Department of Homeland Security
DHS Directives System
Instruction Number: 4300A
Instructions U
Revision Number: 00
Issue Date: 04/28/2022

DHS INFORMATION TECHNOLOGY SECURITY PROGRAM: PUBLIC KEY INFRASTRUCTURE INSTRUCTION

Purpose

The U.S. Department of Homeland Security (DHS) has implemented a Public Key Infrastructure (PKI) to provide security services to facilitate the accomplishment of its missions. DHS has contracted with the U.S. Department of the Treasury (TREAS) to host, operate, and maintain DHS CA4, Directory Services, and Online Certificate Status Protocol (OCSP) Services under the U.S. PKI Shared Services Provider (SSP) Program. The DHS PCA issues all human public key certificates required for Homeland Security Presidential Directive 12 (HSPD-12) DHS Personal Identity Verification (PIV) Cards and Derived PIV credentials, and all non-PIV and non-human public key certificates a by DHS. The Registration Authority (RA) functions for the DHS PCA are performed in-house by DHS.

This instruction also defines and documents requirements, guidance, and procedures to implement Public Key Infrastructure (PKI) policy in accordance with FCPCA and U.S. Department of Treasury policy within the Department, including Headquarters and all Components. This instruction also defines and documents requirements, guidance, and procedures to implement DHS Internal Use Non-Person Entity (NPE) PKI policy in accordance with the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.

Scope

The DHS PCA is subordinate to the U.S. Department of the Treasury Root CA (TREAS ROOT CA). The TREAS ROOT CA is cross-certified with the U.S. Common Policy Framework Root CA (FCPCA). The DHS PCA issues certificates under the "*X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework*" [U.S. CPF CP]. The "*X.509 Certificate Practice Statement for Department of Treasury Subordinate Certificate Authorities*" [TREAS SubCAs CPS] states the practices that will be followed by the DHS PCA to comply with the [U.S. CPF CP] and thereby establish the assurance that can be placed in the certificates it issues.

Additionally, this instruction pertains to the DHS need for internal use only (not publicly trusted) Non-Person Entity (NPE) certificates (also known as device certificates) and implementations of both Enterprise and Component NPEs in accordance with DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.

Definitions

i. Public Key Certificate – Used to obtain subscribers' public keys in a trusted manner. Once a certificate is obtained, the public key can be used:
   a. To encrypt data for that subscriber so that only that subscriber can decrypt it
   b. To verify that digitally signed data was signed by that subscriber, thereby authenticating the identity of the signing subscriber, and the integrity of the signed data

ii. Public Key Infrastructure - An architected set of systems and services that provide a foundation for enabling the use of public key cryptography. This is necessary in order to implement strong security services and to allow the use of digital signatures. The principal Components of a PKI are the public key certificates, registration authorities (RA), certificate authorities (CA), directory, certificate revocation lists (CRL), and a governing certificate policy.

iii. Public/Private Key Pair - A single public/private key pair and its associated certificate issued to an NPE may be used for signing (including authentication), key management (for encryption), or both. Device certificates do not assert non-repudiation.

PKI Processes and Procedures

i. Encryption:

   a. Systems requiring encryption comply with the following methods:
   - Products using FIPS 197 Advanced Encryption Standard (AES) algorithms with at least 256 bit encryption that has been validated under FIPS 140-2
   - National Security Agency (NSA) Type 2 or Type 1 encryption
   (Note: The use of triple Data Encryption Standard [3DES] and FIPS 140-1 is no longer permitted.)

   b. Components develop and maintain encryption plans for sensitive information systems.

   c. Components use only cryptographic modules that are FIPS 197 (e.g. AES-256) compliant and have received FIPS 140-2 validation at the level appropriate to their intended use.

   d. Whenever practical, electronic transmission of Sensitive Information and FOUO information (e.g., data, Web site, or email) shall be by approved secure communications systems or systems that use other protective measures such as Public Key Infrastructure (PKI) or transport layer security (e.g., https)

   e. DHS shall provide key recovery for DHS CA4-issued certificates

ii. DHS Federal PKI (FPKI):

   a. DHS implements a DHS Public Key Infrastructure (PKI) that is part of the FPKI to facilitate the use of PKI within DHS, and to facilitate the interoperable use of PKI between DHS and its external mission and business partners, such as other Federal agencies; state, local and tribal governments; public and private sector entities; and U.S. citizens

b. The DHS CISO is the DHS PKI Policy Authority (PKIPA) to provide PKI policy oversight for all DHS PKIs. A detailed description of DHS PKIPA roles and responsibilities is provided in the Registration Practice Statement for the DHS Principal Certification Authority,

c. The DHS CISO represents DHS on the Federal PKI Policy Authority (FPKIPA).

d. The DHS PKIPA appoints a PKI Management Authority (PKIMA) to provide management and operational oversight for all DHS PKIs. A detailed description of DHS PKIMA roles and responsibilities is provided in the Registration Practice Statement for the DHS Principal Certification Authority.

e. Component CISOs/ISSMs are responsible for management oversight of the DHS PCA RA activities and personnel within the Component.

f. The DHS FPKI is governed by the U.S. Common Policy Framework certificate policy approved by the FPKIPA, and by the relevant portions of the Department of the Treasury Infrastructure (PKI) X.509 Certificate Policy approved by the Department of the Treasury Policy Management Authority (PMA).

g. DHS has a single DHS Principal CA (i.e. named DHS CA4) that has the U.S. Common Policy Root CA as its trust anchor. The DHS Principal CA is operated for DHS by the Department of Treasury under the Federal Shared Service Provider (SSP) program.

h. The DHS Principal CA is the only DHS CA subordinated to the Treasury Root CA. Additional DHS CAs subordinate to the DHS Principal CA are not permitted.

i. The DHS Principal CA has a trust path resolving to the U.S. Common Policy Root CA via the Treasury Root CA. Establishing direct trust relationships with any other CAs is not permitted. The U.S. Common Policy Root CA is cross-certified with the Federal Bridge CA at the high, medium hardware, and medium assurance levels.

j. The DHS Principal CA operates under an X.509 Certification Practice Statement (CPS). The CPS complies with the U.S. Common Policy Framework and the Treasury Certificate Policy. Since the Department of the Treasury, as the SSP for DHS, operates the DHS Principal CA, the Department of the Treasury PKI Policy Management Authority approves the CPS for the DHS Principal CA. DHS operates two Registration Authorities for the DHS Principal CA (CA4). The DHS PCA Registration Authority (DHS PCA RA) is responsible for performing the life-cycle administration for non-PIV certificates, and the DHS PCA PIV Registration Authority (DHS PCI PIV RA) is responsible for performing the life-cycle administration of PIV certificates. The two DHS Registration Authorities for the DHS Principal CA operate under the Registration Practice Statement for the DHS Principal Certification Authority (RPS). The RPS is approved by the DHS PKIMA and the DHS PKIPA, and is approved for conformance to the U.S. Common Policy Framework and the Treasury Certificate Policy by the Department of the Treasury PKI Policy Management Authority.

k. The DHS PKIMA ensures that all DHS PCA Registration Authority (DHS PCA RA) operates in compliance with the RPS. The DHS PIV Card Issuer (PCI)

Organization Identity Management Official (DHS OIMO) ensures that its DHS PCA PIV Registration Authority (DHS PCI PIV RA) operates in compliance with the RPS.

l. The DHS Principal CA undergoes regular PKI compliance audits as required by the U.S. Common Policy Framework. The audit findings, report, and Plans of Action and Milestones (POA&Ms) that address deficiencies found are provided to the DHS PKIPA and DHS PKIMA

m. The DHS Principal CA archives records as required by the U.S. Common Policy Framework, the Treasury Certificate Policy, and the DHS Principal CA CPS.

n. The DHS Principal CA issues certificates only to internal DHS entities, e.g., Person Entities (PEs) such as employees, contractors, affiliates, roles, groups, and NPEs such as hardware devices, systems, and applications. External entities that require certificates to securely interact with DHS acquire the certificates from: (1) another Federal Agency's PKI or SSP PKI operating under the U.S. Common Policy Framework or (2) a non-Federal Agency PKI that is cross-certified with the FBCA at medium, medium Hardware, PIV-I, or high assurance level).

o. Only the DHS Principal CA issues certificates to DHS PEs, i.e., DHS employees, contractors, affiliates, roles and group entities. Types of PE certificates that may be issued include authentication, digital signature verification and encryption certificates, including certificates for DHS Personal Identity Verification (PIV) Cards, code signing and content signing, as well as all other types of certificates allowed under the U.S. Common Policy. Only the DHS Principal CA issues certificates to DHS NPEs, i.e., hardware devices, systems and applications, when any of the following conditions apply:

    i. There are external relying parties for the certificates.

    ii. The certificates will be used to protect sensitive DHS data or to authenticate to operational systems containing sensitive information, and

    iii. The certificates are not explicitly authorized to be issued by DHS Internal Use NPE CAs in the DHS X.509 Internal Use NPE Certificate Policy.

p. The Treasury Root CA is used by Relying Parties in DHS as the trust anchor for the validation of certificates issued by the DHS Principal CA (DHS CA4). The U.S. Common Root CA is used by Relying Parties external to DHS as the trust anchor for the validation of certificates issued by the DHS Principal CA (DHS CA4).

q. Only certificates that are issued by the DHS Principal CA under the U.S. Common Policy Framework at medium assurance or above are used to protect sensitive DHS data or to authenticate to operational systems containing sensitive data. Certificates issued by test, pilot, third party, self-signed or other CAs are not used to protect sensitive information, or to authenticate to DHS operational systems containing sensitive information.

r. For all external-facing DHS web services, compliance with OMB Memorandum 15-13 and 17-06 (use of HTTPS and HSTS) is mandatory.

For all external-facing DHS web services:

i. Where the browsers used by external relying parties are unable to validate DHS Transport Layer Security (TLS) certificates, these web services will require the use of a publicly trusted (commercial) certificate.

ii. This certificate must be from a Certificate Authority where the operating entity has established a level of trust with the U.S. Government Services Administration (GSA) as a Trust Service.

iii. Use of certificates issued from Public Cas not listed with the Government Services Administration (GSA) as a Trust Service should be obtained after approval by the DHS CISO.

For all internal-facing DHS web services:

i. DHS-issued certificates may be practical for web services within the internal DHS.gov domain

ii. The use by DHS of any CA or PKI services not listed on GSA Trust Service list is prohibited unless approved in writing by the DHS CISO on a case-by-case basis.

s. Commercial applications or appliances used by DHS that require the use of PKI certificates obtain those certificates from the DHS Principal CA or a DHS Component Internal Use NPE CA, as appropriate. Commercial applications or appliances, that require the use of a proprietary CA implemented as an internal feature, are not acquired or used, unless prior concurrence by the DHS PKIMA and approval by the DHS PKIPA are obtained.

t. Certificate trust stores contain root certificates, each of which is the trust anchor for a PKI. Certificates in trust stores are implicitly trusted by certificate validation software. Vendors' products come pre-populated with many root certificates in their trust stores, including certificates for PKIs that DHS does not want to implicitly trust.

DHS Components manage the content of installed product's trust stores, including:

- Leveraging automated management, such as with Microsoft Group Policy Objects (GPOs)
- Removing all certificates that have passed their expiration date
- Removing all certificates that are no longer trusted
- Removing all certificates that are no longer required

u. Commercial products used by DHS and applications developed by DHS that enable the use of PKI at a minimum support the following cryptographic algorithms and associated key sizes:

- SHA 1 and SHA 256

- RSA 1024 and 2048

- AES 128 and 256

Whenever possible, they should also support use of the following algorithms and associated key sizes, to ensure future interoperability across the Federal PKI and PKIs cross-certified with the Federal Bridge Certification Authority.
- SHA 384 and 512

- RSA 3072

- Elliptic Curve 224, 256, and 384

- ECDSA 224 and 256

(Note: Older algorithms and smaller key sizes (e.g., SHA 1 and RSA 1024) should continue to be supported since they may be required to validate digital signatures executed in the past and to decrypt objects encrypted in the past using the older algorithms and key sizes.)

Subscriber private keys are not used by more than one entity, with the following exceptions:

- Authorized members of a Group Subscriber, may use the Group's private keys.

- Multiple systems or devices in a high availability configuration may use a single Key pair providing the Subject Alternative Name (SAN) field within the SSL certificate identifies all of the devices with which the key is to be shared.

iii. DHS Internal Use NPE PKI

a. At the DHS Enterprise-level, a single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented to issue certificates to DHS NPEs to support NPE-to-NPE authentication across DHS networks, where the certificates have no external relying parties.
At the DHS Component-level, a DHS Component may implement one or more DHS Internal Use Non-Person Entity (NPE) PKIs for use solely by that Component to issue certificates to that Component's NPEs to support NPE-to-NPE authentication on that Component's networks, where the certificates have no external relying parties.

b. A detailed description of DHS PKIPA roles and responsibilities is provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.

c. A detailed description of DHS PKIMA roles and responsibilities is provided in the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.

d. DHS Internal Use NPE PKIs are governed by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines approved by the DHS PKIPA.

e. A single DHS Enterprise Internal Use Non-Person Entity (NPE) PKI may be implemented.

A DHS Component may implement one or more DHS Internal Use NPE PKIs. Each PKI is a hierarchical PKI with one or more levels.

- For a single-level hierarchy, the PKI consists of a single self-signed Internal Use

NPE CA.

-For a two-level hierarchy, the PKI consists of a single self-signed Internal Use NPE Root CA at the top level, and one or more Internal Use NPE CAs that are each directly subordinated to the Internal Use NPE Root CA

- Additional Internal Use NPE CAs may be directly subordinated to an existing subordinate Internal Use NPE CA, thereby adding an additional level to the hierarchy.

The requirements and process for implementing a DHS Enterprise Internal Use Non-Person Entity (NPE) Root and Subordinate CAs, and for implementing a DHS Component Internal Use NPE Root and Subordinate CAs are specified in the NPE PKI Configuration and Operation Practices Guidelines.

f. If a DHS Internal Use NPE PKI consists of a single NPE CA, the CA is self-signed and function as its own trust anchor.
If a DHS Internal Use NPE PKI is a multi-level hierarchical PKI, with a Root and subordinate CAs, the trust path from the subordinate CAs resolves to the Root CA as the PKI's trust anchor.
A request to implement trust relationships between DHS Component Internal Use Non-Person Entity (NPE) PKIs, or between the DHS Enterprise Internal Use Non-Person Entity (NPE) PKI and a DHS Component Internal Use Non-Person Entity (NPE) PKI be submitted to the DHS PKIMA for review and approved by the DHS PKIPA.

g. The DHS PKIMA ensures that every DHS Internal Use NPE CA operates in compliance with the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.

h. Every DHS Internal Use NPE CA undergoes regular PKI compliance assessments as required by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines. The assessment report, findings, and Plans of Action and Milestones (POA&Ms) that address the deficiencies found, are provided to the DHS PKIPA and DHS PKIMA.

i. Every DHS Internal Use NPE CA (Root and Subordinates) archives records as required by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.

j. DHS Enterprise Internal Use Non-Person Entity (NPE) CAs issue only to DHS NPEs (i.e., hardware devices and systems) when all of the following conditions apply:

- There are no relying parties for the certificates external to DHS
- The certificates are explicitly authorized to be issued by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines.

DHS Component Internal Use NPE CAs issue authentication certificates only to DHS Component NPEs (i.e., hardware devices and systems) when all of the following conditions apply:

-There are no relying parties for the certificates external to the DHS Component

-The certificates are explicitly authorized to be issued by the DHS Internal Use NPE PKI Configuration and Operation Practices Guidelines

A DHS Enterprise Internal Use NPE Root CA may issue a CA certificate to subordinate a DHS Enterprise Internal Use NPE CA to the Root CA.

A DHS Component Internal Use NPE CA may issue a CA certificate to subordinate a DHS Component Internal Use NPE CA for that Component to itself

A DHS Enterprise Internal Use NPE CA may issue a CA certificate to subordinate a DHS Enterprise Internal Use NPE CA to itself.

A DHS Component Internal Use NPE CA may issue a CA certificate to subordinate a DHS Component Internal Use NPE CA for that Component to itself.