Fermilab PKI Certificate Policy and Certification Practices Statement

May 6, 2003

1. **INTRODUCTION**

1.1. **Overview**

This document follows the structure suggested in RFC 2527.

The public key infrastructure of Fermilab comprises three certificate authorities: the KCA, the Service CA and the Top-Level CA. The KCA is a replicated online service that issues short-lived certificates based on presentation of a Kerberos-authenticated request. The Service CA issues longer-lived certificates for services. The Top-Level CA certifies the other two and is not normally instantiated on any computing device. When the function of the Top-Level CA is needed, its private key is assembled on a non-networked computer with a freshly installed OS. The private key is assembled from shares held by several trusted individuals.

1.2. **Identification**

Document title
Fermilab PKI Certificate Policy and Certification Practices Statement

Document version
Revision: 1.3

Document date
Date: 2003/05/06 19:17:57 UTC

OID
1.3.6.1.4.1.14147.1.5.1

1.3. **Community and Applicability**

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

1.3.1. **Certification Authorities**

The Fermilab Top-Level CA certifies only other Fermilab CAs. Those other CAs are the KCA and the Service CA. The keys it certifies are valid for Digital Signature, Certificate Signing, and CRL Signing.

1.3.2. **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.

1.3.3. **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 Digitial Signature and Key Encipherment. Its certificates are intended for use with Grid and Web applications.

The Service CA issues certificates to services which operate on Fermilab and affiliated computers. Services are either a generic ‘‘host’’ service associated with a specific computer or a more specific service offered on a single computer or a cluster. The keys certified by the Service CA are valid for Digitial Signature and Key Encipherment. Its certificates are intended for use with Grid and Web applications.

1.4. **Contact Details**

The Fermilab PKI is extablished, maintained and operated by the Fermilab Computer Security Team. The contact person for this document is the Fermilab Computer Security Coordinator.

Matt Crawford
Fermilab MS-369
PO Box 500
Batavia IL 60510
USA

Phone: +1 630 840 3461
Fax: +1 630 840 6345
Email: nightwatch@fnal.gov

2. GENERAL PROVISIONS

2.1. Obligations

2.1.1. CA Obligations

The Fermilab PKI will

* Accept service certificate requests and revocation requests from Fermilab authorized system and application maintainers; notify such requesters of issued and revoked certificates.

* Accept Kerberos-authenticated requests for user 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.

  (The Top-Level CA facilitates replacement of KCA and service CA keys with minimal impact on subscribers and relying parties.)

2.1.2. 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 spokeperson of a Fermilab experiment.

2.1.3. 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.

2.1.4. **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.

2.2. **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 and its agents make no guarantee about the security or suitability of a service that is identified by a Fermilab certificate. The certification service is run with a reasonable level of security, but it is provided on a best effort only basis. It does not warrant its procedures and it will take no responsibility for problems arising from its operation, or for the use made of the certificates it provides.

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

2.3. **Financial Responsibility**

No financial responsibility is accepted.

2.4. **Interpretation and Enforcement**

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

2.5. **Fees**

No fees are charged.

2.6. **Publication and Repositories**

2.6.1. **Publication of CA information**

The Fermilab PKI will operate an online repository that contains

* Fermilab CA certificates.

* Certificate Revocation Lists for the Top-Level and Service CAs.

* A copy of this policy.

* Other information deemed relevant to the Fermilab PKI.

2.6.2. **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, or every two weeks if there are no changes.

* Fermilab PKI documents will be published in the repository as they are approved.

2.6.3. **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.

2.6.4. **Repository Location**

http://computing.fnal.gov/security/pki/

2.7. **Compliance Audit**

The Fermilab PKI will not be audited by an outside party. Certifying, cross-certifying, and relying organizations may request a review of Fermilab PKI operation.

2.8. **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.

2.9. **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.

3. **IDENTIFICATION AND AUTHENTICATION**

3.1. **Initial Registration**

3.1.1. **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, issued by the Top-Level CA (or by an external certifying or cross-certifying CA). A CN component will follow the OU, naming the CA.

OU=Services

for a service (including a host) certificate issued by the Service CA. A CN component will follow the OU, naming the service and the fully qualified domain name (FQDN) at which the service can be contacted, separated by a slash character. When the service is https, the service name and separator will be absent, and there may be multiple FQDNs expressed as a sequence of CN components and/or as a regular expression in a single CN component.

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 USERID component containing the user's Fermilab computer account name.

OU=Automata

for a certificate issued by the KCA to an automated process acting at the instigation of a user or service. If the process is acting for a specific user, the user's full name and userid follow as above. Otherwise, this component is followed by an OU component containing the division, section, or experiment responsible for the process and a USERID component containing the Fermilab computer account assigned to the activity.

3.1.2. 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. The CN component of the subject name in service certificates includes the fully qualified DNS name of the service, which is usually that of the host supporting the service. The structure of a service's CN is designed to support SSL, TLS and Globus services.

3.1.3. Name Interpretation

The subject DN of service certificates will contain a component with OU=Services, while that of user certificates will contain OU=People. CA Certificates will contain OU=Certificate Authorities.

3.1.4. 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.

3.1.5. Name Disputes

The Fermilab PKI will resolve disputes as it sees fit.

3.1.6. Method to Prove Possession of Private Key

No stipulation.

3.1.7. 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.

3.2. 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.

3.3. Revocation Requests

Requests for revocation of service certificates from Fermilab computer security personnel and from administrators of the systems hosting the services in question will be honored. User certificates, having short lifetimes, will normally not be revoked. CA Certificates will only be revoked at the instigation of Fermilab computer security personnel.

4. OPERATIONAL REQUIREMENTS

4.1. Certificate Application

Users apply for user certificates from the KCA using a Kerberos-authenticated protocol. System and application administrators may request service certificates by emailing a certificate signing request conforming to Fermilab PKI requirements. Valid CA certificate requests can only come from Fermilab computer security personnel.

4.2. Certificate Issuance

User certificates are issued immediately to the user upon successful execution of the Kerberos certificate request protocol. Service certificates are returned to the requesting system or application administrator through email. CA certificates are issued only to Fermilab computer security personnel.

4.3. Certificate Acceptance

No stipulation.

4.4. Certificate Suspension and Revocation

Certificates issued by the Fermilab PKI will not be suspended.

4.4.1. Circumstances for Revocation

User certificates, because of their short lifetimes, will not normally revoked. Service and CA 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.

4.4.2. **Requesting Revocation**

System or application administrators may request revocation of a service certificate, as can Fermilab computer security personnel. The latter may also request revocation of a CA certificate.

4.4.3. **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.

4.4.4. **CRL Issuance Frequency**

CRLs for the Service and Top-Level CAs will be issued upon any change in their contents, or monthly if there are no changes.

4.4.5. **Online Revocation/Status Checking Availability**

The most recent CRL will be available online.

4.4.6. **Revocation/Status Checking Requirements**

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

4.5. **Security Audit Procedures**

No stipulation.

4.6. **Records Archival**

No stipulation.

4.7. **Key Changeover**

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

4.8. 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 if the Service CA is corrupted or compromised its certificate must be revoked by the Top-Level CA and a new key generated. This information will be disseminated to subscribers and known relying parties.

Compromise of the Top-Level CA would mean the exposure of a theshold number of shares of the private key, while corruption or loss would mean loss of all shares except a sub-threshold set. In either event a new key would be generated and the subordinate CA public keys re-signed. All subscribers and known relying parties would be notified as promptly and directly as possible.

4.9. 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.

5. PHYSICAL, PROCEDURAL, AND PERSONNEL SECURITY CONTROLS

5.1. Physical Security Controls

The KCA and Service CA hosts are Sun Solaris servers 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 ‘‘administrative’’ principals assigned to computer security professionals. These principals are subject to the strongest password length, complexity, and lifetime policy and are not permitted to forward credentials.

5.2. Procedural Controls

The Top-Level CA is not present on any host except when in use to issue a CA certificate or CRL. Its secret key is shared by the Shamir polynomial method. When the key is needed, the OS is booted from unwritable media and shares of the key are loaded, with all participating share holders present. No secrets will be stored on magnetic media during the task. In particular, paging space is not used.

5.3. Personnel Security Controls

All persons with access to a CA’s secret key, or a share of the Top-Level CA’s key, will be full-time Fermilab employees in the computer security organization. When any holder of a share of the Top-Level key leaves the Laboratory, or no longer has a computer security role, the secret key shall be reassembled from shares and divided into new shares. The old shares shall all be destroyed.

6. **TECHNICAL SECURITY CONTROLS**

6.1. **Key Pair Generation and Installation**

6.1.1. **Private Key Generation**

The Fermilab PKI does not generate any private keys but its own. KCA and Service CA keys are generated on the systems where they will be used, and the Certificate Signing Requests will be transported on removable media. The Top-Level CA key is generated on a system booted from unwritable media and split into shares, without intermediate data being stored on magnetic media.

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 is limited to the lifetime of the Kerberos credentials used to obtain them, which is currently no more than 26 hours.

System and service administrators will generate private keys for their services, on the service hosts themselves if at all possible.

6.1.2. **Private Key Delivery to Entity**

Not necessary.

6.1.3. **Public Key Delivery to Certificate Issuer**

User public keys are delivered under Kerberos authentication and integrity protection. Service public keys are delivered, signed, by email and verified by personal contact. CA public keys are hand-carried by computer security personnel.

6.1.4. **CA Public Key Delivery to Users**

The public key of the Top-Level CA 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. The public keys of the KCA and Service CA may then be verified through the Top-Level CA's public key.

6.1.5. **Key Sizes**

Public RSA keys shorter than 512 bits will not be signed. Public RSA keys shorter than 1024 bits will not be certified for a period longer than seven days.

6.1.6. **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 and Service 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.

6.2. **Private Key Protection**

6.2.1. **Key Generation Modules**

No stipulation

6.2.2. **Multiperson Control**

The Top-Level CA's key is held in 3-out-of-7 multiperson control.

6.2.3. **Key Escrow**

Not Supported

6.2.4. **Private Key Archival and Backup**

Not supported.

6.2.5. **CA Private Key Activation**

The Service CA key can be activiated by anyone with login access to the system and the private key's passphrase. That set is restricted to members of the Fermilab computer security team. The Top-Level CA key requires the threshold number of shares to be brought together on a system.

6.3. **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 Top-Level CA key lifetime is five years. The Service CA and KCA key lifetimes are two and one-half years.

6.4. **Activation Data**

The Service CA private key is encrypted under a pass phrase. The KCA key is not encrypted.

6.5. **Computer Security Controls**

The Service CA and KCA run 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, using unforwardable credentials.

The Top-Level CA exists only on a computer booted from unwritable media and only until that computer is shut down or the CA key is erased from memory.

6.6. **Life Cycle Security Controls**

No Stipulation

6.7. **Network Security Controls**

The Top-Level CA will never be connected to a network. The Service CA and KCA are behind Fermilab's network perimeter, subject to strict packet filtering and traffic monitoring for intrusion detection.

6.8. **Cryptographic Module Engineering Controls**

No Stipulation

7. **CERTIFICATE AND CRL PROFILES**

7.1. **Certificate Profiles**

7.1.1. **Service Certificates**

Subject:
  DC=gov/DC=fnal/O=Fermilab/OU=Services/CN=<svcname>/<f.q.d.n>
Issuer:
  DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Service CA
Validity:
   (up to a 13 month period)
Subject Public Key Info:
  (provided by applicant - recommend RSA, 1024 bits)
X509v3 Extensions
  SubjectAltName:

```
    DNS:<f.q.d.n>
    Email:(responsible party or group)
  Netscape SSL Server Name:
    <f.q.d.n>
  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, Object Signing
  Netscape CA Policy URL:
    http://computing.fnal.gov/security/pki/FNAL-Cert-Pol-Svc.pdf
  Netscape Comment:
    "Service certificate issued by Fermilab CA"
```

For a web server, the <svcname> and slash character will be omitted from the Subject Common Name. For a Grid service, the <svcname> will be ‘‘host’’ or some more specific service.

7.1.2. **User Certificates**

```
Subject:
  DC=gov/DC=fnal/O=Fermilab/OU=People/CN=<Full Name>/UserID=<acct>
Issuer:
  DC=gov/DC=fnal/O=Fermilab/OU=Certificate Authorities/CN=Kerberized CA
Validity:
   (depends on lifetime of Kerberos ticket presented)
Subject Public Key Info:
  (provided by applicant - minimum RSA length is 512 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://computing.fnal.gov/security/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.

7.1.3. **Certificate Policy Object Identifier**

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

7.2. **CRL Profile**

The CRL is in version 1 format.

8. **Specification Administration**

8.1. **Specification Change Procedures**

Peer PKI operators will be notified of changes.

8.2. **Publication**

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

8.2.1. **CPS Approval Procedures**

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