Public Key Infrastructure (PKI) Technical Specifications (Version 1): Part C - Concept of Operations

1. Introduction

1.1 Purpose of the FPKI

The Federal Public Key Infrastructure (PKI) will support secure Federal Government use of information resources and the National Information Infrastructure (NII). The Federal PKI will establish the facilities, specifications and policies needed by Federal departments and agencies to use public key based certificates for information system security, Electronic Commerce, secure communications, and E-mail with each other as well as with entities of other branches of the Federal Government, state and local governments, business and the public. The Federal PKI will facilitate secure communications and information processing for unclassified but sensitive (UBS) applications.

The Federal PKI will support secure communications between Federal agencies and departments. However, PKI support for secure communications with business, the general public, other branches of the Federal Government and state and local governments is vital. This Concept of Operations document (CONOPS) defines the operation of that part of the overall PKI that supports the operation of Federal agencies. The Federal PKI does not focus inward to secure communications and information systems only within a closed Government community, rather its purpose is to provide Federal users secure information access and communications with the entire nation and the rest of the world.

1.2 Basic Concepts

Digital signatures are based on the concept of a public-private key pair. A signatory, Alice, has a private key which she must keep a secret, and an associated public key, which is made public. A digital document (a message or file) is signed by Alice with her private key, and the signature may be verified with Alice's public key. Digital signatures can provide three important security services:

- *integrity*: any change to a signed document will cause the signature verification to fail;
- *source non-repudiation*: since only Alice knows her private key, only she can sign a document with it;
- *authentication*: Bob can authenticate Alice's identity, if he knows her public key, by having her sign a challenge. If the signature can be verified with Alice's public key, it must have been signed by Alice.

In addition, public key technology can provide confidentiality to Bob and Alice:

- Bob can encrypt a message with Alice's public key, which can only be decrypted her private key, or:

- Bob can encrypt a traffic key in Alice's public key and send it to her, She can then decrypt the traffic key with her private key, and Bob and Alice can then use that traffic key with a symmetric key encryption algorithm to encrypt a message between them. This is commonly done because symmetric key encryption is generally much faster than public key encryption.

Public key certificates are digital documents that, at a minimum, contain the name and public key of a user, and are digitally signed by a certification authority (CA). The purpose of a certificate is to reliably associate a users name and public key. Bob, trusting the CA and knowing its public key, may reliably obtain Alice's public key from her certificate by verifying the signature on the certificate.

In addition to CAs there are organizational registration authorities (ORA), that do not themselves issue certificates, but who register or vouch for the identity of users to a CA that issues them a certificate, and management authorities that approve or coordinate the policies used to operate CAs and ORAs and to issue certificates.

Figure 1 shows a "PKI-centric" view of certificate-base security services. The security services enabled by a PKI are shown as circles around the periphery of the PKI and the underlying information, security servers that support them. At the center is the core PKI, which is concerned with issuing and managing certificates. The first ring is the PKI clients that use the certificates, and the next ring shows various security specific servers and agents that provide or facilitate various security services. An incomplete outer ring of general information and communications services is shown at the bottom, to highlight some general services that, while not specifically security related, are important to the security services.

The core Federal PKI consists of CAs and ORAs that manage public key certificates used by Fed-

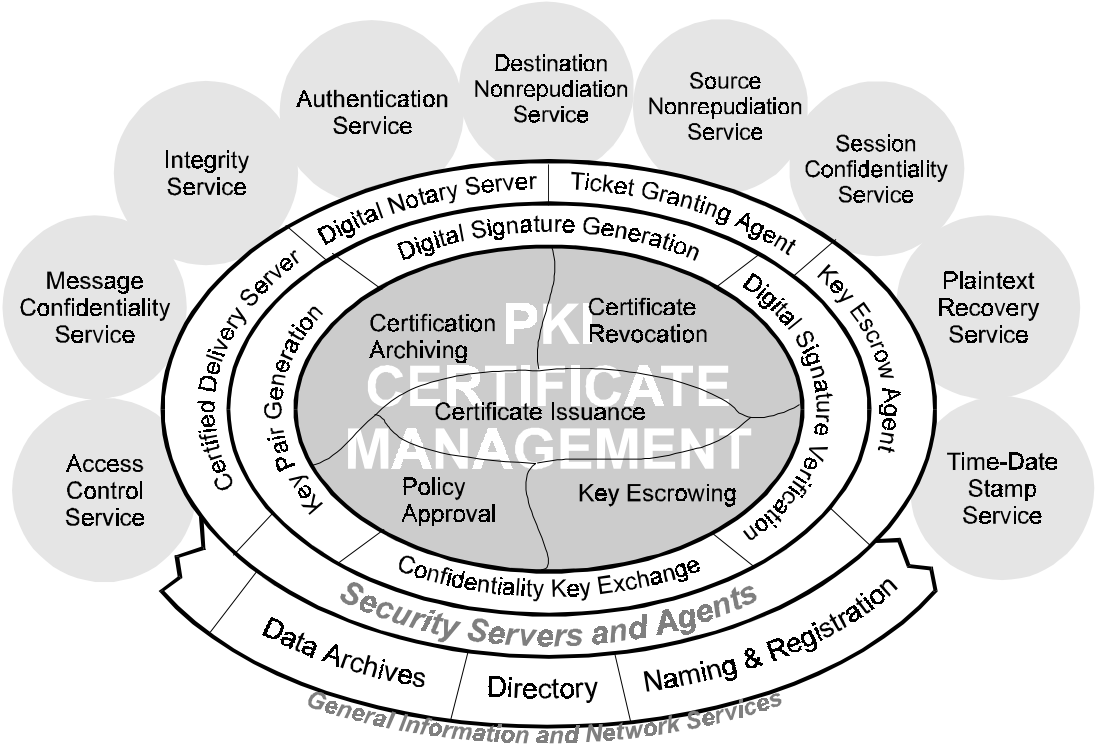

Figure 1 - A PKI Centerd View of Security Services

eral departments and agencies for unclassified, sensitive applications. The core Federal PKI will:

1. issue public key certificates;

2. revoke public key certificates when required;

3. establish the policies that govern the issuance and revocation of certificates;

4. archive the information needed to validate the certificates at a later date;

5. in some cases, the core PKI may escrow (save a copy of) private keys used for confidentiality key establishment, typically by turning it over to a special fiduciary called a key escrow agent.

PKI Clients will use the public key certificates that are issued and managed by the PKI to provide security services to Federal users. PKI clients perform four primitive functions with and for certificates:

1. public-private key pair generation;

2. digital signature generation;

3. digital signature verification;

4. confidentiality key exchange or distribution.

The first function, key pair generation, can also be performed by CAs or ORAs, but generation of digital signature key pairs by the clients helps to maintain the integrity of the system, since only the client then ever possesses the private key used for digital signatures. The last three functions enable a variety of public key based security protocols and services by direct client to client protocols, including authentication, access control based on an authenticated identity or role, nonrepudiation services, and confidentiality.

A number of servers and agents support the infrastructure and clients and clients may obtain security services from these servers and agents. The full range of servers and agents that may be needed is not fully understood, and is still evolving, but they may include:

- *digital notaries*: A digital notary provides a service analogous to a notary public; A notary may also provides a trusted date and time stamp for a document, that proves that it existed at a point in time and, may also verify the signatures on a signed document;

- *key escrow agent*: CAs may turn copies of copies of private keys used for confidentiality key management over to a trusted key escrow agent, or may require that the private key be given to a trusted key escrow agent as a condition for issuing a key management certificate. The purpose of key escrow is to allow decryption of encrypted data when keys are lost, or for management supervision or law enforcement purposes. It is useful to separate the CA and key escrow functions because, while the only secret a CA inherently need protect or access is its own private key, a key escrow agent must store, protect, and provide carefully controlled access to a large number of user private keys. Key escrow agents usually provide for split control of

escrowed keys, so that the cooperation of two or more agents is required to access the keys. Private keys used for digital signatures should never be escrowed;

- *certified delivery agents*: These servers provide a destination non-repudiation service, analogous to certified mail or process servers, to prove that a message was received by a possibly uncooperative recipient, or that a good faith attempt was made to deliver the message;

- *ticket granting agents*: These agents provide cryptographic digital "tickets" that can be used for access to systems or data. They can use either public key or symmetric key cryptography, and provide a means of centralizing and managing access control in distributed systems.

Three general information and network services are of particular significance to the PKI:

- *directories:* Directories provide a way to provide information about a user or entity whose name is known, for example the user's phone number, his e-mail address, or, of particular interest to the PKI, his certificate. Conversely, certificates provide an access control mechanism for directories;

- *data archives*: Archives provide a very long term repository for storing information. The life time of CAs may be relatively short. But it may be important to verify the validity of signatures on very old documents. CAs must make provision to store the information needed to verify the signatures of its users, in archives that will be able to make the data available at a much later date, perhaps centuries later;

- *naming and registration*: in a distributed environment, many objects must have unique names. This is true for security objects, for example certificate subjects and issuers, must have unique names.

If general purpose directories and digital archives do not become broadly established, the Federal PKI itself may need to operate directories that can be used to obtain certificates, archives that store the data necessary to verify old digital signatures, and certain other servers that provide services such as notary services. Other services or agents may be provided by commercial service providers outside the Federal PKI and be used by Federal users. The servers of particular interest to the PKI are discussed more detail in section 10.

2. PKI Services

The PKI will provide the services and facilities needed for UBS secure Federal information processing and use of the NII, including:

- digital signatures for:
  - authentication;
  - integrity;
  - non-repudiation.
- management of symmetric keys for UBS level confidentiality for:
  - communications confidentiality session keys;
  - e-mail confidentiality message keys.

Table 1 - X.509 v3 Certificate

version	version number; an integer, value is "2" for version 3	
serial number	unique identifier for each certificate generated by issuer; integer	
signature	algorithm identifier	algorithm used to sign certificate
	parameters	any parameters needed
issuer	name of issuer (X.500 "distinguished name", a sequence of RelativeDistinguishedNames that uniquely identify a directory object),	
validity	notBefore	UTCTime
	notAfter	UTCTime
subject	name of subject (X.500 "distinguished name")	
subject's public key info	algorithm identifier	subject's signature algorithm
	public key	subject's public key
issuer unique identifier	(optional) contains additional information about the subject; must be version 2 or higher - not used by the Federal PKI.	
subject unique identifier	(optional) contains additional information about the issuer; must be version 2 or higher - not used by the Federal PKI.	
extensions	(optional)	
issuer's signature		

- symmetric key encryption of communications sessions or sessions for confidentiality.

The PKI will provide the services and facilities needed for secure information access, communication, messaging and electronic commerce with commercial and personal users employing common defacto and formal security standards and using mainstream commercial security products; As far as practical, the Federal PKI will be implemented with ordinary COTS security products.

3. PKI Data Structures

Three basic data structures defined in the X.509 standard are used by the Federal PKI: certificates, cross-certificates and Certificate Revocation Lists (CRL).

3.1 Nomenclature and Typographical Conventions

Certificates, cross-certificates and CRLs are all directory attributes from the X.509 standard, and defined there in the ASN.1 syntax[ref xxx]. Formal names in ASN.1 are written without spaces and the separate words in the names are indicated by capitalizing the first letter of each word but the first. For example, the formal ASN.1 name of a cross-certificate is "crossCertificatePair," while the formal name of a certificate is "certificate." In this CONOPS, when it is useful to be very specific that a word means a particular formal directory attribute, as defined in X.509, they are shown in their ASN.1 form, set in boldface type, for example: **certificate**, **crossCertificatePair,** and **certificateRevocationList**. However, frequent use of this convention does not contribute to readability, and where it is not necessary to stress the formalism, "plain English" names are used in normal roman typeface.

Table 2 - X.509 Standard Extensions and the FPKI

Extension	Used by FPKI		Critical
Key and policy information			
authorityKeyIdentifier			No
keyIdentifier	Opt:	use to hold KMID* of CA key used to sign certificate	
certIssuer	No		
certSerialNumber	No		
keyAttributes			No
keyIdentifier	Opt:	use to hold KMID* of user key	
keyAttributes	No		
privateKeyValidity	Yes:	validity period of private key	
certificatePolicies	Yes:	OID of policies the certificate is issued in accordance with; holds at least Federal Assurance Level ID	No
keyUsageRestriction	Opt.:	indicates per-policy restrictions on key use	Yes
policyMappings	Opt.:	lists equivalent policies in CA certificates.	No
Subject and issuer attributes			
subjectAltName	No		No
issuerAltName	No		No
subjectDirectoryAttributes	Opt.:	May be used to hold PKI unique directory attributes; PKI Classification, privilege Flags, PKI Categories; used by MISSI***	No
Certification path constraints			
basicConstraints			Yes
subjectType	Yes	specifies CA or end entity	
pathLengthConstraint	Yes	applies only to CAs, limits following path length	
subtreesConstraint	Yes:**	Applies to CA certificates; limits namespace for which certificates may be issued;	
nameConstraints			Yes
policySet	Opt.:	indicates policies for which constraints apply.	
nameSpaceConstraint	Yes:**	Applies to CA certificates; limits namespace for which certificates may be issued;	
nameSubordConstraint	Opt.:	enforce rigid naming hierarchy where needed	
policyConstraints			Yes
policySet	Opt.	all policies that must apply to certificates issued by a CA	
requireExplicitPolicy	Opt.	All certificates must contain an acceptable policy indicator in the certificatePolicies extension	
inhibitPolicyMapping	Opt.	skipCerts value of zero; for all certs but PAA.	

* KMID: Keying Material Identifier; used by MISSI certificates to uniquely identify key pairs.
** At this point it is not clear which of these fields will be used, or if both will be needed.
*** MISSI: Multilevel Information Systems Security Initiate.
Yes required for either all FPKI CA or all end entity certificates (or both) as indicated
No not used in FPKI certificates
Opt. Used in some FPKI certificates as appropriate

3.2 Certificates

The Federal PKI will use X.509 v3 certificates. The X.509 v3 **certificate** is illustrated in Table 1.

These certificates are digitally signed using the private key of the issuing CA. Certificates issued for Federal users will be signed using the Digital Signature Standard (DSS) defined in FIPS PUB 186. A number of optional extension fields are being standardized [DAM 95]. In addition, federal specific extensions may be defined and incorporated in Federal certificates. Certificates may be stored in hardware based tokens or cryptographic modules. Certificates, however, in general, need not be protected and can be stored on any digital medium.

The optional extensions that have been defined for standardization include extensions that:

- identify the policies under which the certificate was issued;
- map equivalent policies in different domains;
- require subsequent certificates in a certification path to include specific policy identifiers, or inhibit policy mapping;
- limit the subject name space for subsequent certificates in the certification path;
- restrict key usage;
- limit the number of subsequent certificates in a certification path;
- distinguish between a CA certificate and an end-entity certificate.

Extensions may be labeled *critical*. A verifier must be able to process any critical extension, or it must not verify the certificate. The Federal PKI will use these standardized extensions as needed and will require that all Federal certificates include certain extensions and that all clients be capable of processing certain extensions if they are present. Table 2 summarizes the standardized optional extensions to the X.509 certificate and their intended use in the FPKI. Additional material on certificate extensions is contained in [PROF 95].

The primary purpose of an X.509 certificate is to associate the subject's public key and name. Public keys may be used to verify signatures, or to manage keys used with symmetric key algorithms for confidentiality. The algorithm used in the Federal PKI for digital signatures is not intended for confidentiality key management. A separate algorithm will be used for confidentiality key exchange. Separate certificates will be used in the Federal PKI for digital signatures and key management.

3.3 Cross-Certificates

CAs may cross-certify each other, that is each issue the other a certificate and combine the two certificates in a single directory attribute called a **crossCertificatePair**. The attribute **crossCertificatePair** supports chains of trust that run in both directions and are needed to implement trust models that begin at the CA which issued the users certificate, rather than trust models where trust originates from a common "root"CA.

A **crossCertificatePair**, includes two certificates, **forward** and **reverse**. The subject of the forward certificate is the issuer of the reverse certificate and vice-versa. When CA A cross certifies with CA B, in A's crossCertificatePair attribute, A is the issuer of **forward**, and B is the issuer of

reverse. In B's crossCertificatePair attribute, B is the issuer of **forward** and A is the issuer of **reverse**.

3.4 Certificate Revocation Lists

It is at times necessary to revoke certificates, for example when the certificate holder leaves the issuing organization or when the private key is compromised. The mechanism defined in X.509 for revoking certificates is the Certificate Revocation List (CRL). The X.509 v2 CRL is illustrated in Table 3.

A CRL is issued and signed by the CA that is revoking certificates. It contains a list of the unexpired certificates that have been revoked. Since the CRL contains the time it was issued, and the time the next CRL will be issued, a user can determine if a copy of the CRL is still current. Federal CAs will issue CRLs at periodic intervals. Optional extensions defined for the X.509 CRL also allow identification of the reason for including a certificate in a CRL.

Several considerations apply to the use of CRLs in the Federal PKI:

- CRLs are periodically "pulled" from directories and cached by verifiers. This results in some potential delay in notifications of suspected key compromises. "Push" models have been used for distributing a Compromised Key List (CKL), but in the broad context of a large Federal PKI a CKL might become unworkably large for push type distribution, and it is unclear to whom should it be pushed;
- X.509 CRLs must be issued by the CA that issued the revoked certificates. This complicates maintaining and verifying consolidated CRLs for the entire Federal PKI (which might be useful for a CKL);
- For a large Federal PKI the communications needed to access CRLs could become quite large and the cost of distributing CRLs is also potentially large [MITRE 94]. Delta CRLs (which include only new revocations since some defined time) and CRL distribution points (which include only revocations for a particular arc of the name-space) are constructs defined in X.509, which may facilitate cost effective use of CRLs.

The Federal PKI will use the X.509 v2 CRL for certificate revocation. Since communications costs for distributing the CRLs will be significant, the Federal PKI will follow the "pull" distribution model, that is verifiers will request CRLs from directories on an as needed basis. CRLs will be maintained by CAs for the certificates they issue. CRL distribution points will be used to reduce the size of individual CRLs and minimize communications costs. Since local hard disk storage is relatively inexpensive, and since CRLs need not be stored in trusted memory, it is anticipated that a CRL, once retrieved by a client verifier, will be retained in a local cache memory until the issuance date of the next update (which is stated in the CRL), to reduce communications costs. The **reasonCode** extension will be used to identify the reason for the revocation, including key compromise, affiliation change, and so on. The period for CRLs will be a compromise, balancing the delay in distributing revocation notices to verifiers against the communications costs of frequent updates. Special, "off-cycle" CRLs , containing only certificates with compromised keys , may be issued by CAs as needed. Client verifiers may check for these special CRLs when they verify signatures for critical applications.

Table 3 - X.509 v2 Certificate Revocation List

signature	algorithm identifier	algorithm used to sign CRL
	parameters	any parameters needed
issuer	name of CRL issuer (X.500 "distinguished name," a sequence of RelativeDistinguishedNames that uniquely identify a directory object)	
this update	UTCTime	update timestamp
next update	UTCTime	optional time of next update
revoked certificates	list of revoked certificates	
CRL extensions (optional) zero or more extensions	optional extensions	if "true" extension must be processed
	extension parameters	
issuer's signature		

serial number	serial number of revoked certificate (unique for the issuer)	
revocation date	UCT Time	
crl entry extensions (optional) zero or more extensions	critical flag	if "true" extension must be processed
	extension parameter	

CRL Extension Fields

Extension	Used by Federal PKI		Critical
CRL extensions			
cRLNumber	Yes:	Used to provide a CRL sequence number	No
CRL Entry Extensions			
cRLReason	Yes:	identifies reason for CRL entry, e.g. key compromise, affiliation change...	No
expirationDate	?	used if certificates are held, applies to expiration of hold	No
instructionCode	?	identifier to indicate action taken on encountering a held certificate	No
invalidity Date	Yes	date of known or suspected compromise	No

3.5 Attribute Certificates

Attribute certificates are not defined in X.509, but are defined in the proposed X9.30 standard. An attribute certificate is a signed by an attribute authority and is a digital document stating some attribute of the subject. For example, attribute certificates may indicate security clearance levels, credit limits, authority to obligate the government, access privileges and so on. This information might alternatively be included in Federally defined extensions to X.509 signature certificates, but this kind of information may be managed by very different authorities than the CAs that issue signature certificates, and may change much more frequently than public-private key pairs would ordinarily change. Therefore it is anticipated that only attributes that are very frequently used with digital signatures, and that change very infrequently, should be bound in digital signatures certificates, and that separate attribute certificates will be needed in the Federal PKI. Further study is needed to fully define the role of attribute certificates in the Federal PKI.

4. PKI Certification Path Architecture

In a PKI trust is transferred by certification paths, that is along chains of certificates. A signature is verified by verifying the signatures on a chain of certificates until the certificate of a CA is reached that is trusted by the verifier, and whose public key is known to the verifier.

4.1 Certification Path Topologies

CAs can issue certificates to each other in a systematic and ordered way or in a more flexible and less ordered way. The systematic, ordered topology of certification paths that is normally employed is a hierarchy, while the more general topology is a network of cross-certified CAs. The two alternatives are illustrated in Figure 2 and described below:

- *Hierarchical*: Authorities are arranged hierarchically under a "root" CA that issues certificates to subordinate CAs. These CAs may issue certificates to CAs below them in the hierarchy, or to users. In a hierarchical PKI, the public key of the root CA is known to every user, and any user's certificate may be verified by verifying the *certification path* of certificates that leads back to the root CA. Alice verifies Bob's certificate, issued by CA4, then CA4's certificate, issued by CA2, and then CA2's certificate issued by CA1, the root, whose public key she knows;

- *Network*: Independent CA's cross certify each other (that is issue certificates to each other), resulting in a general network of trust relationships between CAs. Figure 2(b) illustrates a network of authorities. A user knows the public key of a CA near himself, generally the one that issued his certificate, and verifies the certificates of other users by verifying a certification path of certificates that leads back to that trusted CA. So, for example, Alice knows the public key of CA3, while Bob knows the public key of CA4. There are several certification paths that lead from Bob to Alice, but the shortest requires Alice to verify Bob's certificate, issued by CA4, then CA4's certificate issued by CA5 and finally CA5's certificate, issued by CA3. CA3 is Alice's CA and she trusts CA3 and knows its public key.

The hierarchical certification path architecture has some advantages:

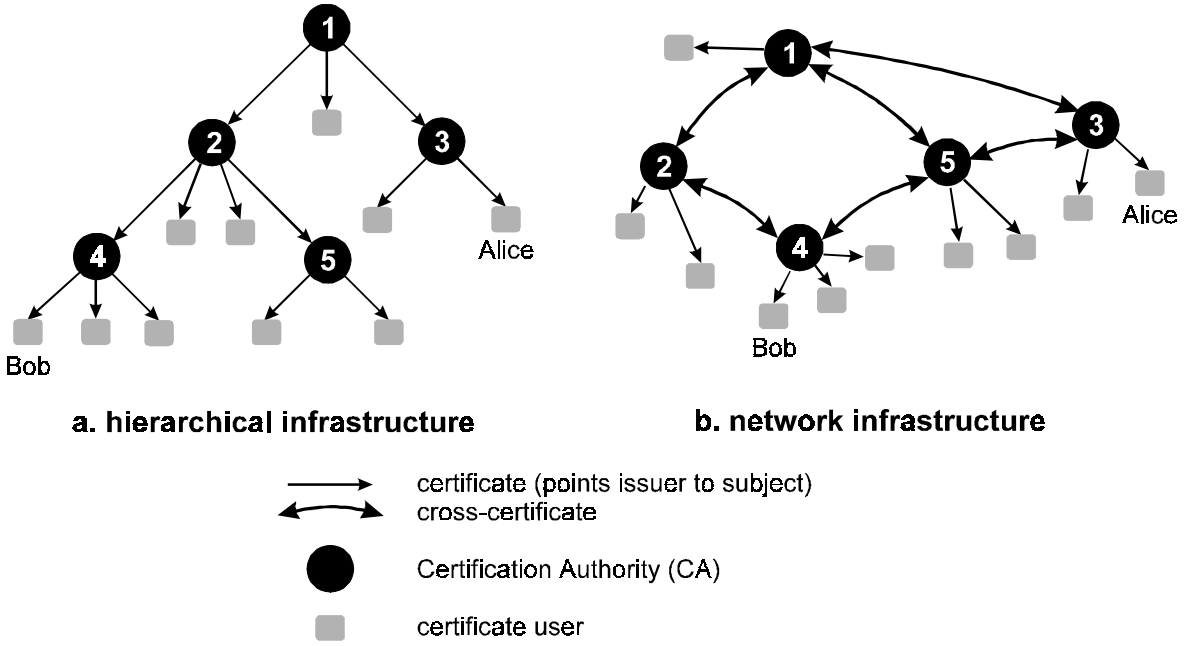

Figure 2 -Different PKI Infrastructure Topologies

- The organizational management structure of many organizations such as the government is largely hierarchical. Trust relationships are frequently aligned with organizational structure, so it is natural to align the certification path with the organizational structure;
- The hierarchy may be aligned with hierarchical directory names;
- The certification path search strategy is straightforward;
- Important existing Federal PKI components are designed hierarchically;
- Each user has a certification path back to the root. The user can provide his path to any other user and any user can verify the path, since all users know the root's public key.

A strictly hierarchical certification path architecture also has some disadvantages:

- It is improbable that there will be a single root CA for the world PKI;
- Commercial and business trust relationships are not necessarily hierarchical;
- Compromise of the root private key is catastrophic and recovery requires the secure distribution of the new public key to every user.

The network certification path architecture has some advantages:

- It is flexible, facilitates ad hoc associations and trusted relationships, and reflects the bilateral trust relationships of business;
- A user must trust at least the CA that issued its own certificate in any PKI, and it is reasonable to make this the foundation of all trust relationships;
- CAs that are organizationally remote, but whose users work together with a high degree of trust, can be directly cross-certified under a high trust policy that is not extended to other CAs and is higher than would be practical through a long, hierarchical chain of certificates;
- It allows direct cross-certification of CAs whose users communicate frequently, reducing certification path processing load;

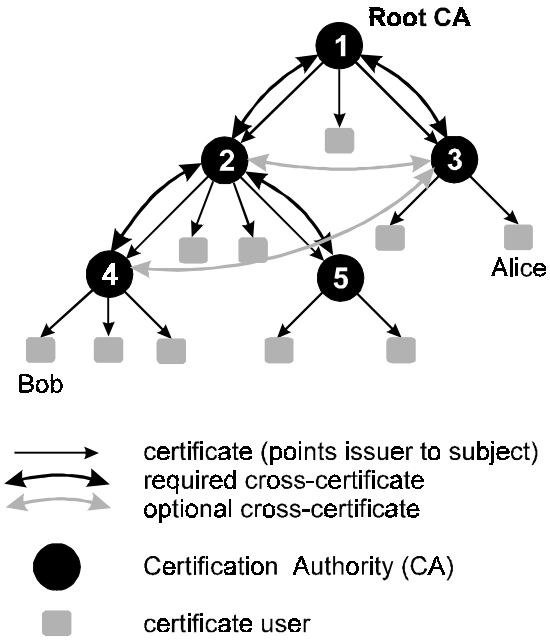

Figure 3 - Federal PKI Certification Path Architecture

- Recovery from the compromise of any CA's private key requires only that the new public key (and certificates signed with the corresponding new private key) be securely distributed to the holders of certificates from that CA.

The network PKI also has at least two disadvantages:

- Certification path search strategies can be more complex;
- A user cannot provide a single certification path that is guaranteed to enable verification of his signatures by all other users of the PKI;.

4.2 The Federal Certification Path Architecture

The Federal certification path architecture is established by the certificates and cross-certificates that Federal CAs issue to each other. It is illustrated in Figure 3. It combines both the hierarchical and the network topologies. Specifically:

- There will be a hierarchical path of certificates leading from the root CA to its subordinate CAs, and from each of these CAs to their subordinates, and so on, until every end user is issued a certificate that has a certification path from the root CA;
- Each Federal CA will have a single parent. There will be one or more instance of the directory attribute **certificate** holding certificates issued by that parent. Therefore there will be only one hierarchical path to the root CA based on the directory attribute **certificate**. Any other certificates held by a CA, from any other issuer, will be posted in the directory in a **crossCertificatePair**;
- In parallel to the certificates hierarchically linking CAs to the root will be **crossCertificatePair**s attributes also linking those CAs. These parallel **crossCertificatePairs** are required and are shown in Figure 3 as black double-headed arrows. This will allow client applications that perform certification path verification from the verifier's parent CA, using the **crossCertificatePair** directory attribute, to operate from any Federal CA;

- Federal CAs may cross-certify each other along paths that do not parallel the hierarchy leading to the root. Optional **crossCertificatePair**s are shown in Figure 3 as gray double-headed arrows. Guidance on cross-certification is given in section 4.2.3 below.

If Alice now wishes to verify Bob's signature, she can apply either a certification path search strategy that relies on her trust in her parent CA, CA3, or one that verifies Bob's certification path back to the root. In general, Federal PKI clients and applications may follow either a strategy that verifies the certification path to the root CA, or (if the CAs have issued the requisite certificates) back to their own CA.

4.2.1 Path and policy verification constraints

The X.509 v3 certificates used in the Federal PKI state the policies under which they were issued, and specify constraints on the policies and subject names of subsequent certifications in a certification path. Therefore, at each step of a certification path verification it is necessary to verify that:

- the certificate issuer's signature is valid;
- the certificate is current (i.e., has neither been expired nor revoked);
- a policy identified in the optional policy identifier extension is consistent with the policy requirements of the application;
- the policy constraints imposed by previous certificates in the path are satisfied;
- the path length constraints imposed by previous certificates in the path are satisfied;
- the subject name is consistent with any name constraints imposed by previous certificates in the certification path.

4.2.2 Verification that certificate are current

Three modes of verifying that certificates are current (i.e., have not expired nor been revoked) will be supported:

1. The currentness of client certificates is checked by accessing a trusted on-line directory each time the certificate is used. This mode of verification provides the best check of the current validity of the certificate, and can accompany simultaneous funds transfers, verification of specific privileges, current account balances, and the like. It is particularly advantageous when the certificate is used to effect a financial transaction and real time communication is needed for that purpose. But this method of certificate verification has additional communications and directory response time burdens; some CAs may not be supported by directories that can accommodate real-time certificate by certificate verification, and some clients may not have ready access to the communications needed to support this mode of verification;
2. The currentness of client certificates is checked using Certificate Revocation Lists (CRL), that are periodically retrieved by client systems from directories. CRLs may optionally be supplemented by Compromised Key Lists (CKLs) listing certificates that are revoked because they are believed to have been compromised. An unexpired client certificate, which is not listed in the appropriate current CRL, is presumed to be current. Clients may include their certificates with signed files, or exchange certificates during authentication protocols, to facilitate operation and minimize directory accesses. Clients may also cache the certificates of peer entities and CRLs to minimize communications requirements. This mode of verifying certificate cur-

rentness reduces the need for communications with directories and the response time constraints of directories, while still providing protection against the use of revoked certificates;

3. Unexpired certificates are accepted as current without further checks. In this mode of operation clients normally include their certificates (or a complete certificate path) with messages or files, exchange certificates during authentication protocols, and may cache the certificates of peer entities. This mode of validation does not protect against the use of unexpired certificates that have been revoked, but is adequate for some applications.

Users must determine the method of verifying the currentness of certificates appropriate for their applications. A single client may use all three methods, depending on the nature of the transaction, or the sensitivity of the data being accessed.

4.2.3 Cross-certification in the Federal PKI

Federal CAs may cross-certify other Federal CAs, and in some cases may cross-certify non-Federal CAs. Cross-certification requires that the two CAs involved evaluate the policies each uses and make a decision about the policies that apply to the cross-certificates.

CAs cross-certify by issuing each other a certificate. CA X issues a certificate to CA Y and CA Y issues a certificate to CA X. The two certificates are put in a directory as a **crossCertificatePair**, and are not individually stored in the directory. The directory entry for CA X holds a **crossCertificatePair** containing two certificates, one called **forward**, containing the certificate issued by X to Y, and one labeled **reverse**, containing the certificate issued by Y to X. In Y's directory entry there is a "mirror image" **crossCertificatePair**, where the **forward** certificates is the certificate issued by Y to X, and the **reverse** certificate is the certificate issued by X to Y.

For the Federal PKI three functions have been identified for cross-certificates. These functions have been assigned names as follows:

- ***General cross-certificates***: these cross-certificates supplement the certification hierarchy and allow the use of shorter certification-paths. General cross-certificates are governed by rules, described in section 5, so that the propagation of trust, when they are used, is equivalent to the propagation that would result from the use of the hierarchical certification paths to the root CA. They are appropriate when cross-certification will shorten the verification paths and improve performance of frequently used certification paths;
- ***Special cross-certificates***: these cross-certificates provide certification paths that do not conform to the restrictions imposed hierarchically along the path from the root CA. Special cross-certificates may only be created between "leaf" CAs, that is CAs with a hierarchical certification path to the root with a **pathLengthConstraint** (see section 5.4) value that blocks further propagation of trust along the hierarchical certification path to another CA. A **pathLengthConstraint** value of zero is included in the two certificates of special cross-certificates. Therefore only the subjects of certificates issued by the two CAs can use the less restrictive certification path. Special cross-certificates are appropriate when some users of each of the two CAs operate under policies that allow a higher trust level or less restrictions than would otherwise be permitted;
- ***Hierarchical cross-certificates***: these cross-certificates exactly parallel the hierarchical certification path to the root CA. The **forward** certificate of each **crossCertificatePair** for a superior CA is the certificate it issues to the subordinate CA. These cross-certificates are used to

ensure that clients that trust the CA that issued their certificate, and verify certification paths from their own CA, can always find a certification path to any certificate issued in the Federal CA. Hierarchical cross-certificates are required in the Federal PKI.

4.2.4 Directories and other ways to get certification paths

Directories provide a way to find certification paths. Directories may be maintained for broader purposes than the public key infrastructure, and such general directories may be used by the PKI, however some directories may be established by specific CAs. Each CA, including the Root, will either maintain or be associated with a directory.

Each CA will post its **certificate**s and **crossCertificatePair**s in that directory. CAs will use the same directory to periodically post Certificate Revocation Lists (CRLs) of revoked certificates in that directory. User certificates should normally be posted in a directory associated with their issuing CA, but may also be posted in some other directory otherwise associated with the user.

Directories are not ordinarily trusted. That is, validity of certificates or CRLs obtained from directories is established by actually verifying the signatures through a certification path back to a signature by a trusted authority whose public key is independently known to the verifier. Moreover, since CRLs are issued periodically, a check of the most recent CRL only proves that a certificate had not been revoked as of the time the CRL was posted. However some Federal CAs may operate trusted "real-time" directory servers that verify the current status of the certificates issued by that CA and sign the status reports, providing the freshest possible check of the current validity of certificates.

Users may include their certification path with signed documents. Signature verifiers may verify that path back to a trusted CA whose public key is known to the verifier. Such a verification is as secure as verification of a certification path found through accessing directory servers. Similarly, CRLs may be circulated and verified, if current.

5. FPKI Management

The management structure of the FPKI is intended to provide coherent, unified management of the transfer of trust between users of the PKI, while still allowing sufficient local autonomy and flexibility for agencies to expeditiously carry out their business. The Federal PKI will be managed to ensure the integrity of trust relationships established throughout the federal government. The hierarchical certification path defined for the Federal PKI will be used in the management of the Federal PKI. The emphasis in PKI management is to ensure that trust is propagated appropriately between CAs, so that users of one CA are less likely to be adversely affected by the actions of another CA. Management of the Federal PKI is not intended to restrict the services provided by a CA to users holding certificates it issued, nor to protect them from the consequences of the actions of their own CA.

5.1 Policy Management Authorities

PKI management authorities have purview over the operational policies (see section 5.2.1) of Federal CAs and some of the certificate extensions of one or more CAs. Every CA operates under the control of a PKI management authority or under the direct control of the PAA. Management authorities approve CA operational policies and certificate issuance policies (see section 5.2.2).

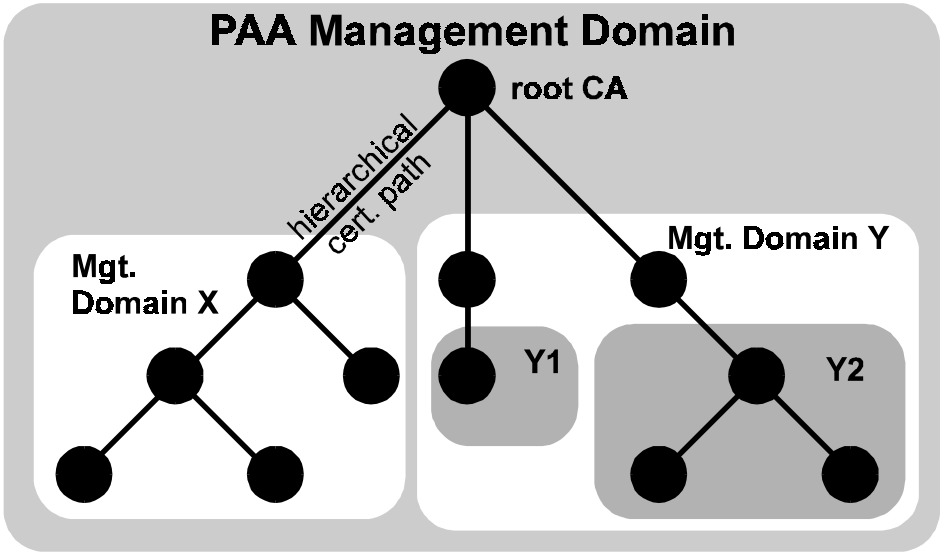

Figure 4 - Nested Domains of FPKI Management Authorities

5.1.1 The Policy Approving Authority (PAA)

The PAA is associated with the root CA and is responsible for the overall management of the Federal PKI. CAs within the Federal PKI will operate under policies approved by the PAA or by subordinate policy management authorities delegated policy management responsibility by the PAA. All certificates issued within the Federal PKI will be issued under specified certificate issuance policies. The PAA and subordinate policy management authorities may use certificate extension fields to restrict the name space for which the certificates issued by CAs will be recognized by other Federal CAs and will use certificate extensions to limit the depth of the paths from the root. The PAA and subordinate management authorities will use the certificate-policies extension of certificates to provide a framework for assigning a level of trust to certificates throughout the Federal PKI.

5.1.2 Subordinate Policy Management Authorities

The PAA may delegate management and policy approval authority to subordinate PKI policy management authorities, as appropriate. The nested structure of PKI policy management authorities takes advantage of the hierarchical certification path for management, and can be viewed as a nested structure of PKI management domains as shown in Figure 4. However, as illustrated, the domains of a PKI policy management authority need not be confided to a single subtree.

5.2 Policies

Each CA within the Federal PKI will operate under a single specified *CA operational policy*. All CA operational policies are approved by the PAA. All certificates issued within the Federal PKI are issued under a specified *certificate issuance policy*. Certificates issued within the Federal PKI will contain a *Federal-Assurance-Level-ID* within the certificate-policies extension, and may contain other policy information as well. The subject of policies is defined in more detail in [POL 95].

5.2.1 Operational Policies

An *operational policy* is a policy that explicitly defines the operation of a CA and its ORAs. This includes:

- backup procedures;
- record archiving procedures;
- restrictions and qualifications of operations personnel;
- functional roles of CA operators;
- physical protection afforded to the CA;
- 140-1 level requirements for CA cryptographic modules;
- access controls for CA private keys;
- ORA operational procedures.

CA and ORA operational policies should be posted in a repository with appropriate visibility such as the NIST Computer Security Objects Register (CSOR). CA operational policies that are the basis for PAA approved Federal Assurance Level IDs must be registered in the CSOR.

5.2.2 Certificate Issuance Policy

A *certificate issuance policy* states the requirements or constraints under which certificates are issued. At a minimum, this includes:

- the identification requirements for users or other CAs being certified;
- procedures required of certificate holders for the generation, safe keeping, revocation, and archiving of key material;

A certificate issuance policy may also include:

- a statement of the community or name-space for which the CA intends to issue certificates;
- any limitations or constraints on the trust that should be placed in the certificate.

Certificate issuance policies should be posted in a repository with appropriate visibility, such as the CSOR. Certificate issuance policies may be stated in the certificate policies extension of certificates. Certificate issuance policies that are the basis for FPKI-sanctioned Certificate Policies must be registered in the CSOR.

5.2.3 Federal Assurance Level

A *Federal assurance level* is a an indication of the general level of trust that can be placed in a certificate, which will be broadly understood throughout the Federal PKI. A small set of Federal Assurance Level values (e.g., low, medium, high) will be assigned object identifiers. A single Federal Assurance Level will be stated in every certificate in the Federal PKI, and stated as **PolicyInformation** in the **certificatePolicies** field of every Federal certificate.

The PAA will determine the highest the highest Federal assurance level that may be assigned to a certificate by a CA. For end-entity certificates this will be based upon the combination of the operational policy of the CA that signed the certificate, and the issuance policy used to issue the cer-

tificate. For CA certificates the Federal assurance level will be based upon the operational policy of the CA that issued the certificate.

The Federal assurance level will provide a consistent trust level framework throughout the Federal PKI. When a certification path is verified, the verifier may use the Federal assurance level to decide if it can place sufficient trust in the certification path.

Each Federal assurance level, included by CA, X, in the certificate it issues to a subordinate, Y, is independent of the Federal assurance level assigned to X by its parent. Therefore the Federal assurance level included by X in Y's certificate, may be higher, equal or lower than the level assigned to X.

5.2.4 Certificate Policy Field contents

The **certificatePolicies** extension in Federal PKI certificates will be used to identify the policies that apply to a certificate. For signature certificates issued to CAs the **certificatePolicies** field will contain the identifier of a Federal assurance level, that states the highest level of trust that can be supported through this certification path, as determined by the issuing CA and its policy management authority;

For signature certificates issued to end-entities, the **certificatePolicies** field will normally contain the identifier of a Federal assurance level, that states the highest level of assurance that can be accorded to the use of this certificate to prove identity. Note that this might be a higher level than could be supported by the parent CAs own signature certificate; in this case the higher assurance level will not propagate outside the domain of the issuing CA and its subordinates.

The use of the **certificatePolicies** field for key management certificates is not understood at this time.

5.2.5 Use of Federal Assurance Levels by Verifiers

The X.509 standard specifies that the inputs to the certification path processing includes a set of initial-policy identifiers, which identifies one or more certificate policies, any one of which would be acceptable for the certification path processing. At each stage of the certification path processing the verifier requires that there be at least one member of the acceptable policy set appear in the **certificatePolicies** field.

Although the determination total set of Federal assurance levels is not yet defined, assume for the sake of illustration that the Federal assurance levels *low, medium* and *high* have been defined. A verifier which wished to require an assurance level of at least *medium*, would include both *medium* and *high*, but not *low,* in the set of initial-policy identifiers.

5.2.6 Cross-Certificate Assurance Level Management

Assurance level management for **crossCertificatePair**s differs for general and special cross certificates:

- ***General cross-certificates***: when a CA, X, cross-certifies with another CA, Y, it evaluates the certification path of Y back to the root. The value of the Federal assurance level included in the certificate X issues to Y is not greater than the lowest Federal assurance level found in the

path back to the root. In the terms of the assurarance level example of section 5.2.5 above, if a third level CA had a certificate with a Federal assurance level of *medium*, and its parent CA had a certificate from the root with a Federal assurance level of *high*, then the highest Federal assurance level that could be assigned to the third level CA in general cross certificates would be *medium*;

- ***Special cross-certificates***: when a CA, X, cross-certifies with another CA, Y, the Federal assurance level included in the certificate X issues to Y is independent of Y's certification path back to the root. Rather, it reflects the special relationship that may exist between X and Y;

- ***Hierarchical cross-certificates:*** The **forward** certificate of a superior CA's **crossCertificatePair** is the certificate issued by the superior to a subordinate CA. The **reverse** certificate may include the highest Federal Assurance Level ID, or a lower level if the appropriate policy management authority wishes to restrict the assurance level of all certification paths outside the domain of the subordinate CA.

5.3 Name Space Management

The Federal PKI will use the certificate extensions for restricting name space (i.e., **subtreesConstraint** or **nameConstraints**) to manage the propagation of trust through certification paths.

5.3.1 Hierarchical Management

As determined by the PAA, the root CA will use certificate extensions to limit the name space to which trust propagates between its subordinate branches. In turn, each subordinate CA may include name space restrictions in the certificates it issues to its subordinates, that limit the propagation of trust between its branches. These restrictions included in the certificate by a CA, may be more or less restrictive than the restrictions included in the CA's certificate from its superior.

Certificate issuance policies may also limit the name space for which a CA may issue certificates. These certificate issuance policies may be more or less restrictive than the name space restrictions imposed through the hierarchical path back to the root. For example, a Federal CA, X, may elect to issue certificates to users with names outside the name space included in the certificate issued to X by its superior, if doing so in accordance with its certificate issuance policies. CAs may issue end-entity certificates, to non-federal entities, if it is within the scope of its certificate issuance policies to do so.

However, trust of certificates issued by X to subjects outside the name space defined by its superior, in the name space restrictions in X's root path certificate, will extend only to:

- other holders of certificates issued by X;
- holders of certificates from CAs with a special cross-certificate with X.

5.3.2 Cross-Certificate Management

Name space management for cross-certificates differs for general and special cross certificates:

- ***General cross certificates***: when a Federal CA, X, cross-certifies with another Federal CA, Y, X will verify Y's certification path back to the root CA, and the name space restrictions included in the certificate issued to Y by its superior. X will include name space restrictions in

the certificate it issues to Y that are at least as restrictive as the restrictions in the certification path to the root CA. Similarly, Y will restrict the name space in the certificate it issues to X, to be at least as restrictive as the restrictions in X's certification path to the root CA. General cross-certification between Federal and non-Federal CAs requires that the certification path to the root CA allow issuance of certificates to non-Federal names, and, furthermore, requires specific approval from the PAA;

- ***Special cross-certificates***: Cross-certifying CAs may have special trust relationships that imply mutual trust greater than that passed through the normal hierarchical path from the root CA. In such cases the name space restrictions included in the certificates of the cross-certificate-pair may be less restrictive than those from certificates issued by superiors;
- ***Hierarchical cross-certificates***: the **forward** certificate of a superior CA's **crossCertificatePair** is the certificate issued by the superior to a subordinate CA. The **reverse** certificate may include no name space restriction, or may include a name space restriction if the appropriate management authority wishes to restrict the transfer of trust for certification paths outside the domain of the subordinate CA.

5.4 Path Length Management

The **pathLenConstraint** field of the basicConstraints provides a mechanism to limit the length of certification paths. A CA with a certificate whose **pathLengthConstraint** value is zero, may only propagate trust to end-entities. The PAA will assign a **pathLenConstraint** value for each certificate the root CA issues, that limits the depth of each tree. Successive subordinate CAs may choose to further restrict path length with the **pathLengthConstraint** to a level that is less than that implied by decent from the root CA.

5.4.1 Cross-Certificate Management

Path length management for cross-certificate-pairs differs for general and special cross certificates, as well as hierarchical cross-certificate-pairs:

- ***General cross-certificates***: when a Federal CA, X, cross-certifies with another Federal CA, Y, X will verify Y's certification path back to the root CA, and the path length remaining to the CA to issue certificates to subordinate CAs. X will include a value in the **pathLengthConstraint** field the certificate it issues to Y that is at least as restrictive as the restrictions in the certification path to the root CA. Similarly, Y will include a **pathLengthConstraint** field in the certificate it issues to X, that is at least as restrictive as the restrictions in X's certification path to the root CA;
- ***Special cross-certificates***: the pathLengthConstraint field value for special cross -certificate-pairs is always zero. This means that special cross-certificate-pairs only transfer trust to the immediate end-entities holding certificates issued by the cross-certified CAs;
- ***Hierarchical cross-certificates***: the **forward** certificate of a superior CA's **crossCertificatePair** is the certificate issued by the superior to a subordinate CA. The **reverse** certificate may include no **pathLengthConstraint** field, or may include a **PathLenConstraint** field if the appropriate management authority wishes to restrict the length of certification paths outside the domain of the subordinate CA.

6. Attribute Authorities

Attribute authorities issue attribute certificates. While attribute authorities may be operated in conjunction with a CA, they may be entirely separate. In general, attribute authorities are associated with privileges, roles and access controls. An attribute authority is issued a signature certificate by a CA.

7. Compromise Recovery

Compromise recovery is a significant concern in the PKI. Provisions are needed to recover from compromises of private keys. The detailed policies for recovery from key compromise are stated in [POL 95]. This section summarizes the principles of compromise recovery.

7.1 Compromise of User Keys

Recovery from compromised user keys is the responsibility of the CA that issued the certificate that has been compromised. The compromised certificate is added to the next CRL, and, if the policy of the authority is to issue CKLs, on the next CKL. It may be the policy of an authority to issue a new CKL each time a compromise is discovered, or to issue the CKL at the discretion of the authority, whenever needed. The client may be issued a new certificate by the authority if appropriate.

A user may sign a message to the CA that issued his certificate, stating that the private key has been compromised and requesting that the certificate be revoked, using the compromised private key. ORAs may also request CAs to revoke certificates issued through their registration process, if a key compromise is detected.

7.2 Compromise of CA Keys

Compromise of the private key of a CA invalidates all the certificates issued by that authority, since it results in the possibility of certificates forged with the compromised private key. In general, recovery from the compromise of a CA private key requires:

- the generation of a generation of a new CA public-private key pair;
- the revocation of the compromised CA certificate by its parent CA. This invalidates the certification paths of all entities subordinate to the compromised CA;
- the issuance of a new certificate from the parent of the compromised CA;
- the issuance of new certificates, signed with the new CA private key, to replace the certificates issued with the compromised key.

Since compromise of the CA private key does not itself compromise the private keys of its subordinates (although it may allow the forgery of certificates), it is not, in general necessary to replace the subordinate public-private key pairs, and the new certificates may retain the old user public key. However, it is necessary to provide all subjects of certificates signed with the compromised key with new certificates and the public key of the CA, by a secure process.

Therefore, if a root CA private key is compromised, all its subordinate CAs may be issued new certificates with their old user public key, and the certification path for certificates issued by subordinate CAs may be restored without issuing new certificates to users. However it is necessary to notify all users of the PKI of the new root public key by a secure process.

7.3 ORA Compromise

If an ORA key is compromised, it is possible that user certificates may have been issued to fictitious users, or with incorrect attributes. Recovery requires revocation of all certificates issued through the compromised ORA using the compromised key. If the compromise date is known, then it is only necessary to revoke certificates issued after the compromise occurred. If the ORA has retained complete, uncompromised records of the users who applied for certificates through the ORA, then new certificates may be automatically issued to users whose certificates have been revoked. Otherwise, users whose certificates are revoked, must reapply to the ORA to be issued a new certificate.

8. Implementation Technologies

8.1 Clients

Availability of PKI client functionality to every Federal information system and every Federal user is needed. Some users require the assurance that is best provided by personal hardware cryptographic tokens. Other users and applications cannot justify the additional expense of cryptographic hardware and tokens for every client (i.e., every PC, every data terminal, every workstation). Entirely software based solutions are appropriate for many clients and their applications. Hardware and software based clients must be capable of secure interoperation.

8.1.1 Software Implementation

To allow government users universal availability of an affordable suite of security services (i.e., signature based authentication, integrity, and confidentiality key exchange, as well as confidentiality for communications sessions or messaging) for computer data and communications, the PKI will include a suite of algorithms and protocols that:

- provide the following security services:
  - public key digital signatures for:
    - ◊ authentication;
    - ◊ integrity.
  - certificate or public key based symmetric key exchange/agreement for:
    - ◊ messaging confidentiality;
    - ◊ communications session confidentiality;
  - symmetric key encryption based confidentiality.
- may be implemented entirely in software for PKI clients;
- use publicly disclosed algorithms that need not be protected;
- may be run on untrusted computer systems (i.e., systems that have not been verified as conforming to any trust criteria).

Technical policies for implementing PKI client software cryptographic modules and storing private keys are stated in [POL 95]. The implementation of client cryptographic modules affects the level of assurance accorded to certificates and signatures. Accordingly some high assurance policies for issuing certificates will require hardware cryptographic tokens.

8.1.2 Hardware Implementation

Alternatively, user keying material may be retained in trusted hardware cryptographic modules and signatures or session keys generated on that trusted module. Such modules will not export user signature private keys. Access to the cryptographic functionality of the module may be protected by passwords, or possibly by other means such as biometrics.

The PKI may also support algorithms that are not publicly disclosed and for which software implementations are not authorized. Such algorithms will be implemented in trusted cryptographic modules.

Some high assurance policies for issuing certificates will require use of hardware cryptographic tokens.

8.2 Authorities

The systems used by CAs to sign certificates will require a high level of assurance. Technical policies governing the assurance required in the implementation of CAs is stated in [POL 95].

9. Interoperation

The PKI will support secure communications with business, other branches of the Federal Government, the public, state and local governments, as well as between Federal departments and agencies. Interoperation may also be required with Federal users of Type 1 cryptography. The Federal PKI will therefore support and interoperate with a broad range of technologies, as appropriate, including commonly used technologies that are not approved for use to protect UBS communications between Federal users. [MOD 95] contains a more detailed treatment of interoperation issues.

9.1 Interoperation with the Type 1 Infrastructure

The primary burden for interoperation between Type 1 users and the Federal PKI rests with the Type 1 users:

- Type 1 Certificate Authorities may also issue PKI certificates;
- Type 1 tokens and modules may also support PKI certificates and algorithms;
- the impact of the PKI design on the ability of the existing Type 1 infrastructure to support the PKI will be considered in the design of the PKI.

9.2 Interoperation with non-Federal Users

9.2.1 Algorithms

The predominant digital signature and messaging key exchange algorithm used outside the Federal Government is RSA [RIV 78]. The RSA algorithm is also commonly used for session key exchanges. RSA is not an approved federal standard. The requirements of Federal users to interoperate with non-Federal entities varies greatly and the extent to which they support interoperation will vary, however some Federal users may need to interoperate securely with users of RSA signatures and Diffie-Hellman key exchanges. Interoperation with non-Federal users is based on the following assumptions:

- RSA is the commercial defacto standard algorithm for digital signatures and key exchange;
- The DSS is the signature standard used by the Federal PKI;
- There are two forms of cryptographic applications of interest:
    1. open generic applications such as secure e-mail;
    2. proprietary security features of commercial products.
- The Federal PKI applies primarily to the first case, open generic applications, and is not expected to provided certificates for the proprietary security provisions of particular unique products or services;
- Government agencies and employees will be permitted to join external PKI as a means of conduction official business as required, with appropriate waivers of FIPS 186.

The basic principles of interoperation between users of the Federal PKI and other PKIs are:

- The Federal PKI supports only DSS signature certificates. Federal users who require RSA signature capability must waive FIPS 186 and obtain RSA certificates from another PKI;

- Federal PKI users may verify the RSA signatures of nonfederal parties, in accordance with the their security policy. Note: this requires either a change to the applicability statement of FIPS 186 or an agency by agency waiver of FIPS 186;

- Federal PKI users may use the RSA or Diffie-Hellman algorithms to distribute or exchange symmetric confidentiality message or session keys.

Federal use of public key algorithms that are not FIPS approved, such as RSA, when implemented in proprietary systems, is not necessarily a Federal PKI interoperability problem, since such proprietary systems are not intended for broad interoperability, and may not use a formal PKI. Nevertheless, use of algorithms that are not FIPS approved to protect government information resources does generally require a waiver.

9.2.2 Cross-Certification

The Federal PAA must approve all general cross-certificates with non-Federal CAs. The optional policy mapping, path length constraint, and the subtrees constraint extension fields of the X.509 v3 certificates may be used by the PAA to constrain the use of cross certification links with non-federal CAs and infrastructures. Special cross-certificates between Federal and non-Federal CAs do not require approval of the PAA, since trust propagates only to those Federal users who hold certificates from the cross-certified Federal CA.

Waivers to FIPS 186 may be required for Federal use of certification paths that do not use Federally approved digital signature algorithms.

9.2.3 Certificates Issued to non-Federal Users

Federal CAs may issue end-entity certificates to non-Federal users in accordance with their certificate issuance policy. Name space constraints in the hierarchical root path may, however, limit propagation of trust to certificates issued to subjects with non-Federal names. In the case where a Federal CA issues a certificate to an end-entity outside the name space specified in its hierarchical root path, trust would propagate only to holders of certificates from that CA, and not to the Federal PKI in general.

10. Servers and Agents

Some security related servers and agents may be operated by the Federal PKI, or be used by the Federal PKI. The important services that have been identified are described in some detail below. The following list is not exhaustive, and a need for additional kinds of security servers and agents may be identified.

10.1 Directory Services

The PKI will make use of directory services. Conceptually, at least, these services will be based on the X.500 standard which provides a unified framework for all directory services. More pragmatically, there are a variety of directory services that follow the X.500 model to a greater or lesser degree. It is uncertain that *the Directory,* a unified global service as conceived in the X.500 standard will become reality. The PKI does not depend on the specific details of X.500 directories, but it does require for many purposes and applications that clients can access certificates and Certificate Revocation Lists through directory services of some kind.

The directory provide a means for obtaining the certificates of clients and certificate authorities themselves as well as certificate revocation lists. This allows clients to verify certification paths and that unexpired certificates have not been revoked. It will also allow clients to use the recipient's public key, from his certificate, to send an encrypted message, without prior key negotiation. In some cases directory servers may be maintained by the authorities that issue and manage certificates, but this need not be the case, and more general directories maintained for routing or location services may also provide directory information, including certificates.

Some directory servers may provide a "trusted service," that is the certificates or the information on the status of certificates they provide in response to queries may be accepted as current and valid without further verification. Such trusted directory service require that the directory authenticate itself to the user and that the directory queries between the user and the trusted directory be secured.

Other directory servers may be "untrusted," that is a user obtaining a certificate or a Certificate Revocation List (CRL) from such servers must verify the certificate by:

- verifying the certification path (a chain of certificates where each of the issuer signatures has been verified) back to some authority that is trusted by the user, and;

- checking that the certificate to be verified is not contained in the current Certificate Revocation List (CRL) of the issuing authority. The CRL itself, if obtained from an untrusted directory server, must be verified by verifying its CA certification path.

Access to some directory servers or the certificates of specific users may be restricted.

10.2 Servers and Agents

The infrastructure will be augmented by a variety of security-related servers and agents. These servers or agents will generally be trusted users with certificates issued by some appropriate authority. They will support the needs of users, or, in some cases, of the Federal PKI hierarchy itself. In this section these servers are described in terms, such as digital notary, and document recorder that approximate services now available for paper documents. The sections below describe some of the services may be provided. This aspect of the infrastructure is not well understood, and the actual digital servers that emerge may be combined in other ways, and given other names.

10.2.1 Digital Notary Servers

The digital notary server provides a service roughly equivalent to a notary public. Digital notaries operate on the message digests of digital and the digital signatures that may be applied to those documents, rather than the documents themselves. The digital notary may offer at least two services:

- to add a time-date stamp to a message digest of a document and sign the message digest plus the time-date stamp. This notarization provides proof that the document existed at a particular point in time and is the date-time stamp service of Figure 1;
- to verify the signatures applied to a signed document and generate a signed, dated notarization statement that includes the message digest of the subject document and the distinguished names of each of the signatories.

The certificates of notaries should be registered in a permanent archive. The notary keeps a log of the notarizations but not copies of the documents.

10.2.2 Digital Recorder Servers and Archives

The digital recorder server provides the service of a document recorder, that is a document archive where documents may be registered for safekeeping and to make a permanent record. The digital recorder permanently retains, under its sole control, a dated copy of digital documents registered with it. The digital recorder will, upon request, issue a signed copy of recorded documents, stating the date of registration.

Among the uses of digital registries are the key (or certificate) archiving service of Figure 1. They can provide a repository for expired certificates, to allow the verification of signatures on old documents. If digital documents are to replace paper documents, then it must be possible to verify digital signatures long after the certificates used to sign the documents have expired, and after the authorities that issued the certificates have ceased to exist. To be useful for this purpose, a digital registry must be a permanent archive, independent of particular authorities.

The verification of the authenticity of signed digital documents, long after they were signed, presents particular problems. The advantage of digital documents in archives is that they can be copied as often as needed without any alteration or degradation, which is generally impossible with analog records. This allows a perfect copy to be maintained through many generations of copies. The disadvantage of digital documents for archival purposes is that, as a practical matter digital storage media have a short useful life, and documents must be copied frequently to maintain them [Rothen 95]. Therefore, the physical forensic evidence that may help to authenticate original old paper documents is not available for digital documents. Moreover, we must assume that any presently secure digital signature technology may eventually fall to advances in computer power and cryptography.

Since any present digital signature technology may ultimately be compromised by future progress in computing power and cryptography, the validity of recorded documents does not primarily depend on any digital signature made by the recorder at the time of document registration. Rather the validity of recorded documents depends on the physical control of the registered copy of the document by the trusted recorder. If a recorder has retained an accurate dated copy of a signed digital document, if a true copy of the signer's certificate exists, and if it were impractical to forge the signature at the time the document was registered, then verification of the signature is meaningful even after it becomes possible to forge the signature.

For truly long term verification of certificates and signatures, it is not sufficient to register only the certificates of the authorities themselves, because we must assume that it will eventually be possible to derive the authority's private key for any current public key and forge a certificate. Registering all certificates issued by an authority would allow detection of certificates forged at a later date. Similarly, signed digital documents whose authenticity may be important at a much later date, must registered contemporaneously with their signing. Then, knowing from the registry:

1. the contents and signature of a document that was registered on a given date, and,
2. the complete certificate path supporting the signatures;

It is possible to verify the authenticity of the document at a later time, even after it is practical to derive the private key from the public key.

However, very long term (i.e., for centuries) digital archive services are problematic, due to the rapid rate of change of digital media, applications and file formats, and the uncertain storage lifetimes of digital media [Rothen 95]. Any presently practical digital archive must periodically copy data onto new media, for even where a storage medium has a long lifetime, data readers for the storage medium will become unavailable after newer media come into use. This means that a requirement to maintain long term archives of large numbers of public key certificates is potentially burdensome. . Unless registries are funded from public tax moneys, they will need to charge a registration fee sufficient to maintain copies of the documents in perpetuity.

One possible partial solution is to require the PKI itself to maintain a record of all the certificates it issues for a relatively short period, say 10 years, and to permanently archive in a digital registry only the certificates of authorities themselves. A user, wishing to register a signed document, should then also register the certificates of the signatories with the document, and bear the cost of registering both.

For the Federal PKI, the certificate archiving function is expected to ultimately be the responsibility of the National Archive.

10.2.3 Digital Certified Delivery Servers

Proper maintenance and design of the PKI makes it difficult for users to repudiate their own signatures. While digital nonrepudiation can be accomplished by cooperating parties without a trusted server, cooperation is not always assured. Certified delivery servers provide services analogous to those of process servers and certified or registered mail. A digital nonrepudiation server provides a trusted third party that can verify that a digital document was in fact delivered to its intended recipient, or that a good faith, best effort was made to deliver the document, even without the cooperation of the intended recipient. The Federal Government may need nonrepudiation servers, but they are not needed to support the operation of the PKI itself.

10.2.4 Ticket Granting Agents

Ticket granting agents issue tickets that grant limited-time access to information resources. Although now widely used with symmetric key rather than public key authentication systems, they can also be used with public key technology to centralize management of access control. In effect, an Organizational Registration Authority (ORA) that does not issue certificates itself, but vouches for the identity of prospective certificate holders to a certification authority, is a ticket granting agent.

10.2.5 Key Escrow Agents

Key escrow agents provide a trusted, secure repository for keying material. Key escrow agents can protect users against the loss of stored data due to lost keys, and provide for legally authorized interception of encrypted data communications, or allow management monitoring of the use of information resources. Key escrow for law enforcement interception is an automatic feature of the Escrowed Encryption Standard [FIPS 185].

List of Acronyms

CA	Certification Authority
CKL	Compromises Key List
CRL	Certificate Revocation List
CSOR	Computer Security Objects Register
FPKI	Federal PKI
MISSI	Multilevel Information Systems Security Initiative
OID	Object IDentifier
ORA	Organizational Registration Authority
PAA	Policy Approval Authority
PKI	Public Key Infrastructure
UBS	Unclassified But Sensitive

References

[DAM 95] ISO/IEC JTC 1/SC 21 document, *Draft Amendments DAM 4 to ISO/IEC 9594-2, DAM 2 to ISO/IEC 9594-6, DAM 1 to ISO/IEC 9594-7, and DAM 1 to ISO/IEC 9594-8 on Certificate Extensions,* August 1, 1995.

[FIPS 46] FIPS PUB 46-2, *Data Encryption Standard (DES),* NIST, 1993.

[FIPS 180] FIPS PUB 180, *Secure Hash Standard,* NIST, 1993.

[FIPS 140] FIPS 140-1, *Security Requirements for Cryptographic Modules*, NIST, 1994.

[FIPS 185] FIPS PUB 185*, Escrowed Encryption Standard (EES),* NIST, 1994.

[FIPS 186] FIPS PUB 186, *Digital Signature Standard (DSS),* NIST, 1994.

[Garf 95] Simon Garfinkle, *PGP: Pretty Good Privacy*, O'Reilly & Associates, Inc., 1995.

[MOD 95] TWG-95-89, *Public Key Infrastructure Models of Cross-Certification and Accommodation,* 09/04/95.

[POL 95] TWG-95-81, *Technical Security Policy for the Federal PKI*, 25 Aug. 1995

[PROF 95] TWG-95-88, *Public Key Infrastructure (PKI) Federal X.509 Certificate Profile,* 15 September 1995

[RIV 78] Ronald L. Rivest, Adi Shamir and Leonard L. Adleman, "A Method for Obtaining Public Key Signatures and Public Key Cryptosystems,*" Communications of the ACM,* 21 (1978).

[Rothen 95] Rothenberf, Jeff, "Ensuring the Longevity of Digital Documents," *Scientific American*, Vol. 72, no. 1, Jan 1995, pp. 42-47.

[X.500 93] CCITT Recommendation X.500, *The Directory,* 1993.

[X.509 93] CCITT Recommendation 509, *The Directory: Authentication Framework,* 1993.