Committee on National Security Systems

CNSSD No. 506
9 October 2012

NATIONAL DIRECTIVE TO IMPLEMENT PUBLIC KEY INFRASTRUCTURE FOR THE PROTECTION OF SYSTEMS OPERATING ON SECRET LEVEL NETWORKS

THIS DOCUMENT PRESCRIBES MINIMUM STANDARDS
YOUR DEPARTMENT OR AGENCY MAY REQUIRE FURTHER
IMPLEMENTATION

CHAIR

FOREWORD

1. CNSS Directive No. 506 outlines the requirements for integrating the use of certificates issued by the National Security Systems (NSS) Public Key Infrastructure (PKI) into systems operating on Secret level networks to protect resources while achieving interoperability and controlled information sharing. It also identifies specific requirements and deadlines for achieving this goal.

2. CNSS Policy No. 25, *National Policy for Public Key Infrastructure in National Security Systems*, reference 1, established the NSS-PKI, outlined the measures for using the NSS-PKI to protect information on national security systems, required CNSS Member Agencies to obtain PKI support from the NSS-PKI, and established the NSS-PKI Member Governing Body (MGB) to oversee and provide additional guidance for the NSS-PKI. The scope of CNSS Directive No. 506 is also defined in accordance with Executive Order (EO) 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, reference 2, to include any classified system operated by, on behalf of, or in support of any federal agency.

3. The NSS-PKI MGB developed CNSS Instruction No. 1300, *National Instruction On Public Key Infrastructure X.509 Certificate Policy*, reference 3, which identifies the requirements for the operation of the NSS-PKI. The NSS-PKI MGB also coordinated with the National Security Agency (NSA) to establish the NSS-PKI Root Certification Authority (CA), bringing the NSS-PKI into operational status.

4. The president identified cybersecurity as one of the top priorities of his administration. By issuing (E.O.) 13587, Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information, the president established requirements for the protection of all classified networks and systems, as well as the secure sharing of classified information by authorized users. CNSS Directive No. 506 is consistent with E.O. 13587. Additionally, Initiative #7 of The Comprehensive National Cybersecurity Initiative specifically addresses the need to increase the security of our classified networks. In addition, OMB Memorandum M-11-11 outlines a plan for using Personal Identity Verification (PIV) credentials to protect access to unclassified federal information systems.

This Directive is available from the CNSS Secretariat, as noted below, or the CNSS website: http://www.cnss.gov.

/s/

TERESA M. TAKAI

NATIONAL DIRECTIVE TO IMPLEMENT PUBLIC KEY INFRASTRUCTURE FOR THE PROTECTION OF SYSTEMS OPERATING ON SECRET LEVEL NETWORKS

SECTION I—PURPOSE

1. This Directive establishes the requirement for all federal agencies to implement the National Security Systems Public Key Infrastructure (NSS-PKI) to promote interoperability and secure information sharing between federal departments and agencies and to use PKI to provide strong authentication to their systems operating on Secret level networks.

SECTION II—AUTHORITY

2. The authority to issue this Directive derives from National Security Directive 42, which outlines the roles and responsibilities for securing national security systems, consistent with applicable law, E.O. 12333, as amended, and other Presidential directives.

3. Nothing in this Directive should be interpreted as altering or superseding the existing authorities of the Director of National Intelligence.

SECTION III—SCOPE

4. This Directive applies to all departments and agencies of the United States Government (USG), and their supporting contractors, agents, and non-federal affiliates who own, operate, or maintain NSS operating at the Secret level. For purposes of this Directive, PKI refers to products and services that provide and manage X.509 certificates for public key cryptography.

SECTION IV—POLICY

5. This Directive mandates the development and implementation of a comprehensive approach to the use of PKI to protect U.S. Government NSS. All departments and agencies of the USG, and their supporting contractors, agents, and non-federal affiliates who own, operate, or maintain NSS operating at the Secret level shall follow this directive in the implementation and use of NSS-PKI for all systems residing on Secret-level networks, including systems that reside on closed operational networks. Federal Government departments and agencies shall ensure that the implementation of NSS-PKI adheres to the requirements of this Directive by implementing the following measures:

a. **Policy:** All departments and agencies of the USG operating systems on Secret level networks shall establish an agency implementation plan and directive for the issuance, integration and use of certificates issued by the NSS-PKI to authenticate users and strengthen access control decisions to agency NSSs. In addition, all federal agencies shall include provisions in their agency plans and policies covering the operation and use of NSS-PKI by the supporting contractors, agents and non-federal affiliates for whom they sponsor access to classified information.

1) No later than thirty days from the signature of this directive, each department and agency of the USG operating systems on Secret level networks shall designate an agency lead official for ensuring the execution of the agency NSS-PKI implementation plan and provide contact information to the NSS-PKI Policy Management Authority (PMA) as defined in CNSSI No. 1300, reference 3.

2) No later than ninety days from the signature of this directive, each department and agency of the USG operating systems on Secret level networks shall develop a NSS-PKI implementation plan that identifies agency milestones for achieving the use of NSS-PKI across all agency systems and the issuance of certificates to agency employees, contractors, agents and non-federal affiliates; and, submit the plan to the NSS-PKI PMA as defined in CNSSI No. 1300, reference 3.

3) By 1 February 2013, each department and agency of the USG operating systems on Secret level networks shall establish a directive specifying the use of NSS-PKI for the following capabilities:

a) As the means of authentication for access to that agency’s networks that interconnect with other departments and agencies of the USG operating classified networks.

b) As the preferred means of authentication for access to closed operational networks. Requests to operate a local PKI in lieu of the NSS-PKI for a closed network shall be approved by the CNSS to ensure that the business need is compelling and that the proposed implementation is cost-effective and will not adversely affect the potential capability for interoperability between the domains. Authorization to operate a local PKI for a closed operational network in lieu of the NSS-PKI shall be obtained from the NSS-PKI PMA.

c) As the means of authentication for access to information resources as determined by the agency.

b. **Interoperability:** No later than six months after the ability to issue certificates by the Common Service Provider (CSP), if a member agency has users that require access to another member agency’s resources on Secret level networks that have been PKI enabled, it is the user agency’s responsibility to ensure that the user has NSS-PKI hardware certificates and the requisite hardware and software. After this date, failure to have a NSS-PKI solution in place may limit or eliminate access to some classified networks and systems that require NSS-PKI-based authentication. This interoperability support shall include the following:

1) Implement processes to provide certificates housed on hardware tokens to individuals who require access to applications that require NSS-PKI for authentication. Except where operationally justified by the agency to the NSS-PKI MGB, NSS-PKI certificates issued to human subscribers shall be housed on NSA-approved smart cards or other NSA-approved tokens.

2) Implement processes to provide certificates to systems and devices to support device authentication to applications that require NSS-PKI.

3) Ensure that guards and other mechanisms established to interconnect agency networks can support NSS-PKI requirements, including digital signatures, end-to-end encryption and access to CA certificates and Certificate Revocation Lists (CRL).

4) Ensure that agency email systems can accept digitally signed emails.

5) Give priority to certificate issuance to users that require access to another member agency's resources.

6) Support interoperability with foreign affiliates. The CNSS MGB will provide further guidance via separate correspondence.

c. **Full Operations:** No later than twenty-four months after the ability to issue certificates by the CSP, all CNSS Member Agencies and non-CNSS federal agencies operating systems on Secret level networks shall have fully implemented the agency directive specifying the use of NSS-PKI to better secure access to Information Technology (IT) resources, including cryptographic network logon with PKI hardware tokens and support for email signature and encryption.

SECTION V—RESPONSIBILITIES

6. Each department and agency of the USG operating systems on Secret level networks shall:

a. Adhere to the NSS-PKI standards specified in CNSS Policy No. 25 to protect national security systems and the information that resides therein.

b. Designate an agency lead official for ensuring the issuance of the agency's implementation plan and directive.

c. Identify funding to implement and sustain the agency's NSS-PKI capability.

d. Implement policy specifying the use of NSS-PKI as the means of authentication.

e. Implement directive and processes to issue certificates to agency employees, contractors, agents and non-federal affiliates with accounts on the agency's Secret-level networks.

f. Implement processes to use NSS-PKI for authentication, digital signature, and encryption.

g. For member agencies using the Common Service Provider (CSP), execute the appropriate Memorandum of Agreement with the CSP detailing roles and responsibilities.

h. Implement processes to enable use of NSS-PKI for authentication to agency applications and websites.

i. Prepare a quarterly report on the status of the agency's NSS-PKI implementation and submit to the NSS-PKI PMA. This report should address technical and resource limitations that may delay implementation.

7. The NSS-PKI PMA shall:

a. Coordinate with agency lead officials for the implementation of this directive.

b. Review agency NSS-PKI implementation plans and quarterly updates.

c. Prepare a quarterly status report to the CNSS Chair.

d. Approve agency and CSP Certification Practice Statements (CPS)

8. The NSS-PKI Member Governing Body shall:

a. Coordinate with the NSS-PKI PMA to review and comment on agency NSS-PKI implementation plans and quarterly updates.

b. Coordinate with agency lead officials to support interoperability of NSS-PKI solutions across agencies.

c. Review and recommend approval of agency and CSP CPSs in a timely fashion to ensure the availability of certificates to support the use of NSS-PKI.

9. The NSS-PKI CSP, as operated by DISA, shall:

a. Provide a mechanism for issuing certificates on a fee for service basis for agencies that choose not to operate their own Certificate Authorities (CA) under the NSS-PKI Root CA.

b. Provide a mechanism for providing subscriber tokens on a fee for service basis.

c. Provide regular CRL updates.

SECTION VI—DEFINITIONS

10. Terms used in this directive are defined in Annex A, CNSS Policy No. 25, reference 1, and CNSS Instruction No. 4009, National Information Assurance (IA) Glossary, Reference 6.

SECTION VII - REFERENCES

11. See Annex B. Future updates to referenced documents shall be considered applicable to this directive.

Enclosures:
ANNEX A - Definitions
ANNEX B – References

ANNEX A

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 (MGB): The 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 Provider (CSP): A federal organization that provides NSS-PKI support to other federal organizations, academia and industrial partners requiring classified NSS-PKI support but without their own self-managed infrastructure.

Federal PKI Architecture: The federal PKI architecture is framework or policies, directives, procedures, and services to provide PKI to unclassified networks, the Personal Identity Verification (PIV)/Common Access Card (CAC) identity credential, and various other PKI implementations at the unclassified level.

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.

Non-federal Affiliate: Non-Executive branch USG organizations, including domestic and foreign organizations.

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, directives, 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, directives, 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.

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.

ANNEX B

REFERENCES

1. (U) Committee on National Security Systems Policy Number 25 (CNSSP 25), *National Policy For Public Key Infrastructure in National Security Systems*, March 2009

2. (U) Executive Order 13587, *Structural Reforms to Improve the Security of Classified Networks and the Responsible Sharing and Safeguarding of Classified Information*, October 7, 2011

3. (U) Committee on National Security Systems Instruction Number 1300 (CNSSI 1300), *National Instruction On Public Key Infrastructure X.509 Certificate Policy*, current edition

4. (U) National Security Directive (NSD)-42, *National Policy for the Security of National Security Telecommunications and Information Systems,* July 5, 1990

5. (U) Executive Order 13526, *Classified National Security Information*, December 2009

6. (U) Committee on National Security Systems Instruction Number 4009 (CNSSI 4009), *National Information Assurance (IA) Glossary*, current edition

RELATED DOCUMENTS

1. (U) Committee on National Security Systems Policy Number 15 (CNSSP 15), *National Information Assurance Policy on the Use of Public Standards for the Secure Sharing of Information Among National Security Systems*, March 2010

2. (U) Committee on National Security Systems Instruction Number 1253 (CNSSI 1253), *Security Categorization and Control Selection for National Security Systems*, dated March 2012

3. (U) National Security Presidential Directive 54/Homeland Security Presidential Directive 23, *Cybersecurity Policy*, January 8, 2009