

# Fermilab PKI Certificate Policy and Certification Practices Statement

## INTRODUCTION

### Overview

This document follows the structure suggested in RFC 3647.

The public key infrastructure of Fermilab consists of the Kerberos Certificate Authority (KCA). The KCA is a replicated online service that issues short-lived certificates based on presentation of a Kerberos-authenticated request.

### Identification

Document title

Fermilab PKI Certificate Policy and Certification Practices Statement

Document version

Revision: 1.8

Document date

Date: February 2009

OID

1.3.6.1.4.1.14147.1.8.1.SC 2

### Community and Applicability

This document describes the policies and operation of an infrastructure which will be termed the "Fermilab PKI."

### Certification Authorities

The keys that the Fermilab Kerberos CA certifies are valid for Digital Signature, Certificate Signing, and CRL Signing.

### Registration Authorities

There are three categories of users: employees, visitors and contractors, each registered by a different authority within Fermilab. Employees are registered by Fermilab Personnel Department, visitors by the Users Office and contractors by the Procurement Office. In all cases, approval of the individuals' identity information and legitimate connection with Fermilab is performed. These registration authorities enroll people into a common registry, making them "Fermilab Users" and eligible for certification.

### End Entities

The KCA issues certificates to Fermilab Users and to automated processes acting for users

or services at their instigation. The keys it certifies are valid for Digital Signature and Key Encipherment. Its certificates are intended for use with Grid and Web applications.

### **Contact Details**

The Fermilab PKI is established, maintained and operated by the Fermilab Computer Security Team. The technical contact person for this document is:

Frank J. Nagy  
Fermilab MS-368  
PO Box 500  
Batavia IL 60510  
USA

Phone: +1 630 840 4935

Fax: +1 630 840 8208

Email: [nightwatch@fnal.gov](mailto:nightwatch@fnal.gov)

The policy contact person for this document is:

Irwin Gaines  
Fermilab MS-369  
PO Box 500  
Batavia IL 60510  
USA

Phone: +1 630 840 4022

Fax: +1 630 840 8208

Email: [nightwatch@fnal.gov](mailto:nightwatch@fnal.gov)

## **GENERAL PROVISIONS**

### **Obligations**

#### **CA Obligations**

The Fermilab PKI will:

- Accept Kerberos-authenticated requests for user and robot certificates from Fermilab employees, subcontractors, and visitors, or processes initiated by them.
- Publish CRLs in a timely manner and in well-known locations.
- Protect and, when necessary or prudent, replace CA private keys.

#### **RA Obligations**

RAs are not involved in the handling or verification of cryptographic keys. They are

responsible only for verifying the identities and roles of users and either issuing a physical identification card or establishing a trusted contact path to a Visitor through a Fermilab division or section head or a spokesperson of a Fermilab experiment.

### **Subscriber Obligations**

Subscribers must:

- Make only accurate representations in requests for certificates.
- Exercise all reasonable care in protecting the private keys corresponding to their certificates, including but not limited to never storing them on a networked file system or otherwise transmitting them over a network.
- Ensure that the private keys corresponding to their issued service certificates are stored in a manner that minimizes the risk of exposure.
- Observe restrictions on private key and certificate use.
- Promptly notify the CA operators of any incident involving a possibility of exposure of a private key.

### **Relying Party Obligations**

Relying parties must:

- Be cognizant of the provisions of this document.
- Verify any self-signed certificates to their own satisfaction using out-of-band means.
- Accept responsibility for checking any relevant CRLs before accepting the validity of a certificate.
- Observe restrictions on private key and certificate use.
- Not presume any authorization of an end entity based on possession of a certificate from the Fermilab PKI or its corresponding private key.

### **Liability**

The Fermilab PKI is operated substantially in accordance with Fermilab's own risk analysis. No liability, explicit or implicit, is accepted.

The Fermilab PKI denies any financial or any other kind of responsibility for damages or impairments resulting from its operation.

### **Financial Responsibility**

No financial responsibility is accepted.

## **Interpretation and Enforcement**

This policy is subordinate to all applicable U.S. government laws, as well as Department of Energy (DOE) orders.

### **Fees**

No fees are charged.

## **Publication and Repositories**

### **Publication of CA information**

The Fermilab PKI will operate an online repository that contains:

- Fermilab CA certificates.
- Certificate Revocation Lists.
- A copy of this policy.
- Other information deemed relevant to the Fermilab PKI.

This information will be retained for audit purposes for at least three years.

### **Frequency of Publication**

- CA certificates will be published in the repository as soon as they are issued.
- CRLs will be published as soon as they are updated.
- Fermilab PKI documents will be published in the repository as they are approved.

### **Access Controls**

The CA publication repository is always available, outside of maintenance times and unforeseen failures.

The Fermilab PKI imposes no restrictions on the accessibility of published information.

### **Repository Location**

<http://security.fnal.gov/pki/> (for general information and KCA policy)

and

<http://security.fnal.gov/cookbook/TrustingCertificates.html> (for certificate and CRL repository)

### **Compliance Audit**

The Fermilab PKI will be audited by representatives of the TAG-PMA<sup>[g1]</sup>. Certifying, cross-certifying, and relying organizations may request a review of Fermilab PKI operation.

The CA records and archives all requests for certificates, along with all the issued certificates, all the requests for revocation and the login/logout/reboot of the issuing machine.

The CA keeps these records for at least three years. These records will be made available to external auditors in the course of their work as auditor.

The CA accepts being audited by other IGTF accredited CAs to verify its compliance with the rules and procedures specified in this document.

## **Confidentiality Policy**

The Fermilab PKI does not have access to subscribers' private keys. It considers the contents of CRLs and certificates, including subscribers' names and Fermilab userids, to be public information. For identification of authorized users, it may rely on other organizations within Fermilab, some of which may have private information. If so, the Fermilab PKI does not obtain or store copies of such private information.

## **Intellectual Property Rights**

The Fermilab PKI asserts no ownership rights in certificates issued to subscribers. No claims are made regarding documents produced by the Fermilab CA other than as specified in Fermilab's operating contract with the U.S. Department of Energy. Acknowledgment is hereby given to the DOE Science Grid and to the CERN Certification Authority for inspiration of parts of this document.

# **IDENTIFICATION AND AUTHENTICATION**

## **Initial Registration**

### **Types of Names**

Subject distinguished names are X.500 names, with components varying depending on the type of certificate. Certificates issued by the KCA will include as a Subject Alternative Name the Kerberos principal name which was authenticated for issuance of the certificate.

All subject distinguished names in certificates issued by the Fermilab PKI begin with ``DC=gov, DC=fnal, O=Fermilab''. The next component will be one of:

OU=Certificate Authorities

for a CA's certificate. A CN component will follow the OU, naming the CA, for the KCA this will be "Kerberized CA HSM".

OU=People

for a user's certificate, issued by the KCA. A CN component will follow containing the user's full name, after which will appear a UID component containing the user's

Fermilab computer account name.

OU=Robots

for a certificate issued by the KCA to an automated process acting at the instigation of a user. This is usually followed by a CN component naming the automata; this is "cron" for standard cron jobs. The process can only act for a specific authorized user, and the certificate will contain the user's full name and UID as above. These robot certificates are for use in cron jobs by authorized individuals only, and the certificates are only issued after the same user authentication that is required for individual certificates.

### **Name Meanings**

The CN component of the subject name in user certificates has no semantic significance, but should have a reasonable association with the name of the user.

### **Name Interpretation**

The subject DN of user certificates will contain OU=People. CA Certificates will contain OU=Certificate Authorities.

### **Name Uniqueness**

Each subject name certified by the Fermilab PKI will be unique. User certificates include the Fermilab-assigned account name of the user, which disambiguate any similar or identical common names. Credentials (Kerberos principles) are only issued to specific individuals whose personal information is permanently stored in the laboratory CNAS database.

### **Name Disputes**

The Fermilab PKI will resolve disputes as it sees fit.

### **Method to Prove Possession of Private Key**

No stipulation.

### **Authentication of Individual Identity**

User identity will be authenticated by the KCA through Kerberos 5 credentials. Requests for service certificates must come from a valid Fermilab User and will be checked against registered system administrator information. Private keys must not be shared by end entities (users).

### **Rekeying**

Every user certificate request is treated as an initial registration. Subsequent Service and CA certificate requests also follow the same respective validation steps as initial requests.

### **Revocation Requests**

User certificates, having short lifetimes, will rarely need to be revoked. KCA certificates will only be revoked at the instigation of Fermilab computer security personnel.

## **OPERATIONAL REQUIREMENTS**

### **Certificate Application**

Users apply for user certificates from the KCA using a Kerberos-authenticated protocol. Valid CA and special certificate requests can only come from Fermilab computer security personnel.

### **Certificate Issuance**

User certificates are issued immediately to the user upon successful execution of the Kerberos certificate request protocol. CA and special certificates are issued only to Fermilab computer security personnel.

### **Certificate Acceptance**

No stipulation.

### **Certificate Message Digests**

The message digests are generated by SHA1.

### **Certificate Suspension and Revocation**

Certificates issued by the Fermilab PKI will not be suspended.

### **Circumstances for Revocation**

User certificates, because of their short lifetimes, will rarely need to be revoked. User certificates will be revoked in any of the following circumstances.

- The private key is suspected or reported to be lost or exposed.
- The information in the certificate is believed to be, or to have become inaccurate.
- The certificate is reported to no longer be needed.
- A new certificate with the same Subject DN is to be issued.

### **Requesting Revocation**

Fermilab computer security personnel may request revocation of a CA or user certificate.

### **Verifying Revocation Requests.**

A revocation request signed with the private key of the affected certificate is always valid.

Other revocation requests are subject to the same verification procedures as a corresponding certificate request.

### **CRL Issuance Frequency**

The CRL for the Kerberos CA will be issued upon any change in its contents. Normally the Kerberos CA's CRL will be empty.

### **Online Revocation/Status Checking Availability**

The most recent CRL will be available online.

### **Revocation/Status Checking Requirements**

Relying parties are advised to obtain and consult a valid CRL.

### **Security Audit Procedures**

The CA will maintain a list of the trusted individuals who operate the CA and review this list each year.

### **Records Archival**

Records will be maintained for audit purposes for at least three years..

### **Key Changeover**

The community of known relying parties will be notified of any new CA public key, and they may then obtain it in the same manner as the previous CA certificates. KCA keys will be changed only at long intervals, unless lost or compromised.

### **Compromise and Disaster Recovery**

The KCA is a replicated service, so if one instance is corrupted but uncompromised it will be restored using data from another instance.

If a KCA instance is compromised or corrupted, its certificate must be revoked and a new key generated. This information will be disseminated to subscribers and known relying parties.

### **CA Termination**

When the Fermilab PKI terminates its services the fact will be advertised, particularly to users and known relying parties. All valid CA certificates will be revoked and the final CRLs will be offered for storage at some willing facility.

## **PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS**

## **Physical Security Controls**

The KCA hosts are Dell PowerEdge servers running Windows Server 2003. They are located in keycard-controlled computer rooms where all occupants are required to wear Fermilab ID cards or be accompanied. They run no extraneous network services and are kept current with respect to relevant security patches. Login access is subject to Kerberos authentication and permitted only for principals assigned to Central Support Group Administrators, whose responsibilities are detailed in the Security Infrastructure Major Application Security Plan. There are no shared passwords; any login access is authenticated to a specific individual.

## **Network Security Controls**

The KCA hosts reside within the security infrastructure major application, which has a documented and reviewed security plan describing the security controls to protect the network. This plan is available for review by the PMA. Network controls are in place both at the site border and at the routers and switches which separate network segments inside the border. Controls include static blocking of particular protocols or IP addresses, dynamic blocking when anomalous activity is detected, monitoring of network traffic with both commercial and custom intrusion detection equipment, and scanning for network and system vulnerabilities.

Currently one KCA server resides on network segment 9 in a locked network device room on the 8<sup>th</sup> floor of Wilson Hall. This network segment contains only the KDC and LDAP and windows domain controllers.. The other KCA server resides in the locked computer room on the 2<sup>nd</sup> floor of the Feynmann Computing Center, on network segment 110. This segment contains only security infrastructure devices.

## **Procedural Controls**

No stipulation.

## **Private Key Protection Controls**

The KCA private key is resident in nCipher nShield Hardware Security Modules. Access to the KCA hosts to which the HSMs are attached is protected by physical and network security described above. A written copy of the private key resides in a locked cabinet in a locked office, to which only two members of the Computer Security Team have access. This physical copy can be used to reload the private key into the HSMs during disaster recovery.

## **Personnel Security Controls**

All persons with access to the KCA's private key storage cabinet will be full-time Fermilab employees in the computer security organization.

# TECHNICAL SECURITY CONTROLS

## Key Pair Generation and Installation

### Private Key Generation

The Fermilab KCA infrastructure does not generate any private keys but its own. Its key length is 2048 bits.

User private keys will be generated by KCA client software on the host where they will be stored. They will be stored on non-networked filesystems. They will normally be stored in the clear, but the lifetimes of the associated public-key certificates are limited to the lifetime of the Kerberos credentials used to obtain them, which is cannot be longer than one week.

### Private Key Delivery to Entity

Not necessary.

### Public Key Delivery to Certificate Issuer

User public keys are delivered under Kerberos authentication and integrity protection.

### CA Public Key Delivery to Users

The public key of the KCA is delivered to subscribers and potential relying parties through publication and other unauthenticated channels (except where a secured infrastructure such as PGP or CA cross-certification may already exist) and must be verified through non-digital means to the satisfaction of each relying party.

### Key Sizes

Public RSA keys shorter than 1024 bits will not be signed.

### Key Usage

The Fermilab PKI does not enforce key usage restrictions by any means beyond the X.509v3 extensions in the certificates it issues. In User certificates, those extensions will mark the associated keys as valid for Digital Signature and Key Encipherment. CA certificates will have the Key Usage extension set to allow Digital Signature, Certificate Signing, and CRL Signing.

Certificates issued by the Fermilab PKI are not recommended to be used for non-repudiation, data confidentiality or message integrity.

### Private Key Protection

## **Key Generation Modules**

No stipulation

## **Multiperson Control**

No stipulation.

## **Key Escrow**

Not Supported.

## **Private Key Archival and Backup**

A copy of the KCA private key is kept on a locked cabinet in the locked computer security team office.

## **CA Private Key Activation**

The KCA key can only be activated by access to the Hardware Security Module. That access is restricted to members of the Fermilab computer security team.

## **Other Aspects of Key Pair Management**

End entity keys are not archived by the Fermilab PKI. CA keys are not archived beyond their validity period. The KCA key lifetime is ten years.

## **Activation Data**

The KCA key is resident in the nCipher Hardware Security Module and is not accessible, but is only used to sign appropriate certificate requests.

## **Computer Security Controls**

The KCA runs on computer systems which are used only for Fermilab PKI operations, and which can be accessed only with physical presence or Kerberos network authentication and encryption.

## **Life Cycle Security Controls**

No Stipulation

## **Network Security Controls**

The KCA is behind Fermilab's network perimeter, subject to strict packet filtering and traffic monitoring for intrusion detection.

## **Cryptographic Module Engineering Controls**

No Stipulation

## CERTIFICATE AND CRL PROFILES

End entity certificates are in X509v3 format and are RFC3280 compliant.

### Certificate Profiles

#### User Certificates

Subject:

DC=gov/DC=fnal/O=Fermilab/OU=People/CN=<Full Name>/CN=UID:<acct>

Issuer:

DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Kerberized CA HSM

Validity:

(depends on lifetime of Kerberos ticket presented)

Subject Public Key Info:

(provided by applicant - minimum RSA length is 1024 bits)

X509v3 Extensions

SubjectAltName:

Other Name:

Kerberos Principal:<principal>

Email:<acct>@fnal.gov

Basic Constraints (critical):

CA:false

X509v3 Subject Key Identifier

...

X509v3 Authority Key Identifier

...

Key Usage (critical):

Digital Signature, Key Encipherment

Netscape Cert Type:

SSL Client, SSL Server, S/MIME, Object Signing

Netscape CA Policy URL:

<http://security.fnal.gov/pki/FNAL-Cert-Pol-KCA.pdf>

Netscape Comment:

"User certificate issued by Fermilab Kerberos-based CA"

<acct> represents the first component of the user's Kerberos principal name. <Full Name> is obtained from Fermilab personnel, visitor and contract records.

#### Robot Certificates

Same as user certificates except the subject shows OU=Robot and adds a CN=cron field:

Subject:

DC=gov/DC=fnal/O=Fermilab/OU=Robots/CN=<Full Name>/CN=UID:<acct>/C=cron

## **Certificate Policy Object Identifier**

iso(1) org(3) dod(6) iana(1) private(4) enterprises(1) Fermilab(14147) security(1) documents(5) CPS(1).

## **CRL Profile**

The CRL is in version 2 format.

# **SPECIFICATION ADMINISTRATION**

## **Specification Change Procedures**

Peer PKI operators will be notified of changes.

## **Publication**

The policy will be available at <http://computing.fnal.gov/security/pki/>.

## **CPS Approval Procedures**

The Fermilab computer security team approves practices compliant with this policy and statement.

---

[\[g1\]](#) The profile says " Each SLCS CA must accept being audited by other accredited CAs to verify its compliance with the rules and procedures specified in its CP/CPS document." Representgatives of the TAGPMA are exactly the other accredited CAs described in the profile.