Chapter 9

PUBLIC KEY CRYPTOGRAPHY AND KEY MANAGEMENT

CONTENTS

1. GENERAL

a. The use and management of certificate-based public key cryptography for the Department of Energy (DOE) requires the establishment of a public key infrastructure (PKI). This chapter defines the policy related to roles, requirements, and responsibilities for establishing and maintaining a DOE PKI and the documentation necessary to ensure that all certificates are managed in a manner that maintains the overall trust required to support a viable PKI.

b. Public key certificates are used by Certification Authorities (CAs) to identify, validate, and bind an individual's identity to a public key. In so doing, CAs operate in compliance with two separate documents that define the applicability of the public key certificates—the certificate policy(ies) and the certification practice statement—each of which is discussed in Section 7 of this chapter.

c. The public key cryptographic systems described in this chapter may not be used to provide security for classified information transmitted across open networks or stored on computer systems that do not meet the requirements for open storage of classified information. In both cases, encryption and protection methods approved by the National Security Agency (NSA) must be used.

2. SCOPE

a. This chapter does not require any DOE or DOE contractor facility to use public key cryptography or establish a CA. Many applications that can use public key cryptography (asymmetric cryptography) can also be satisfied by using other forms of encryption (symmetric cryptography). The decision to use public key certificates is left to the discretion of the parties responsible for those applications. If establishment of a CA creates a financial or operational burden on an organization, that organization can instead use certificates issued by other DOE CAs or pursue alternative methods.

b. This policy applies to both DOE CAs and CAs operated on behalf of the DOE who:

(1) Participate in or cross-certify with the DOE PKI operated by the DOE Policy Management Authority (PMA);

(2) Issue certificates that are used for symmetric key exchange to protect Unclassified Controlled Nuclear Information (UCNI), DOE Official Use Only (OUO) information, and other Federal Unclassified information that is deemed sensitive by the data owner;

(3) Issue certificates that are used to establish financial transactions for, or on behalf of, DOE for which the relying parties require a digital signature, unless a pre-arrangement is made that transfers funding without relying on the security of the certificate; or

(4) Issue certificates that are used to establish or verify the electronic identity of entities for need-to-know protection of classified information or resources where authority to receive such information or access has been pre-established.

c. Approved and authorized DOE public key systems must strive to comply with all applicable Federal laws, regulations, and standards and should be designed to be consistent with the Federal PKI. For most applications, this compatibility will provide an extension of trust to the public key systems of other Federal agencies. DOE public key certificates may be used by other Federal agencies, DOE employees, contractors, subcontractors, vendors, and customers. This chapter was written under the assumption that X.509 Version 3 (or later) certificates will be used throughout DOE. Use of certificates other than X.509 Version 3 or later is discouraged.

3. PURPOSE

a. This chapter sets forth requirements for DOE Elements that have implemented or plan to implement public key systems within the scope of this chapter, Paragraph 2b. DOE Elements that comply with these requirements may use digital signature for authentication, data integrity, and non-repudiation as specified in the applicable certificate policy (CP). Certificates issued in accordance with this chapter may be used for key exchange of symmetric encryption keys for data privacy, as defined in the applicable CP, provided that all encryption algorithms are Federal Information Processing Standard (FIPS) compliant.

b. Issuance of a public key certificate in conformance with this chapter does not automatically convey access privileges to any computers or systems or confer authority in any business applications. Such authority and privileges are normally established through other mechanisms, such as approval by the data owner, business process owner, and/or local security official, as appropriate.

c. Additionally, CPs are required and must be approved by the Policy Management Authority (PMA). In some cases, a different process for approving CPs may be required. Such issues are to be addressed to the Office of Cyber Security (SO-33), as the Chair of the PMA for handling. Certification practice statements (CPSs) are also required and must be approved by either the PMA, appropriate DOE Operations Office, site CIO, or other CIO-appointed representative, prior to the issuance of certificates by the CA. This chapter also addresses establishment of the organizational structure and responsibilities of the CAs, Registration Authorities (RAs), and End Entities (EEs).

d. The requirements specified within this chapter must be used by the PMA to establish minimum DOE operational policies and procedures and to assess CA operations.

4. TERMINOLOGY

a. Certificate Policy (CP) - A named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements.

b. Certificate Revocation List (CRL) - A list of revoked certificates that have not yet expired.

c. Certification Authority (CA) - An entity that signs, issues, and manages public key certificates. The CA may be the third party in a three-party trust model.

d. Certification Path - A set of certificates that provide a chain or path of trust from the relying party to the entity whose public key is required by the relying party.

e. Certification Practice Statement (CPS) - A specific written declaration of the practices that a CA employs in issuing certificates. This declaration explicitly governs the operation of a CA, its RAs, and its EEs.

f. Compromised Key - A private key that has been exposed to unauthorized access, or that has been lost, stolen, or subjected to circumstances in which compromise could reasonably be assumed possible. This exposure can apply to the key or activation data, such as PIN numbers.

g. Directory - A database used to store and distribute public key certificates, certificate revocation lists, and other certificate-related information. A directory is sometimes referred to as a repository.

h. DOE Public Key Infrastructure (PKI) - The PKI that has been established to support the use of public key cryptography for the Department of Energy in conducting DOE business and protecting DOE information.

i. Encryption - The use of an encryption algorithm for rendering data unintelligible by executing a series of conversions controlled by a key.

j. End Entity (EE) - Any user of a certificate, generally an individual; however, also includes hardware, such as servers, etc.

k. Government Information - As defined by the Office of Management and Budget (OMB), Circular No. A-130, “Management of Federal Information Resources,” dated 2-8-96, all information created, processed, disseminated, or disposed of by or for the Federal government.

l. Policy Approving Authority (PAA) - The entity who defines and approves the security policy under which the Policy Certification Authority operates.

m. Policy Certification Authority (PCA) - The entity who formulates the policy and operational procedures under which it and its subordinates issue and manage public key certificates.

n. Policy Management Authority (PMA) - The entity comprised of the PAA, the PCA, a representative of each site with a CA, and/or other representatives from sites participating in the DOE PKI. The PMA must operate under the oversight of the PCA and address issues that affect the DOE PKI.

o. Private Key - The portion of a cryptographic key pair in an asymmetric encryption system that is known only to the owner of the key pair.

p. Public Key - The portion of a cryptographic key pair in an asymmetric encryption system that is distributed for use by individuals other than the owner.

q. Public Key Certificate - A digitally signed document used to identify, validate, and bind an individual's identity to a public key, also referred to in this chapter as a certificate. The certificate format in this chapter is based on the X.509 Version 3 certificate.

r. Public Key Cryptography - A form of cryptography that uses a pair of mathematically related keys to encrypt and decrypt information. The relationship between the key pairs is such that information encrypted with one of the keys can be decrypted only with the other key of the pair.

s. Public Key Infrastructure - An infrastructure consisting of hardware, software, roles, and responsibilities necessary to support the use of public key cryptography.

t. Registration Authority - An entity designated by the CA to authenticate the identity and the organizational affiliation of an EE and to perform other functions as defined in the applicable CP and CPS.

u. Relying Party - A recipient of a certificate who acts in reliance on that certificate and/or digital signature verified using that certificate. In this document, the terms "certificate user" and "relying party" are used interchangeably.

v. Split Knowledge - Separation of data or information into two or more parts, each of which is constantly under the control of separate authorities or teams so that no one individual or team knows all the data or information.

w. Trust - Confidence that the components of a system will perform in a way that will not violate the security policy governing the use of the system.

5. GUIDANCE DOCUMENTS

a. S. Chokhani and W. Ford, "Certificate Policy and Certification Practice Statement Framework" (Draft)

b. Booz-Allen & Hamilton Inc., "Federal Public Key Infrastructure (PKI) Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extension Profile" (Draft)

c. ISO/IEC/11770-1:1996, "Information Technology-Security Techniques-Key Management- Part 1: Framework"

d. ISO/IEC 9594-8, 2/6/97, "Banking - Certificate Management"

e. National Institute of Standards and Technology, "Minimum Interoperability Specification for PKI Components" (Draft)

f. National Institute of Standards and Technology, "Public Key Infrastructure (PKI) Technical Specifications (Version 2.1): Part C- Concept of Operations" (Draft)

6. ROLES AND RESPONSIBILITIES. The DOE PKI is comprised of the Policy Approving Authority (PAA), Policy Certification Authority (PCA), Policy Management Authority (PMA), Certification Authorities (CAs), Registration Authorities (RAs), End Entities (EEs), and the Directory Service (DS). The following subsections describe the responsibilities of each role.

a. Policy Approving Authority. The Chief Information Officer, SO-30, serves as the DOE PAA. The PAA evaluates and approves overall PKI policy and practices and manages the certificates. The PAA delegates oversight for PKI operation to the PCA and periodically reviews PCA practices for consistency and operational efficiency.

b. Policy Certification Authority. The Office of Chief Information Officer, Office of Cyber Security (SO-33), serves as the DOE PCA. The PCA is the chair of the PMA and is responsible for developing and issuing policy, approving CPs, reviewing CPSs, and conducting assistance visits for the CAs. The PCA, through the PMA, is also responsible for coordinating distinguished names for the CAs, maintaining a master registration list of all DOE CAs and CPs, and providing policy object identifiers for all approved CPs.

c. Policy Management Authority. The PMA is comprised of the PAA, the PCA, a representative of each site with a CA, and/or other representatives from sites participating in the DOE PKI. The PMA must operate under the oversight of the PCA and address issues that affect the DOE PKI.

d. Certification Authority. A CA may be designated at each site, as necessary, to support local needs and to provide a certification path to other CAs within the Department, if needed. The operation of a CA is viewed as a sensitive function in much the same way as issuing of badges, dispensing of cash, etc. As such, personnel should be assigned CA responsibilities with the same rigor that is applied to other sensitive functions. The name of the CA should be forwarded to the PCA for participation in the PMA and for inclusion on the distribution list for receipt of pertinent information. The number of CAs should be kept to a minimum for operational and cost efficiency. Each CA must have sufficient resources to maintain operations in conformity with the applicable CPs and CPSs.

(1) A CA is responsible for:

(a) Issuing certificates to authorized entities in accordance with the requirements of this chapter and the approved CPs and CPSs under which they operate;

(b) Maintaining records as described in Section 11 of this chapter;

(c) Making public key certificate and certificate revocation information available to all certificate users as specified in the applicable CP;

(d) Complying with the DOE policy and legal requirements for emergency key recovery of EE private keys used for privacy data decryption;

(e) Ensuring that all subordinate RAs and EEs are aware of their responsibilities to comply with established policies and procedures;

(f) Authorizing the RA to begin his/her duties upon completion of the RA registration;

(g) Ensuring that the RA will obtain all software, hardware, and training necessary to perform his/her assigned duties;

(h) Providing the EE with the necessary software and training to generate the public/private key pair and comply with the DOE policies and procedures; and

(i) Maintaining their private signing key in a manner compliant with the approved CPs and CPSs.

(2) CA Registration. Each CA is subject to an audit at startup to ensure compliance with predetermined criteria developed by the PMA. The PCA will coordinate CA-distinguished names as defined in the CPs and CPSs. In no case will the CA's keys, used for signing certificates, be exported in clear form. CA keys that are external to the public key system must be provided sufficient protection to ensure they are not compromised. The protection measures must be documented in the CPS.

e. Registration Authority.

(1) An RA may be designated, as required, at each facility and will operate under the authority of the CAs as specifically defined in the applicable CP. Typical responsibilities of the RA would include:

(a) Maintaining his/her private signing key in a manner designated in the approved CPs and CPSs;

(b) Ensuring that the EE has the necessary software and training to generate the public/private key pair and comply with the DOE policies and procedures; and

(c) Maintaining records as described in Section 11 of this chapter.

(2) RA Registration. Because the RA is a link in the trust chain, each RA must be formally designated to operate in support of the CA. Ideally, the RA should appear in person before the CA and present proof of identification. If the RA cannot appear in person or his/her appearance is cost-prohibitive, the CA may use other measures to positively verify the identity of the RA.

f. End Entity Sponsor. The End Entity Sponsor (EES) may be any member of management within DOE, its contractors, and/or subcontractors who recognizes that a DOE or non-DOE EE has an operational need for a public key certificate. The EE could be a vendor or partner outside of DOE who has a limited, temporary need for a DOE certificate in order to accomplish or support a specific DOE function or mission associated with DOE. An EES is not required in all situations. The EES is responsible for the following:

(1) Validating the EE's affiliation with the EES;

(2) Verifying the accuracy and completeness of the EE's certificate information; and

(3) Notifying the CA or RA of any termination of sponsoring relationship.

g. End Entity.

(1) The EE may be any DOE employee, contractor, vendor, business associate, or proxy for a computer system who has a valid operational need for a public key certificate. The EE agrees to comply with all policies and procedures prescribed in the applicable CPs and CPSs. EEs are responsible for the following:

(a) Providing complete and accurate certificate information;

(b) Protecting their private keys in accordance with the approved CPs and CPSs; and

(c) Notifying the CA or RA immediately of any actual or suspected loss or compromise of private key.

(2) End Entity Registration. The requirements for EE registration and renewal will be specified in the CPs and CPSs.

7. **CERTIFICATE MANAGEMENT.** The CPs and CPSs are the principal documents providing certificate management for a CA. The description of each and their respective requirements are described in this section.

a. Certificate Policies.

(1) General. A certificate policy (CP) is a named set of rules that indicates the applicability of a certificate to a particular community and/or class of applications with common security requirements. Accordingly, the CP defines certificate applicability and the general operational requirements that a CA must follow when issuing certificates. CAs who write their own CPs must forward them to the PMA for approval. Some situations require a different process for approving CPs. Such exceptions must be addressed to SO-33 as the Chair of the PMA. Another option is for CAs to implement certificate policies that have already been written and approved.

A CA must issue only certificates specified in the applicable approved CPs. In addition, each CA must use the appropriate CPs to develop a detailed and site-specific CPS in order to define the procedures for issuing, maintaining, revoking, and archiving certificates.

(2) Requirements. If a CA issues a certificate under more than one CP, a CP designation must be included in the certificate in a cryptographically secure manner. The CP must identify the management, community, and applicability of the certificates. All CPs must be approved by the PMA and the policy object identifier (OID) must be registered with the PCA.

At a minimum, a CP must address the following topical areas:

(a) Community and applicability of the certificate in accordance with the X.509 definition of CP;

(b) Roles and obligation of participating entities;

(c) Identification and authentication of entities;

(d) Public key certificate issuance, management, archives, and revocation (including reasons and authorities for revocation);

(e) Private decryption key issuance, management, archival, and recovery;

(f) Cryptographic security requirements for public key, private key, and key exchange mechanisms;

(g) Physical security and access controls for critical components;

(h) Computer security and network security protection for critical components;

(i) Cross-certification agreements; and

(j) CP document administration and publication.

b. Certification Practice Statements.

(1) General. A certification practice statement (CPS) is a specific written declaration of the practices that a CA employs in issuing certificates. This declaration explicitly governs operation of a CA, its RAs, and EEs. A CPS must be written by each CA and identify specific methods and procedures for operating the CA and managing the certificates. All CPSs must be reviewed and approved by the PMA, appropriate DOE Operations Office, site CIO, or other site-CIO-appointed representative, prior to the issuance of certificates by the CA. Field sites providing CPS approval must forward notification to SO-33, as the Chair of the PMA, along with a copy of the CPS.

(2) Requirements. A CPS must identify the CPs to which it applies, and at a minimum, address the following topics:

(a) Record archiving procedures;

(b) Restrictions and qualifications of operations personnel;

(c) Functional roles of CA operators;

(d) Identification and authentication of entities;

(e) Public key certificate issuance, management, archival, and revocation including revocation procedures;

(f) Private key issuance and management, and the procedures for archival and recovery of private decryption keys;

(g) Cryptographic security mechanisms used for public and private keys and key exchange mechanisms;

(h) Profiles for certificates and certificate revocation lists, if used;

(i) Physical security and access controls for critical components;

(j) Computer and network security practices for critical components;

(k) Cross-certification agreements;

(l) CPSs that document administration and publication; and

(m) Backup procedures.

c. Cross-Certification. Cross-certification is a mechanism that enables two CAs to exchange certificates, thereby establishing a trusted relationship. Cross-certification is intended to simplify certificate paths for efficiency (i.e., shorter verification paths). This differs from the strict hierarchy model wherein trust is passed down along branching certificate paths. The DOE PKI is organized as a hierarchy for administration purposes. For operational purposes, cross-certification allows the establishment of a network of trust relationships among approved CAs inside and outside DOE. Cross-certification outside of DOE might create a significant risk for the CA, as well as the other users of PKI at DOE. For that reason, SO-33, as the Chair to the DOE PMA, must be notified of the intent to cross-certify outside the Department 30 calendar days prior to exchanging CA certificates.

Under certain circumstances, the DOE PCA can function as a root CA and provide cross-certification and policy mapping between the CAs operating in the DOE PKI and CAs of other agencies or organizations, if needed.

d. Directory Service (DS). The DOE public key directory will be based on the X.500 directory concept or other directory concepts that foster compatibility. The directory must initially consist of a collection of local directories, managed by CAs who cooperate to create a DOE public key database of information. The information in the directory is collectively known as the Directory Information Base. Each entity in the directory is considered an object and all objects are defined by a set of entries recognized as public key certificates bound to the entity. Access to the DS for certificate verification will not be controlled unless required for security reasons. The DS must also store the most recent Certification Revocation List (CRL) developed by the CA. The DS must authenticate all entities attempting to modify certificates and CRLs. Access to the system running the service must be strictly controlled and limited to the appropriate personnel.

8. KEY MANAGEMENT

a. General. Operational policy and key management procedures are the foundation of trust in the DOE public key system. These policies and procedures define the actions necessary to identify entities and generate cryptographic keys and certificates that bind them to the entities. Just as important are the procedures for securing, revoking, archiving, and disabling keys.

The level of trust and security of the DOE PKI is directly related to the generation of certificates and cryptographic keys and the protection of the keys. All entities are responsible for protecting their private keys in a manner that ensures that trust, in accordance with the applicable CPs and CPSs.

b. Use of Approved Cryptographic Algorithms and Software. Cryptographic algorithms, software implementations, and computing methods used for public key encryption, digital signatures, cryptographic hash functions, key exchange, and other security functions performed by a CA, RA, or EE must be certified by the National Institute of Standards and Technology as being compliant with applicable FIPS requirements, or as otherwise approved by the DOE PCA.

The following FIPS are applicable:

(1) FIPS 46-2, “Data Encryption Standard,” December 1993;

(2) FIPS 140-1, “Security requirements for Cryptographic Modules,” January 1994;

(3) FIPS 171, “Key Management Using ANSI X9.17," April 1992;

(4) FIPS 180-1, “Secure Hash Standard,” April 1995;

(5) FIPS 185, “Escrowed Encryption Standard,” February 1994; and

(6) FIPS 186-1, “Digital Signature Standard,” December 1998.

c. Compromised Key Recovery. Recovery of a compromised key is a significant PKI concern. The following sub-sections summarize the principles of compromised key recovery.

(1) Compromise of Certification Authority Keys. The PCA must be notified immediately of any CA key suspected of being compromised. Compromise of a CA's private key invalidates all of the certificates issued by that CA from the time of the compromise because certificates could be forged. Recovery from the compromise of a CA private key may require the following:

(a) Immediate notification of all CAs who are cross-certified with the compromised CA;

(b) Revocation of the compromised CA certificate by the CA or PCA, which invalidates the certification path of all entities subordinate to the compromised CA;

(c) Generation of a new CA public-private key pair;

(d) Issuance of a new certificate by the CA or PCA; and

(e) Issuance of new certificates signed with the new CA private key to replace the certificates signed with the compromised key.

Procedures for recovery of a compromised CA key must be defined in the CPs and CPSs.

(2) Compromise of Registration Authority Keys. If an RA key is compromised, it is possible that EE certificates generated by that RA may have been issued to fictitious EEs or with incorrect attributes. If the compromise date is known, it is only necessary to revoke certificates issued after the compromise occurred. If the RA has retained complete EE records, and these records are not compromised, new certificates may be automatically issued to EEs whose certificates have been revoked. Otherwise, EEs whose certificates are revoked must reapply to the RA to be issued a new certificate. Recovery procedures must be specified in the CPs and CPSs.

(3) Compromise of End Entity Keys. Recovery from the compromise of an EE's private key is the responsibility of the CA who issued the certificate. The affected certificate will be added to the next CRL or other certificate revocation mechanism that may be maintained by the CA. The EE will be issued a new certificate by the CA. Recovery from a compromised EE key will be defined in the CPS.

d. Emergency Key Recovery. All DOE information can be accessed by the local authorized DOE authorities for official business in accordance with established procedures. To support recovery of encrypted DOE information, the CA will maintain the capability to recover the private decryption key of any entity's encryption key-pair. Key recovery must be addressed in the applicable CPs and CPSs. The following three access conditions must be addressed:

(1) Key owner access;

(2) Non-key owner access excluding law enforcement; and

(3) Law enforcement access.

If key recovery is an automatic feature of the PKI, the CA who issued the certificate must be responsible for proper operation of the feature. Users of software applications with no automatic key recovery mechanisms must provide for key recovery through a trusted third party; for example, the Information System Security Officer (ISSO) for the system or the Organizational Administrator. The private signing key must always be under the control of the user who created it and under no circumstances will the private signing key be recoverable.

Upon acceptance of the public key certificate, the EE agrees to comply with this policy and authorized requests for emergency key recovery.

e. Archiving of Certificates and Keys. Archiving for the purpose of validating digital signatures and retrieving encrypted documents presents a number of technical, business, policy, and legal issues. Ideally, each CA must provide a protected archive to facilitate the processing of all valid, revoked, and compromised public signature verification keys and private decryption keys from the CA down to the EE. This must be defined in the appropriate CPs. Because of the associated costs and complexity of decryption, long-term storage of encrypted documents is discouraged. DOE will address long-term archiving issues and provide additional direction in future revisions to this chapter once the technology has sufficiently matured.

9. SECURITY. The Certification Authority Workstation (CAW) hardware and software used to generate or store certificates or keys must be afforded adequate security commensurate with the risk and magnitude of the potential harm resulting from the loss, misuse, or unauthorized access to or modification of information. At a minimum, the CAW and associated equipment must be located in an area where access is controlled. Additional controls may be designated in the CPs and CPSs. Compliance with this chapter, applicable CPs, and CPSs does not negate the authority and requirements of other security programs, such as Computer Security, Physical Security, Personnel Security, etc.

10. AUDITING.

a. The DOE PCA, SO-33, is responsible for conducting periodic audits of CAs to document compliance with the applicable CPs and CPSs. Periodic auditing will be the mechanism by which the PCA ensures that trust in the DOE PKI is verified and maintained. The PCA will audit in order to evaluate criteria that could affect the integrity of the entire PKI, such as, but not limited to the following:

(1) CA operational procedures;

(2) Cross-certification; and

(3) Physical, personnel, and software security.

b. The PCA may delegate this audit responsibility to the local cognizant DOE office. In this case, the results of the audit must be forwarded to the PCA. Each CA must audit the RAs and EEs to ensure compliance with the applicable CPs and CPSs. The CA will generally be concerned with local requirements and the operation of functions subordinate to the CA. Audits performed by the PCA and/or cognizant DOE office and the CA need not be performed at the same time or with the same frequency.

11. RECORDS. Records that document the procedures followed to ensure the integrity of the DOE public key system must be maintained. Each CA and RA must maintain a record system that will document key management operations, such as key generation, backup, recovery, and disabling, together with the identity of the person authorizing the operation, as specified in the CPs and CPSs. Auditable records must be maintained in a manner that prevents unauthorized modification or destruction of the records. Records must be retained as specified by the local Records Management Program.

12. TRAINING.

a. The PCA must formulate, schedule, and conduct training for CAs. CA training must consist of defining operational policy and developing proficiency in key management duties. Training must also cover requirements for establishing identity and documentation.

b. CAs must be responsible for training the RAs and the user community. The CA must ensure that the RA is thoroughly familiar with provisions for identifying EEs. The CA must provide all the necessary software, hardware, and documentation for RAs to carry out their responsibilities. The CA may specify training requirements for the user community but, at a minimum, training must provide the user with the knowledge needed to use the features of the DOE public key system and an understanding of how and why the private key component needs to be protected.