CHAPTER 6, PART 3
USE OF PUBLIC KEY INFRASTRUCTURE (PKI)

1 BACKGROUND

PKI is an enabler of trust that provides strong user identification, confidential communication, data integrity, and evidence for non-repudiation among individuals that may or may not have had prior knowledge of each other. Non-repudiation provides a proof-of-participation in an action or transaction by establishing that an user's private key was used to digitally sign an electronic business transaction. The trust that PKI facilitates is enterprise-wide through distinct, yet integrated policies and technology components. These policies and components explicitly identify and determine the roles, responsibilities, constraints, range of use, and services available.

Mathematically related key pairs both public and private are generated through the use of PKI technology. While the users' private key is safeguarded, their public key is linked to identifying information in a digitally signed public key certificate certifying their ownership of both public and private keys. The certificate and the keys are used in systems and applications to represent the user or individual identified by the certificate. A user must have one current key pair for encryption and decryption, and a second key pair for digital signature and signature verification.

The public key can be accessed by anyone. Only the person to whom the Private Key is issued has knowledge of this key; it is never revealed or transmitted. What one key in the pair encrypts, only the other key can decrypt. The keys are mathematically related in such a way that it is almost impossible to guess one key from the other. For example, a user (BOB) can send a message to another user (CAROL) by encrypting the message with CAROL's public key because only CAROL holds the private key to decrypt it. For authenticity (digital signature), BOB can send CAROL a message encrypted with his private key. CAROL can be certain it came from BOB because it can be decrypted only by using BOB's public key. The identity of BOB is verifiable because only BOB has access to his private key.

A digital signature is an electronic signature that can be used to authenticate the identity of the sender of a message or the signer of a document. Besides being easily transportable, it can also ensure that the content of the message or document that has been sent is unchanged. When time-stamped, the ability to ensure that the original signed message arrived means that the sender cannot easily repudiate it later.

Certification Authorities (CAs) represent the people, processes, and tools to create digital certificates that securely bind the names of users to their public keys. The following parties rely on the appropriate level of trust with respect to the creation and use of public key certificates: the individual Subscriber or entity identified by the certificate; the Certification Authority who issues the certificate; the Registration or Validation Authority that provides certificate validation services in certain implementations; and the Relying Party (company, agency or individual) relying on the certificate.

As long as users trust a CA and its policies for issuing and managing certificates, they can trust certificates issued by the CA. The CA investigates individuals and verifies their identity, binding that identity to the public key and verifying that the individual has the private key. Levels of trust are placed on the level of identification and verification required by the certificate level (i.e. low, medium, high). The FBCA will assist in the interoperability between CAs. In this process, the FBCA will establish level of assurance translations between agencies.

Interoperability is a critical issue for Public Key Infrastructures. Interoperability deals with interaction between systems directly supporting and/or consuming PKI-related services (component-level interoperability), compatibility between two peers, regardless of the supplier of the application or any ancillary infrastructure components used to support the application (application-level interoperability), and issues and options associated with achieving interoperability between two otherwise isolated PKI domains (inter-domain interoperability).

Traditional PKI architectures fall into one of three configurations: a single CA, a mesh of CAs, or a hierarchy of CAs. The PKI architecture that contains a single CA provides the PKI services for all the users of the PKI and its users place their trust in the only CA. Mesh PKIs have multiple trust points.

A hierarchy of CAs has two levels: the Root CA and subordinate CAs. The Root CA is responsible for administering the policy and procedures for the entire PKI system and the Subordinate CAs are responsible for binding users to their public key. The Root CA is the PKI component that is able to facilitate the integration of the USDA member agencies separate PKI applications. From a larger context, this architecture will facilitate secure interoperability for such technologies as virtual private networks, database access, authentication/access control to remote computing resources, and future PKI applications.

As more USDA agencies develop CAs whose processes have been certified, the Cyber Security Office reserves the right to establish a PKI Root CA at the Department level. Agencies can also outsource their CA services, but must comply with this policy.

USDA's PKI efforts will further be enhanced by its ability to interoperate with disparate PKI domains (cross-certification), an inherent feature to providing electronic government services across the department. Cross-certification provides a trust framework by evaluating digital credentials against a set standard. The Federal Bridge Certification Authority (FBCA) supports interoperability among Federal Agency PKI domains in a peer-to-peer fashion. The policies and procedures of the FBCA are governed by the Federal PKI Policy Authority, which has responsibility for mapping a CA's policies and practices against the FBCA standard.

2 POLICY

All agencies and mission areas whose major support systems have a security requirement for non-repudiation will use digital signature. It is the policy of the United States Department of Agriculture to encourage the use of PKI in satisfying system security requirements for non-repudiation. Agencies must satisfy the following procedural requirements prior to deployment of a Public Key Infrastructure.

Policy Exception Requirements – Agencies will submit all policy exception requests directly to the ACIO for Cyber Security. Exceptions to policy will be considered only in terms of implementation timeframes; exceptions will not be granted to the requirement to conform to this policy. Exceptions that are approved will be interim in nature and will require that each

agency report this Granted Policy Exception (GPE) as a Plan of Action & Milestone (POA&M) in their FISMA reporting, with a GPE notation, until full compliance is achieved. Interim exceptions expire with each fiscal year. Compliance exceptions that require longer durations will be renewed on an annual basis with a updated timeline for completion**.** CS will monitor all approved exceptions.

3 PROCEDURES

a Develop a business case model for PKI to determine its applicability in the organization's business strategies. A business case outlines and justifies the total cost of developing a PKI, including any associated IT development costs. It also determines what level of security is appropriate, identifies risks, determines benefits, legal and regulatory compliance constraints and identifies possible alternatives.

b Devise a PKI Strategy and Implementation Plan that will serve as a roadmap for deployment. This plan should essentially define: 1) how the PKI will be operated; 2) how trust will be passed between entities; 3) the PKI architecture and its components; 4) how applications are to be PKI-enabled; 5) how the PKI will be tested and supported; and 6) a detailed project plan.

c Conduct a risk analysis to review the existing information security infrastructure and to assess the readiness of the targeted PKI organization. Security in any system should be commensurate with its risks. The risk analysis forms a more objective basis for determining which security controls are appropriate and cost effective.

d Develop a Certificate Policy that maps to the FBCA certificate policy. The certificate policy is a descriptive document that identifies how the PKI environment will operate and it supports the creation/use of a certificate. This policy is the primary vehicle for establishing whether a certificate is fit for the purpose for which it is presented. The agency must explicitly describe any liability or financial responsibility accepted from the use of these certificates.

e Establish a Certification Practice Statement. The CPS is the statement of practices that a certification authority employs in issuing certificates and contains much greater detail than a Certificate Policy. Any agreement signed between certificate authorities, government entities, or third party contractors must be approved by the Office of the General Counsel.

f Devise a Subscriber Agreement. The subscriber agreement requires subscribers to accept certain responsibilities and obligations with respect to the use of the certificate or with respect to the protection of the private key corresponding to the public key contained in the certificate. It also establishes subscriber liability and also serves as an enforcement mechanism in the event those obligations are breached.

g Establish a compliance review requirement that will include but is not limited to a compliance audit of: the agency Certificate Policy, the operational compliance audit of the Certificate Practice Statements, and the actual operation of the PKI.

h Support the recovery of decryption keys for information as it traverses the network and while at rest. A key recovery policy will be established by each agency.

i Develop and maintain the Program and System Security Plan in accordance OCIO Interim Guidance CS-002, Information Cyber Security Plan Call, relevant laws, regulations and guidelines. (See publications cited in the Reference Section)

j Audit PKIs annually in accordance with USDA requirements.

k Meet USDA physical security requirements for controlling and securing IT restricted space.

l Require all personnel that have access to the CA to obtain a high security clearance. (OGC wants this clarified as to type of clearance)

m Implement an effective configuration management program and develop site configuration management plans and procedure documents.

n Maintain USDA's C2 Level of Trust security controls for all security devices used for creation, delivery, and authentication. USDA's C2 security is a standard applied at the operating system level to limit risk to the digital certificates used in PKI technology. Only individuals who have an "ongoing business need" would have access to PKI technology. This standard assures that individuals without a legitimate need are not given access to PKI data. All operating systems containing these devices will be in a hardened state.

o Support interoperability through the cross-certification of external certificates. Agencies may elect to interoperate without using the FBCA. Those agencies that elect to do so will employ levels of assurance that mimic those set forth in FBCA Certificate policy.

p Scan all security devices monthly.

q Require only in-person proofing before a Registration Authority, Local Registration Authority (LRA), Trusted Agent or an entity certified by a State or Federal Agency as being authorized to confirm identities for the issuance of certificates for the purpose of using digital signature.

r Use the X.509 Version 3 Standard for all Digital Certificates and the X.509 version 2 standard for Certificate Revocation Lists used within USDA. A X.500 Distinguished Name (DN) naming convention that is consistent among all USDA agencies will be used, but must be flexible enough to allow individual agencies to make use of existing identification information.

s Use only FIPs 140-2 compliant cryptographic algorithms.

The word "assurance" means how well a Relying Party can be certain of the identity binding between the public key and the individual whose subject name is cited in the certificate. USDA will use 4 assurance levels based on the sensitivity of the data being processed. The lowest levels, basic and rudimentary, will not be used for sensitive information nor use digital signature to satisfy non-repudiation. The following assurance levels will be used for these certificates:

Requirements and Specifications			
Digital Certificate Type	Registration and Application	Private Key Generation and Storage Options	Recommended Reliance Limit
High Assurance Digital Certificate	▪ In person (2 forms of pic ID)	Select One: ▪ Smart Card ▪ USB Token	▪ **Sensitive but Unclassified Data** ▪ **Threats to data high; consequences of security failure high;** ▪ **High Dollar value transactions; high fraud risk; risk of malicious access to private data high**
Medium Assurance Digital Certificate **NOTE: MEDIUM ASSURANCE CERTIFICATES MAY ONLY BE USSUED BY HIGH LEVEL AGENCY LOCAL REGISTRATION AUTHORITIES AND ALL PRIVATE KEYS MUST BE STORED ON FIPS STANDARD SMART CARDS/TOKENS AT THE TIME OF USE.**	▪ In person (2 forms of pic ID)	Select One: ▪ Smart Card ▪ USB Token ▪ Software	▪ **Sensitive but Unclassified Data** ▪ **Risk/consequence of data compromise moderate; includes substantial $ value transactions & risk of fraud; risk of malicious access to private data substantial**
Basic Assurance Digital Certificate **(Will not support non-repudiation)**	▪ In person (1 form of ID) or trusted manager	Select One: ▪ Smart Card ▪ USB Token ▪ Software	▪ **Sensitive Data** ▪ **Risk/consequence of compromise not major; risk of malicious access to private data not high**
Rudimentary Assurance Digital Certificate **(will not support non-repudiation)**	▪ Online Application	▪ 128-bit Browser ▪ IE 5.0 and later ▪ Netscape 4.08 and later, 4.7x	▪ **Unclassified Data** ▪ **Risk/consequence of compromise not major** ▪ **Insufficient for**

		recommended	**transactions requiring confidentiality and authentication** **Used primarily to provide data integrity to the information being signed**

The PKI must go through a formal certification and accreditation (C&A) process before it can be deployed in the operational environment. An independent Third Party must certify all USDA PKI systems. System certification is a formal procedure for testing security safeguards in a computer system or major application to determine if they meet applicable requirements and specifications. System accreditation is the formal authorization by a management official for system operation and an explicit acceptance of the associated risk. The management official ensures that all equipment resident on the network under his authority is operated using approved security standards. All C&A evaluations or annual reviews must be conducted by a third party who must have not developed the present PKI solution or have any other business relationship.

If the Office of Cyber Security establishes a Root Certificate Authority at the department level, those agencies whose CAs were created before the USDA Root Certificate Authority was operational, will be "grand-fathered" into the USDA PKI hierarchy until the agency's certificates issued during that time have expired**.**

4 RESPONSIBILITIES

a The Associate CIO for Cyber Security will:

(1) Periodically review and update this notice as required;

(2) Provide security standards for implementation of PKI in USDA information technology environments that handle sensitive data and require non-repudiation;

(3) Review agency plans to implement this policy;

(4) Review requests for exceptions or exceptions to this policy; and

(5) Conduct reviews of USDA agencies and mission areas to ensure compliance with this policy.

b The Associate CIO for Information Resources Management (IRM) will:

(1) Support the policy and procedures contained in this chapter to ensure that appropriate security protection is provided to all USDA managed networks, systems and servers; and

(2) Receive, review and coordinate a response with the Associate CIO for Cyber Security to any exception requests for exceptions to this policy.

c Agency Chief Information Officer will:

(1) Ensure the provisions of this policy are implemented;

(2) Assure that the requirements of PKI policy are satisfied prior to deployment of this technology on any system;

(3) Ensure that a back up of the encryption private key(s) is obtained that will be securely stored so encrypted documents may be historically retrieved. The signing private key will exist only on the key token or profile issued to the individual. The solution must provide a means for archival of private decryption keys, and support for the recovery of a private decryption key on request;

(4) Ensure that agency server administrators, staff offices responsible for server administration, ISSPMs and security staff are acquainted and comply with the provisions of OCIO Cyber Security Guidance Regarding C2 Controlled Access Protection (CS-013 dated 3/6/02);

(5) Assure that agency server administrators, staff offices responsible for server administration, information system security program managers and security staff are trained to implement and, maintain PKI at a functional C2 level and fully understand the ongoing responsibilities to preserve that level of server security.

d Agency Information Systems Security Program Manager will:

(1) Monitor all agency PKI installations to ensure that the provisions of this policy are followed;

(2) Coordinate with agency server administrators to ensure that precautions are taken to properly preserve the required level of server security;

(3) Coordinate with agency personnel to ensure proper certification and accreditation occur on all PKI systems prior to deployment;

(4) Coordinate with agency system owners to ensure that PKI private key pairs are properly stored.

e System Administrators/Security Administrators responsible for server administration will:

(1) Monitor vendor release notes for new security patches, service packs, software upgrades and updates;

(2) Follow internal configuration management practices in installing security patches and updates; and

(3) Maintain a configuration control manual that documents all changes to the servers with sensitive information.

-END-