Federal Public Key Infrastructure (PKI) Technical Specifications (Version 1)
Part A: Requirements

1. High-Level Requirements 1
    1.1 User Requirements for a Federal PKI 1
    1.2 Management Requirements for Federal PKI 2

2. Functional Requirements for a Federal PKI 3
    2.1 User Requirements for a Federal PKI 3
        2.1.1 Create and Post Certificates 3
        2.1.2 Revoke Certificates 4
        2.1.3 Obtain, Interpret, and Verify Certificates 4
    2.2 Management Requirements for a Federal PKI 5
        2.2.1 Scalability and Manageability 5
        2.2.2 Issue Certificates 6
        2.2.3 Manage Certificates 7
        2.2.4 Ensure Interoperability 8
        2.2.5 Set and Enforce Internal Policy 9
        2.2.6 Set Policy Regarding Non-Federal PKIs 10

3. Detailed Requirements 10
    3.1 PKI Objects 10
        3.1.1 Certificates 11
        3.1.2 Cross-Certificate-Pairs 12
        3.1.3 Certificate Revocation Lists 12
        3.1.4 Compromised Key Lists 12
        3.1.5 Policy Objects 12
    3.2 PKI Components 13
        3.2.1 Policy Approving Authority 13
        3.2.2 Certificate Authorities 13
        3.2.3 Organizational Registration Authorities 14
        3.2.4 PKI Clients 15
        3.2.5 Directory Servers 15

PKI-TWG 96-

Requirements for the Federal Public Key Infrastructure (Version 1)
January 31, 1996
wpolk@nist.gov, editor
This document is an ongoing project of the Public Key Infrastructure
Technical Working Group.

This document defines the functional and technical requirements fort the Federal Public Key Infrastructure (PKI.) A PKI is a certificate management infrastructure which issues and provides access to public key certificates. A federal PKI would support a broad range of security services for the federal government. Implementation of the Federal PKI is the goal of the Federal Public Key Infrastructure Steering Committee (PKI-SC). This document is a product of the PKI-SC's Technical Working Group, and complements the Technical Working Group's *Technical Security Policy* [TSP] and *Concept of Operations* [CONOPS] documents.

The document derives detailed requirements for the various objects and entities which comprise a PKI in an iterative fashion. The document begins by presenting the high-level requirements of users and managers. Functional requirements specific to a PKI meeting these high-level requirements are pstated. Finally, detailed requirements for each component of the PKI are derived from the functional requirements.

1. High-Level Requirements

This section presents the high-level requirements of federal PKI users and managers. These requirements are independent of any particular implementation or architecture for security services.

1.1 User Requirements for a Federal PKI

Federal PKI users need to exchange information and perform electronic commerce across commercial networks while maintaining appropriate and cost-effective security for federal data and applications. Federal PKI users require the ability to participate fully in electronic commerce and communicate securely:

- within their own agencies;
- with the U.S. public and business community;
- with other government agencies;
- with local governments; and
- with foreign entities.

Federal PKI users depend upon insecure government and commercial networks (including the public

switched network, the Internet, and broadcast LANs) and commercial off-the-shelf (COTS) applications due to cost and interoperability considerations. Federal PKI users require security services for this environment with minimal performance impact. Federal users must be able to utilize commercially available security services as well as those provided by the government.

These user requirements can be achieved by development of a federal PKI to support the basic security services (e.g., integrity, confidentiality, and non-repudiation).[1]

1.2 Management Requirements for Federal PKI

Federal management is encouraging the use of commercial networks to increase the efficiency of government and to deliver services more cost-effectively. Provision of security services will allow additional government functions to be performed electronically, enhancing efficiency and reducing cost. However, there are several management requirements that must be met by a federal PKI:

- controlled cost;
- legally binding results;
- access to keys when appropriate; and
- satisfy applicable federal regulations.

The need to control costs implies requirements for COTS products, software-based solutions, and the use of standard protocols and information formats.

The PKI must enforce appropriate policies. These policies must be sufficient for legally binding signatures, so that parallel paper trails with physical signatures are not required. Four criteria have been proposed for digital signature applications:

- the private key(s) must be under the sole control of the user;
- the key pair must be unique to the user;
- it must be capable of being verified; and
- it must be linked to the data in such a manner that if the data is changed the signature is invalidated upon verification.

The Federal PKI must support these criteria.

The PKI must allow proper management of government information resources by facilitating recovery of lost confidentiality keys and permitting access to encrypted information where required for supervision, quality control, or law enforcement. Key recovery mechanisms must not weaken the legally binding nature of signatures generated by federal PKI users. Government standards and policies must be supported and maintained by the Federal PKI. In particular, the PKI must employ

---

[1] A Public Key Infrastructure cannot address the general problem of availability, but the PKI itself should be designed to ensure its own availability.

appropriate cryptographic algorithms and protocols.

These management requirements can be satisfied by development of a federal PKI to bind users' identity to their public keys.

2. Functional Requirements for a Federal PKI

A PKI with appropriate functionality can satisfy the high level requirements of both users and managers. This section examines the functional requirements imposed on a public key infrastructure to support the user and management requirements identified in Section 1.

2.1 User Requirements for a Federal PKI

User's requirements specific to a PKI can be derived from the High-Level Requirements. These are functional requirements that must be met by a federal PKI.

The PKI must provide users with the following capabilities:

- create and post certificates;
- revoke certificates; and
- obtain, interpret, and verify certificates.

These are the basic functions of a certificate management system. Note that the latter capability implies that users can generate and verify digital signatures, and can obtain the current status of a certificate.

Such a PKI can enable users to:

- verify the identity of a message sender based upon the sender's public key certificate;
- verify message integrity and detect message alteration;
- exchange keys for confidentiality;
- authenticate identity based on a public key certificate; and
- specify subject attributes, such as security clearance, privileges, etc.

These services can be enabled by the implementation of a certificate management system, but are not required to implement such a system. The federal PKI must not prevent such services, but does not support them directly.

2.1.1 Create and Post Certificates

The creation and posting of certificates is an infrastructure service that is required by the user. This service permits a user to:

- obtain a public-private key pair[2];
- obtain the corresponding public key certificate;
- have the certificate bound to their identity with a specified level of assurance; and
- make the certificate available to any user who wishes to obtain it.

Binding the certificate to its owners identity requires personal presentation of credentials to a Federal PKI representative. The type and number of credentials required may vary; this should be reflected in the certificate[3]. For convenience, initial registration should be a local service. Subsequent generation of certificates should be performed remotely, in an automated fashion.

2.1.2 Revoke Certificates

Users must be able to revoke the binding between their identity and a public key when the private key has been lost or compromised, or the status of the user changes.[4] This information must be available in a timely fashion.

2.1.3 Obtain, Interpret, and Verify Certificates

Users must be able to determine if they can trust a signature for a particular application. This requires verification of certificates and certificate chains, and evaluating the assurance associated with the binding of identity to a certificate.

Users must be able to obtain certificates for a particular user, parse it correctly, and determine the current status of the certificate. This process must be entirely automated.

- Users must be able to obtain certificates for a named entity in an automated fashion.
- The certificate format must be known, so that it can be interpreted in an automated fashion.
- The certificates must be signed by an appropriate algorithm so that users can verify the certificate chain and verify the binding of user and certificate.
- Certificate revocation information must be available to ensure compromised certificates are not exploited.

To verify certificate chains, users must be able to verify a series of digitally signed messages

---

[2] In most cases, users should generate their own public-private key pairs. This provides the strongest binding for non-repudiation purposes. In special cases, the PKI may generate key pairs for users.

[3] The [TSP] specifies three levels of assurance reflecting the type and number of credentials.

[4] For example, the identity stated in the certificate may imply organizational relationships. These relationships change (e.g., job change or retirement) and the certificate becomes invalid.

(certificates). This requires that:

- the keys are associated with an appropriate algorithm;
- the messages are hashed with an appropriate algorithm; and
- the message formats are known to the receiver.

Finally, the user must be able to determine if the policy under which a certificate was issued is acceptable for a particular application.

2.2 Management Requirements for a Federal PKI

The Federal PKI must meet both technical and policy-oriented management requirements. The infrastructure must be:

- scalable and manageable;
- issue certificates; and
- manage certificates.

The infrastructure must also:

- ensure interoperability within the government;
- set policy on certificates and their use; and
- negotiate and set policy for interoperation with users of non-federal PKIs.

An acceptable Federal PKI will meet the technical requirements and allow management to set and enforce appropriate policies.

2.2.1 Scalability and Manageability

The Federal PKI must be able to manage certificates for a large distributed work force cost-effectively while enforcing clear and consistent policy. This implies that the Federal PKI must be flexible, scalable, manageable, and uniform. These requirements directly affect the structure of the Federal PKI.

There are three basic architectures for a PKI: a single centralized authority; a hierarchical structure of Certificate Management Authorities; or a collection of cross-certified certification authorities (CAs). A centralized authority is relatively inflexible and does not scale well. A hierarchical PKI is scalable, can enforce uniform policy, ensure interoperability within the PKI, and set policy for interoperation with users of non-federal PKI(s). A collection of cross-certified CAs is flexible and scalable, but difficult to manage; it requires each CA to enforce policy and set policy for interoperation with users of other Federal CAs and non-Federal PKIs.

Managerial requirements argue for a hierarchy of certificate authorities. However, the flexibility of cross-certification is required to meet local requirements, enhance performance, and interoperate

with non-federal PKIs. A hybrid architecture can be devised with a hierarchical management structure that permits cross-certification.

Such an architecture is described in the Proposed Federal PKI Concept of Operations. The architecture is based upon a hierarchy of certificate authorities. Organizational Registration Authorities (ORAs) are associated with CAs (usually at the lowest level in the hierarchy.) A Directory Service (DS) maintains and distributes the database of certificates.

A Policy Approval Authority (PAA) manages the CAs through this hierarchical structure. Cross-certificates which violate the hierarchical structure are permitted to meet local requirements and enhance performance, as permitted by the PAA's guidelines.

2.2.2 Issue Certificates

The Federal PKI will issue signature and key exchange certificates to properly identified federal users at their organizations' request. Renewal of certificates will be performed electronically where assurance requirements permit.[5]

Identification

The Federal PKI will issue certificates to users with appropriate identification and organizational credentials at the request of their organization. Certificates will not be issued without management approval, regardless of credentials. The type and number of credentials will be defined by the PKI's policy.

Keys and Algorithms

The Federal PKI will only issue certificates signed with strong keys and algorithms. Where certificates contain encryption or signature keys, the algorithm and key length must be sufficient that it is computationally infeasible to:

- forge signatures;
- make undetected alterations to signed files; or
- obtain confidentiality keys exchanged through supported key distribution mechanisms during the expected lifetime of the information.

The Federal PKI will not generate signature keys for PKI users, although it may provide the equipment. Each agency will determine if the PKI will generate key management keys for their PKI users.

The Federal PKI will maintain logs of public keys, and will reject requests to issue new certificates

[5] The assurance associated with the binding for electronically renewed certificates is lower than for certificates issued by an ORA. The assurance falls with each electronic renewal.

which re-use old keys. This ensures uniqueness of private keys.

Escrowing of Keys

The Federal PKI will support escrowing of key distribution and key encrypting keys where required by management. If retained, keying materials must always be held by approved key escrow agents. Escrowed keys must be cryptographically split into two or more parts, each of which will be entrusted to a separate fiduciary.

Attributes

The federal PKI will manage attribute certificates for owners of PKI signature certificates at their organization's request. Standard attributes will be defined to enhance interoperability, but locally defined attributes will be permitted to maximize utility of the infrastructure.

2.2.3 Manage Certificates

Certificate Distribution

At a minimum, the Federal PKI will support distribution of certificates through directory services. The directory server(s) will chain to the directory servers of other PKIs, as approved by the PAA. Additional distribution services may be offered to meet local requirements.

Revocation

The Federal PKI will provide one or more mechanisms to verify the validity of certificates. CRLs will be available from on-line directories. Unauthorized generation or modification of CRLs must be prevented by employing digital signatures. CRLs must be posted at regular intervals so that users can ensure that they have the most current information. Optionally, current CRLs may be available from the CAs themselves.

The Federal PKI must also support push-down mechanisms for key compromise and other critical events. Such mechanisms must be available to communities with special security requirements. There will be no requirement to employ these mechanisms in the Federal PKI.

The Federal PKI may also include a trusted directory mechanism for real-time certificate validation. Such a mechanism would provide the most current information to critical applications. Trusted directories could be maintained by the PKI, or may be offered by vendors as value-added services.

Archiving

The Federal PKI will maintain a permanent archive of certificates so that business and legal requirements for electronic commerce can be met. The CA can maintain its own archive, or use of an approved third party server.

At a minimum, all certificates issued to CAs and all CRLs must be archived. It is unclear if a record of all certificates issued is required to meet business and legal requirements.

Archives must be maintained, even when a CA or archive server is disbanded. These archives will be maintained by the Federal PKI.

2.2.4 Ensure Interoperability

The Federal PKI will ensure interoperability of PKI entities (CAs, ORAs, and the DS) and PKI clients by selecting appropriate standards to support PKI transactions. Certain algorithms and information formats must be supported within the Federal PKI due to their status as formal or de facto standards.

Federal policy requires that Federal Information Processing Standards (FIPS) will be used where possible. Where no FIPS exist, international or national standards are preferred. De facto standards may be used where formal standards are unavailable.

The set of standard algorithms and information formats is not comprehensive. Non-standard algorithms and information formats may be implemented within the Federal PKI where no standard exists to meet a particular need, unless explicitly forbidden by law or regulation.

Signature Standards

Federal users are required to use DSS for signatures for communications within the government. These requirements are found in FIPS 140-1, *Security Requirements for Cryptographic Modules*, 180-1, *Secure Hash Standard*, and 186, *Digital Signature Standard*. Federal PKI certificates will contain a DSS public key and will be signed with a DSS signature.

RSA is the de facto standard public key algorithm for digital signatures and encryption in the United States and the world. RSA is also widely used for key exchange and E-mail key distribution in secure E-mail applications. Requirements for communication with the private sector may require some Federal PKI users to verify RSA signatures.[6]

Directory Services

X.500 provides the basic specification for implementing directory services. The Federal PKI must support X.500 directory services for key distribution to private sector entities. (Proprietary solutions for trusted directories may be required for certain government and private sector applications.)

Certificate Formats

---

[6] Note that verification of RSA signatures by federal PKI users or issuance of RSA certificates by the Federal PKI requires a waiver of FIPS 140-1, 180-1 and 186.

The X.509 standard is widely used for Public Key Certificate formats. The Federal PKI certificate format(s) will conform to X.509, version 3 and use ISO standard extensions. This will provide maximum compatibility and facilitate local requirements through extensions.

Certificate Revocation List Formats

The Federal PKI will issue Certificate Revocation Lists (CRLs) conforming to the X.509 version 2 CRL format. The Federal PKI will use optional features of the format, such as delta CRLs or distribution points, to control communication costs for CRLs.

2.2.5 Set and Enforce Internal Policy

A common high-level security policy is required to provide uniformity and establish minimum requirements for individual agency policies within the federal PKI. The Federal PKI policy will:

- establish procedural requirements for handling PKI information;
- establish security requirements for PKI CAs and ORAs;
- cryptographic requirements;
- require strong identification of users;
- certification and authentication of CAs and ORAs; and
- promote the establishment of value-added servers.

PKI Information

The Federal PKI will establish guidelines for the archiving, logging, and auditing of PKI entities. These guidelines will specify minimum contents of archives and logs and length of time they must be maintained. Audit standards will address the generation and systematic review of system audit trails.

Security Requirements for CAs and ORAs

CAs and ORAs will be implemented and maintained in a secure fashion, to ensure the validity of the Federal PKI's certificates and CRLs. The Federal PKI will establish security requirements for CAs and ORAs. These requirements will specify minimum levels of assurance (of hardware and software), physical security, personnel security and emanations security. PKI CAs will be required to develop and implement disaster recovery plans.

Cryptographic Requirements

The Federal PKI will develop requirements for cryptographic modules for PKI entities and users. Federal PKI Policy will identify appropriate signature, encryption, and key exchange algorithms and authentication protocols for use by Federal PKI users. PKI Policy will encourage and support the use of these standard algorithms. PKI policy will specify the assurance level (from FIPS 140-1) required of implementations for PKI components and users.

Identification of Users

To maintain the integrity of the system, minimum standards of identification for creation of new user certificates will be established in the Federal PKI Policy. Certificates may be issued under more stringent requirements to meet local requirements.

Certification and Accreditation of CAs and ORAs

To ensure the integrity of the infrastructure, all CAs and ORAs will be periodically reviewed to ensure that they are implementing the appropriate PKI Security Policy. A CA accreditation process must be established to perform these reviews. The PAA will initiate third party audits against the stated policy and review the results. If the security and procedures are found to jeopardize the binding of user and certificate, all subordinate certificates will be revoked. New certificates may be issued after the violations are corrected.

The PAA will determine the period between reviews, credentials for auditors, and the response associated with particular failures or oversights will be specified in the Federal PKI Policy.

2.2.6 Set Policy Regarding Non-Federal PKIs

The Federal PKI will have clearly defined policies regarding non-federal PKIs, and will only cross-certify with PKIs that meet or exceed those policies. Policies must be reviewed and a third party audit of the PKI confirming adherence to the written policy must be performed before cross certification. Cross certification will be established by issuing certificates from the Federal PKI PAA to the appropriate CA and vice versa.

3. Detailed Requirements

The Functional Requirements and Standards Requirements may be merged to produce a set of detailed requirements for the Federal PKI. This section describes the requirements for the primary objects and components of the Federal PKI. The primary objects in the Federal PKI are the Certificate Format, Certificate Revocation List, and Compromised Key Lists. The PKI components are the Client Workstations, CAs, Directory Servers.

The requirements for PKI objects address the format and content of the objects. The requirements for components describe the transaction sets, protocol support, and general functionality of each component.

3.1 PKI Objects

To support the required security services, the federal PKI must manage five basic objects:

- certificates;
- cross-certificate pairs;

- certificate revocation lists (CRLs;)
- compromised key lists (CKLs;) and
- security policies.

3.1.1 Certificates

The Federal PKI public key certificate format will be a an X.509 Version 3 certificate, and will support three basic classes of certificates: public key certificates to support signature applications, key management certificates to support key exchange for confidentiality purposes, and attribute certificates which specify user privileges or role or indicate federal PKI accreditation of third party services.

All signature and key exchange certificates will contain, at a minimum:

- the distinguished name of the user or entity;
- the validity period;
- the public key and its parameters;
- key usage field;
- algorithm field;
- one or more policy identifiers;
- the name of the issuing authority; and
- the issuing authority's DSA signature.

A government wide naming scheme, probably based on X.520, is required to ensure assignment of unique names. The maximum validity periods will be specified in the Technical Security Policy. The public key parameters must be included with the public key to ensure interoperability with other PKIs. The key usage field will differentiate between signature and key management certificates. The algorithm field will support multiple signature and public key encryption algorithms as new algorithms are approved for federal use as well as ranges of key sizes for immediate use with DSS. A user certificate will also include one or more policy identifier fields indicating the security policies governing its issuance. CA certificates may include policy constraint fields indicating the set of policies for which it may issue certificates.

The certificate may also contain a non-negative integer field specifying the number of electronic renewals permitted for this certificate.[7]

Certificates issued to CAs may also contain the following fields:

- subtreesConstraint field;
- nameConstraint field;
- policy restrictions;
- policy mappings;

---

[7] The number of electronic renewals permitted is decremented by one upon each renewal, and when it reaches zero, the certificate must be re-issued through the initial certification procedure.

Attribute certificates will contain, at a minimum:

- the distinguished name of the user or entity;
- the validity period;
- the attribute field;
- the name of the issuing authority; and
- the issuing authority's DSA signature.

Attribute formats and the procedures for creation, distribution, and revocation of attribute certificates will reflect local requirements and will not be determined by the Federal PKI.

3.1.2 Cross-Certificate-Pairs

The Federal PKI will support the X.509 cross-certificate-pair construct to build bi-directional chains of trust between CAs. The cross-certificate-pair construct contains two certificates: a "forward" certificate and a "reverse" certificate. The subject of the "forward" certificate is the issuer of the "reverse" certificate and vice-versa.

For the certificates defining the hierarchical architecture of the Federal PKI, the forward certificate will define the path leading from the root. Only the forward certificate is required in this case; the reverse certificate may not be included in some of these cross-certificate-pairs.

Cross-certificate-pairs may also define new paths that do not parallel the hierarchy leading to the root. In this case, there is no semantic difference between the forward and reverse certificates. Constraints for cross-certificate-pairs that do not parallel the hierarchy are specified in the *Concept of Operations* document.

3.1.3 Certificate Revocation Lists

The Federal PKI public key certificate revocation list will be based on the X.509 Version 2 CRL. The format will support:

- modular presentation of CRLs; and
- knowledge of why certificates were revoked.

Modular presentation of CRLs is a critical performance issue. Some applications may accept signatures corresponding to revoked certificates, depending upon the time frame and the reason for revocation. Reason codes will be required for all CRL entries.

3.1.4 Compromised Key Lists

The Federal PKI Compromised Key Lists (CKLs) will support rapid dissemination of key compromises throughout the infrastructure. This requires that all CAs support a common CKL format and generate CKLs for exchange within the infrastructure. The frequency of CKL generation is a Technical Policy issue.

3.1.5 Policy Objects

The Federal PKI will support a policy object which is issued by CAs. Policy Objects will contain, at a minimum:

- the distinguished name of the user or entity;
- the validity period;
- the policy field;
- the name of the issuing authority;
- the issuing authority's DSA signature;
- the name of the approving authority; and
- the approving authority's DSA signature.

The federal PKI will define standard formats for conveying policy information.[8] All Policy Certificates issued by entities within the Federal PKI will conform to this format.

3.2 PKI Components

This section describes the functionality of each class of PKI components. As described in section 2.2, the PKI is assumed to include the following components:

- a Policy Approving Authority (PAA);
- Certificate Management Authorities (CAs);
- Organizational Registration Authorities (ORAs);
- PKI client workstations; and
- Directory Servers.

3.2.1 Policy Approving Authority

The Federal PKI PAA must:

- establish policy for CAs and ORAs, including:
  - personnel security;
  - archiving, logging and auditing; and
  - physical and systems security.
- review compliance of CAs and ORAs;
- set policy for internal cross-certification;
- establish policy identifiers for use throughout the Federal PKI; and
- approve cross-certification between the root CA and non-federal PKIs.

3.2.2 Certificate Authorities

Federal PKI CAs will:

- generate and verify DSS signatures;
- generate and verify Federal PKI certificates;
- access X.500 directory service using DAP;

[8] Sample ASN.1 policy objects are provided in [TSP] and [Interop].

- generate CRLs and CKLs;
- generate DSA key pairs and perform quality tests;
- confirm that certificate requestors possess the private key corresponding to the public key in the requested certificate;
- maintain a permanent archive directly or through use of a third party digital archiving service;
- accept electronic certificate issuance and renewal requests;
- verify uniqueness of subordinate names;
- generate cross-certificate pairs;
- verify uniqueness of public keys;
- maintain secure off-line storage for private key backup;
- perform weekly backups;
- log transactions to non-volatile storage media; and
- support required communication protocols.

CAs must be able to generate cross-certificate pairs, containing at a minimum the forward certificate, to represent the hierarchy leading from the root. Optionally, CAs may be able to generate reverse certificates to provide "full" cross-certificate-pairs. The root CA must be able to generate "full" cross-certificate pairs to support mutual recognition with non-federal PKIs.

Optionally, CAs may support the generation of cross-certificate-pairs with other CAs within the Federal PKI to define trust paths that are not parallel to the hierarchical structure.

CAs will use standard Internet protocols for inter-CA and CA-DSA transactions. CA-ORA transactions may be implemented using any appropriate networking technology (e.g., LANs) or via dial-up access as required by local systems.

Optionally, CAs may maintain a database of information regarding owners of certificates issued. This information would include contact information, such as phone numbers and electronic mail addresses, and may include private user information such as social security numbers and their mother's maiden name. This would facilitate recovery from CA compromise and remote user revocation requests, but would also impose additional security requirements from the Privacy Act.

CAs, PCAs and PAAs must generate their own policy objects; all policy objects are signed by the PAA.

CAs will only issue certificates to users at the request of their organizations. A CA may optionally confirm that the organization has requested a certificate for this user. The CA must delegate this function to its ORAs if it does not perform it directly.

CAs may return approved certificates to the requesting ORA or the requesting user.

3.2.3 Organizational Registration Authorities

The Federal PKI's Organizational Registration Authorities (ORAs) will sign certificate requests for users who appear in person with appropriate identification. ORAs may also confirm that the organization has requested a certificate for this user. ORAs will vouch for signature certificates that:

- conform to the Federal PKI certificate format;
- are signed with DSS signatures;
- include DSS public keys; and
- are specifically marked as signature certificates.

The ORA will not generate key pairs for users, but may supply the equipment for this function. If users will receive private keys on diskettes, the equipment must encrypt private keys with DES.

ORAs will interact with CAs using appropriate communications protocols as determined by the CA.

Optionally, ORAs may maintain a database of information regarding owners of certificates issued. This information might include private user information such as social security numbers and their mother's maiden name to facilitate personal authentication. This would facilitate remote user revocation requests, but would also impose additional security requirements from the Privacy Act. (Note that ORA compromise does not invalidate previously issued user certificates. No contact database is required unless we wish to facilitate compromise recovery for the parent CA.)

3.2.4 PKI Clients

Federal PKI clients must provide the following capabilities to participate fully in the Federal PKI:

- generate DSS signatures;
- verify DSS signatures;
- interpret X.509 V3 certificates;
- interpret federal PKI certificate revocation lists;
- determine the status of a federal PKI certificate;
- interpretation of policy identifier and constraint fields; and
- obtain certificates from X.500 directory servers using DAP or LDAP.

This is the minimum functionality for verification of certificate chains and status. Given a message format, this will also enable users to sign and verify DSS signatures from other users of the Federal PKI.

Clients with a limited role (i.e., sign only) may implement a subset of this functionality.

3.2.5 Directory Servers

Federal PKI directory servers will support the X.500 directory service, including both the DAP and LDAP access protocols. The directory servers will support access via dial-up and the Internet access. The directory servers will chain to directories maintained by cross-certified PKIs. The directory will make all published certificates available upon request.

The directory will include all current and recent certificates, cross-certificate-pairs and CRLs issued by the federal PKI CAs. Certificates and cross-certificate-pairs must be maintained in the directory for some time period after expiration or revocation to facilitate verification of documents signed just before the certificate was revoked or expired. The length of time the certificate should be maintained is a Technical Policy issue.

The directory will also contain all security policy objects issued by federal PKI CAs. A policy object may not be revoked, although a CAs privileges to issue certificates under that policy might be. Procedures for deletion of obsolete policies are to be determined.

References

[TSP] Noel Nazario, Ed. Federal Public Key Infrastructure (PKI) Technical Specification: Part B - **Technical Security Policy**. TWG96-001, 24 January 1996.

[ConOps] William Burr, Ed. Federal Public Key Infrastructure (PKI) Technical Specification: Part C - **Concept of Operations**. TWG-95-108, 16 November 1995.

[Interop] Federal Public Key Infrastructure (PKI) Technical Specification: Part D - **Interoperability Profiles**. CygnaCom Solutions, Inc. Draft 27 September, 1995.