Committee on National Security Systems

CNSS POLICY No.25
March 2009

NATIONAL POLICY FOR

PUBLIC KEY INFRASTRUCTURE IN

NATIONAL SECURITY SYSTEMS

.

CHAIR

FOREWORD

1. (U) The CNSS Subcommittee chartered a Public Key Infrastructure Working Group (PKIWG) to scope requirements for public key technology to protect information on Secret and Unclassified NSS. Following exhaustive research and analysis, the PKIWG produced a study, *Recommendation for a Public Key Infrastructure for Secret and Below Classified Networks Interoperability*,[1] outlining the necessary system architecture design, trust relationships, and organizational infrastructure implementation for PKI supported NSS.

2. (U) The PKIWG is now developing a baseline for PKI interoperability and information sharing requirements for Secret and Unclassified NSS based on a hierarchical model, for promulgation across the Federal Government. This NSS Public Key Infrastructure (NSS-PKI) baseline will facilitate identity authentication, technical non-repudiation, data integrity, and communications privacy interoperability on these networks among trusted participating entities. It will also fill the gap between the unclassified arena, managed by the Federal Public Key Infrastructure Policy Authority, and the highly classified arena, managed by the Intelligence Community (IC).

3. (U) CNSS Policy No. 25 outlines the measures for using the NSS-PKI to protect information on national security systems.

4. (U) Copies of this policy are available from the CNSS Secretariat, or the CNSS website: www.cnss.gov.

//s//
JOHN G. GRIMES

[1] *Copies of this study are available from the CNSS Secretariat, or the CNSS website: www.cnss.gov.*

NATIONAL POLICY
FOR PUBLIC KEY INFRASTRUCTURE IN
NATIONAL SECURITY SYSTEMS

SECTION I – PURPOSE AND SCOPE

1. (U) This policy applies to the Secret and Unclassified National Security Systems (NSS) of all Federal Government Departments and Agencies and their supporting contractors and agents. This policy does not apply to NSS processing Top Secret information. Secret and Top Secret information is defined in Executive Order 12958, as amended, reference (a).

2. (U) This policy establishes the requirement for all Federal Departments and Agencies to have a Public Key Infrastructure (PKI) to manage and support their Secret and Unclassified NSS. It also establishes a CNSS PKI Member Governing Body to oversee and provide additional guidance for the NSS-PKI hierarchy.

3. (U) For purposes of this policy, PKI refers to products and services that provide and manage X.509 certificates for public key cryptography.

SECTION III – REFERENCES

4. (U) See Annex A.

SECTION IV – DEFINITIONS

5. (U) Terms used in this policy are defined in Annex B or in Committee on National Security Systems Instruction No. 4009, reference (b).

SECTION V – POLICY

6. (U) All Federal Departments and Agencies, and their supporting contractors, shall follow this PKI Policy in the development and use of PKI throughout the information systems lifecycle.

7. (U) NSS operating at the unclassified level shall obtain PKI support from the established Federal PKI Architecture[2].

8. (U) NSS operating at the Secret level shall obtain PKI support from the NSS-PKI.

9. (U) The NSS-PKI hierarchy shall rest on a Root Certificate Authority (CA) operated on behalf of the national security community in accordance with policies established by the CNSS PKI Member Governing Body. The NSS-PKI Root CA shall serve as the anchor of trust for the NSS-PKI. All entities participating in the NSS-PKI shall be members of the CNSS PKI Member Governing Body.

   a. The NSS-PKI Root CA shall establish a trust relationship with each of the legacy CAs (i.e., the Department of Defense and the Federal Bureau of Investigation) until they are converted to the hierarchical model.

   b. The NSS-PKI shall support establishment of a Common Services subordinate CA. Federal partners that do not directly operate a subordinate CA shall acquire NSS-PKI certificates from this Common Services Provider.

   c. The NSS-PKI Policy Management Authority (PMA) shall establish the NSS-PKI Certificate Policy (CP) through the CNSS Policy Development Structure, the Root CA Certification Practices Statement (CPS), and the NSS-PKI framework, in accordance with policies established by the CNSS PKI Member Governing Body.

   d. The NSS-PKI participating entities shall use PKI for accessing network services, connecting to web services, and signing information.

   e. Initial NSS-PKI implementation will facilitate identity authentication, technical non-repudiation, data integrity, and communications privacy interoperability within a single security classification domain.

   f. The PKI cryptographic components, to include hardware security modules and user hardware tokens, will be reviewed and approved by NSA before use; validation of the approval shall be reflected in each participating organization’s CPS.

SECTION VI – RESPONSIBILITIES

10. (U) Each participating Federal Government Department and Agency shall:

   a. Adhere to the NSS-PKI standards specified in this policy to protect national security systems and the information that resides therein

   b. Establish a subordinate Certificate Authority (CA) responsible for all aspects of the issuance and management of certificates to users and devices or obtain NSS-PKI certificate services from the Common Services Provider

[2] http://www.cio.gov/fpkia/ - link to the Federal PKI architecture site

c. Establish an Agency NSS-PKI Management Authority or Agency NSS-PKI point of contact (POC) for those using the Common Services Provider, who will be: (1) responsible for all aspects of the management of the NSS-PKI program for that agency; and, (2) a participant in the CNSS PKI Member Governing Body

d. Prepare and submit to the CNSS PKI Member Governing Body (if directly operating a subordinate CA), through the NSS-PKI PMA, a CPS that conforms to the requirements of the NSS-PKI CP and Root CA CPS

11. (U) The Director, National Security Agency (DIRNSA) shall:

a. Maintain and operate the NSS-PKI Root CA on behalf of the community.

b. Serve as the NSS-PKI (PMA) as the national manager for NSS established under NSD-42 Reference (c).

12. (U) The CNSS PKI Member Governing Body shall:

a. Maintain and enhance the NSS-PKI hierarchy and its governing policies.

b. Develop additional policy guidance to address PKI interoperability with non-Federal partners and establishment of trust relationships among CAs participating in the NSS-PKI.

13. (U) NSS-PKI member entities shall:

a. Maintain and operate subordinate NSS-PKI CAs, or acquire such support from the Common Services Provider.

b. Participate in the CNSS PKI Member Governing Body.

c. Use PKI services to protect and control access to NSS information.

14. (U) The Department of Defense and the Federal Bureau of Investigation shall establish and implement a migration plan to issue new certificates under the NSS-PKI infrastructure.

15. (U) The Common Services Provider shall be responsible for preparation and submission of a CPS that conforms to the requirements of the NSS-PKI CP and Root CA CPS.

Enclosures:

ANNEX A – References
ANNEX B – Acronyms

ANNEX A
REFERENCES

a. Executive Order 12958, “Classified National Security Information,” March 2003, as amended.

b. Committee on National Security Systems Instruction No. 4009, “National Information Assurance (IA) Glossary,” current edition

c. National Security Directive (NSD) 42, National Policy for the Security of National Security Telecommunications and Information Systems

ANNEX B
DEFINITIONS

Certification Authority (CA) —An authority trusted by one or more users to issue and manage X.509 public key certificates and CRLs.

Certificate Policy (CP) —A certificate policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A certificate policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.

Certificate Practice Statement (CPS)—A statement of the practices that a CA employs in issuing, suspending, revoking, and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services).

CNSS Public Key Infrastructure (PKI) Member Governing Body: that group, comprised of representatives of CNSS Member PKI Agency Certificate Management Authorities (ACMA), responsible for NSS PKI: policy management; operational direction and approval; internal audit and corrective action approval and monitoring; and, external cross certification review and acceptance. The Member Governing Body conducts the policy, management, operational, security, and administrative reviews of all aspects of NSS PKI, and makes recommendations to the Policy Management Authority (PMA) for implementation approval.

Common Services Providers: Federal organizations that provide NSS PKI support to other federal organizations, academia, and industrial partners requiring classified NSS PKI support but without their own self-managed infrastructure.

Federal Public Key Infrastructure Policy Authority: The FPKIPA is a Federal Government body responsible for setting, implementing, and administering policy decisions regarding the Federal PKI Architecture.

NSS Public Key Infrastructure: The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates on Secret and below national security systems. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates. Unclassified NSS PKI systems follow the requirements of, and obtain support from, the Federal PKI Architecture.

Public Key Infrastructure: A set of policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public/private key pairs, including the ability to issue, maintain, and revoke public key certificates.

Public Key Infrastructure Working Group: A working group established in accordance with the provisions of National Security Directive (NSD) 42 by the Co-chairs of the CNSS Subcommittee to scope requirements for PKI interoperability beyond the unclassified level; to work PKI Interoperability issues under CNSS sponsorship and coordinate efforts with the broader federal community while expanding efforts with our International Partners; and, to develop draft CNSS PKI policies, directives, instructions and/or advisory/information memoranda to address interoperability of PKI environments.

Policy Management Authority: Authority that oversees the creation and update of certificate policies, reviews certification practice statements, reviews the results of CA audits for policy compliance, evaluates non-domain policies for acceptance within the domain, and generally oversees and manages the PKI certificate policies.