certificate, CRL, and OCSP profiles

7.1 Certificate profile

All certificates issued by CERN CA conform to the Internet PKI profile (PKIX) for X.509 certificates as defined by RFC 3280.

7.1.1 Version number(s)

Only X.509 version 3 certificates are issued by CERN LCG IOTA Certification Authority.

7.1.2 Certificate extensions

The extensions to the X.509 v3 certificate that shall be present in CERN LCG IOTA Certification Authority certificates are:

For proxy certificates:

- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage (critical): Digital Signature, Key Encipherment
- Enhanced Key Usage: Client Authentication (1.3.6.1.5.5.7.3.2)
- CRL Distribution Points: ldap URI and http URI.
- Certificate Policies: OID of this CP (see 7.1.6) and OID of the Authentication Profile for Identifier-Only Trust Assurance with Secured Infrastructure[4]

For CA certificates:

- Basic Constraints: critical ca: true;
- Subject Key Identifier: hash
- Authority Key Identifier: keyid
- Key Usage: critical, digitalSignature, nonRepudiation, KeyCertSign, cRLSign
- Extended Key Usage timeStamping
- CRL Distribution Points: ldap URI and http URI.
- Certificate Policies: OID

7.1.3 Algorithm object identifiers

The OIDs for algorithms used for signatures of certificates issued by CERN LCG IOTA Certification Authority are according to:

- hash function: sha512 2.16.840.1.101.3.4.2.3
- encryption: rsaEncryption 1.2.840.113549.1.1.1
- signature: sha512RSA 1.2.840.113549.1.1.13

7.1.4 Name forms

Each entity issued by CERN LCG IOTA Certification Authority has a unique and unambiguous Distinguished Name (DN). CERN CA prefers that organizations use domain component naming.

- Issuer subject:
    - CN=CERN LCG IOTA Certification Authority, DC=CERN, DC=CH
- User certificates subject:
    - CN=*Unique ID*, O=*Federation*, DC=STS, DC=CERN, DC=CH
- Proxy certificate subject:
    - CN=*Proxy ID*, CN=*Unique ID*, O=*Federation*, DC=STS, DC=CERN, DC=CH

For the meanings of the fields, see 3.1.1.

7.1.5 Name constraints

There are no other name constraints than those that are to be derived from the stipulations in 7.1.4, 3.1.1 and 3.1.2.

7.1.6 Certificate policy object identifier

The OID of this CP is: 1.3.6.1.4.1.96.10.7.2.1.1.0

7.1.7 Usage of Policy Constraints extension

No stipulation.

7.1.8 Policy qualifiers syntax and semantics

No stipulation.

7.1.9 Processing semantics for the critical Certificate Policies extension

No stipulation.

7.2 CRL profile

7.2.1 Version number(s)

CERN LCG IOTA Certification Authority creates and publishes X.509 v2 CRLs signed with SHA-512 algorithm.

7.2.2 CRL and CRL entry extensions

CERN LCG IOTA Certification Authority issues complete CRLs for all certificates issued by itself. The CRL includes the date by which the next CRL shall be issued. A new CRL must be issued before this date if new revocations are issued.

The CRL extensions that shall be included are:

- The Authority Key Identifier
- The CRL Number

The CRL entry extensions that will be included are:

- CRL Reason Code
- Invalidity Date

8 Compliance audit and other assessments

8.1 Frequency or circumstances of assessment

CERN LCG IOTA Certification Authority 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

The assessments are made by personnel of CERN CA or members of the CERN community. An external audit can be performed by any academic institution or relying party. If other trusted CAs or relying parties request an external assessment, the costs of the assessment must be paid by the requesting party, except for the costs of CERN CA personnel and infrastructure.

8.4 Topics covered by assessment

The audit will verify that the services provided by the CA comply with the latest approved version of the CP/CPS.

8.5 Actions taken as a result of deficiency

In case of a deficiency, the CERN 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 CERN CA staff will make the result publicly available on the CERN CA web site with all relevant details.

9 Other business and legal matters

9.1 Fees

No fees are charged for the CERN LCG IOTA Certification Authority certification service and therefore there are no financial encumbrances.

9.1.1 Certificate issuance or renewal fees

See 9.1.

9.1.2 Certificate access fees

See 9.1.

9.1.3 Revocation or status information access fees

See 9.1.

9.1.4 Fees for other services

See 9.1.

9.1.5 Refund policy

See 9.1.

9.2 Financial responsibility

No Financial responsibility is accepted for certificates issued under this policy.

9.2.1 Insurance coverage

No stipulation.

9.2.2 Other assets

No stipulation.

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

CERN LCG IOTA Certification Authority does not retain any specific private information. All required information is taken from CERN central registration databases, therefore CERN User services privacy plan applies.

9.4.2 Information treated as private
See 9.4.1.

9.4.3 Information not deemed private
See 9.4.1.

9.4.4 Responsibility to protect private information
See 9.4.1.

9.4.5 Notice and consent to use private information
See 9.4.1.

9.4.6 Disclosure pursuant to judicial or administrative process
See 9.4.1.

9.4.7 Other information disclosure circumstances
See 9.4.1.

9.5 Intellectual property rights
CERN LCG IOTA Certification Authority does not claim any intellectual property rights on certificates which are issued.

Parts if this document are inspired or even copied (in no particular order) from the CNRS, the Baltic Grid, pkIRISGrid, SWITCH and may indirectly derive from documents they draw from.

Anybody may freely copy from any version of the CERN LCG IOTA Certification Authority's Certificate Policy and Certification Practices Statement provided they include an acknowledgment of the source.

9.6 Representations and warranties
9.6.1 CA representations and warranties
No stipulation.

9.6.2 RA representations and warranties
No stipulation.

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
CERN LCG IOTA Certification Authority uses software and procedures for the authentication of entities that, to the best of its knowledge, perform as required by this CP/CPS document. However it declines any warranty as to their full correctness. Also CERN LCG IOTA Certification Authority cannot be held responsible for any misuse of its certificate by a

subscriber or any other party in possession of the corresponding private key, and of any unchecked acceptance of any of its certificates by a relying party.

Any relying party that accepts a certificate for any usage for which it was not issued does so on its own risk and responsibility.

9.8 Limitations of liability

CERN LCG IOTA Certification Authority 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

CERN LCG IOTA Certification Authority declines any payment of indemnities for damages arising from the use or rejection of certificates it issues.

End entities shall indemnify and hold harmless CERN LCG IOTA Certification Authority 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 CERN LCG IOTA Certification Authority 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 superseded 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 e-mail communications between the CA and its accredited RAs must be signed with a certified key.

All e-mail communications between the CA or an RA and a subscriber must be signed with a certified key in order to have the value of a proof. All requests for any action must be signed.

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

The amended CP/CPS document shall be published on CERN LCG IOTA Certification Authority Web pages at least 2 weeks before it becomes effective.

CERN LCG IOTA Certification Authority will inform its subscribers and all relying parties it knows of by means of an e-mail.

9.12.3 Circumstances under which OID must be changed

Substantial changes shall cause the OID to be changed. The decision is made by the CERN LCG IOTA Certification Authority manager and submitted to the EUGridPMA for approval.

9.13 Dispute resolution provisions

Disputes arising out of the CP/CPS shall be resolved by the CERN CA manager.

9.14 Governing law

CERN LCG IOTA Certification Authority and its operation are subject to the French and Swiss laws. All legal disputes arising from the content of this CP/CPS document, the operation of CERN LCG IOTA Certification Authority and its accredited RAs, the use of their services, the acceptance and use of any certificate issued by CERN LCG IOTA Certification Authority shall be treated according to French and Swiss laws.

9.15 Compliance with applicable law

All activities relating to the request, issuance, use or acceptance of a CERN LCG IOTA Certification Authority certificate must comply with the French and Swiss laws.

Activities initiated from or destined for another country than France or Switzerland must also comply with that country's law.

9.16 Miscellaneous provisions

9.16.1 Entire agreement

This CP/CPS document supersedes 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 CERN LCG IOTA Certification Authority will be dealt with immediately by the EUGridPMA.

9.17 Other provisions

No stipulation.

10 Bibliography

[1] The European Organization for Nuclear Research – http://www.cern.ch

[2] S. Chokani, W. Ford, R. Sabett, C. Merrill and S. Wu, "Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework", RFC 3647, November 2003 - http://www.ietf.org/rfc/rfc3647.txt

[3] CERN Administrative Circular 11 (this document might require a valid CERN account, or a CERN network connection to be accessed):

http://cern.ch/humanresources/internal/admin_services/admincirc/English.doc/AC-111.pdf

[4] Authentication Profile for Identifier-Only Trust Assurance with Secured Infrastructure Version 4.3, OID 1.2.840.113612.5.2.2.6.1
https://www.eugridpma.org/guidelines/iota/IOTA-Secured-Infra-AP-1.0.pdf