Department of Defense
Public Key Infrastructure
Functional Interface Specification
Version 3.0

September 2010

Record of Changes

No.	Date	Reference	A=Add M=Modify D=Delete	Description of Change
1	16 Sep 10		M	New Version

Table of Contents

Table of Contents

viii

List of Figures

List of Tables

List of Tables

List of Tables

1 Introduction

This document describes the functional interface to the Department of Defense (DoD) Public Key Infrastructure. The purpose of this Specification is to provide information to allow various DoD and vendor organizations to acquire or develop applications that will be capable of interacting with and using the DoD PKI.

1.1 Scope

This document is an update to the *Department of Defense Class 3 Public Key Infrastructure Interface Specification, Version 2.0* [PKI-IF], which was released in June 2007. The DoD PKI has evolved since that specification was written, and the interface has changed accordingly. Major changes include support for additional types of certificates and new capabilities. New certificate types provide support for roles, organizations, alternate tokens, and the Homeland Security Presidential Directive 12 (HSPD-12) Personnel Identification Verification (PIV).[HSPD-12]. The PKI will also produce certificates for entities such as devices that are not people-related; these entities are known Non-Person Entities (NPEs). The DoD PKI has added certificates to allow the DoD PKI to interoperate with the Federal Bridge Certification Authority (FBCA) and with the Federal Public Key Infrastructure (FPKI) Common Policy framework [FPKI]. The FPKI provides a capability for various government agencies' and their partners' PKIs to interoperate. To make certificate revocation information more readily available, the DoD PKI has enhanced its Robust Certificate Validation Service (RCVS). The PKI has incorporated changes that correspond to evolution of the Internet Engineering Task Force (IETF) Request for Comments (RFC) 5280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile* [RFC5280].

The Specification serves as a living document that will be updated periodically as necessary to address anticipated or actual changes to the interface. The document uses past tense to describe specific past and present features of the DoD PKI. The use of past tense will obviate any need to rewrite sections of the document when current features become past or previous features. The present or future tense will describe aspects of the PKI that are likely to transcend periodic PKI changes and remain accurate over time.

1.2 Standards-Based Services

The DoD PKI services are standards-based and follow standards that the IETF issues as RFCs. The IETF standards are often founded on the work of other standards bodies, such as the International Telecommunication Union (ITU). However, the IETF may tailor the foundation standard. The tailoring of standards may involve adding to and deleting from the foundation standard or changing the designation of some options that were considered optional or required. The IETF standards are those with which vendors and their products are most likely to comply.

1.3 Intended Audience

This document assumes that readers are familiar with PKI and its concepts and standards. Specifically, the document assumes that readers are familiar with Certification Authorities (CAs); operations; systems and their components; communications and related protocols; data

objects, such as certificates, certificate requests, and CRLs; and certificate status-checking concepts and approaches.

1.4 Notation Conventions

This document uses a small set of notation conventions for representing values or commands used within the DoD PKI. A different font represents data values stored in PKI data objects. Square brackets ([ ]) enclose optional items. Angle brackets (< >) enclose "meta" content that describes but is not a literal values. A vertical bar (|) separates alternatives that are bounded by parenthesis. For example, the line below represents a pattern for a string that has a last name followed by a first name separated by a period. The string may include either a middle initial or middle name following the first name and separated by a period.

CN=<lastname>.<firstname>[.(<middle_initial> | <middle_name>)]

Any of the following strings would satisfy the preceding description:

CN=DOE.JOHN

CN=DOE.JOHN.J

CN=DOE.JOHN.JAMES

1.5 Certificate Profile References

The DoD PKI has undergone a few major stages or releases since its creation in 1998. Each release involved changes to the infrastructure systems and capabilities, and the profiles (contents) of the certificates. The DoD PKI is currently in Release 3. Systems, services, and products or earlier releases are no longer in use. In late 2005, the DoD PKI began to update certificate profiles. In 2008, additional changes were made to certificate profiles. The information provided in a certificate did not materially change. The DoD PKI will evolve to the updated profiles. The DoD PKI will continue to support certificates issued under the previous profiles until the certificates expire. The DoD will follow the most recent updated profile when issuing new certificates. To simplify the description of the differences between the profiles, this document gives names to the profiles. The term Profile 3 (P3) refers to the original Release 3 certificate profile. Profile 3.1(P3.1) refers to the updated certificate profile that began in 2005; Profile 3.2(P3.2) refers to the updated certificate profile that began in 2008, and Profile 3.3 (P3.3) refers to the updated certificate profile that went into effect when the DoD PKI began using the Secure Hash Algorithm-256 (SHA-256) in its digital signatures. Section 2 describes the specifics of the updated certificate profiles but, as a brief summary, these profile changes included:

Profile 3.1:

- Creation of a new root CA with a 2048-bit signature key
- Changes to CA names to eliminate their association with Class 3
- Changes to the certificate content to assist PKI-enabled applications to construct certificate paths
- Changes to the certificate content to support additional protocols, repositories, and methods for obtaining certificate status

Profile 3.2:

- Addition of the Subject Directory Attribute Extension to hold the subject's citizenship information
- Support for the PIV program by including new values in extensions, adding a PIV authentication certificate for individuals, and adding other certificates to support PIV management
- Creation of a separate Interoperability Root CA (IRCA) to support integration with the FPKI and allied PKIs. A related set of intermediate cross-certificates was also issued to allow certificate chains to transcend the various cooperating PKIs.

Profile 3.3:

- The National Institute of Standards and Technology (NIST) published a draft standard [SP800-131] requiring the use of longer hash algorithms with digital signatures ideally beginning in 2011. When the DoD implemented this change, it affected virtually all signatures created by the PKI and changed the profiles of PKI objects.

1.6 Document Organization

The DoD PKI interface has several aspects. The PKI is a collection of information products and services. The PKI uses several subsystems, and each subsystem has an interface. The PKI interface` involves requests and responses which employ a communication protocol and formats for the information contained within the requests and responses. There are different protocols for interacting with the CA, the repository for obtaining certificates and CRLs, and the RCVS.

The remaining sections of this document each describe an aspect of the interface to the DoD PKI. Section 2 describes the profiles, or contents, of certificates that the DoD PKI issues. Section 3 describes the profile for CRLs. Section 4 describes the directory service which is repository for DoD PKI certificates and CRLs. The Global Directory Service (GDS) is the DoD PKI directory service. Users may retrieve certificates and CRLs from the GDS. Section 5 describes the RCVS. RCVS uses the Online Certificate Status Protocol (OCSP) to provide the status of individual certificates. Section 6 describes the interface to the Certificate Management System (CMS). Each of these sections concludes with a subsection that discusses future changes to the DoD PKI related to the section's topic. Section 7 identifies future services that could add to or significantly change DoD PKI services. Appendix AAppendix provides information on Object Identifiers (OIDs). Appendix B provides details on DoD PKI Uniform Resource Locators (URLs). Appendix C provides details on Organizational Units (OUs). Appendix D provides details about DoD PKI services on the Secret Internet Protocol Router Network (SIPRNet).

2 Certificate Profiles

This section describes the profiles of certificates that the DoD PKI issues. Through the DoD PKI, CAs issue certificates to certificate owners or subjects. The section describes certificates for three types of entities: root CAs, intermediate and signing CAs, and End-Entity (EE) certificates. Root CA certificates are *self-signed* certificates and serve as *trust anchors*. The certificates are trust anchors because the public keys contained in these certificates serve as the basis for making decisions about the trust and validity of other certificates. These certificates must be delivered *out of band* through trustworthy means to the *relying parties* who rely on DoD PKI certificates. Intermediate and signing CAs receive their certificates from a root CA. Intermediate CAs issue certificates to other CAs, while signing CAs issue certificates to EEs. The EEs are the *subjects* or *owners* of their certificates.

The DoD PKI has evolved since its inception. Initially, the PKI had a simple CA hierarchy consisting of the Class 3 Root CA, signing CAs, and EEs. Initially, EEs were individuals and servers. The DoD PKI now has other components and issues a wider variety of certificates. The DoD PKI operates the External CA (ECA) to issue certificates to entities that are outside of the DoD but must communicate with the DoD. Figure 1 shows the DoD PKI's internal environment.

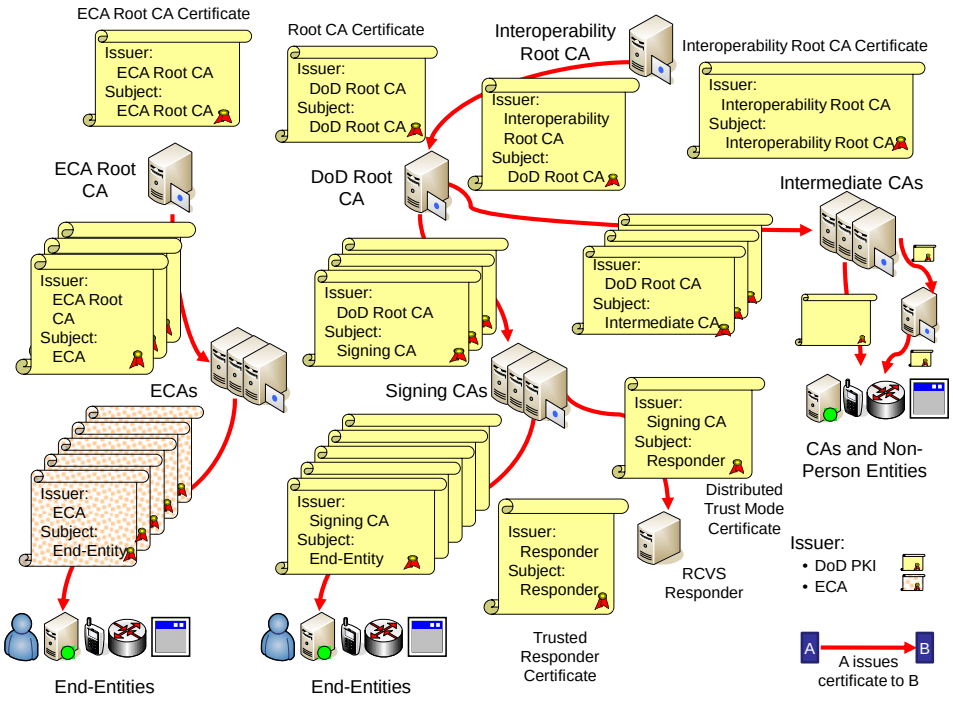

Figure 1: DoD PKI Internal Certificate Environment

As other organizations outside the DoD implemented PKIs, the DoD PKI Program Management Office (PMO) took steps to allow interoperability. To allow PKI interoperability, a CA in one PKI issues a certificate to a CA in the other PKI. This certificate is a cross-certificate. As a result, certificates descending from the cross-certificate's subject CA are

acceptable to the community that trusts the cross-certificate's issuer (or an ancestor). Often the cross-certificates exist as pairs where each of the CAs issues a certificate to the other.

The DoD created special root CAs to support this interoperability with other PKIs. The DoD Interoperability Root CA 1, the IRCA, was created to cross-certify the DoD PKI with the FPKI. Interoperability with the FPKI is provided through cross-certificates between the IRCA and the FBCA. Other interoperability root CAs may be created to allow interoperability with other communities such as allies and coalitions. Relying parties that support only internal DoD activities will continue to trust the DoD Root CAs. Relying parties that interact with entities outside the DoD will trust the appropriate Interoperability Root CA. Figure 2 shows the cross-certificate environment in which the DoD PKI operates. The figure focuses on cross-certified CAs and omits subordinate CAs and EEs.

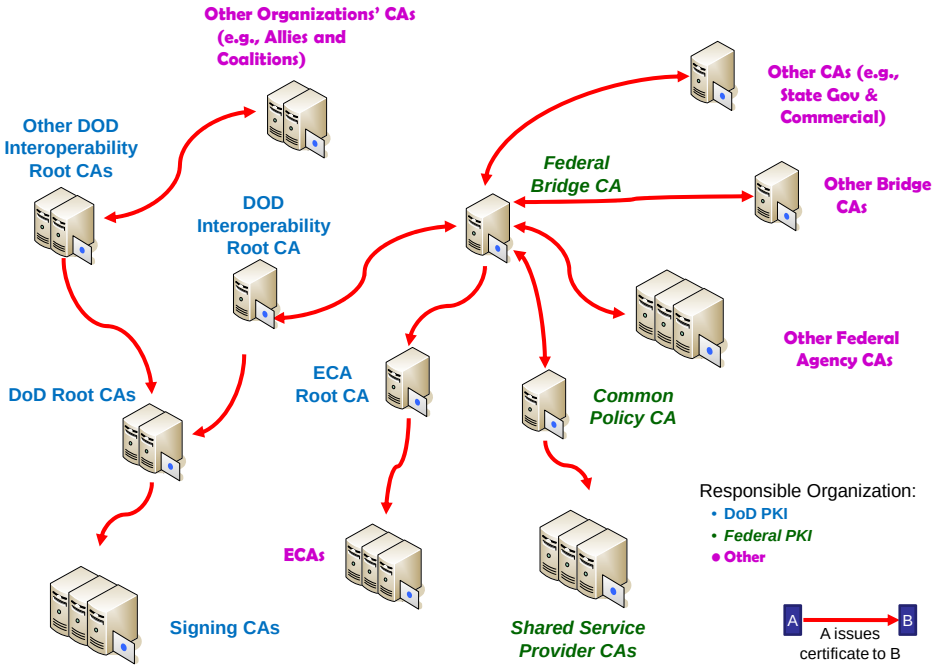

Figure 2: DoD PKI Interoperability with External PKIs

The remainder of this section describes the various profiles for certificates that the DoD PKI issued. Section 2.1 describes the certificate fields and their common or default content. This section provides a basis for describing certificate profiles and identifies the certificate fields and extensions that the DoD PKI certificates use. Sections 2.2, 2.3, and 2.4 describe the profiles for root CAs, intermediate and signing CAs, and EE certificates, respectively.

2.1 Certificate Fields and Common Contents

The DoD PKI issues certificates based on the IETF standard for certificate profiles [RFC5280].The DoD PKI does not use all of the options provided by the standard. Some fields and extensions are found in all DoD PKI certificates, some fields and extensions are never used, and some extensions' use depends on the specific certificate's profile. Table 1 shows certificate fields along with their use. The *Use* column indicates whether the field is

always present (A) or never present (N). The *Content* column describes the content of the field. Default values are provided where most profiles share a common value. Where appropriate, differences in the content of a field based on the DoD PKI release are noted.

The DoD PKI uses the industry standard Rivest-Shamir-Adleman (RSA) public key algorithm. The CA signatures on certificates initially used RSA in conjunction with the Secure Hash Algorithm-1 (SHA-1). The RSA key length was 1024 bits until P3.1, when the PKI created a second root CA with a 2048-bit key. Subsequent signing CAs also had 2048 keys. With P3.2, the default size for all keys was 2048. Starting with P3.3, all signatures used the SHA-256. The length of an SHA-256 hash is longer than an SHA-1 hash; their lengths are 256 bits and 160 bits, respectively.

Two of the certificate fields, Issuer and Subject, contain the name of the certificate's issuing and owning entities, respectively. The names follow the general structure for Distinguished Names (DNs) from the ITU X.500 Directory standards [X.500]. The details of the names used in DoD PKI certificates are found in Section 4.3. The Validity field contains a pair of dates (including time) that determine the beginning and ending dates for the certificate's validity period. The dates are represented in Coordinated Universal Time (UTC) format. This format allows only two characters to represent the year. The UTC format represents time in the Greenwich Mean Time (GMT) or Zulu time zone.

Table 1: Standard Certificate Fields

Certificate Field	Use	Content
Version	A	Default: X.509 Version 3 indicated by the value: 2.
Serial Number	A	Default: Unique integer for the issuing CA.
Signature Algorithm	A	Default prior to P3.3: sha1WithRSAEncryption (1.2.840.113549.1.1.5). Default starting with P3.3: sha256WithRSAEncryption (1.2.840.113549.1.1.11).
Issuer	A	DN of the issuing CA. The DN values use the Printable String character set.
Validity	A	The *not before* and *not after* times are represented in UTC format. Period length varies by profile. Valid: not before: Mon Dec 13 10:00:10 GMT 2004 not after: Wed Dec 05 10:00:10 GMT 2029
Subject	A	Certificate owner's DN. Format varies by profile.

Certificate Fields and Common Contents

2-4

Certificate Field	Use	Content
Subject Public Key Info	A	Default is RSA: rsaEncryption (1.2.840.113549.1.1.1). Prior to P3.1, the default modulus length was 1024 bits. Starting with P3.1, the default length for keys used by CAs was 2048 bits. Starting with P3.2, the default length for all keys was 2048 bits.
Unique Identifiers	N	No plans for use.
Extensions	A	Extensions used vary by profile.
Signature Algorithm	A	Default: sha1WithRSAEncryption (1.2.840.113549.1.1.5).
Signature Value	A	Default: The actual encrypted hash value.

All DoD PKI certificates include standards-based certificate extensions. The specific extensions and their contents may vary among the certificate profiles. Table 2 lists the standard extensions and provides information on their use, criticality, and how their use may change in the near future. The *Use* column indicates whether the extension is always (A), never (N), or sometimes (S) used. The *Critical* column has the same entries indicating whether the extension is marked as *Critical* in the certificate. The *Future* column has entries to indicate whether the DoD PKI has definitive plans to use the extension in the near future (D) or is considering possible future use of the extension (P). The entry is empty if there are no foreseeable plans to use the extension. The *Content* column has information about the extension's values and explains any sometimes (S) entries in the *Use* or *Critical* columns and entries in the *Future* column. The content entry also specifies default values that are common to multiple certificate profiles.

Many of the extensions described in RFC 5280 [RFC5280] contain optional fields. Throughout this document, the discussion of an extension's inclusion in a certificate profile will not mention an optional field unless it is used. For example, the description of the Basic Constraints extension will not mention the path length constraint unless the profile asserts a path length constraint value.

Table 2: Standard Certificate Extensions

Certificate Extension	Use	Critical	Future	Content
Standard Extensions				
Authority Key Identifier (AKI)	S	N		All certificates except root certificates. Default: Key Identifier form using the 20-byte SHA-1 hash of the binary Distinguished Encoding Rules (DERs) encoding of the signing CA's public key information.
Subject Key Identifier (SKI)	A	N		Default: 20-byte SHA-1 hash of the binary DER encoding of subject's public key information.
Key Usage (KU)	S	A		Present in all certificates except root certificates prior to P3.1 and in self-issued OCSP signing certificates. Default for P3.1 Root, signing, and intermediate CA certificates: digitalSignature, keyCertSign, and cRLSign. EEs usually have either digitalSignature or keyEncipherment ,but may have both. EEs with digitalSignature may also have nonRepudiation.
Certificate Policies (CP)	S	N		Signing and intermediate CA certificates assert policies under which the CA may issue certificates. Many EE certificates assert the specific policies that apply to the certificate.
Policy Mappings (PMs)	S	N		Used in cross certificates with CAs belonging to organizations external to the DoD such as the FBCA.
Subject Alternative Name (SAN)	S	N		Used in some EE certificates.

Certificate Fields and Common Contents

Certificate Extension	Use	Critical	Future	Content
Issuer Alternative Name (IAN)	S	N		For DoD P3 and prior certificates, held the Lightweight Directory Access Protocol (LDAP) URL to the issuer's entry in the directory. After P3, this extension was not used. Information about the issuer may be accessed through the Authority Information Access (AIA) extension.
Subject Directory Attributes (SDAs)	S	N		Not used prior to P3.2. Starting with P3.2, contains the citizenship attribute for individual subscribers for certain situations.
Basic Constraints (BC)	S	A		Present in CA certificates but not in EE certificates (except self-signed OCSP responder certificates). Beginning with P3.2, the path length component of this extension was used. The default path length value was 0 but there were exceptions that are noted in the description of affected CA certificates.
Name Constraints (NC)	S	S	D	Used in FBCA and ECA certificates. Critical when used in ECA certificates.
Policy Constraints (PCs)	N	N	D	Used in cross-certificates in conjunction with the FBCA. The extension may be marked critical at some time in the future.
Extended Key Usage (EKU)	S	S		Used in some EE certificates. Critical in OCSP responder certificates.
CRL Distribution Points (CDP)	S	N		Present in intermediate and signing CAs and EE certificates. Prior to P3.1, used LDAP URL for the issuing CA's CRL attribute in the appropriate PKI directory. Before P3, used LDAP URL that points to GDS and included a HyperText Transfer Protocol (HTTP) URL for the CRL. Beginning with P3.2, the LDAP URL was dropped in some certificates.
Inhibit any Policy	N			

Certificate Extension	Use	Critical	Future	Content
Freshest CRL	N			
Private Internet Extensions				
Authority Information Access (AIA)	S	N		Used in most EE certificates starting with P3.1. Provided HTTP pointers to retrieve the issuer's certificates and to an OCSP responder capable of providing the status of the certificate.
Subject Information Access (SIA)	S	N		Used in certain cross-certificates involving intermediate CA certificates, to conform to the Federal PKI Certificate Profile and to facilitate cross-certificate path building.

The remaining sections describe the profiles for the various certificates. The discussions of the individual profiles will identify the contents of the specific certificate profiles that differ from the defaults described above.

Several extensions appear in multiple certificate profiles. The common extensions are IAN, CDP, AIA, and SIA. These extensions contain pointers to repositories for information needed by relying parties. The pointers are in the form of URLs. The DoD PKI PMO defined several certificate policies that are included in the Certificate Policies Extension. Relationships exist among values contained in related certificates. The relationships may be between values in a certificate and the certificate of its issuer. The following subsections describe the common URL references, the common extensions and the values they contain, the certificate policies, and the value relationships.

2.1.1 URL References and Their Responses

DoD PKI certificates contain internal references based on the LDAP and HTTP. Originally, all references were LDAP references. Later, HTTP references were added giving two methods to retrieve information objects such as CRLs and certificates. HTTP was the recommended method and was listed first when both methods were available. Because of security issues associated with LDAP, some sites blocked the standard ports associated with LDAP. For this reason, HTTP became the preferred method because LDAP access was not guaranteed.

The URL references are specific to allow direct retrieval of information needed by relying parties. Table 3 shows the specific information available through the URLs. HTTP references contain the protocol, host name, path, and query, as appropriate. The HTTP references return a media type appropriate for the information requested. LDAP references include the protocol, the host, the DN for an entry, and the attribute or attributes containing the needed information.

Table 3: DoD PKI URL References

Information Type	LDAP Attribute	HTTP Media Type
CRL	*certificateRevocationList;binary*	*application/pkix-crl*
CA Certificate(s)	*cACertificate;binary* or *crossCertificatePair;binary*	Responses with a single certificate: *application/pkix-cert* [RFC 2585]. Responses with multiple certificates are encoded as a certificates-only message in accordance with RFC 2797 with media type: *application/pkcs7-mime*

2.1.2 HTTP URL Forms

The initial HTTP references used within certificates involved dynamic URLs. This is an example of a dynamic URL:

http://crl.disa.mil/getcrl?DoD%20CA-23

This URL is dynamic because it includes a question mark (*?*). The part before the *?* identifies a program, routine, or script running on the Web server and the part following the *?* contains parameters or variables for use of the program, routine, or script. An example of a static URL is:

http://crl.disa.mil/crl/DODCA_23.crl

This static URL does not contain a *?* and appears to request a file residing on the Web server.

Initially certificate references contained dynamic HTTP URLs but were later changed to static URLs. Table 4 below shows the dynamic URLs used in certificates and the corresponding static URL. The static URLs appear to refer to files residing on the Web server. The CA names were compressed in the static URLs. CA names in the static form omit spaces and change hyphens (-) to underscores (_).[1] The URLs containing the "issued to" or "issued by" collection of certificates have "_IT" or "_IB", respectively, added to the end of the CA name to distinguish the two collections. The remaining subsections describe the situations where the two forms were used in certificates.

[1] The changes to the CA name format allow the responses to be stored as files with the same file name as referenced in the URL. Spaces, plus signs, and hyphens sometimes are not allowed in file names or create problems when included in file names.

Table 4: Dynamic URLs and Their Corresponding Static URLs

Dynamic URL	Corresponding Static URL
http://crl.disa.mil/getcrl?DoD%20CA-23	http://crl.disa.mil/crl/DODCA_23.crl
http://crl.disa.mil/getsign?DOD%20CA-19	http://crl.disa.mil/sign/DODCA_19.cer
http://crl.disa.mil/getissuedto?DOD%20CA-19	http://crl.disa.mil/issuedto/DODCA_19_IT.p7c
http://crl.disa.mil/getissuedby?DOD%20CA-19	http://crl.disa.mil/issuedby/DODCA_19_IB.p7c

2.1.3 Common IAN Use

Prior to P3.1, the IAN contained an LDAP URL that pointed to the entry in the PKI directory for the CA that issued the certificate. Relying parties could use the URL to locate information about the issuer, including the issuer's certificate. The IETF added the AIA extension. The purpose of this extension was to provide a reference to the issuer's certificate. With the inclusion of the AIA in P3.1 by the DoD PKI, the IAN was no longer used after P3.

The value found in the IAN was an LDAP URL for the issuing CA's directory entry. The URL appeared under the Uniform Resource Identifier (URI) option for names used in the IAN. An example of the entry found in the IAN for a certificate issued by CA-6 is:

ldap://ds-4.c3pki.den.disa.mil/cn=DoD CLASS 3 CA-6,ou=PKI,ou=DoD, o=U.S. Government, c=US

The actual value contained in the IAN encoded special characters in accordance with the practice for URL content. [RFC1738] The URL encoded value corresponding to the above value would be:

ldap://ds-4.c3pki.den.disa.mil/cn%3dDOD%20CLASS%203%20CA-6%2c ou%3dPKI%2cou%3dDoD%2co%3dU.S.%20Government%2cc%3dUS

2.1.4 Common CDP Use

The content of the CDP changed with DoD PKI P3.1. The CDP prior to P3.1 contained a single LDAP reference to the CRL attribute in the issuing CA's entry in the PKI directory. Starting with P3.1, the entry contained two alternative URLs using HTTP and LDAP. The next subsections elaborate on the content.

2.1.4.1 CDP Prior to P3.1

The P3 and earlier CDP entries were similar to the IAN. The CDP pointed to the CRL attribute in the issuing CA's entry in the PKI directory. The CDP contained an LDAP reference using the URI alternative name format. For example, the CDP entry in a certificate that CA-6 issued would be the URL encoded [RFC1738]form of:

ldap://ds-4.c3pki.den.disa.mil/cn=DoD CLASS 3 CA-6,ou=PKI,ou=DoD, o=U.S. Government, c=US?certificaterevocationlist;binary

2-10

2.1.4.2 CDP after P3

CDP entries after P3 contained two alternative URLs to retrieve the issuing CA's CRL. Both alternatives used the URI format for names. The first URL was an HTTP reference that returns the CRL in binary DER format. The returned value's media-type is *application/pkix-crl*. An example of the HTTP URL for a certificate that CA-19 issued would be the URL:

http://crl.gds.disa.mil/getcrl?DoD%20CA-19

This dynamic URL was subsequently changed to a static URL of the form:

http://crl.disa.mil/crl/DODCA_19.crl

The second CDP URL is an LDAP reference similar to that contained in certificates issued prior to P3.1, but different host names were used.[2] An example prior to URL encoding is:

ldap://crl.gds.disa.mil/cn=DoD CA-23,ou=PKI,ou=DoD,
o=U.S. Government, c=US?certificaterevocationlist;binary

This LDAP reference was dropped in some certificates beginning with P3.2.

2.1.5 Common AIA Use

The AIA was not used prior to P3.1. The AIA contained values for two possible access methods: CA Issuers and OCSP. The access location values for each used the URI form for names and contained HTTP references. The CA Issuers' reference returned the certificate issued to the issuer of the certificate. The media type of the value returned is either application*/pkix-cert* or *application/pkcs7-mime* depending on whether the value has only one or multiple certificates, respectively. Certificates contained in the issuers' reference will generally include certificates stored in the caCertificate attribute and the *issuedToThisCA* [3] components of the crossCertificatePair attribute in the Issuer's directory entry.[4] When the value contains multiple certificates, relying parties should make no assumptions about the ordering of the certificates. An example of this URL contained in an individual's identity certificate issued by CA-19 is:

http://crl.disa.mil/getsign?DoD%20CA-19

This dynamic URL was later changed to a static URL of the form:

http://crl.disa.mil/sign/DODCA_19.cer

An example of the URL contained in the Root CA 2's certificate to signing CA-19 is:

http://crl.disa.mil/getIssuedTo?DoD%20Root%20CA%202

This dynamic URL was later changed to a static URL of the form:

---

[2] This Specification does not show all of the previously used host name patterns. The PKI supported URI references embedded in certificates for as long as the certificates were active.

[3] The *issued to* component was previously known as the *forward* component of the pair [RFC4158].

[4] Section 4.4 describes the use of cross-certificate pairs in the DoD PKI directories.

http://crl.disa.mil/issuedto/DODROOTCA2_IT.p7c

The OCSP reference has the URL for an OCSP responder. The request and response formats, contents, and use of HTTP follow the OCSP standard [RFC2560]. Section 5 describes the interface to the OCSP responder.

2.1.6 Common SIA Use

The SIA was not used prior to P3.2. The SIA contained values for the CA Repository access method. This access method value contained HTTP references. A reference returned the certificates that the subject issued. The media type of the value returned is either application*/pkix-certificate* or *application/pkcs7-mime* depending on whether the value has only one or multiple certificates respectively. Certificates contained in the reference will generally include certificates stored in the *issuedByThisCA*[5] components of the crossCertificatePair attribute in the Subject's directory entry. When the value contains multiple certificates, relying parties should make no assumptions about the ordering of the certificates. Examples of these URLs in a certificate issued to the DoD Root CA 2 by the Interoperability Root CA 1 are the URL encoded forms of:

http://crl.disa.mil/getIssuedBy?DoD Root CA 2

and

ldap://crl.gds.disa.mil/CN= DoD Root CA 2, OU=PKI, OU=DoD,O=U.S. Government, C=US?crossCertificatePair;binary

The dynamic HTTP URL was later changed to a static URL of the form:

http://crl.disa.mil/issuedby/DODROOTCA2_IB.p7c

2.1.7 Certificate Policies

Since its inception, the DoD PKI has included the CP Extension. This extension contains a list of certificate policies. Certificate policies are individually indentified by an OID. The extension contains the policies that state the intended use for EE certificates. For CA certificates, the extension contains the set of policies that may appear in descendants' certificates. The policies in the CA certificate limit the certification paths that can include the CA certificate.

The DoD created new certificate policies with P3.2 and referenced policies belonging to other PKIs with which the DoD interoperated. Initially, the DoD PKI issued EE certificates with one of two policies: id-US-dod-medium[6] and id-US-dod-mediumHardware. Signing CAs included those two policies and a third policy that was reserved for possible future use. Starting with P3.2, the DoD renamed the future use OID to id-US-dod-PIV-Auth[7] and created three new policies. The new policies were counterparts to the other three but for 2048-bit keys.

---

[5] The *issued by* component was previously known as the *reverse* component of the pair [RFC4158].

[6] The id-US-dod-medium and id-US-dod-mediumhardware formerly had the names id-US-class3 and id-US-dod-class3hardware, respectively, and have the same respective OIDs.

[7] The id-US-dod-PIV-Auth OID was deprecated and not used.

Certificate Fields and Common Contents

2-12

Certificates issued for 2048-bit keys asserted both the appropriate 2048-bit policy and its 1024-bit counterpart. Asserting both policies allowed the 2048-bit key to be used by relying parties that checked for the 1024-bit policy.

Starting with P3.2, some certificates' CP extension began to include policies from the FBCA and from the FPKI Common Policy PKIs. The FBCA policies were only used in the Policy Mapping Extension in certificates issued to CAs outside of the DoD PKI. Both CA and EE certificates issued after the FPKI approved the DoD PKI's participation under the FPKI Common Policy contain policies from the FPKI Common Policy. Signing CA certificates contain five common policies: common policy, hardware, devices, authentication, and card-authentication. Initially, only one EE certificate, the PIV Authentication certificate (see Section 2.4.1.4), contained an FPKI certificate policy, the common authentication policy. The other common policies may be asserted as appropriate in the future. Table 5 lists the Certificate Policies by name. Appendix A provides the specific OIDs.

Table 5: Certificate Policies

Policy	Purpose
DoD Policies	
id-US-dod-medium	Private key is 1024 bits and protected in a software token (or possibly a hardware token whose assurance is below that required for the medium hardware policy)
id-US-dod-mediumhardware	Private key is 1024 bits and protected in a hardware token
id-US-dod-medium-2048	Same as id-US-dod-medium but private key is 2048 bits.
id-US-dod-mediumhardware-2048	Same as id-US-dod-mediumhardware but Private key is 2048 bits.
FBCA Policies	See FBCA Certificate Policy [FBCACP]
id-fpki-certpcy-rudimentaryAssurance	Not used
id-fpki-certpcy-basicAssurance	Not used
id-fpki-certpcy-mediumAssurance	Roughly equivalent to id-US-dod-medium
id-fpki-certpcy-medium-CBP	Not used
id-fpki-certpcy-mediumHW	Roughly equivalent to id-US-dod-mediumhardware
id-fpki-certpcy-mediumHW-CBP	Not used

Policy	Purpose
id-fpki-certpcy-highAssurance	High assurance certificates as recognized by the FBCA.
id-fpki-certpcy-testAssurance	Not used
FPKI Common Policies	See FPKI Common Policy Certificate Policy [FPKICP]
id-fpki-common-policy	Roughly equivalent to id-US-dod-medium-2048
id-fpki-common-hardware	Roughly equivalent to id-US-dod-mediumhardware-2048
id-fpki-common-devices	Not used
id-fpki-common-authentication	Used in PIV authentication certificates (see Section 2.4.1.4)
id-fpki-common-High	Not used
id-fpki-common-cardAuth	Not used

2.1.8 Relationships between Certificates in a Certificate Chain

Certain fields in the certificates belonging to an entity and its issuer are related. The relationships exist among names, key identifiers, and validity periods. For example, the name in a certificate's issuer field is the same as the name in a subject field in the issuer's certificate. Figure 3 illustrates this relationship.

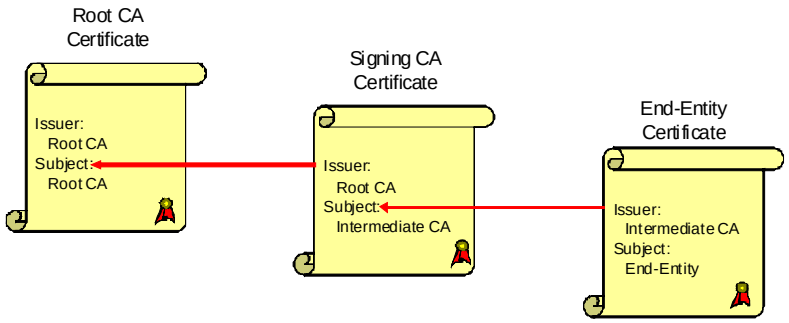

Figure 3: Relationship among Names in a Certificate Path

A similar relationship exists between the SKI extension in a CA certificate and the AKI extension in certificates the CA issued. The SKI and AKI have the same values.

The chaining of the names is essential to path construction and validation. The key identifier assists in finding the needed certificate among several certificates issued to the same subject. Although the DoD PKI has not issued multiple certificates to a CA that have the same subject name but different keys, it may do so at some time in the future.

The validity periods for DoD PKI-issued certificates are related. The validity period in an issuer's certificate encompasses the validity period in any of the certificates that it issues. This relationship ensures that if the effective date for constructing a certificate path is within an EE's validity period, then the date is also within the validity period of ancestor certificates in the path. Although the DoD PKI certificate validity periods are related, path validation must ensure that each certificate in a path is valid on the effective date of use for the path's construction and validation.

For paths that involve certificates issued outside of the DoD PKI (i.e., cross-certificates), the relationship among validity periods of certificates in a path may not apply. Again, the path construction and validation must ensure all certificates were valid on the effective date of the validation.

2.1.9 Profile Default Values

The discussion above identified certificate and extensions fields that are common to one or more of the more detailed and specific profiles. When a specific profile uses these default values, the entry in the profile table will state that it has a default value rather than repeat the description of the content.

2.2 Root Certification Authority Certificates

The DoD PKI has had several root CAs. This section describes the DoD PKI root CAs' certificates, starting with those used in P3. The DoD PKI also maintains an ECA Root CA for certificates issued under the DoD PKI's ECA program and an IRCA. The ECA Root CA issues certificates to commercial CAs that issue ECA EE certificates. The IRCA serves as a root CA that provides for interoperability with the FPKI.

Root certificates are self-issued and self-signed. Consequently, the certificates have the following characteristics:

- The certificate's issuer and subject are same.
- The certificate's subject's public key is the same public key that can be used to validate the root CA certificate.

The only other self-signed certificates in the DoD PKI were for the RCVS responders. Since the responder only signs RCVS responses and not certificates for other entities, the responder is an EE rather than a CA. Section 2.4.8 describes the responder's certificate.

The next subsections describe the profiles for the root CAs' certificates. The DoD root certificates have slightly different formats. The following subsections describe the DoD root certificates and their differences.

2.2.1 P3 Root CA

The P3 Root CA's certificate profile is described in the tables below. Table 6 shows certificate fields that distinguish the P3 Root CA certificate. Omitted fields have the default values described previously. Although the P3 Root CA's validity period extended to the year 2020, the P3 Root CA was scheduled for retirement in 2010. At that time, all certificates descended from the P3 Root CA had expired. Table 7 identifies the P3 Root CA's certificate extensions and the values they contained. The entries in the *Critical* column of this and subsequent

certificate extension tables are Yes (Y) or No (N) to indicate whether the extension is (Y) or is not (N) critical. The *Future* column has entries to indicate if future use of the extension is contemplated.

The P3 Root CA and its descendent CAs no longer issue new certificates. The CA continued to issue CRLs while there were active descendent EEs. The CA issued CRLs for a period after the active EEs expired until it was formally retired.

Table 6: P3 Root CA Certificate Fields

Certificate Field	Content
Serial number	4
Issuer/Subject	CN=DoD CLASS 3 Root CA, OU=PKI,OU=DoD,O=U.S. Government,C=US
Validity	20-year validity period: Valid: not before: Fri May 19 13:13:00 GMT 2000 not after: Thu May 14 013:13:00 GMT 2020

Table 7: P3 Root CA Certificate Extensions

Certificate Extension	Critical	Future	Content
Basic Constraints	N		CA: yes
Subject Key Identifier	N		Default

2.2.2 P3.1 Root CA

The P3.1 Root CA's certificate profile is described in the tables below. The strength of this CA's key was improved by increasing the key length to 2048 bits. Table 8 shows certificate fields that distinguish the P3.1 Root CA certificate. Omitted fields have the default values described previously. Table 9 identifies the P3.1 Root CA's certificate extensions and the values they contain.

Table 8: P3.1 Root CA Certificate Fields

Certificate Field	Content
Serial number	5
Issuer/Subject	CN=DoD Root CA 2,OU=PKI,OU=DoD, O=U.S. Government,C=US
Validity	25-year validity period: Valid: not before: Mon Dec 13 15:00:10 GMT 2004 not after: Wed Dec 05 15:00:10 GMT 2029
Subject Public Key Info	RSA with 2048-bit modulus.

Table 9: P3.1 Root CA Certificate Extensions

Certificate Extension	Critical	Future	Content
Basic Constraints	Y		CA: yes
Key Usage	N		digitalSignature, keyCertSign, and cRLSign
Subject Key Identifier	N		Default.

2.2.3 External Certification Authority Root CAs

The DoD PKI has issued two ECA Root CAs. The primary difference between the two CAs was their key length. The first CA had a 1024-bit key, while the second CA had a 2048-bit key. The second CA certificate also contained additional extensions relative to the first. The next two subsections describe the two ECA Root CAs.

2.2.3.1 Original External Certification Authority Root CA

The original ECA Root CA's certificate profile is described in the tables below. Table 10 shows certificate fields that distinguish the ECA Root CA's certificate. Omitted fields have the default values described previously. Table 11 identifies the ECA Root CA's certificate extensions and the values they contain. The certificate has both the SKI and AKI extensions, although their core identifier values are identical. The certificate also contains the certificate policy identifiers for the ECA certificate policies. An OID serves as an identifier for each of the ECA certificate policies. The table uses the name given to the OID in the global OID registry. Appendix A contains information about the OIDs referenced in this document.

Table 10: ECA Root CA Certificate Fields

Certificate Field	Content
Serial number	14
Issuer/Subject	CN=ECA Root CA,OU=ECA,O=U.S. Government, C=US
Validity	36-year validity period: Valid: not before: Mon Jun 14 10:20:09 GMT 2004 not after: Thu Jun 14 10:20:09 GMT 2040

Table 11: ECA Root CA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature, keyCertSign, and cRLSign
Basic Constraints	Y		CA: yes
Certificate Policies	N		Policy Identifiers: id-eca-medium id-eca-medium-hardware
Subject Key Identifier	N		Default.
Authority Key Identifier	N		Default.

2.2.3.2 External Certification Authority Root CA 2

The ECA Root CA 2's certificate profile is described in the tables below. Table 12 shows certificate fields that distinguish the ECA Root CA 2's certificate. Omitted fields have the default values described previously. Table 13 identifies the ECA Root CA 2's certificate extensions and the values they contain. The certificate has an SIA extension that has HTTP and LDAP links to obtain information about certificates that the CA issued to other CAs.

Table 12: ECA Root CA 2 Certificate Fields

Certificate Field	Content
Serial number	5

2-18

Certificate Field	Content
Issuer/Subject	CN=ECA Root CA 2,OU=ECA,O=U.S. Government, C=US
Validity	20-year validity period: Valid: not before: Fri Apr 04 14 24:49 GMT 2008 not after: Thu Mar 30 14:24:49 GMT 2028

Table 13: ECA Root CA 2 Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature, keyCertSign, and cRLSign
Basic Constraints	Y		CA: yes
Subject Key Identifier	N		Default.
Subject Information Access	N		Contains an HTTP and an LDAP reference to find certificates that the CA issued.

2.2.4 Interoperability Root CA

The IRCA's certificate profile is described in the tables below. Its general profile is the same as that for the ECA Root CA 2. Table 14 shows certificate fields that distinguish the IRCA's certificate. Omitted fields have the default values described previously. Table 15 identifies the IRCA's certificate extensions and the values they contain.

Access to the actual root certificate was limited. Most DoD relying parties should only trust DoD-issued certificates and not trust certificates issued outside of the DoD for normal activities. Organizations and applications that must interoperate with the broader FPKI community had to obtain the IRCA certificate through special channels.

Table 14: IRCA Certificate Fields

Certificate Field	Content
Serial number	<unique integer>
Issuer/Subject	CN=Interoperability Root CA 1,OU=PKI,OU=DoD, O=U.S. Government, C=US

Certificate Field	Content
Validity	20-year validity period:

Table 15: IRCA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature, keyCertSign, and cRLSign
Basic Constraints	Y		CA: yes
Subject Key Identifier	N		Default.
Subject Information Access	N		Contains an HTTP and an LDAP reference to find certificates that the CA issued.

2.2.5 Other Interoperability Root CAs

Additional Root CAs may be created to enable the DoD PKI to interoperate with other PKIs. The other PKIs will belong to different communities of interest. The communities may be members of international organizations or business partners and consortia. The profiles for the root certificates will likely be similar to the profiles used for the ECA's and IRCA's certificates.

2.3 Intermediate and Signing Certification Authority Certificates

The DoD PKI issues several types of certificates for intermediate and signing CAs. Intermediate and signing CAs are not root CAs. Instead, they receive certificates from a root CA that authorizes the CAs to issue certificates subsequently to other entities. The DoD PKI operates multiple signing CAs to issue certificates to DoD EEs.[8] The DoD PKI also issued signing CA certificates under the ECA Root CAs to commercial vendors that are authorized to issue ECA certificates to EEs. The DoD PKI participated in the FBCA program using the IRCA to allow PKIs operated by various FBCA partner organizations to interoperate. A pair of cross-certificates was issued between the IRCA and the FBCA. Because these certificates are not self-signed, they are included in this discussion of intermediate CA certificates. The following subsections describe the signing and intermediate CA certificate profiles.

[8] The term *intermediate CA* has different meanings. Web browsers generally use the term to refer to CAs that are not root CAs. The FPKI defines the term to refer to CAs that only issue certificates to other CAs. This document will use the FPKI definition. Signing CAs issue certificates to EEs.

2-20

2.3.1 DoD PKI Signing CAs' Certificates

The DoD PKI signing CAs sign certificates for DoD EEs. The DoD has designated CAs with the primary purpose of signing either identity or e-mail certificates. CAs restricted to signing e-mail certificates have *Email* in their Common Name (CN). The signing CA certificates are different for each PKI release, but the certificates follow the defaults for the releases. Table 16 shows certificate fields that distinguish the signing CAs' certificates. The issuer's name corresponds to the root CA for the relevant release. The CA DNs included *Class 3* for signing CAs prior to P3.1 and omitted mention of a class starting with P3.1. Omitted fields have the default values described previously. The validity period has been 6 years for the signing CAs. This period may change and should not be assumed. The validity period will always be a range within the issuing root CA's validity period and will encompass the validity period of any EE certificates that the CA issues. Table 17 identifies the signing CA certificate extensions and the values they contain. The IAN and CDP follow the defaults for the relevant release.

Table 16: Signing CA Certificate Fields

Certificate Field	Content
Issuer	One of the root CAs, such as: CN=<Root CA>,OU=PKI,OU=DoD, O=U.S. Government,C=US
Validity	Validity period for legacy signing CAs has been 6 years, but the period length may change and should not be assumed to be 6 years in all cases.
Subject	CN=DoD [Class 3][Email]CA-<n>,OU=PKI, OU=DoD,O=U.S. Government,C=US
Subject Public Key Info	RSA with 1024-bit modulus prior to P3.2. Profile 3.2 changed modulus to 2048 bits.

Table 17: Signing CA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature, keyCertSign, and cRLSign
Basic Constraints	Y		CA: yes; Path Length Constraint: 0 The path length constraint was absent prior to P3.2.

Certificate Extension	Critical	Future	Content
Certificate Policies	N		Policy Identifiers prior to P3.2: id-US-dod-medium id-US-dod-mediumhardware reserved for future use Policy Identifiers after P3.1: id-US-dod-medium id-US-dod-mediumhardware id-US-dod-PIV-Auth[9] id-US-dod-medium-2048 id-US-dod-mediumhardware-2048 id-US-dod-PIV-Auth-2048[9] id-fpki-common-policy id-fpki-common-hardware id-fpki-common-devices id-fpki-common-authentication id-fpki-common-cardAuth
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default for release.
Issuer Alternate Name	N		Present for CAs prior to P3.1.
Policy Constraints	N		Require explicit policy: 0
Authority Key Identifier	N		Default.

2.3.2 ECA Certificates

The DoD PKI issues certificates to CAs that the DoD PKI has approved to operate as ECAs. These certificates are issued under an ECA Root CA. Commercial organizations operate ECAs. The ECAs sign certificates for EEs that are external to the DoD but need to interoperate with DoD organizations using the DoD PKI. Table 18 shows certificate fields that distinguish the ECA certificates. The ECA Root CAwill be the issuer. The subject's CN will vary and may not follow a specific structure or format. The remainder of the subject's DN will specify the CA's subtree under the ECA's subtree in the GDS directory (see Section 4.2). Omitted fields have the default values described previously. The validity period has been 6

[9] The PIV-Auth policies never appeared in EE certificates. Instead, the EE certificates intended for authentication purposes asserted the *id-fpki-common-authentication* policy.

2-22

years for the ECAs but may vary and must not be assumed always to be 6 years. The validity period will always be within the issuing ECA Root CA's validity period and will encompass the validity period of any EE certificates that the CA issues. Table 19 identifies the ECA's certificate extensions and the values they contain. Initially, the ECA certificates included a Name Constraints extension that restricted the subject name in certificates that the ECA issued. The subject's DN must be under the subtree allocated to the ECA in the GDS Directory Information Tree (DIT). Because some popular applications did not always correctly interpret this extension, the extension was removed, and certificates were reissued to the ECAs without the Name Constraints extension. The extension may be reinstated in the future. Applications should be capable of processing the Name Constraints extension.

The ECAs have some flexibility to determine extensions and their values. Some ECAs will include optional information in the CP extension to allow relying parties to find the applicable Certification Practice Statement (CPS). Some ECAs may be allowed to include additional extensions for their use. General applications must not rely upon any extensions unique to individual ECAs. More information on the ECA program, its participating ECAs, ECA certificates, and related documents may be found at the ECA Web site [ECA].

Table 18: ECA Certificate Fields

Certificate Field	Content
Issuer	ECA Root CAs: CN=ECA Root CA,OU=ECA, O=U.S. Government,C=US or CN=ECA Root CA 2,OU=ECA, O=U.S. Government,C=US
Validity	Validity period may vary but will generally be 6 years.
Subject	CN=<common name>,OU=Certification Authorities OU=ECA,OU=DoD,O=U.S. Government,C=US
Subject Public Key Info	RSA with 1024-bit modulus for certificates issued by ECA Root CA. 2048-bit modulus for certificates issued by ECA Root CA 2.

Table 19: ECA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature, keyCertSign, and cRLSign
Basic Constraints	Y		CA: yes; Path Length Constraint: 0

Certificate Extension	Critical	Future	Content
Certificate Policies	N		Policy Identifiers: id-eca-medium id-eca-medium-hardware May include policy qualifiers.
Subject Key Identifier	N		Default.
Authority Key Identifier	N		Default.
CRL Distribution Points	N		May have LDAP or HTTP URL(s) for the CRL. The host involved may include either or both DoD and ECA-operated systems.
Name Constraints	N		Permitted Subtrees: Base: directory name: OU=<ECA Identifier>,OU=ECA, O=U.S. Government, c=US minimum:0 Base: rfc822name: minimum:0
Authority Information Access	N		Optional. May be present. May contain either or both CA Issuer and OCSP component.

2.3.3 Federal Bridge Certification Authority Cross-Certificates

Full participation in the FBCA involves issuing a pair of cross-certificates. The CAs that are the subjects of the cross-certificates are intermediate CAs. Ideally, a participating CA and the FBCA each issued certificates to the other. With these cross certificates, trust chains can be constructed between an EE certificate the partner PKI issued and the trust anchor of any other partner, and between the partner's trust anchor and any EE certificate issued by any other partner CA.

These cross certificates are similar to other CA certificates but employ more extensions. The additional extensions primarily restrict or limit the certificates that FBCA partners may accept from other partners. The extensions constrain the DN forms and specify rules for mapping between a partner's certificate policies and FBCA certificate policies. The AIA, SIA, and CDP extension contents reference FBCA resources for CA certificates and CRLs produced external to the DoD PKI.

Intermediate and Signing Certification Authority Certificates

2-24 Because of differences in the operations of the FBCA and its partner PKIs, the validity period in an issuer's certificate may not contain the validity period in a subordinate certificate in a certificate chain that involves the FBCA.

Information on the FBCA program can be found on the FBCA Web site [FBCA]. The FBCA is the authoritative source for information identifying the FBCA partners, current policies, profiles for FBCA-issued certificates and CRLs, and information on how to use and interact with the FBCA components.

Initially, the DoD PMO considered cross-certifying the DoD Root CAs with the FBCA. The FBCA issued a cross-certificate to the DoD Class 3 Root CA. However, the DoD PKI did not issue a cross-certificate to the FBCA in the same timeframe. The DoD PKI subsequently created the IRCA (see Section 2.2.4) for cross-certifying with the FBCA and the FPKI. The Interoperability Root CA and related cross-certificates were depicted in Figure 2. Only those organizations needing to interoperate with the FBCA community should trust the Interoperability Root CA.

The following subsections describe the cross-certificates between the DoD PKI and FPKI involving the FBCA.

2.3.3.1 FBCA-to-DoD Class 3 Root CA Certificate

This subsection describes the cross-certificate that the FBCA issued to the DoD Class 3 Root CA. The certificate allowed applications to construct certificate chains between an FBCA partner agency's root CA and EEs issued by the DoD PKI. Figure 4 illustrates the role of the certificate in certificate chains. Because the FBCA issued this certificate, the content of the certificate was not under the direct control of the DoD PKI and was subject to change. Table 20 shows certificate fields that distinguish the FBCA-to-DoD Class 3 Root CA cross-certificate. Table 21 identifies the certificate extensions and the values they contain. The policy-mapping extension asserts that the DoD Class 3 certificate policies were equivalent to their counterpart FBCA-medium certificate policies [FBCA].

Since multiple organizations' PKIs may issue certificates to the FBCA, the CA Issuers' portion of the AIA differed from and was more complex than the default. The relying party must construct a path from the EE's certificate to the relying party's agency's root CA. The path was different for each agency. Relying parties in FBCA partner agencies needed to be able to find the certificate that their agency issued to the FBCA. The AIA for FBCA certificates has pointers to certificate collections that relying parties needed to examine to find the one that connected their agency to the FBCA.

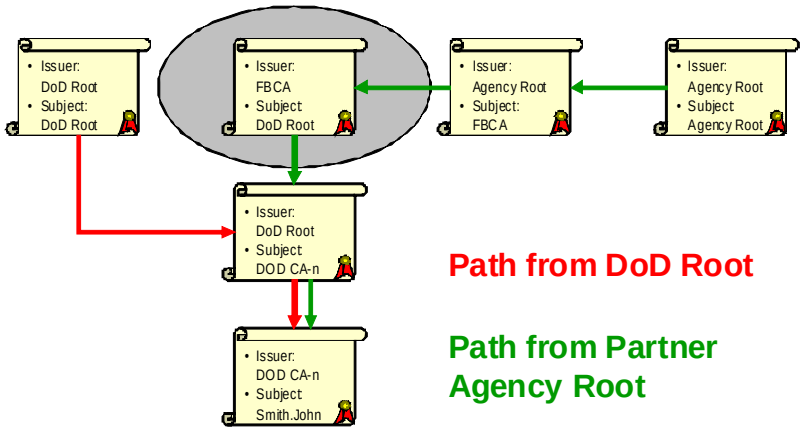

Figure 4: Certificate Chains Using the FBCA-to-DoD Root CA Certificate

Table 20: FBCA-to-DoD Root CA Certificate Fields

Certificate Field	Content
Issuer	FBCA DN. Example: OU=Entrust,OU=FBCA,O=U.S. Government,C=US
Validity	Variable validity period length. There is no guarantee that the validity period will encompass the validity period of certificates that descend from the CA that is the subject of this certificate.
Subject	DoD Root CA DN. Example: CN=DoD CLASS 3 Root CA,OU=PKI, OU=DoD,O=U.S. Government,C=US
Subject Public Key Info	RSA with 1024- or 2048-bit modulus as appropriate for the subject root CA.

Table 21: FBCA-to-DoD Root CA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		keyCertSign and cRLSign

Certificate Extension	Critical	Future	Content
Name Constraints	Y		Permitted subtrees: Directory name: OU=PKI,OU=DoD, O=U.S. Government,C=US Minimum: 0
Basic Constraints	Y		CA: yes
Policy Mappings	N		Policy Mappings: id-fpki-certpcy-mediumAssurance = id-US-dod-medium id-fpki-certpcy-mediumAssurance = id-US-dod-mediumhardware
Entrust Version[10]	N		Version identification of the Entrust System used for FBCA.
Subject Key Identifier	N		Default.
Certificate Policies	N		Policy Identifiers: id-fpki-certpcy-mediumAssurance
CRL Distribution Points	N		Multiple distribution points, to include directory name, a URI for an LDAP reference, and an HTTP URL. References are to FBCA servers. Example: directoryName: CN=CRL1,OU=Entrust,OU=FBCA, O=U.S. Government,C=US
Authority Information Access	N		Two CA Issuers' access locations. One contains an LDAP URL for the *cACertificate;binary* and *crossCertificatePair;binary* attributes in the FBCA's directory entry. The other has an HTTP URL that retrieves CA certificates that have been issued to the FBCA as an *application/pkcs7-mime* type. The references are to FBCA servers.

[10] The Entrust OID id-entrust-version-number identifies this extension.

Certificate Extension	Critical	Future	Content
Authority Key Identifier	N		Default.

2.3.3.2 DoD Root CA-to-FBCA Certificate

As stated earlier, the DoD PKI did not issue a cross-certificate to the FBCA.

2.3.3.3 FBCA-to-IRCA Certificate

This subsection describes the cross-certificate that the FBCA issued to the DoD Interoperability Root CA. The certificate allows applications to construct certificate chains between an FBCA partner agency's root CA and EEs issued by the DoD PKI. Figure 5 illustrates the role of the certificate in certificate chains. Because the FBCA issued this certificate, the content of the certificate was not under the direct control of the DoD PKI and was subject to change. Table 22 shows certificate fields that distinguish the FBCA-to-IRCA certificate. Table 23 identifies the certificate extensions and the values they contain. The policy-mapping extension asserts that the DoD medium certificate policies are equivalent to the FBCA-medium policy. [FBCA]

Since multiple organizations' PKIs may issue certificates to the FBCA, the CA Issuers' portion of the AIA differs from and is more complex than the default. The relying party must construct a path from the EE's certificate to the relying party's agency's root CA. The path will be different for each agency. Relying parties in FBCA partner agencies need to be able to find the certificate that their agency issued to the FBCA. The AIA for FBCA certificates has pointers to certificate collections that relying parties will need to examine to find the one that connects their agency to the FBCA.

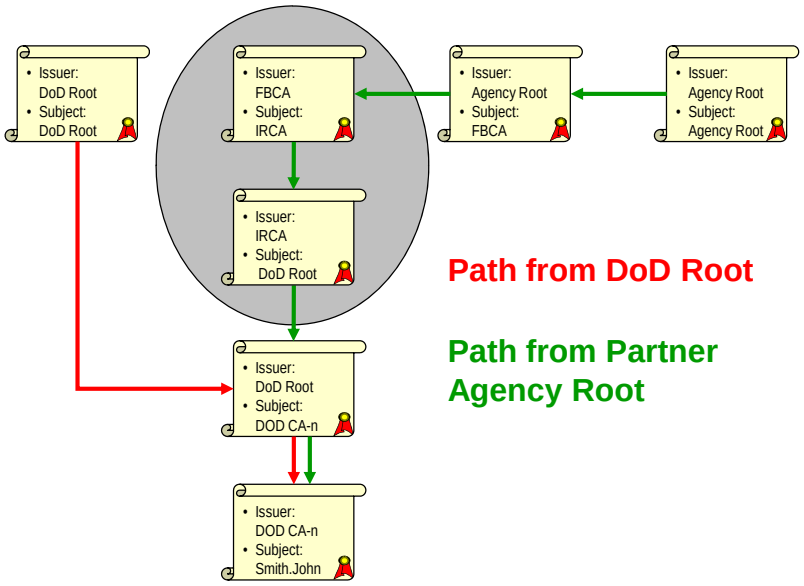

Figure 5: Certificate Chains Using the FBCA-to-IRCA Certificate

Table 22: FBCA-to-IRCA Certificate Fields

Certificate Field	Content
Issuer	FBCA DN. Example: OU=Entrust,OU=FBCA,O=U.S. Government,C=US
Validity	Variable validity period length. There is no guarantee that the validity period will encompass the validity period of certificates that descend from the CA that is the subject of this certificate.
Subject	DoD Root CA DN. Example: CN=DoD Interoperability Root CA 1, OU=PKI, OU=DoD, O=U.S. Government,C=US
Subject Public Key Info	RSA with 2048-bit modulus.

Table 23: FBCA-to-IRCA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		keyCertSign and cRLSign

Certificate Extension	Critical	Future	Content
Name Constraints	Y		Permitted subtrees: Directory name: OU=DoD, O=U.S. Government,C=US Minimum: 0
Basic Constraints	Y		CA: yes
Policy Mappings	N		Policy Mappings: id-fpki-certpcy-mediumAssurance = id-US-dod-medium id-fpki-certpcy-mediumHardware = id-US-dod-mediumhardware
Entrust Version[11]	N		Version identification of the Entrust System used for FBCA.
Subject Key Identifier	N		Default.
Certificate Policies	N		Policy Identifiers: id-fpki-certpcy-mediumAssurance id-fpki-certpcy-mediumHW id-fpki-common-authentication[12]
CRL Distribution Points	N		Multiple distribution points, to include directory name, a URI for an LDAP reference, and an HTTP URL. The hosts for these URL references are FBCA resources. Example: directoryName: CN=CRL2,OU=Entrust,OU=FBCA, O=U.S. Government,C=US

[11] The Entrust OID id-entrust-version-number identifies this extension.

[12] Early versions of this certificate omitted the *id-fpki-common-authentication* policy.

Certificate Extension	Critical	Future	Content
Authority Information Access	N		Two CA Issuers' access locations. One contains an LDAP URL for the *cACertificate;binary* and *crossCertificatePair;binary* attributes in the FBCA's directory entry. The other has an HTTP URL that retrieves CA certificates that have been issued to the FBCA as an *application/pkcs7-mime* type. These URLs reference FBCA resources.
Subject Information Access	N		Subject information access caRepository fields that have either LDAP or HTTP references to certificates issued by the subject CA. The targets of these URLs are servers operated by the DoD.
Authority Key Identifier	N		Default.

2.3.3.4 IRCA-to-FBCA Certificate

This section describes the member of the cross-certificate pair that the IRCA issued to the FBCA. The certificate allows applications to construct certificate chains between the DoD Interoperability Root CA and EEs with certificates issued by FBCA partners. Figure 6 illustrates certificate chains involving the cross-certificate. Table 24 shows certificate fields that distinguish the IRCA-to -FBCA cross-certificate. Table 25 identifies the certificate extensions and the values they contain. The policy mappings extension mapped certificate policies from the FBCA environment to the equivalent DoD certificate policies. The mappings consider the FBCA high assurance certificate policy to be equivalent to the DoD medium assurance certificate policies. The Name Constraints extension excludes any certificates issued by CAs external to the DoD with DNs that appear to be internal to the DoD.

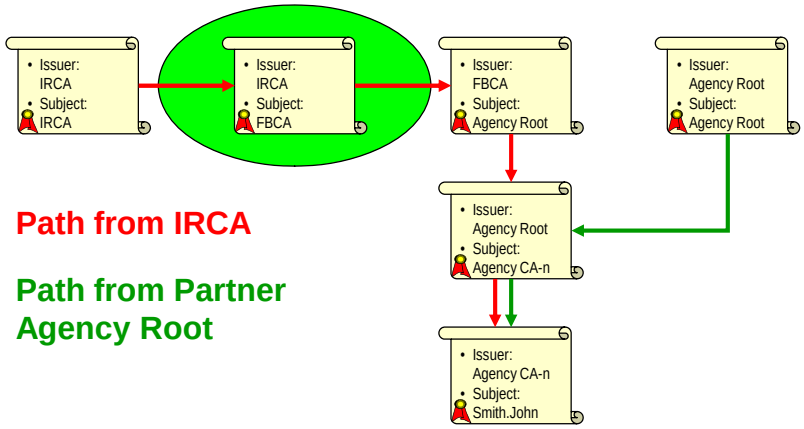

Figure 6: Certificate Chains Using the IRCA-to-FBCA Certificate

Table 24: IRCA-to-FBCA Certificate Fields

Certificate Field	Content
Issuer	CN=DoD Interoperability Root CA 1, OU=PKI, OU=DoD, O=U.S. Government,C=US
Validity	Variable validity period length. There is no guarantee that the validity period will encompass the validity period of certificates that descend from the CA that is the subject of this certificate.
Subject	OU=Entrust,OU=FBCA,O=U.S. Government,C=US
Subject Public Key Info	RSA with 2048-bit modulus.

Table 25: IRCA-to-FBCA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		keyCertSign and cRLSign
Name Constraints	Y		Excluded subtrees: Directory name: OU=PKI,OU=DoD, O=U.S. Government,C=US
Basic Constraints	Y		CA: yes
Policy Constraints	Y		Require explicit policy: 0

Certificate Extension	Critical	Future	Content
Policy Mappings	N		Policy Mappings: id-US-dod-medium= id-fpki-certpcy-highAssurance id-US-dod-mediumhardware= id-fpki-certpcy-highAssurance
Subject Key Identifier	N		Default.
Certificate Policies	N		Policy Identifiers: id-US-dod-medium id-US-dod-mediumhardware
CRL Distribution Points	N		Same HTTP and LDAP URLs as contained in other intermediate CAs. The URLs retrieve the Interoperability Root CA's CRL. Pointers to additional FBCA repositories may be included.
Authority Key Identifier	N		Default.
Subject Information Access	N		An HTTP and LDAP caRepository URI references to FPKI servers.
Authority Information Access	N		An HTTP and LDAP caIssuers entry containing URIs to retrieve certificates issued to the IRCA and an HTTP OCSP reference. References are to DoD servers.

2.3.4 Interoperability Root CA Cross-Certificates

Intermediate certificates from the Interoperability Root CA to the DOD Root CAs were necessary to construct certificate paths from DoD EEs through the FBCA to other FBCA participating root CAs. Table 26 shows selected fields in the certificates. Table 27 shows the certificates' extensions and their content.

Table 26: IRCA-to-Root CA Certificate Fields

Certificate Field	Content
Issuer	CN=DoD Interoperability Root CA 1, OU=PKI, OU=DoD, O=U.S. Government,C=US

Certificate Field	Content
Validity	Variable validity period length. There is no guarantee that the validity period will encompass the validity period of certificates that descend from the CA that is the subject of this certificate.
Subject	DoD Root CA DN. Example: CN=DoD Root CA 2,OU=PKI,OU=DoD, O=U.S. Government,C=US
Subject Public Key Info	RSA with 2048-bit modulus.

Table 27: IRCA-to-Root CA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		keyCertSign and cRLSign
Basic Constraints	Y		CA: yes
Subject Key Identifier	N		Default.
Certificate Policies	N		Policy Identifiers: id-US-dod-medium id-US-dod-mediumhardware id-fpki-common-authentication[13]
CRL Distribution Points	N		HTTP and LDAP URLs to the IRCA's CRL.
Authority Information Access	N		Default.
Subject Information Access	N		HTTP and LDAP references. The Root CA's *issued by* collection will include all of the signing CAs that have received certificates from the Root CA.
Policy Constraints	Y		Require explicit policy: 0
Authority Key Identifier	N		Default.

[13] Early versions of this certificate omitted the *id-fpki-common-authentication* policy.

2-34

2.3.5 Intermediate CAs and Their Certificates

The DoD began a new series of DoD Intermediate CAs. DoD Intermediate CAs issue certificates to descendent CAs that serve special purposes and selected EEs. Although the descendent CAs are part of the DoD PKI CA hierarchy, organizations external to the DoD PKI operate these CAs for special purposes. Descriptions of the descendent CAs' operations and their certificate and CRL profiles are outside the scope of this document.

This subsection describes the certificates issued to DoD Intermediate CAs. Table 28 shows certificate fields that distinguish the DoD Intermediate CAs' certificates. Table 29 identifies the certificate extensions and the values they contain. The BC extension specifies a path length of 1, which allows the DoD Intermediate CA to issue certificates to immediate subordinate CAs but does not allow those subordinate CAs to issue certificates to additonal CAs.

Table 28: DoD Intermediate CA Certificate Fields

Certificate Field	Content
Issuer	CN=DoD Root CA 2,OU=PKI,OU=DoD, O=U.S. Government,C=US
Validity	Variable validity period length. There is no guarantee that the validity period will encompass the validity period of certificates that descend from the CA that is the subject of this certificate.
Subject	DoD Intermediate CA DN. Example: CN=DoD Intermediate CA-<n>,OU=PKI, OU=DoD,O=U.S. Government,C=US
Subject Public Key Info	RSA with 2048-bit modulus.

Table 29: DoD Intermediate CA Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		keyCertSign and cRLSign
Basic Constraints	Y		CA: yes, Path Length Constraint: 1
Subject Key Identifier	N		Default.

Certificate Extension	Critical	Future	Content
Certificate Policies	N		Policy Identifiers: id-US-dod-medium id-US-dod-mediumhardware id-US-dod-medium-2048 id-US-dod-mediumhardware -2048
CRL Distribution Points	N		HTTP URL to the issuing root's CRL.
Authority Information Access	N		Default.
Policy Constraints	N		
Authority Key Identifier	N		Default.

2.4 End-Entity Certificates

The previous subsections described certificates belonging to CAs that issued certificates to other subscriber entities. This section describes the certificates issued to subscribers that are EEs. EEs do not issue certificates to others. EEs control the private keys associated with the public key in their certificates. The certificates allow subscribers and relying parties to communicate securely.

The DoD PKI issues several types of EE certificates based on the entity type (e.g., an individual or a server) or the intended application (e.g., e-mail). The entities to which the DoD PKI issues certificates include individuals, servers, devices, code-signing organizations, domain controllers, and OCSP responders. The following subsections provide details on the various types of EE certificates that the DoD PKI issues.

2.4.1 User Certificates

The DoD PKI issued four types of certificates to individuals: the basic identity, e-mail signature, e-mail encryption, and PIV authentication certificates. The DoD has designated CAs with the primary purpose of signing either identity or e-mail certificates. CAs restricted to signing e-mail certificates have the word *Email* in their CNs. The e-mail signing CAs issue only affects e-mail certificates. The remaining (non-e-mail) signing CAs issue identity and PIV authentication certificates. The user certificates are different for each PKI release, but the certificates follow the defaults for the releases. Table 30 lists certificate fields common to user certificates. The issuer name identifies the issuing signing CA for the relevant release. The validity period varies based on the user's circumstances but will not generally exceed 3 years. This period may change and its length should not be assumed. The validity period will always be within the issuing signing CA's validity period. The subject field contains a DN for the individual. The DN is an identifier that is intended to be unique to each individual. The CN component provides for the individual's uniqueness and contains the individual's name and a

ten-character numeric string. The numeric string is either the individual's Electronic Data Interchange-Person Identifier (EDIPI) or the individual's Universal Identifier (UID). The DN also includes an Organizational Unit (OU) component for the individual's major DoD unit. This organizational unit is at the Combatant Command, Service, or Agency (C/S/A) level of the DoD organization. Section 4.3.3 contains more information on the format of DNs for individuals. Table 31 identifies common user certificate extensions and the values they contain. The IAN and CDP follow the defaults for the relevant release. The SDA extension includes the citizenship attribute which provides the individual's country of citizenship. The attribute will generally be single-valued but technically may be multi-valued. The content of the KU extension varied based on the type of certificate. The e-mail certificates had additional extensions: SAN and EKU. The following subsections describe the differences among the types of user certificates.

Table 30: User Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing signing CA: CN=DoD [Class 3][Email]CA-<n>,OU=PKI, OU=DoD,O=U.S. Government,C=US
Validity	Validity period will not generally exceed 3 years, but the period length may change and should not be assumed always to be 3 years.
Subject	X.500 DN: CN=<name>,OU=<C/S/A>,OU=PKI, OU=DoD,O=U.S. Government,C=US
Subject Public Key Info	RSA with 1024-bit modulus prior to P3.2. RSA with 2048-bit modulus after P3.1.

Table 31: User Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		Varies based on type of user certificate.

Certificate Extension	Critical	Future	Content
Certificate Policies	N		Policy Identifiers: id-US-dod-medium or id-US-dod-mediumhardware Certificates with 2048-bit keys also included the appropriate 2048-bit policy: id-US-dod-medium-2048 or id-US-dod-mediumhardware-2048
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default for release.
Issuer Alternative Name	N		Present with default content prior to P3.1.
Subject Directory Attributes	N		Starting with P3.2, contains the countryOfCitizenship attribute. The attribute value is the two-letter abbreviation of the individual's country of citizenship. The two-letter values are from ISO 3166-1-alpha-2 codes [ISO3166].
Authority Information Access	N		Present with default content after P3.
Authority Key Identifier	N		Default.

2.4.1.1 Basic Identity Certificate

The basic identity certificate has the extensions identified for the common user certificate. The KU content is listed in Table 32.

Table 32: Basic Identity Certificate-Unique Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature and nonRepudiation

2-38

2.4.1.2 E-mail Signature Certificate

The e-mail signature certificate has the same KU values as the basic identity certificate and includes the individual's e-mail address in the SAN extension. The profile for e-mail signature certificates on the Common Access Card (CAC) card was modified to allow the certificates' use in conjunction with Microsoft Windows Smart Card logon. Certificates associated with CAC contain the EKU extension and have a second name in the SAN extension. The second name is the User Principal Name (UPN). The UPN associates the certificate's subject with a Windows user account. Table 33 shows the extensions that are unique to e-mail signature certificates.

Table 33: E-mail Signature Certificate-Unique Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature and nonRepudiation
Extended Key Usage	N		Present only in certificates asserting the certificate policy, id-US-dod-mediumhardware. OIDs for: id-kp-smartcard_logon id-kp-emailProtection id-kp-clientAuth
Subject Alternative Name	N		rfc822Name: <subject's e-mail address> Certificates asserting the certificate policy, id-US-dod-mediumhardware, have a second name: otherName: [14] id-nt_principal_name=<edipi>@mil

2.4.1.3 E-mail Encryption Certificate

The e-mail encryption certificate has a KU usage value that differs from the previous identity and e-mail signing certificates and has a SAN that contains only the owner's e-mail address. Table 34 lists the certificate extensions that are unique to e-mail encryption certificates.

[14] UPN is the familiar name for the Microsoft OID id—nt_principal_name.

Table 34: E-mail Encryption Certificate-Unique Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		keyEncipherment
Subject Alternative Name	N		rfc822Name: <subject's e-mail address>

2.4.1.4 PIV Authentication Certificate

The PKI began issuing PIV authentication certificates starting with Profile 3.2 to comply with the HSPD-12 PIV requirements. This certificate is similar to the basic identity certificate with differences in the contents of the KU, EKU, and SAN extensions. Table 35 lists the certificate extensions that are unique to PIV authentication certificates. The KU extension only asserts the digital signature usage. The certificate includes an EKU and SAN extension. The EKU extension asserts the smartcard logon and client authentication uses. The SAN includes the Federal Agency Smart Credential Number (FASC-N) and the Principal Name. Federal Information Processing Standard (FIPS) 201 and its family of standards prescribe the format of the FASC-N [FIPS201]. The FASC-N is encoded in 25 8-bit bytes. The 25 bytes actually pack 40 5-bit characters. Each character is a 4-bit value with a 5th parity bit. The first 39 characters are Binary Coded Decimals (BCDs) with certain values above 9 representing special characters such as field separators. The 40th character has the bitwise parity for the previous 39 characters. The value of the Principal Name is derived from the FASC-N and is a 16-character numeric string. The numeric string consists of the EDIPI (10 characters) followed by the organization (1 character), organizational identifier (4 characters), and person category (1 character) codes. An additional difference is the inclusion of the *id-fpki-common-authentication* policy in certificates issued after the FPKI approved DoD participation in the PIV program.

Table 35: PIV Authentication Certificate-Unique Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature
Certificate Policies	N		Certificates issued after the FPKI approved DoD participation in the PIV program asserted the following policy in addition to the policies identified earlier: id-fpki-common-authentication

End-Entity Certificates

Certificate Extension	Critical	Future	Content
Extended Key Usage	N		OIDs for: id-kp-smartcard_logon id-kp-clientAuth
Subject Alternative Name	N		otherName: id-nt_principal_name=<edipi+>@mil otherName: pivFASC-N=<encodedFASC-N>

2.4.2 Server and Device Certificates

The DoD PKI also issues certificates to entities other than people. NPEs, such as servers and routers, use public key cryptography and certificates to authenticate the parties involved in communications and to secure the information communicated. Transport Layer Security (TLS), Secure Sockets Layer (SSL), and Internet Protocol Security (IPSec) are examples of such communications protocols.

2.4.2.1 Basic Server and Device Certificates

The basic profile for server and device certificates is similar to the profile for identity certificates. The differences are the subject name certificate field and the values in the KU extension. These certificates have both P3 and P3.1 versions. The subject's CN value is usually either the server or device's Domain Name Service (DNS) name or Internet Protocol (IP) address. Table 36 lists the basic server certificate fields. Table 37 lists the basic server certificate extensions.

Table 36: Basic Server Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing signing CA: CN=DoD [Class 3]CA-<n>,OU=PKI, OU=DoD,O=U.S. Government,C=US
Validity	Validity period will not exceed 3 years, but the period length may change and should not be assumed always to be 3 years.

Certificate Field	Content
Subject	X.500 DN: CN=<host name|IP address>, OU=<C/S/A>,OU=PKI, OU=DoD, O=U.S. Government,C=US
Subject Public Key Info	RSA with 1024-bit modulus. Modulus may change to 2048 bits in the future.

Table 37: Basic Server Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature and keyEncipherment
Certificate Policies	N		id-US-dod-medium id-US-dod-medium-2048 will also be included when the key length is 2048
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default for release.
Issuer Alternate Name	N		Present with default content prior to P3.1.
Authority Information Access	N		Present with default content for CAs after P3.
Authority Key Identifier	N		Default.

2.4.2.2 Extended Server or Device Certificates

The DoD PKI extended the server and device certificate profiles to allow inclusion of either or both of the SAN and EKU extensions. The SAN extension allows multiple alternative names for the server or device. The server can have multiple network names or IP addresses. Initially, the certificates were *dual SAN* certificates limited to two alternative names. The limitation to two names was relaxed to provide the multi-SAN certificate with more than two alternative names. The multi-SAN profile is the basic server profile with the addition of the SAN extension.

The DoD PKI permits use of the EKU extension in server certificates. The EKU extension is optional. When present, the EKU extension asserts the client and server authentication,

2-42

iKEIntermediate,[15] and any extended key usage OIDs in the EKU. The iKEIntermediate EKU indicates that the certificate subject may use the certificate with the IPSec protocol. The any extended key usage means that the key may be used for purposes beyond those explicitly included in other EKUs. However, applications may require the presence of a specific EKU even when the any extended key usage is present. Table 38 shows the content of the multi-SAN certificate's added SAN extension.

Table 38: Additional Multi-SAN Certificate Extension

Certificate Extension	Critical	Future	Content
Extended Key Usage	N		When present, has the OIDs for: id-kp-serverAuth id-kp-clientAuth iKEIntermediate anyExtendedKeyUsage
Subject Alternative Name	N		Multiple values for SANs of any of the allowed SAN name types (e.g., dNSName, iPAddress, or directoryName).

2.4.3 Code- or Object-Signing Certificates

The DoD PKI allows the use of code- or object-signing certificates that interoperate with the mechanisms that commercial industry employs for securing the distribution of software programs. Programs distributed over the network are known as *mobile code*. The industry practices required a separate profile for the code-signing certificates. Code signing and the related certificates provide assurance to relying parties regarding the source of the code and that the code has not been modified. Table 39 shows the fields in a code-signing certificate. The subject name has a *CS* prefix, an organization name,[16] and unique suffix. The suffix distinguishes individual certificates when an organization has multiple code-signing certificates. Section 4.3.8 describes the format of a code-signing certificate's CN component. Table 40 lists the code-signing certificate extensions.

The private key corresponding to the certificate's public key resides on a hardware token. The certificate asserts the Class 3 hardware certificate policy. The certificate has the EKU extension designating the certificate for code-signing use. A specific individual is responsible for use of the code-signing key and certificate. The SAN has the LDAP URI for the

15 The iKEIntermediate was a proposed EKU for use with IPSec. Early draft standards initially included but later dropped the EKU. RFC 4809, Requirements for an IPsec Certificate Management Profile, explicitly states no EKUs are required for IPSEC. [RFC4809]

16 Note that the organization in most cases will be at a lower level than the OUs contained in the certificate's subject name field.

individual's directory entry. This URI includes the individual's DN (the DN in the individual's identity certificate).

Table 39: Code-Signing Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing signing CA: CN=DoD [Class 3]CA-<n>,OU=PKI, OU=DoD,O=U.S. Government,C=US
Validity	Validity period will not exceed 3 years, but the period length may change and should not be assumed always to be 3 years.
Subject	X.500 DN: CN=CS.<organization name>.<unique suffix>, OU=<C/S/A>,OU=PKI, OU=DoD, O=U.S. Government,C=US
Subject Public Key Info	RSA with 2048-bit modulus starting with P3.2. RSA with 1024-bit modulus prior to P3.2.

Table 40: Code-Signing Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature
Certificate Policies	N		Policy Identifier: id-US-dod-mediumhardware id-US-dod-mediumhardware-2048 will also be included when the key length is 2048
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default for release.
Authority Information Access	N		Default for release.
Extended Key Usage	N		id-kp-codeSigning
Issuer Alternate Name	N		Default for release.

Certificate Extension	Critical	Future	Content
Subject alternative Name	N		URI containing the LDAP URL for the directory entry of the individual who is responsible for the certificate's use.
Authority Key Identifier	N		Default.

2.4.4 Domain Controller Certificates

The DoD PKI issues certificates for Microsoft Domain Controllers (DCs). DCs are systems crucial to the security of the Microsoft Windows environment for versions of Windows starting with Windows 2000. The DC certificate is similar to a server certificate. Table 41 shows a DC certificate's unique fields. The subject DN has only a CN component whose value is the DC's host name. Table 42 shows the DC certificate's extensions. The certificate includes a Microsoft extension, Certificate Template Name, which has a value to indicate the certificate is for a DC. The EKU has values to allow the certificate to be used for both TLS server and client authentication. The SAN extension must contain the Globally Unique Identifier (GUID) of the DC object in the Microsoft Active Directory and the DC's DNS name.

Table 41: Domain Controller Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing signing CA: CN=DoD [Class 3]CA-<n>,OU=PKI, OU=DoD,O=U.S. Government,C=US
Validity	Validity period will not exceed 3 years, but the period length may change and should not be assumed always to be 3 years.
Subject	X.500 DN: CN=<host name|IP address>
Subject Public Key Info	RSA with 1024-bit modulus initially but later changed to 2048 bits.

Table 42: Domain Controller Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature and keyEncipherment
Certificate Policies	N		Policy Identifier: id-US-dod-medium id-US-dod-medium-2048 will also be included when the key length is 2048
Microsoft Certificate Template[17]	N		BMPString: DomainController
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default.
Authority Information Access	N		Default for release.
Extended Key Usage	N		OIDs for: id-kp-serverAuth id-kp-clientAuth
Subject alternative Name	N		otherNames: id-ntds_replication=<GUID Octets> dNSName=<host name>
Authority Key Identifier	N		Default.

2.4.5 Alternate Token Certificates

The Alternate Token certificates were previously known as Administrator certificates. The Administrator Token certificates allowed system administrators working with Microsoft Windows environments to separate their administrator and individual identities. These certificates allowed organizations to require the use of smart cards for logon. This certificate was also as a substitute for a CAC when an individual was not eligible to receive a CAC. The private key associated with the certificate resides on a hardware token.

The profile for this certificate is similar to the profile for the individual e-mail signature certificate. The differences involve the KU, CP, EKU, and SAN extensions. The administrator certificate's KU field only asserts digitalSignature (without nonRepudiation). The certificate asserts the certificate policy associated with software rather than hardware because

[17] The Microsoft OID id-enroll-certtype-extension identifies this extension.

2-46 placing the certificate on a smart card is an administrative responsibility of the issuing Registration Authority (RA).

Because the administrator function does not require an associated e-mail address, e-mail use is not included in the EKU, and the SAN does not include an e-mail address. The EKU asserts smart card logon. The SAN includes an *other name* component with the administrator's Microsoft Windows identifier. This identifier allows the individual to logon as an administrator using a smart card. The remaining certificate extensions follow the defaults for P3.1; these certificates were not issued prior to P3.1. Table 43 lists administrator and alternate token certificate fields. Table 44 lists administrator certificate extensions.

Table 43: Alternate Token Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing signing CA: CN=DoD CA-<n>,OU=PKI,OU=DoD, O=U.S. Government,C=US
Validity	Validity period will not exceed 3 years, but the period length may change and should not be assumed always to be 3 years.
Subject	X.500 DN: CN=<name>,OU=<C/S/A>,OU=PKI,OU=DoD, O=U.S. Government,C=US
Subject Public Key Info	RSA with 1024-bit modulus. Modulus may change to 2048 bits in the future.

Table 44: Alternate Token Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature
Certificate Policies	N		Policy Identifier: id-US-dod-medium id-US-dod-medium-2048 will also be included when the key length is 2048
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default.

Certificate Extension	Critical	Future	Content
Authority Information Access	N		Default.
Extended Key Usage	N		OIDS for: TLS Web Client Authentication Microsoft KP-Smartcard-Logon
Subject Alternative Name	N		otherName: id-nt_principal_name=<account>
Authority Key Identifier	N		Default.

2.4.6 Group and Role Certificates

Group and role certificates are issued to groups or roles rather than to specifically named individuals. Group and role certificates are useful when the signature represents that a group or function rather than a specific individual is responsible for the signature and the activity leading to the signature. Group and role certificates generally are similar to individual certificates. Three separate certificates are possible: identity, e-mail signature, and e-mail encryption. The difference between group and individual certificates is the subject name. The CN component of the group and role certificates names a group or role rather than a particular individual. The CN includes a unique identifier to ensure uniqueness of names. The organization holding the private key is responsible for maintaining any necessary accountability to specific individuals involved in creating the signature. Table 45 and Table 46 show the certificate fields and extensions, respectively, for group certificates. All of the group and role certificates have the certificate fields shown in Table 45. The certificates' extensions vary some. Table 46 shows the extensions found in all of the certificates. The e-mail certificates have additional extensions similar to those found in the corresponding individual certificate.

Table 45: Group and Role Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing signing CA: CN=DoD CA-<n>,OU=PKI,OU=DoD, O=U.S. Government,C=US
Validity	Validity period will not exceed 3 years, but the period length may change and should not be assumed always to be 3 years.

End-Entity Certificates

2-48

Certificate Field	Content
Subject	X.500 DN: CN=<Name of Organization>.<Name of Component>.<Name of Group or Role>.<unique identifier>, OU=<C/S/A>, OU=PKI,OU=DoD, O=U.S. Government,C=US
Subject Public Key Info	RSA with 1024-bit modulus. Modulus may change to 2048 bits in the future.

Table 46: Group and Role Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		Varies based on the type of group or role certificate.
Certificate Policies	N		Policy Identifier: id-US-dod-medium id-US-dod-medium-2048 will also be included when the key length is 2048
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default.
Authority Information Access	N		Default.
Authority Key Identifier	N		Default.

2.4.6.1 Identity Certificate

The identity certificate has the extensions identified for the common user certificate. The KU content is listed in Table 47.

Table 47: Group and Role Identity Certificate-Unique Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature and nonRepudiation

2.4.6.2 E-mail Signature Certificate

The e-mail signature certificates have the same KU values as the identity certificate and include the group or role's e-mail address in the SAN extension. Table 48 shows the extensions that are unique to e-mail signature certificates.

Table 48: Group and Role E-mail Signature Certificate-Unique Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature and nonRepudiation
Subject Alternative Name	N		rfc822Name: <subject's e-mail address>

2.4.6.3 E-mail Encryption Certificate

The e-mail encryption certificates have a KU usage value that differs from the previous identity and e-mail signing certificates, and have a SAN that contains only the owner's e-mail address. Table 49 lists the certificate extensions that are unique to e-mail encryption certificates.

Table 49: Group and Role E-mail Encryption Certificate-Unique Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		keyEncipherment
Subject Alternative Name	N		rfc822Name: <subject's e-mail address>

2.4.7 Content Signer Certificates

Content signer certificates support DoD participation in the PIV program. PIV cards may contain signed data structures that hold the Cardholder Unique Identifier (CHUID) and biometric information (e.g., fingerprints, retinal scans). According to [FIPS201], content signers sign these data structures. Their certificates are essentially the same as individual signature certificates except for the CN value and the inclusion of the EKU extension with a value indicating that the certificate can be used to verify signatures on PIV CHUIDs and biometric information. Because the entities that digitally sign the PIV data structures are systems rather than people, the CN value name differs from the CN for individuals. The DoD

[18] UPN is the familiar name for the Microsoft OID id—nt_principal_name.

End-Entity Certificates

2-50 Intermediate CAs issue content certificates.[19] The EKU extension asserts the id-PIV-content-signing OID to indicate the certificate can be used to verify the CHUID and biometrics. Because of limitation on the available memory in CACs, the CDP extension contains only the HTTP reference; the LDAP reference is omitted. Table 50 and Table 51 show the Content Signer Certificate Fields and Extensions, respectively.

Table 50: Content Signer Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing DoD Intermediate CA: CN=DoD Intermediate CA-<n>,OU=PKI,OU=DoD, O=U.S. Government,C=US
Validity	Validity period was 5 years, but the period length may change and should not be assumed always to be 5 years.
Subject	X.500 DN: CN=<name>,OU=OSD,OU=PKI,OU=DoD, O=U.S. Government,C=US
Subject Public Key Info	RSA with 2048-bit modulus.

Table 51: Content Signer Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature, nonRepudiation
Certificate Policies	N		Policy Identifier: id-US-dod-mediumHardware-2048
Subject Key Identifier	N		Default.
CRL Distribution Points	N		Default except that the LDAP reference is omitted.
Authority Information Access	N		Default.
Extended Key Usage	N		OID for: id-PIV-content-signing
Authority Key Identifier	N		Default.

[19] DoD Intermediate CAs issue the content signer certificates because their certificates have longer validity periods. The issuing CA may change in the future.

2.4.8 Online Certificate Status Protocol Responder Certificates

The DoD PKI operates the RCVS, which uses OCSP. Section 5 describes the operation of the RCVS and the profiles for OCSP requests and responses. OCSP responses are digitally signed. Verification of OCSP responses involves use of a public key contained in the responder's certificate. The profile for the responder's certificate depended on the trust model for the responses. RCVS has used two trust models: Trusted Responder and Distributed Trust Model (DTM). The responder certificate profile is different for each of the trust models; the following subsections describe the profiles for the two models.

2.4.8.1 Trusted Responder Model

The Trusted Responder Model employs a self-signed certificate. The self-signed certificate provides a mechanism for providing the OCSP responder's public key. However, because the certificate is self-signed, it must be delivered out-of-band to relying parties using an independent, secure, and reliable method. The Trusted Responder can respond for certificates issued by any CA for which the responder knows the status. Only one Trusted Responder certificate is necessary. The public key in the one certificate can be used to verify any of the RCVS responses. Table 52 shows the OCSP certificate fields. Since the certificate is self-signed, the contents of the issuer and subject fields are the same. Table 53 shows the certificate's extensions. The certificate has the EKU extension with values to indicate that the certificate is used to authenticate the responder's server and to verify signatures on OCSP responses. The BC extension has the value *false* for CA to indicate that the responder cannot sign certificates. The responder can only sign OCSP responses.

Table 52: Trusted Responder OCSP Certificate Fields

Certificate Field	Content
Issuer/Subject	X.500 DN:[20] CN=dod ocsp ss ,OU=PKI, OU=DoD, O=U.S. Government,C=US
Validity	Validity period will not exceed 3 years, but the period length may change and should not be assumed always to be 3 years.
Subject Public Key Info	RSA with 2048-bit modulus.

[20] Note that the CN component ends with a space character and that the DN has only one OU component. The value of the OU component is the string "PKI, OU=DoD".

Table 53: Trusted Responder OCSP Certificate Extensions

Certificate Extension	Critical	Future	Content
Extended Key Usage	Y		OIDs for: TLS Web Server Authentication OCSPSigning
Subject Key Identifier	N		Default. Not present in all certificates.
Basic Constraints	N		CA: no

2.4.8.2 Distributed Trust Model

The Distributed Trust Model differs from the Trusted Responder Model. With the Distributed Trust Model, a CA issues a certificate to an authorized RCVS responder to sign status information regarding certificates issued by the CA.[21] Each CA issued a certificate to the RCVS responder. The responder signs the response and includes its certificate from the CA that issued the target certificate. Table 54 shows the OCSP certificate fields, and Table 55 shows the certificate's extensions. Section 4.3.6 describes the format for the responder names used in the certificate's subject field. The certificate has the EKU extension to indicate that the certificate is used to both create and verify signatures on OCSP responses. The certificate has the OCSP No Check extension to inform relying parties that they need not check the validity of the responder's certificate. The CP extension will assert the policy appropriate to the key length of the issuing CA.

Table 54: DTM OCSP Certificate Fields

Certificate Field	Content
Issuer	X.500 DN of the issuing CA: CN=DoD [Intermediate|Email] CA-<n>,OU=PKI,OU=DoD, O=U.S. Government,C=US
Validity	The validity period will be short relative to the validity period of other certificates (e.g., 45 days). No assumptions should be made about validity period.

[21] The OCSP Standard, RFC 2560, uses the term *authorized responder* to refer to the Distributed Trust Modeldistributed trust model.

Certificate Field	Content
Subject	X.500 DN: A format similar to: CN=OCSP 1D 1,OU=PKI, OU=PKI, OU=DoD, O=U.S. Government, C=US
Subject Public Key Info	RSA with 2048-bit modulus.

Table 55: DTM OCSP Certificate Extensions

Certificate Extension	Critical	Future	Content
Key Usage	Y		digitalSignature, crlSign
Certificate Policies	N		Policy Identifier: id-US-dod-mediumHardware or id-US-dod-mediumHardware-2048
Subject Key Identifier	N		Default.
Authority Information Access	N		Default except that the LDAP reference is omitted.
Extended Key Usage	N		OIDs for: OCSPSigning
OCSP No Check	N		The extension has no content.
Authority Key Identifier	N		Default.

2.5 Future Certificate Profiles

Certificates that the DoD PKI issues will continue to evolve. New certificate profiles may be defined for new applications and existing certificate profiles may be modified. Potential changes to certificates include those listed below:

- New profiles may be created for NPEs. NPEs may encompass various components other than individuals who have network connectivity. These components might include network infrastructure components, such as routers and gateways, and basic communications equipment, such as radios, as well as various platforms and sensors. Platforms and sensors may include vehicles, ships, aircraft, and satellites and the systems they contain. New system architectures, such as those based on Service-Oriented Architectures (SOAs) and Web Services, may generate a need for additional NPEs that differ from those currently issued to servers.

Future Certificate Profiles

2-54

- The certificates issued to individuals may change to eliminate duplication in use. When the PIV authentication certificate was first issued, individuals received four certificates. The number may be reduced to three certificates, one each for authentication, signature, and encryption.
- The DoD PKI may change its use of signing CAs. The PKI may cease to distinguish e-mail signing CAs from other signing CAs.
- Over the next several years, certificate profiles may change to support a new set of cryptographic algorithms. As technology advances, algorithms with greater strength may be needed. RSA key sizes may increase. Advanced hash algorithms such as SHA-256 that produce longer hash values than the current SHA-1 will likely be employed. In the longer term, the PKI will likely transition to the National Security Agency (NSA) Suite B algorithms [NSA-B]. Specifically, keys based on Elliptic Curve Cryptography (ECC) will be used.

3 Certificate Revocation List Profile

The DoD PKI regularly produces CRLs that relying parties may consult before using a particular certificate. The CRL lists certificates that have been revoked and which relying parties should not trust. This section describes the content of a CRL in general and then describes the CRL profile. This section also provides metrics regarding the number and size of the CRLs so that applications will have information regarding the scale of the DoD PKI revocation status checking using CRLs. The section contains a discussion of the measures to improve the effectiveness of CRL distribution. The section concludes with information about the future directions for DoD PKI CRLs.

3.1 CRL General Content

The CRL contains a list of certificates that are not expired but should no longer be trusted. A certificate expires when the current date is later than the *not after* element of its validity period. The CA that issued the revoked certificates digitally signs the CRL. The CA uses the same key to sign certificates and CRLs. The CRL consists of *header* fields and a revoked certificates list. The header fields contain general information about the CRL, such as its issuer and the signature algorithm. The header fields also include two dates: *this update* and *next update*. Both dates include the time. This update is the date and time when the CRL was issued, and the next update is the date by which the CA will issue a new CRL.

The revoked certificates list portion of the CRL identifies the certificates that have been revoked. This list identifies each revoked certificate by its integer serial number along with the date (and time) that the certificate was revoked. The revoked certificates list has no ordering; specifically, the list is neither ordered by serial number nor revocation date. The revoked certificates list does not include expired certificates with the exception that a revoked certificate should appear on one regularly scheduled full CRL after the certificate's expiration.[22]

3.2 CRL Profile

The DoD PKI CRLs were X.509 Version 1 [X.509] CRLs prior to P3.2. After P3.1, the CRLs were Version 2 CRLs. The scope of the CRLs issued is the full and complete list of all revoked certificates; that is, DoD PKI CRLs list all certificates that have been revoked and have not expired. Table 56 lists the CRL fields and their values. All of the DoD PKI CAs issued CRLs. The table's *Use* column indicates whether the field is present always (A) or sometimes (S). The CRLs share a common format. Version 1 CRLs contained neither CRL nor entry extensions. DoD PKI Version 2 CRLs contain two CRL extensions: the AKI and the CRL number. Table 57 summarizes the CRL extensions defined in RFC 5280 and their use in the DoD PKI. This table's *Use* column indicates whether the extension is always (A) or never (N) present. The *Critical* column has Y or N depending on whether the extension is marked *Critical* or *Not critical*, respectively. The *Future* column indicates whether the extension's future use is possible (P) or not likely (N).

---

[22] This exception ensures that a revoked certificate will always appear on at least one CRL. The DoD PKI does not precisely comply with the current RFC 5280 requirement.

3-2

Table 56: CRL Fields

CRL Field	Use	Content
Version	S	Field is implied (not present) for X.509 Version 1 CRLs. The field was present for Version 2 CRLs.
Signature	A	Default prior to P3.3: sha1WithRSAEncryption (1.2.840.113549.1.1.5). Default starting with P3.3: sha256WithRSAEncryption (1.2.840.113549.1.1.11).
Issuer Name	A	DN of the issuer.
This Update	A	Date and time the CRL was issued in UTC format.
Next Update	A	Date and time by which a new CRL will be issued. UTC format.
Revoked Certificates	A	A list of two-element sequences for each revoked certificate. The two-element sequence has an integer identifying the revoked certificate's serial number and a date (and time) specifying the date that the certificate was revoked.
CRL Extensions	S	CRL extensions are only available with Version 2 CRLs.
Signature Algorithm	A	Default prior to P3.3: sha1WithRSAEncryption (1.2.840.113549.1.1.5). Default starting with P3.3: sha256WithRSAEncryption (1.2.840.113549.1.1.11).
Signature	A	The actual signature value.

Table 57: CRL Extensions

Extension	Use	Critical	Future	Content
CRL Extensions				
Authority Key Identifier	A	N		Always used with Version 2 CRLs. Default is the same value as used for the certificate extension of the same name.

Extension	Use	Critical	Future	Content
Issuer Alternative Name	N	N		
CRL Number	A	N		Used with Version 2 CRLs. Will contain increasing sequential numbers.
Delta CRL Indicator	N	Y	P	May be used if delta CRLs are issued.
Issuing Distribution Point	N	Y	P	May be used if the DoD PKI publishes CRLs whose scope is less than the full CRL.
Freshest CRL	N	N	P	May be used if delta CRLs are issued. Would likely contain an appropriate LDAP and/or HTTP reference to obtain the most recent delta CRL.
Authority Information Access	N	N	P	May be used to assist relying parties in finding the CRL issuer's certificate.
CRL Entry Extensions				
Reason Code	N		N	
Hold Instruction Code	N		N	
Invalidity Date	N		N	
Certificate Issuer	N		N	

3.3 CRL Metrics

Because of the large population served by the DoD PKI, the number of revoked certificates is also large. Applications intended to consume CRLs from the DoD PKI must be able to consume large CRLs produced by multiple CAs. The DoD PKI has had over 20 active CAs, and some CRLs have approached 35 megabytes. RCVS is available and may be an alternative to using CRLs (see Section 5).

3.4 CRL Distribution

The DoD PKI began supporting HTTP requests for CRLs after including HTTP references in the CDP and AIA extensions. Enhancements have been made to this support to enable caching mechanisms available with HTTP 1.1. These features reduce bandwidth and improve speed. Specifically, the features allow for:

- Compressing the CRLs for transmission between the source and the requesting client. CRLs can be compressed at the source for transmission and expanded upon receipt. HTTP data payloads can be compressed using GNU ZIP (GZIP). This compression reduces the size of CRLs by more than 60 percent.

- Caching CRLs at intermediate points. CRLs can be stored in content proxies often found at hubs or gateways between networks. An example is the gateway that typically exists between the wide area network and a base or installation network. These gateways may have proxy servers with the capability to cache or retain copies of content from the wide area network delivered through the gateway. Subsequent requests for the same content can be handled by the proxy in some cases rather than forwarding the request to the source to get the same content. The caching disseminates the CRLs to locations closer to the user, allows faster access to CRLs, and consumes less network bandwidth.
- Requesting transmission of a new CRL subject to the condition that an update has been issued since the previously obtained CRL.

Enabling these features required populating selected HTTP headers with information taken from the CRL. Actions are necessary on the part of users and proxy administrators to take advantage of these features. The following subsections address each of the features.

3.4.1 CRL Compression

HTTP 1.1 has provisions to compress information during transmission. Popular Web browsers are enabled to use this feature. Transmissions from many of the Web search services use the feature. The HTTP request for the CRL should include a header element to inform the server that the requesting client is able to receive compressed content.

The figures below (Figure 7 through Figure 11) illustrate the PKI's compression capabilities. Figure 7 shows the header of the CRL requested. Figure 8 shows the HTTP request header for the CRL. This is an ordinary request and does not include any indication that the requesting client can process compressed responses. Figure 9 shows the response. The *Content-length* header element shows that the response payload is 16,229,702 bytes. This is the size of the CRL. Figure 10 shows another request for the CRL. This request includes an *Accept-encoding* element indicating that the client can handle compressed responses. Figure 11 shows the response. The response includes the *Content-encoding* element showing that the content is GZIP compressed. The *Content-length* shows that the CRL has been compressed to 4,882,644 bytes. The compression reduced the amount of data transferred by almost 70 percent relative to the original size.

```
Certificate Revocation List (CRL):
        Version 2 (0x1)
        Signature Algorithm: sha1WithRSAEncryption
        Issuer: C=US,O=U.S. Government,OU=DoD,OU=PKI,CN=DOD EMAIL CA-19
        Last Update: Nov 25 10:00:00 2009 GMT
        Next Update: Dec  2 02:00:00 2009 GMT
        CRL extensions:
            X509v3 Authority Key Identifier:
                keyid:03:6D:7D:B9:C0:41:EF:F6:47:AF:24:1D:3B:98:1C:74:0E:8C:64:DB
            X509v3 CRL Number:  832
```

Figure 7: CRL Header

```
GET /getcrl?DOD+EMAIL+CA-19 HTTP/1.1
User-Agent: curl/7.16.4 (x86_64-pc-linux-gnu) libcurl/7.16.4 OpenSSL/0.9.8e zlib/1.2.3.3 libidn/1.0
Accept: */*
Host: crl.gds.disa.mil
```

Figure 8: HTTP Request (Uncompressed)

CRL Distribution

3-6

```
HTTP/1.1 200 OK
Server: Netscape-Enterprise/6.2 RHAT
Date: Wed, 25 Nov 2009 15:51:12 GMT
Accept-ranges: bytes
Last-modified: Wed, 25 Nov 2009 10:00:00 GMT
Etag: B74D005F7283495A76C9FDEA697946E0EDB6258
Expires: Wed, 02 Dec 2009 02:00:00 GMT
Cache-control: max-age=302400,public,no-transform,must-revalidate
Content-length: 16229702
Content-type: application/pkix-crl
Content-disposition: attachment; filename=DODEMAILCA_19.crl
Connection: keep-alive
```

Figure 9: HTTP Response (Uncompressed)

```
GET /getcrl?DOD+EMAIL+CA-19 HTTP/1.1
User-Agent: curl/7.16.4 (x86_64-pc-linux-gnu) libcurl/7.16.4 OpenSSL/0.9.8e zlib/1.2.3.3 libidn/1.0
Accept: */*
Host: crl.gds.disa.mil
Accept-Encoding: gzip, deflate
```

Figure 10: HTTP Request (Compressed)

```
HTTP/1.1 200 OK
Server: Netscape-Enterprise/6.2 RHAT
Date: Wed, 25 Nov 2009 14:50:01 GMT
Content-disposition: attachment; filename=DODEMAILCA_19.crl
Last-modified: Wed, 25 Nov 2009 10:00:00 GMT
Etag: B74D005F7283495A76C9FDEA697946E0EDB6258
Expires: Wed, 02 Dec 2009 02:00:00 GMT
Cache-control: max-age=302400,public,no-transform,must-revalidate
Content-encoding: gzip
Content-length: 4882644
Content-type: application/pkix-crl
Accept-ranges: bytes
Connection: keep-alive
```

Figure 11: HTTP Response (Compressed)

3.4.2 CRL Caching

The responses to HTTP requests for CRLs now include elements to assist intermediate HTTP proxies to cache the responses. The responses include header elements whose values reflect information from the CRL. The responses shown in Figure 9 and Figure 11 include *Last-modified*, *Expires*, *Etag*, and *Cache-control* elements. The *Last-modified* and *Expires* values are copied from the CRL's *Last Update* and *Next Update* elements respectively (see Figure 7). The *Etag* value is the character string representation of the hexadecimal value of the SHA-1 hash of the CRL. The *Last-modified*, *Expires*, and *Etag* elements uniquely identify the CRL. The Cache-control element informs the proxy about how it should cache and use the cached copy. This element contains several components:

- *Max-age*. This component informs the cache on the maximum length of time to retain the cached CRL. The value is seconds and will not extend beyond the CRL's *Next Update*. The value reflects the PKI estimate of when the cached CRL should be replaced and will generally be earlier than the *Expires* date. The *Next Update* value is usually well after the date that the DoD PKI would normally issue a new update, and the *Max-age* will cause the cache to periodically check for updates issued before the next update.
- *Public*. This component informs the proxy that the value does not require any protection.

- *No-transform*. This component instructs the proxy not to transform the CRL. Transforms might invalidate the CRL's digital signature.
- *Must-revalidate*. This component instructs the proxy to confirm that the CRL is still current before responding with the cached CRL.

3.4.3 Conditional CRL Requests

Clients can use conditional HTTP requests to avoid repeatedly downloading the same CRL. The *If-Modified-Since* header element specifies a date and time, which means that the client only wants to see the full response if and only if the content was created after the specified date and time. Figure 12 illustrates the request and includes an *If-Modified-Since* element. Figure 13 shows the response when a more recent CRL is not available. The response shows that the requested CRL has not been modified (i.e., updated).

```
GET /getcrl?DOD+EMAIL+CA-19 HTTP/1.1

Host: crl.gds.disa.mil

User-Agent: Mozilla/5.0 (Windows; U; Windows NT 5.1; en-US; rv:1.9.1.5) Gecko/20091102
    Firefox/3.5.5 (.NET CLR 3.5.30729)

Accept: text/html,application/xhtml+xml,application/xml;q=0.9,*/*;q=0.8

Accept-Language: en-us,en;q=0.5

Accept-Encoding: gzip,deflate

Accept-Charset: ISO-8859-1,utf-8;q=0.7,*;q=0.7

Keep-Alive: 300

Proxy-Connection: keep-alive

If-Modified-Since: Wed, 25 Nov 2009 10:00:00 GMT
```

Figure 12: HTTP Conditional Request

```
HTTP/1.x 304 Not Modified
Server: Netscape-Enterprise/6.2 RHAT
Date: Tue, 25 Nov 2009 18:23:18 GMT
Accept-Ranges: bytes
Last-Modified: Wed, 25 Nov 2009 10:00:00 GMT
Etag: B74D005F7283495A76C9FDEA697946E0EDB6258
Expires: Wed, 02 Dec 2009 02:00:00 GMT
Cache-Control: max-age=302400,public,no-transform,must-revalidate
Content-Type: application/pkix-crl
Content-Disposition: attachment; filename=DODEMAILCA_19.crl
Age: 0
```

Figure 13: Response to HTTP Conditional Request

3.5 CRL Future Directions

X.509 Version 2 CRLs can support several methods for controlling the size of CRLs by issuing CRLs that are less than full and complete. The approaches for reducing the CRL size include:

- Producing a *delta CRL* that is a CRL limited to listing certificates that have been revoked subsequent to the time when a previous CRL was published.
- Producing a CRL that has a particular scope and does not list all expired certificates. For example, the CRL's scope might limit the CRL to list only revoked certificates that were issued to EEs (not to CAs), had serial numbers in a particular range, were issued to a particular organizational unit (e.g., Army), or were revoked for a particular reason or set of reasons.

The DoD PKI PMO has not selected which, if any, of these approaches to use. RCVS (see Section 5) provides an alternative for providing certificate status that does not require relying parties to handle large CRLs. The DoD PKI is unlikely to employ indirect CRLs because of the complexity of their processing by clients. The DoD PKI is unlikely to employ entry extensions because of their impact on the overall CRL length. For example, inclusion of the codes for the revocation reason would increase CRL size by 64 percent.

4 DoD PKI Directory

The DoD PKI directory is based on the X.500 directory standard [X.500]. This section describes the DoD PKI directory organization. The PKI follows the standards' Distinguished Name conventions. The X.500 naming structure is hierarchical and was designed to provide a unique structure for worldwide use, based on decentralized control of naming.

GDS provides the PKI directory services. Information maintained in the directories is accessible through LDAP. GDS also includes a Web interface that allows users to obtain CRLs and search the directory for certificates.

The following subsections describe the DoD PKI's name hierarchy, the GDS directory structure, the DN conventions for uniquely naming entries in the directory, cross-certificate pair entries, the methods for accessing the directories and the objects they maintain, and future directions for the GDS directory.

4.1 DoD PKI Name Hierarchy

Under the standards process, an organization registers names at each level of the name hierarchy. To ensure that the DoD PKI-naming structure is unique from other X.500 names, all PKI-issued DNs will share a common suffix. This suffix is the base suffix. For the DoD PKI, the base suffix is:

OU=PKI, OU=DoD, O=U. S. Government, C=US[23]

Each successive level of the name hierarchy becomes the suffix for the DNs at the next level of the hierarchy. Figure 14 illustrates the Directory Information Tree for the PKI directory. The PKI's base suffix has four levels. Primary entries at the next level, Level 5, are OUs associated with DoD organizations at the C/S/A level. The OUs at this level include a "Contractor" OU for certificates issued to contractor employees.

Appendix B lists the organizations at Level 5 of the directory. EEs belonging to the PKI infrastructures, such as CAs and OCSP responders, will also exist at Level 5 and will be the only EEs at that level. All other EEs will be at Level 6 and be subordinate to their owning or sponsoring organizations at Level 5. As a result, CAs are not in the naming structure of the entities whose certificates they sign, and no relationship between the issuing CA and EE's DNs exists.

[23] The certificates issued on the Unclassified Internet Protocol Router Network (NIPRNet) and SIPRNet shared this suffix until the National Security Systems (NSS) PKI was created. Certificates issued under NSS had a different suffix.

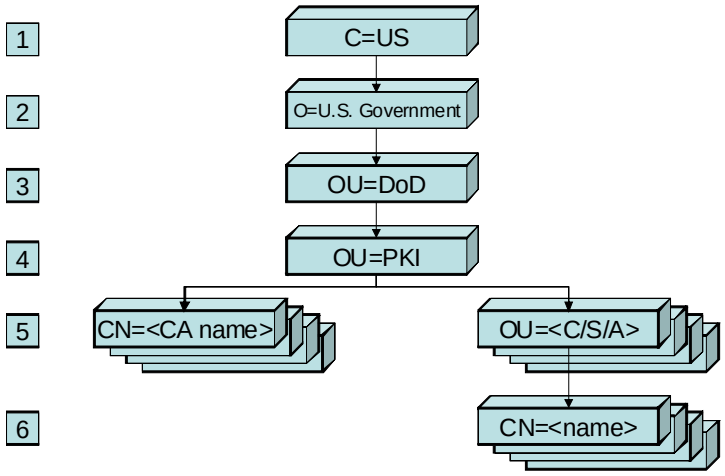

Figure 14: DoD PKI Directory Information Tree

4.2 GDS Directory Structure

GDS consists of two separate but related directories, *DoD411* and *CRL*. Figure 15 illustrates the components of GDS. The following subsections describe the information that each component maintains.

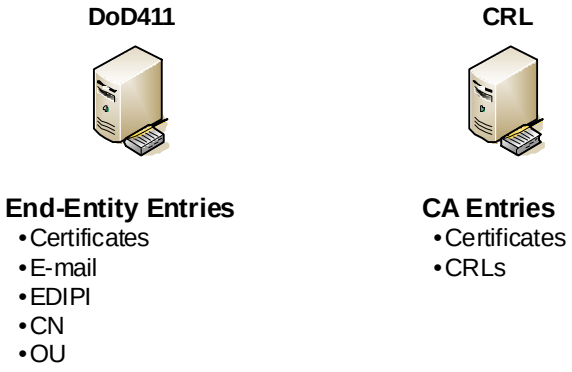

Figure 15: Components of GDS

4.2.1 DoD411 Directory Component

DoD411 is a repository for e-mail encryption certificates issued to EEs, including individuals. The DIT for DoD411 generally follows the naming structure shown above in Figure 14. This component may include entries for the CAs. However, the CA entries do not include CRLs or CA certificates. In DoD411, CA entries are indistinguishable from other EEs in terms of the information maintained in the entry.

4.2.2 CRL Directory Component

As the name suggests, the CRL directory component is a repository for CRLs. It is also a repository for *authority certificates*. Authority certificates are the certificates issued to CAs. These certificates are necessary for constructing certificate paths needed to authenticate and validate the trustworthiness of EE certificates. The CRL directory also serves as a repository

for CA certificates and CRLs belonging to CAs that operate under the ECA program. The CRL directory component has entries for the ECA Root CA and the individual CAs that operate under the ECA program. Because of support for ECA certificates, the DIT is different than that for DoD411. The CRL directory DIT includes a subtree for the ECA OU, which is a peer to the DoD OU under the U. S. Government subtree (O) . Figure 16 illustrates the CRL's DIT.

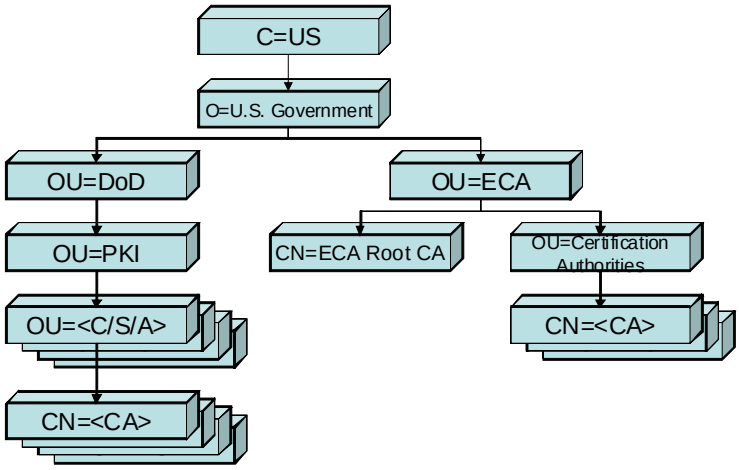

Figure 16: DIT for the CRL Directory Component of GDS

The entries for CAs belong to the *certificationAuthority* objectclass. Members of the certificationAuthority objectclass have *certificateRevocationList;binary* and *cACertificate;binary* attributes to hold the CRL and CA certificate, respectively. CAs involved in cross-certificates may have *crossCertificatePair; binary* to hold cross-certificates (see Section 4.4). The CRL directory component does not have entries for any other EEs.

4.3 Name Conventions

Names that appear in the issuer and subject fields of certificates and in the DNs for directory entries follow the X.500 standards. Names that appear as entries in certificates' issuer or subject fields generally have entries in the GDS directory. Each of the names share a common root or suffix, which is the base suffix described above.

Directory names are hierarchical. The name at each node in a hierarchy provides an additional name component: a Relative Distinguished Name (RDN) to the name of its parent. RDNs in the DoD PKI contain a single attribute with a single value. RDN values may be represented using any of the directory string character sets that RFC 5280 permits. Normally, the values are encoded as Printable Strings, but other string forms are used when the value involves characters not included in the Printable String character set.

All DNs will share the base suffix. DNs for EEs that belong to one of the C/S/A OUs include an OU RDN for the OU. The last RDN component for EEs is a CN. The next subsections describe the Level 5 OUs and CNs.

4.3.1 Level 5 OUs

Appendix B provides a list of the OUs defined for use at Level 5. The Level 5 OUs are fixed and cannot be changed without approval through the DoD PKI Configuration Control Process. [SEP] The format for a Level 5 OU's DN is:

OU=<C/S/A>, OU=PKI, OU=DoD, O=U.S. Government, C=US

This DN becomes a suffix for the entities under it. For example, the suffix for Army EEs would be:

OU=USA, OU=PKI, OU=DoD, O=U.S. Government, C=US

These OUs may change when changes occur to the DoD organizational structure. DoD reorganizations may drive changes to the OUs (e.g., an existing organization may have its name changed or a new organization may be created). In such cases, entries belonging to EEs affected by the change are usually left in place until their certificates require renewal. At that time, the new certificate will use the current OU. In such cases, the directory may retain *deprecated* OUs. The OU will remain in the directory until the entries under it are no longer needed. No new entries will be created. A deprecated OU will be removed when there are no remaining active subordinate entities.

4.3.2 Common Names

CNs vary depending on the type of entity the name references. The following subsections describe the CNs used for various entity types. Entries for CAs are at Level 5; all other EEs are at Level 6.

4.3.2.1 Root CA

The DoD PKI has had two core Root CAs. The relative DN for the Root CA prior to P3.1 was:

cn=DoD CLASS 3 Root CA

The relative DN for the Root CA used for certificates issued after P3 was:

cn=DoD Root CA 2

The DoD PKI also issued root CA certificates to the ECA and IRCA. The relative DNs for these roots were:

cn=ECA Root CA

cn=DoD Interoperability Root CA 1

4.3.2.2 Signing CAs

The signing CAs will also be at Level 5 of the DIT. The CN format for a signing CA prior to P3.1 was:

cn=DoD CLASS 3 CA-<n> (for identity certificates)

or

cn=DoD CLASS 3 EMAIL CA-<n> (for e-mail certificates)

The CN format for a signing CA after P3 was:

cn=DoD CA-<n> (for identity certificates)

or

cn=DoD EMAIL CA-<n> (for e-mail certificates)

Here, **<n>** is a number. Numbers were assigned sequentially to signing CAs as they were created. CAs 1 and 2 were used for DoD PKI Release 1 (with a slightly different CN format). CAs 3 through 10 issued P3 certificates. CAs starting at 11 issued P3.1 certificates. CAs were added as needed to provide scalability, ease management of CA resources, and allow evolution to enhanced products.

4.3.2.3 Intermediate CAs

The intermediate CAs will also be at Level 5 of the DIT. The CN format for an intermediate was:

cn=DoD Intermediate CA-<n>

Here, **<n>** is a number. Numbers were assigned sequentially to intermediate CAs as they were created.

4.3.3 Individuals

A CN will be created by the DoD PKI for each user. An individual's CN consists of several elements separated by periods (.). The elements are last name, first name or initial, middle name or initial, generational qualifier (e.g., Jr, Sr, IV), and a ten-character numeric string.[24] The last name and numeric string components are required; the remaining components are optional depending on the individual's real name.

The ten-character numeric string ensures the uniqueness of CNs. The string may be either a UID or an EDIPI. UIDs begin with a zero (0) character and were issued by Local Registration Authorities (LRAs), who issued certificates for private keys maintained in software. Blocks of sequential UIDs were provided to LRAs who allocated the UIDs sequentially to individuals receiving certificates. Although the UID was intended to remain with the individual, the business process did not ensure persistence or allow relating the UID to other unique identifiers, such as the individual's Social Security Number (SSN). At about the same time that P3.2 was released, changes were made to the software issuance process and EDIPIs replaced UIDs in DNs on nearly all software certificates. UIDs continued to be used only when an individual either did not have an EDIPI or the EDIPI was not available when the certificate was issued.

---

[24] This element is characterized as a string rather than a number because the string may include leading zeros (0).

Name Conventions

When the certificate issuance merged with identity card issuance and used the CAC hardware to store the private key, the DoD PKI used the EDIPI as the numeric string. EDIPIs begin with a one (1). The personnel automatic data systems generate and assign EDIPIs to individuals. The EDIPI association with an individual is maintained in the individual's record in the personnel system and is persistent and essentially permanent. Individuals should maintain the same EDIPI even when the individual has a break in service or legally changes his or her name (e.g., as a result of marriage).

In user certificates issued by the DoD, the entire CN should not exceed 64 characters and will be unique to an individual. Applications should not assume a particular format or convention for the CN components. For example, the DoD personnel system issued identity cards for many years using the individual's middle initial rather than the full middle name. The convention was later changed to employ the individual's full middle name.

The general CN format for individuals is:

CN=<lastName>[.<firstName>][<.middleName>][.<generation_qualifier>].<edipi|uid>

An example CN is:

CN=Smith.John.Carl.Jr.1234567890

In some special cases, slight adjustments to the CN were made. For example, some certificates issued to coalition partners included an abbreviation for their country names.

For software certificates, the name will be based on the name appearing on the individual's military or civilian ID card for military and DoD civilian personnel, respectively, and Social Security card or driver's license for non-DoD personnel.

The CN is the leading RDN in an individual's DN. An example DN for an Air Force person is:

cn=Smith.Sarah.Nicole.1234567890, ou=USAF, ou=PKI, ou=DoD,
o=U.S. Government, c=US

An example DN for a contractor employee is:

cn=Anderson.Jason.Michael.1234567890, ou=CONTRACTOR,
ou=PKI, ou=DoD, o=U.S. Government, c=US

A DoD PKI goal is to provide identifiers for individual certificate holders in their certificate's subject name for which they can be held accountable and which allows relying parties to distinguish the individual named in the certificate. The DoD personnel system creates and permanently maintains an individual's EDIPI. Each individual should have one and only one EDIPI. The same was not true for the UIDs while they were used on software certificates. An individual likely received a new UID each time the individual obtained a new certificate. Reasons for getting a new certificate include renewal of an expired certificate, replacement of a certificate because access to or control over the associated private key was lost, or a break in service or affiliation with a DoD organization. An individual could have had more than one UID.

No correlation between the individual and the UID other than the name components contained in the certificate's subject name were maintained. Thus, in some cases a specific individual could not have been associated with a particular certificate.

Individuals may have multiple CNs. The CNs may differ because the individuals legally changed their names, because of changes in naming conventions used by the individual or the DoD, or because of entry errors when issuing certificates.

The DoD personnel community changed the name conventions for names used on CACs; full middle names were used rather than middle initials. If the CN contains an EDIPI, the EDIPI should be the same in the different CNs. Individuals may have multiple DNs because of differences in the Level 5 OU. Individuals may change their affiliation from one DoD organization to another. Certain individuals may have multiple affiliations. For example, a DoD civilian employee or contractor may also be a member of the Reserves or National Guard. Figure 17 illustrates the relationships between individuals and the various name components.

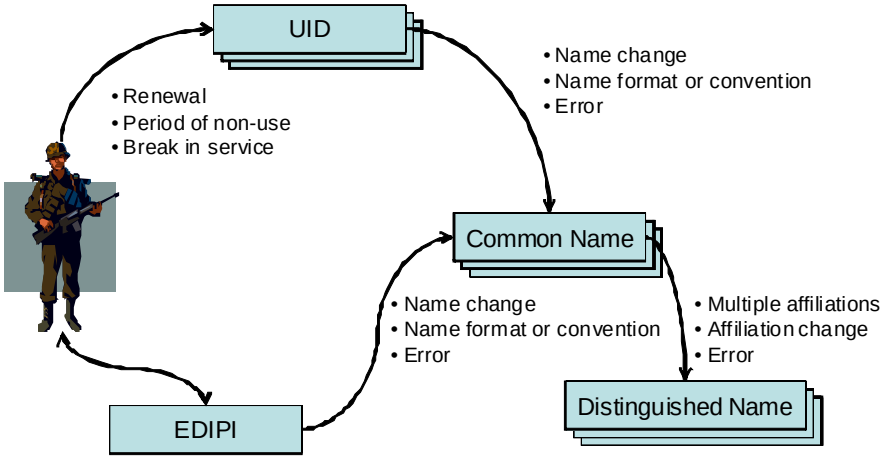

Figure 17: Name Component Relationships

4.3.4 Registration Authorities

The CN RDN for an RA consists of adding a prefix to the RA's individual CN. The format of the RA CN is:

cn=RA.<individual cn>

An example DN for an Army RA is:

cn=RA.Alas.Karen.Magaly Maldonado.0123456789, ou=USA, ou=PKI, ou=DoD, o=U.S. Government, c=US

4.3.5 Local Registration Authorities

The CN RDN for an LRA consists of adding a prefix to the LRA's individual CN. The relative DN for the LRA is:

cn=LRA.<individual cn>

An example DN for a Navy LRA is:

cn=LRA.Malik.Ali.Hassan.6789012345, ou=USN, ou=PKI, ou=DoD, o=U.S. Government, c=US

4.3.6 OCSP Responder Names

OCSP responder DNs generally followed the conventions for other DNs. The CN for responders is different from other CNs. Responder CNs include components to indicate the EE is a responder, the site where the responder is located, whether the responder is distributed (D) or traditional (T), and a serial number that increases each time the responder receives a new certificate from the issuer. The CN has the form:

CN = OCSP <site #>[D|T] <serial>

An example DN for an OCSP responder is:

CN=OCSP 1D 1,OU=PKI, OU=DoD, O=U.S. Government, C=US

4.3.7 Group and Role Names

Group and role certificates generally followed the conventions for other DNs. Their CNs are different from other CNs. The CNs consist of four parts: organization name, component name, role or group name, and a UID. The CN has the form:

cn=<organization name>.<component name>.<group or role name>.<unique identifier>

4.3.8 Code Signing

The CN RDN in a code-signing certificate consists of three parts. The first part is the prefix CS. The second part is the name of the organization responsible for signing code objects. This organization will generally be at an organizational level well below the OU identified in the RDN following the CN. The third part is a name or number that uniquely distinguishes the CN from other CNs belonging to the organization. The organization is responsible for maintaining this uniqueness. The RDN for the code-signing CN is:

cn=CS.<organization name>.<unique name or number>

An example DN for code signing use in the Air Force is:

cn=CS.HQ AFPC.DPDOX.0004, ou=USAF, ou=PKI, ou=DoD, o=U.S. Government, c=US

4.3.9 Servers and Other Devices

Servers and other devices may require certificates to communicate with other entities. Servers and devices may operate autonomously without any direct human control. Devices include

routers and switches. Servers and other devices will reside at Level 6 of the DIT. The CN RDN for a server or device is:

cn=<host name or IP address>

The host name is the server's DNS host name or IP address. Other name formats will be considered as the need arises, as long as uniqueness of the full DN can be guaranteed.

An example of a host name for a server sponsored by the Defense Information Systems Agency (DISA) is:

cn=www.mdw.disa.mil, ou=DISA, ou=PKI, ou=DoD, o=U.S. Government, c=US

Device entries will occur at Level 6 of the DIT.

4.4 Cross-Certificate Pairs

Directory entries for CAs that either issue or are subjects of cross-certificates have entries containing cross-certificate pair attributes. As the name suggests, the attribute holds a pair of certificates with tags 0 and 1. The two certificates are the certificate *issued to* the CA and the certificate *issued by* the CA, respectively.[25] The CA is the subject and issuer of the two respective certificates. The cross-certificates are paired to a partner CA. The partner CA is the issuer and subject, respectively, of the two certificates. The crossCertificatePair;binary is a multi-value attribute that holds a pair for each partner CA that cross-certifies with the CA whose entry contains the pair. In some cases, only one of the certificates may exist. In such case, the certificate has the tag that indicates whether it is the certificate issued to or issued by the CA.

Cross-certificates are useful to relying parties who attempted to construct a certificate path from a trust anchor to an EE. The *issued by* certificates assist in constructing paths from the trust anchor to the EE (top down), and the *issued to* certificates assist in constructing paths from the EE to the trust anchor (bottom up). Certificates that are both self-issued and self-signed are not included in cross-certificate pairs.

The cross-certificate attribute is a target of the caRepository reference in an SIA extension and a caIssuers reference in an AIA extension. The HTTP reference in an AIA extension bundles the *issued to* certificates from the collection of cross-certificate pairs, while the SIA reference bundles the *issued by* certificates.

As an example, the directory entry for the IRCA contained cross-certificate pair attributes. When the DoD PKI was cross-certified only with the FBCA, the IRCA directory entry's cross-certificate attribute had three values as shown in Table 58. The pair related to the FBCA has two certificates since both CAs issued certificates to the other. The pairs related to the other two DoD Root CAs have only the *issued by* component because the two Root CAs received certificates issued by the IRCA. However, the other two Root CAs did not issue certificates to the IRCA.

[25] The *issued by* member of the pair was previously known as the *reverse* member, and the *issued to* member of the pair was previously known as the *forward* member.

Table 58: IRCA Cross-Certificate Pairs

Related CA	Issued to:	Issued by:
FBCA	Certificate FBCA issued to IRCA	Certificate issued by IRCA to FBCA
DoD Class 3 Root CA	Empty/	Certificate issued by IRCA to the DoD Class 3 Root CA
DoD Root CA 2	Empty	Certificate issued by IRCA to the DoD Root CA 2

4.5 Directory Access and Use

The directories are available for relying parties to retrieve CRLs and certificates from the CRL and DoD411 directories, respectively. Access to the directories may be limited based on security considerations and performance impact. The following subsections describe the means of accessing the directories and the controls on directory access.

4.5.1 Directory Access Methods

Relying parties may use either a Web or LDAP interface to the directories. The Web interface is a graphical user interface intended for human interaction using a Web browser. The LDAP interface is intended to provide applications with a method to access directories. LDAP browsers are available that can provide a human with access to the directory through the directory's LDAP interface. Each interface is accessible through a single URL, although the DoD PKI has several instances of the directories positioned worldwide. A global load-balancing system will transparently direct individual accesses to specific directory instances. In the future, the LDAP may change to LDAP over SSL (LDAPS) and require that the clients use certificate-based authentication. Table 59 provides information regarding the URLs or host names used to access the directory. The DoD PKI uses the standard ports for the protocols; the table does not show port numbers.

Table 59: Directory Access Locations

Directory Component	Web URL	LDAP Host
DoD411	https://dod411.gds.disa.mil/	dod411.gds.disa.mil
CRL	http://crl.disa.mil/	crl.gds.disa.mil

Individual CRLs can be retrieved through links on the Web URL or directly using LDAP. The HTTP URL to retrieve a specific CRL is:

http://crl. disa.mil/getcrl?<CA Common Name Value>

The CA's Common Name Value is the URL-encoded form of the CA's CN. The unencoded reference for *DoD E-MAIL CA-12* is:

http://crl.gds.disa.mil/getcrl?DoD EMAIL CA-19

The encoded form is:

http://crl.disa.mil/getcrl?DoD%20EMAIL%20CA-19

This dynamic URL was replaced with the static URL:

http://crl.disa.mil/crl/DoDEMAILCA_19.crl

Both directories employ a limited set of LDAP object classes. The OU entries are instances of the standard LDAP organizationalUnit object class. The OU entries generally have the OU attribute populated with the name of the organization. In the DoD411 component, all EEs are instances of the inetOrgPerson object class. This is true for all EEs, including entities that are not individuals. DoD411 does not contain entries for CAs.[26] Table 60 identifies the attributes that are populated for the inetOrgPerson object class. Some of the attributes for entries other than individuals may not have values. Most of the attributes may be multi-valued.

Table 60: DoD411 Directory End-Entity Attributes

Attribute	Attribute Name	Value
Common Name	CN	Entity Common Name as it appears in certificate's DN.
Object Class	objectClass	inetOrgPerson
Middle Name	initials	Middle name for individuals as extracted from the CN component
Surname	SN	Last name for individuals as extracted from the CN
First Name	givenName	First name for individuals as extracted from the CN
E-mail address	mail	Entity's e-mail address.
Certificates	userCertificate;binary	Certificate in binary format.
Unique Identifier	uid	The EDIPI or UID that appears as a numeric string at the end of the CN for individuals. May have the CN value for entities other than individuals.
EDIPI	employeeNumber	The EDIPI or UID assigned to individuals with CACs or software certificates, respectively.

[26] There may be entries for some CAs because of server certificates issued to the CA.

The EEs in the CRL directory component belong both to the certificationAuthority and intOrgPerson object classes [RFC4523]. The only inetOrgPerson attributes used are CN, SN, and UID. The DoD PKI does not produce Authority Revocation Lists (ARLs). The authorityRevocationList;binary attribute is a required attribute for the certificationAuthority object class but is not given a value in the entries belonging to the object class. The EE entries contain the attributes listed in Table 61.

Table 61: CRL Directory End-Entity Attributes

Attribute	Attribute Name	Value
Common Name	CN	Common Name of CA as it appears in certificate DN.
Object Class	objectClass	certificationAuthority and inetOrgPerson
Surname	SN	Same value as the CN.
Certificates	cACertificate;binary	CA's certificate in binary format. May contain multiple certificates.
CRL	certificateRevocationList; binary	CRL in binary format.
Authority Revocation List	authorityRevocationList: binary	No value is assigned to this attribute in the DoD PKI.
Unique Identifier	uid	Same value as the CN.
Cross-Certificate Pair	crossCertificatePair; binary	The cross-certificates involving a partner CA.

4.5.2 Directory Access and Use Limitations

Access to the directory is limited for security, privacy, and performance. The access limits vary and are subject to change. The security and privacy limits vary based on the desired operation, the source of the directory access, and the amount of information returned. The ability to create, modify, or delete entries is limited and generally not allowed. The ability to read the directory is controlled. The ability to read the directory may be limited based on the source's identity or network address. For example, the directory Web interface may be restricted only to allow access by entities whose identities can be authenticated with SSL/TLS authentication using DoD PKI certificates. The request source may need to be from a network address that is part of the .mil or .gov domains.

The directory may enforce limits to prevent requests that unfairly or unnecessarily use resources. The directory may enforce limits on the following items, for example:

- The number of entries included in the results
- The number of entries that need to be examined during the search
- The time required or used to perform the search

Searches that exceed these limits will be terminated when the limits are exceeded. The directory may or may not provide partial returns of entries found before the limit was exceeded. Applications should always examine the return code associated with searches and retrievals to determine if an error occurred. Results may be only partial if the system returned an error code.

4.5.3 Case Sensitivity

References to the directory entries and their values are not case sensitive. Stored values retain the case that was specified at the time that the entry and attribute values were created or modified. However, searches are not case sensitive. The DoD PKI has varied in the use of case within names for CAs. For example, some CA CNs use *DoD*, while others use *DOD*. Although directory operations function without case sensitivity, other operations, such as path creation and chaining and OCSP request formation, may be sensitive to the exact case used for a DN within a certificate. Applications may be required to use the exact case for DNs and attribute values in such situations.

4.6 Directory Future Directions

The directory will likely evolve over time. Evolutionary directions include aligning the directory DIT with other DoD directories, including certificates other than e-mail encryption (identity and e-mail signature), and revisions to the directory object classes. To align the DIT with other DoD directories, the C/S/A OUs that are now subordinate to the PKI OU would move up a level to become peers of the PKI OU. CA entries and other entities under PKI control would remain under the PKI OU. New entity-type OUs would be created under the C/S/A OUs to distinguish the types of entity (e.g., people, devices, roles). Further OUs may distinguish the type of people (e.g., military, civilian, and contractor) that support the unit. Figure 18 illustrates a possible future DIT with the changes just described.

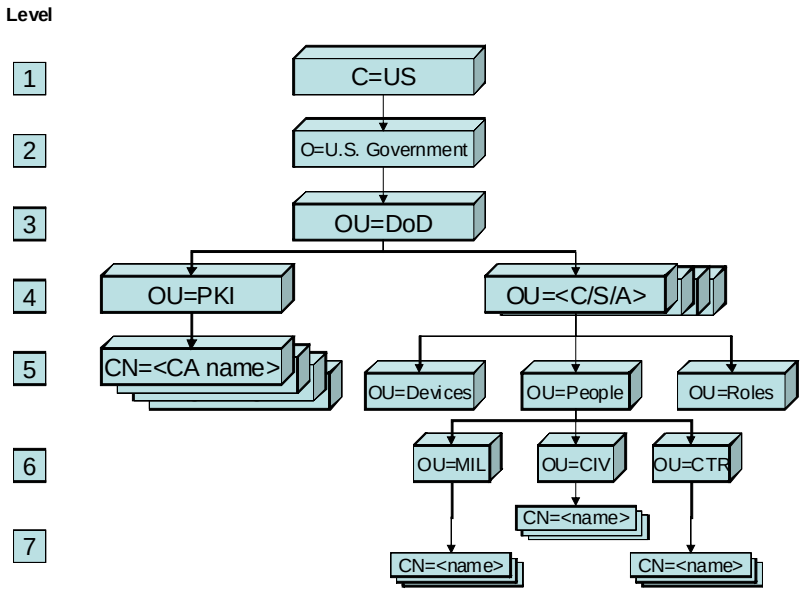

Figure 18: Possible Future DIT

Directory Future Directions

4-14 The directory may evolve to become a repository for certificates other than the e-mail certificates. Applications using signatures have generally included certificates necessary to verify signatures with the signed information. Some applications now provide a means to include a reference to a certificate rather than the actual certificate. Relying parties can retrieve the certificates using the reference. The reference could be to a directory location containing the certificate.

A new set of RFCs for revising LDAP standards has been approved [RFC4510 and RFC4523]. Some changes may occur as directory products evolve to comply with the new standards. The standards revised some of the object classes, including PKI-related objects. The standards revised and renamed the object class for CAs. New object classes have been defined for delta CRLs and CRL distribution points.

The standards community appears to be moving toward using the Unicode Transformation Format-8 (UTF8) Strings as the common representation for string values rather than allowing a choice of character sets. The DoD PKI will evolve to the use of UTF8 Strings as opportunities permit.

5 Robust Certificate Validation Service

The RCVS is based on OCSP [RFC2560]. Using OCSP, a client requests the status of a certificate from an OCSP response server, known as the *responder*, which responds with the status of the certificate. RCVS uses traditional and pre-signed OCSP responders. The traditional responders prepare a response for each request they receive. The pre-signed responders prepare responses in advance and independent of any request. Then the responders provide the appropriate pre-signed response to a request for a certificate's status. To minimize the time required to prepare responses, the pre-signed responses provide the status for several certificates. Currently, the pre-signed responses include 20 certificates, but the DoD PKI could modify that number at any time.

The DoD PKI RCVS follows the basic OCSP Standard, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP* [RFC2560]. RCVS supports the Nonce extension described below but not any of the other extensions contained in the RFC.

The RCVS employs load balancing techniques to distribute requests referencing a central URL to one of several locations that operate OCSP responders. The central URL is:

http://ocsp.disa.mil

The following sections describe OCSP request and response formats, non-standard behavior of the pre-signed responders, and RCVS future directions.

5.1 Supported CAs

RCVS provides the status for certificates that are descendants of the DoD Root CAs. RCVS can provide the status for certificates that the root CAs issue to signing CAs and the certificates that the signing CAs issue. RCVS does not provide status for certificates that ECAs issue or for certificates that the FPKI and its partners issue.[27]

5.2 OCSP Request Format

OCSP requests specify the identities of one or more target certificates for which the requestor wishes to determine the status. The request identifies target certificates using a sequence of four elements: a hash algorithm identifier, a hash of the target certificate's issuer field, a hash of the issuer's public key field of the target certificate, and the serial number of the target certificate. The identified hash algorithm is used to compute the DN and public key hashes. The issuer's public key hash is the same value that appears in the target certificate's AKI extension and the SKI of the certificate belonging to the target certificate's issuer. The standard allows signatures on requests, but the DoD PKI does not require them. Table 62 summarizes the format and content of the request. The *Use* column indicates whether the field is always (A), never (N), or sometimes (S) included in the request.

The only request extension that the RCVS supports is the Nonce extension. The optional Nonce extension, when present, includes a random value that the responder includes in the

[27] Refer to interfaces for the individual ECA and FBCA partner PKIs. The AIA and CDP extensions will likely have references for OCSP responders and CRL retrievals.

5-2 response. The Nonce ensures that the response was prepared explicitly for the request and did not involve the reuse or replay of a previous response.

Table 62: OCSP Request Fields

Field	Use	Content
Version	N	Default is Version 1. Field is implied for Version 1.
Requestor Name	N	
Request List	A	List of Certificate IDs (CertIDs) for target certificates.
CertID	A	A sequence that identifies a target certificate: hash algorithm identifier, hash of the issuer's DN, hash of the issuer's public key, target certificate's serial number
Request Extensions	S	Relying parties wanting the responder to produce a specific response for the request may include the Nonce extension.
Signature Algorithm	N	Default prior to P3.3: sha1WithRSAEncryption (1.2.840.113549.1.1.5). Default starting with P3.3: sha256WithRSAEncryption (1.2.840.113549.1.1.11).
Signature	N	The actual signature value.
Certificates	N	One or more certificates useful in verifying the request's signature.

5.3 OCSP Response Format

The OCSP response varies depending on the responder's ability to respond to the request. If the responder recognizes the request as correctly formatted, the response status is *successful*. Otherwise, the response reports an *error* status. The error may reflect that the request was malformed or that the responder was not capable of responding. The response status is not digitally signed. If the response is successful, it includes a *basic OCSP response*. Table 63 summarizes the general OCSP response and includes the *Use* column to indicate when the fields are present.

Table 63: OCSP Response Fields

Field	Use	Content
Response Status	A	One of the following values: successful (0) malformedRequest (1) internalError (2) tryLater (3) Not Used (4) sigRequired (5) unauthorized (6)
Response Bytes	S	Optional field that is present for responses having the successful status. Field consists of a response type and a response. The response type is an OID: id-pkix-ocsp-basic

When the response status is *successful*, the response includes a *basic OCSP response*. This response is digitally signed. The response has a body and a list of responses. Table 64 shows fields contained in the response along with the use indicator. The body provides information on the responder's identity, the date (and time) when the responder prepared (i.e., signed) the response, the Nonce extension if the request included a Nonce, the signature algorithm identifier, the signature, and, optionally, the responder's certificate that may be used to verify the signature.

The response list has individual responses for each certificate whose status is included in the response. Each response contains the CertID to identify the certificate, its status, and two dates. The dates correspond to the *this update* and *next update* fields of a CRL that was the source for the status. The status is one of the following values: *unknown*, *revoked*, or *good*. The responder provides an *unknown* response if the responder does not recognize or does not maintain status for the certificate's issuer. The response is *revoked* if the certificate has been revoked (i.e., appears on the current CRL). Otherwise, the response is *good*. Table 64 shows the basic OCSP response fields.

The DoD PKI used OCSP responders from multiple vendors. Some of the responders produced pre-signed responses. These responses were based on periodic certificate status updates and were prepared in advance of any requests. For example, the responders may prepare a set of responses upon notification that a CA has published a new CRL. To minimize the number of signature operations, the responders included multiple certificates in the responses. The number of certificates included in a pre-signed response was 20 but may vary.

OCSP Response Format

5-4 Relying party applications must be able to consume these pre-signed responses and locate within the response the certificate whose status was requested.

Only the traditional responder is capable of responding to requests that include the Nonce. The RCVS operates most efficiently with requests that do not contain a Nonce because any responder can respond. Requests with a Nonce must be handled by specific responders and require the additional processing overhead to compute a digital signature for the response. The likelihood that a Nonce request will result in a different response from one without the Nonce is extremely low. Requests should not include a Nonce unless there is an important reason to include it. Applications that generate a large numbers of requests using the Nonce may incur a performance impact.

Table 64: Basic OCSP Response Fields

Field	Use	Content
Version	N	Default is Version 1. Field is implied for Version 1.
Responder ID	A	Responder's identity either by name [1] or by hash [2].
Produced At	A	The date and time that the response was produced in GeneralizedTime format.
Responses	A	A list of *single responses*. Each single response specifies the status of a particular certificate. Each response in the list is a four-item sequence: the CertID of a certificate, the status of the certificate, the *this update* for the certificate's status, the *next update* for the certificate's status. The certificate status is one of: good [0], revoked [1], or unknown [2]. Single response extensions are not supported.
Response Extensions	S	The Nonce extension if the request included the Nonce.
signature Algorithm	A	Default prior to P3.3: sha1WithRSAEncryption (1.2.840.113549.1.1.5). Default starting with P3.3: sha256WithRSAEncryption (1.2.840.113549.1.1.11).
signature	A	The actual signature value.
Certificates	S	The responder's certificate.

5.4 Non-Standard Behavior of Pre-signed Responders

In most circumstances, RCVS responses complied with the OCSP RFC. In certain, unusual circumstances, responses from a pre-signed responder differed from those of a traditional responder. Differences occurred for requests that asked for the status of multiple certificates and for requests for which there was no pre-signed response.

Because responses could have only one signature, pre-signed responses did not incorporate arbitrary, multiple certificates. If a request for the status of multiple certificates was routed to a pre-signed responder, the response may have included one of the certificates in the request (most likely the first) but omitted the status of other certificates. Requests for the status of multiple certificates should have included a Nonce to force the request to a traditional responder which was capable of responding to requests for the status of multiple certificates.

The pre-signed responders had responses for certificates whose validity period included the current time and those certificates likely to be issued before a new set of pre-signed responses was prepared. Requests that were correctly formed but reference CAs that the responder did not recognize would have received a signed *unknown* response from a traditional responder but resulted in an unsigned error response from a pre-signed responder because no appropriate pre-signed response existed. Requests for the status of certificates from supported CAs but involving serial numbers for which no pre-signed response existed would have received a signed *good* response[28] from a traditional responder and an unsigned error from the pre-signed responder.

Later versions of the pre-signed responders were configured to forward requests for which an appropriate pre-signed response was not available to a traditional responder. The traditional responder then prepared a standards-compliant response.

5.5 Trust Models

The OCSP Standard provides a few options for validating OCSP responses. The response has a digital signature that must be verified before trusting and accepting the response. The initial RCVS used the *trusted responder* approach. Parties that relied on the responders had a copy of the public key that should be used to verify the response. These relying parties trusted any response whose signature was verified using the public key. A self-signed certificate containing the public key was used to disseminate the key.

An advantage of the trusted responder approach is that the trusted responder can provide the status of any certificate. The disadvantage of the trusted responder is that the trusted responder's public key must be distributed through a reliable *out-of-band* mechanism to ensure that the relying parties are using the real trusted responder rather than an imposter. Changing the responder's key because of key compromise or key end-of-life status can be difficult because the relying parties' OCSP clients must be configured with the new key in advance and shift to the new key at the same time.

---

[28] The *good* response assumes that a pre-signed response exists for all of the revoked certificates that otherwise would be valid.

The OCSP Standard also provides for an *authorized responder* or DTM approach. Under this approach, a CA may delegate authority to a responder to provide status of certificates that the CA issued. The CA delegates the authority by issuing a certificate to the responder. The certificate has certain entries that designate that it belongs to an OCSP responder. Relying parties can trust a response with the status of certificates issued by the same CA that delegated authority to the responder. Both signatures on the responses and the target certificates can be verified with the CA's public key.

The advantage of the delegated responder approach is that keys do not have to be distributed in advance or out of band. One disadvantage of the delegated responder approach is that the delegated responder's certificate limits the responder's scope to the status of certificates issued by the CA that issued the responder's certificate. Consequently, relying parties may need to route requests to different responders based on the issuer of the certificate whose status is being checked. Also, responders may need to be capable of selecting a certificate and private key to use in composing the response based on the issuer of the certificate whose status was requested.[29]

Checking the validity of a DTM responder's certificate would obviate the value of the responder since checking the responder's certificate would be as difficult as checking the original certificate. The overhead of checking the status of the responder's certificate can be avoided by either using the *no-check* certificate extension in the responder's certificate or providing a small, limited-scope CRL that would include the responder's certificate if it was revoked. The delegated responder's certificate may include a *no-check* extension, which means that the relying party does not need to check the status of the responder's certificate. The *no-check* extension makes the check of the responder's certificate unnecessary; however, the consequence is that a responder's certificate could not be effectively revoked[30] in the event of a compromise of the responder's key. The responder's certificate would likely have a short validity period if it contained the *no-check* extension.

The DoD PKI switched from use of the trusted approach to the delegated approach. Section 2.4.8.2 cited the profile for the delegated mode OCSP responder's certificate.

5.6 RCVS Future Directions

The task of constructing and validating certificate paths can be complex and burdensome for relying parties. The task is more complicated when the certificate path involves cross-certificates. The mechanisms to construct and validate paths generally are part of, or native to, the systems or applications that support relying parties.

A new approach and supporting standards are emerging to provide a server-based service to construct and validate paths. Relying parties can call the service to assist in path construction and validation. The new approach is the Server-Based Certificate Validation Protocol (SCVP)

---

[29] The need for separate private keys could be avoided if the delegating CAs included the same public key in the responder's certificates.

[30] If the responder's certificate were revoked, relying parties would not check its status because of the no-check extension.

[RFC5276]. The DoD PKI PMO will consider and explore the potential use of SCVP within the DoD PKI.

6 Certificate Management System Interface

The CMS provides an interface to the DoD PKI. Applications may request and revoke certificates through this interface. The interface is limited to authorized applications. Information on the interface is not documented here but is available from the DoD PKI PMO once the need for the application and its authorization to use the CMS interface have been duly approved.

The CMS also includes an interface to retrieve information about certificates and their status. This interface is not supported by the DoD PKI and is not authorized for use by applications. The interface may change or be completely shut down without notice by the DoD PKI. The GDS directory provides the repository from which to retrieve certificates and their status.

7 Future Services

The DoD PKI has evolved and will continue to do so. The previous sections described the directions for evolution relative to the existing services. The DoD will consider and implement new services. The services under consideration include:

- Use of Enterprise addresses (e.g., host name) for services. Users will be able to use virtual addresses for the services. The PKI network infrastructure will connect users to one of the specific sites that host the services. Users will not be responsible for selecting one of the specific sites among those offering the services. The Enterprise addresses will be based on global and local load-balancing methods. The DoD PKI has already begun to phase in the use of Enterprise addresses. Enterprise addresses are used to access GDS and RCVS and will eventually be used for most of the DoD PKI services.
- Timestamp Service. This service wraps digital information with a digitally signed timestamp. The Timestamp Authority that adds the timestamp is a trusted third party. The timestamp provides evidence that the digital information existed at the time contained in the timestamp.
- Archival Service. The archival service would provide historical information regarding certificates and their status. The active components of the PKI generally only provide information on certificates that are (or could be) current. The archival services would be used for historical investigations. Information from the archive could assist in determining the validity of a digital signature long after the certificate had expired.[31]
- Path Discovery and Validation. Relying parties currently are responsible for obtaining certificate chains needed to ensure the authenticity and status of an entity's certificate. The effort to obtain and validate a certificate chain becomes more complex in an environment of interoperating PKIs. PKI interoperability is often the result of cross-certifying multiple PKIs. With cross-certification, EE certificates can be involved in multiple chains to different roots or trust anchors. The complexity of the chain processing is also affected by the number of certificate policies asserted in the certificates. Rules may be involved for mapping one organization's policies to those of another organization. A standard for path discovery and validation has emerged [RFC5276]. Provision of services to perform path discovery and validation has the potential to provide consistent and uniform methods for path discovery and validation, and to spare clients from complex processing.

[31] The DoD PKI maintains archives but current retrieval is not fully automated and may require manual processing.

Appendix A Object Identifiers

The major information objects, such as certificates, CRLs, and OCSP requests and responses that the PKI uses or creates, are encoded using the International Telecommunications Union's Abstract Syntax Notation 1 (ASN.1). The standards bodies have provided a mechanism to uniquely name and register objects. The unique names are Object Identifiers (OIDs). Individual standards may define and register new objects. Other standards may reference these objects and include them as components of new objects.

The registry operates as a distributed hierarchy. Authority and responsibility for the administration may be delegated to a subordinate node in the registry. This delegation allows for distributed control and operation of the registry. The registry's branches have taken several directions, to include subject matter domains, geographic regions (e.g., countries), and organizations. Versions of the registry are accessible on the Web (e.g., Object Identifiers Registry[32] and ASN.1 Information Site[33]) although these sites are neither official nor complete.

OIDs have a distinct format. An OID consists of a sequence of numbers separated by a period (.), where the numbers must be between 0 and 16.7 million (2^{24}). The sequence length is unlimited. Each number represents a branch in the tree defined by the preceding numbers. Each proper subsequence represents an object or class of objects. The International Organization for Standardization (ISO) allocated the initial set of numbers. The ISO assigned the initial set to national standards organizations and other organizations. Therefore, OIDs can be allocated by any organization with a unique OID root or arc from which to allocate branches.

OIDs are often represented by either a short or literal form using the number sequence or a long annotated form that adds some textual information. For example, the short form representation for the rsaEncryption object that contains an RSA public key is:

1.2.840.113549.1.1.1

The equivalent long form is:

{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1 }

A shorthand notation is sometimes used for a sequence prefix to avoid repeating the long form. For example, the term pkcs-1 might be created as shorthand for the set of objects defined in RSA Data Security Corporation's Public Key Cryptography Standard (PKCS) 1:

pkcs-1= {iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 }

Then the rsaEncryption object can be referenced as:

{pkcs-1 1 }

---

[32] The URL for the Object Identifiers Registry is http://www.alvestrand.no/objectid/.

[33] The URL for the ASN.1 Information Site is http://asn1.elibel.tm.fr/.

Object Identifiers

A-2

PKI objects make extensive use of OIDs. OIDs are used to denote:

- Certificate and CRL extensions. The extension OID lets users of the certificate or CRL identify the extension and interpret the meaning and content of the extension.
- OCSP request and response extensions.
- Name components for RDNs. Each RDN is an attribute name and value pair (e.g., OU=PKI). The certificate or CRL contains the attribute name's OID rather than the string version of the attribute name.
- Certificate policies.
- Identifiers for encryption algorithms.
- Identifiers for objects containing various encryption keys. Various forms of encryption keys have different formats and components. For example, RSA public keys have two components, a modulus and an exponent.
- Allowed uses for public keys (e.g., EKU extension).
- Objects contained in AIA and SIA extensions.

The remainder of this appendix lists OIDs that are found in DoD PKI objects and are not readily available in standards. Table 65 lists the OIDs. The standards cited in the References include both the OIDs for objects defined in the standard as well as descriptions of the format and content of the objects. Many of the OIDs may be located through the registries mentioned earlier. The IETF's X.509 Public Key Infrastructure Working Group (PKIX) maintains a list of OIDs for their objects (http://www.imc.org/ietf-pkix/pkix-oid.asn).

Table 65: OIDs Used by the DoD PKI

Shorthand Name	Long Form	Use
Organization Arcs		
id-rsadsi	{iso(1) member-body(2) US(840) 113549}	RSA arc
id-microsoft	{iso(1) identified-organization(3) dod(6) internet(1) private(4) enterprises(1) 311}	Microsoft arc
id-entrust	{iso(1) member-body(2) US(840) nortelnetworks(113533) 7}	Entrust arc
id-ansi-x9-62	{iso(1) member-body(2) us(840) ansi-x9-62 (10045) signatures (4)}	ANSI x9-62 arc
pkcs-1	{iso(1) member-body(2) US(840) rsadsi(113549) pkcs(1) 1 }	OIDs defined in RSA's specification for RSA algorithm use [PKCS1]

Shorthand Name	Long Form	Use
id-infosec	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) dod(2) 1}	DoD Infosec arc
id-dod-policies	{id-infosec 11}	DoD certificate policies arc
id-csor	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3)}	NIST's Computer Security Objects Registry arc
id-csor-pki	{joint-iso-ccitt(2) country(16) us(840) organization(1) gov(101) csor(3) 2}	PKI objects under NIST's Computer Security Objects Registry arc
id-certificate-policy	{id-csor-pki 1}	Arc for PKI certificate policies
id-eca-policies	{id-certificate-policy 12}	ECA Policy arc
id-fbca-policies	{id-certificate-policy 3}	FBCA Policy arc (also contains Common Policy certificate policies)
id-pkix	{iso(1) identified-organization(3) dod(6) internet(1) security(5) mechanisms(5) 7}	IETF PKIX arc
PKIX Arcs		
id-mod	{id-pkix 0 }	Modules
id-pe	{id-pkix 1 }	Private certificate extensions
id-qt	{id-pkix 2 }	Policy qualifier types
id-kp	{id-pkix 3 }	Extended key purpose identifiers
id-ad	{id-pkix 48 }	Access descriptors
id-pkix-ocsp	{id-ad 1 }	OCSP-related identifiers and objects

Object Identifiers

Shorthand Name	Long Form	Use
Certificate Extensions		
id-enroll-certtype-extension	{id-microsoft enroll-infra(20) 2}	Microsoft template name extension
id-entrust-version-number	{id-entrust 65 2}	Entrust version number extension
ocsp-no-check	{id-pkix-ocsp 5}	Extension contained in OCSP responder certificates
Encryption Algorithm Identifers and Key Objects		
rsaEncryption	{pkcs-1 1}	Algorithm Identifier for RSA encryption
sha1WithRSAEncryption	{pkcs-1 5}	Algorithm Identifier for digital signatures using SHA-1 hash and RSA encryption
sha256WithRSAEncryption	{pkcs-1 11}	Algorithm Identifier for digital signatures using SHA-256 hash and RSA encryption
sha384WithRSAEncryption	{pkcs-1 12}	Algorithm Identifier for digital signatures using SHA-384 hash and RSA encryption
sha512WithRSAEncryption	{pkcs-1 13}	Algorithm Identifier for digital signatures using SHA-512 hash and RSA encryption
Certificate Policies		
id-US-dod-medium (formerly id-US-dod-class3)	{id-dod-policies 5}	Policy for private keys stored in software
id-US-dod-mediumhardware (formerly id-US-dod-class3hardware)	{id-dod-policies 9}	Policy for private keys stored in hardware (e.g., CAC)
id-US-dod-PIV-Auth (formerly reserved for future use)	{id-dod-policies 10}	Deprecated

Shorthand Name	Long Form	Use
id-US-dod-medium -2048	{id-dod-policies 18}	Policy for 2048-bit private keys stored in software
id-US-dod-mediumhardware-2048	{id-dod-policies 19}	Policy for 2048-bit private keys stored in hardware (e.g., CAC)
id-US-dod-PIV-Auth-2048	{id-dod-policies 20}	Deprecated
id-eca-medium	{id-eca-policies 1}	ECA Medium Assurance Policy with private keys stored in software
id-eca-medium-hardware	{id-eca-policies 2}	ECA Medium Assurance Policy with private keys stored in hardware (e.g., smart card)
id-fpki-certpcy-rudimentaryAssurance	{id-fbca-policies 1}	FBCA Rudimentary Assurance Policy
id-fpki-certpcy-basicAssurance	{id-fbca-policies 2}	FBCA Basic Assurance Policy
id-fpki-certpcy-mediumAssurance	{id-fbca-policies 3}	FBCA Medium Assurance Policy with keys stored in software
id-fpki-certpcy-highAssurance	{id-fbca-policies 4}	FBCA High Assurance Policy
id-fpki-certpcy-testAssurance	{id-fbca-policies 5}	FBCA Test Assurance Policy with keys stored in software
id-fpki-certpcy-mediumHardware	{id-fbca-policies 12}	FBCA Medium Assurance Policy with keys stored in hardware
id-fpki-certpcy-medium-CBP	{id-fbca-policies 14}	FBCA Medium Assurance Policy-Commercial Best Practices with keys stored in software

Object Identifiers

Shorthand Name	Long Form	Use
id-fpki-certpcy-mediumHW-CBP	{id-fbca-policies 15}	FBCA Medium Assurance Policy-Commercial Best Practices with keys stored in hardware
id-fpki-common-policy	{id-fbca-policies 6}	FPKI Common Policy for software-based keys
id-fpki-common-hardware	{id-fbca-policies 7}	FPKI Common Policy for hardware-based keys
id-fpki-common-devices	{id-fbca-policies 8}	FPKI Common Policy for entities
id-fpki-common-authentication	{id-fbca-policies 13}	FPKI Common Policy for individual authentication
id-fpki-common-High	{id-fbca-policies 16}	FPKI Common Policy for High assurance
id-fpki-common-cardAuth	{id-fbca-policies 17}	FPKI Common Policy for authenticating cards
Extended Key Usage (EKU) Identifiers		
anyExtendedKeyUsage	{id-ce-extKeyUsage 0}	Key may used for any purpose in addition to purposes indicated by other EKU OIDs.
id-kp-serverAuth	{id-kp 1 }	Key may be used for TLS/SSL server authentication
id-kp-clientAuth	{id-kp 2 }	Key may be used for TLS/SSL client authentication
id-kp-codeSigning	{id-kp 3 }	Key may be used for signing mobile code or executable modules
id-kp-emailProtection	{id-kp 4 }	Key may be used for signing or encrypting e-mail

Shorthand Name	Long Form	Use
id-kp-smartcard_logon	{id-enroll-certtype-extension 2}	Key may be used to authenticate user with smart card logon
id-kp-OCSPSigning	{id-kp 9 }	Key may be used to sign OCSP responses
id-pkinit-KPClientAuth	{iso(1) org(3) dod(6) internet(1) security(5) kerberosv5(2) pkinit(3) keyPurposeClientAuth(4)}	OBJECT IDENTIFIER ::=
iKEIntermediate	{1.3.6.1.5.5.8.2.2}	Key may be used for IPSec
Access Descriptors For Authority Info Access and Subject Info Authority Extensions		
id-ad-ocsp	{id-ad 1 }	Object is reference for OCSP responder
id-ad-caIssuers	{id-ad 2 }	Object is a reference for the issuing CA's certificate
id-ad-caRepository	{id-ad 5 }	Object is a reference for the issuing CA's certificate
id-ad-timeStamping	{id-ad 3 }	Used when the subject offers timestamping services
OCSP OIDs		
id-pkix-ocsp-basic	{id-pkix-ocsp 1 }	
id-pkix-ocsp-nonce	{id-pkix-ocsp 2 }	
id-pkix-ocsp-crl	{id-pkix-ocsp 3 }	
id-pkix-ocsp-response	{id-pkix-ocsp 4 }	
id-pkix-ocsp-nocheck	{id-pkix-ocsp 5 }	
PIV Objects		
id-piv	{id-csor 6}	Arc for PIV objects

Object Identifiers

Shorthand Name	Long Form	Use
pivFASC-N	{id-piv 6}	Used in the otherName field of the subjectAltName extension in PIV authentication certificates
id-PIV-content-signing	{id-piv 7}	Appears in EKU. Indicates that the public key may be used to verify signatures on PIV CHUIDs and PIV biometrics
id-piv-NACI	{id-piv 9 1}	Certificate extension for National Agency Check with Inquires (NACI)
Other Names		
id-nt_principal_name	{id-enroll-certtype-extension 3}	Microsoft principal name used for smart card logon
id-ntds_replication	{id-microsoft ms-directory-service(25) 1}	Microsoft domain controller GUID
Directory Attributes		
Citizenship	{id-pkix 9 4}	OID for the citizenship attribute

Appendix B DoD PKI URLs

This appendix provides information on how to access information about the DoD PKI and its repositories on the NIPRNet. The remaining sections provide URL references to access the DoD PKI Homepage, the Web browser interface to the DoD PKI directory, and the LDAP interface to the DoD PKI directory, respectively. Appendix D contains information about the DoD PKI on the SIPRNet.

B.1 PKI Home Pages

These URLs provide useful starting points and include links to various resources helpful to DoD PKI users.

http://dodpki.c3pki.chamb.disa.mil

http://dodpki.c3pki.den.disa.mil

B.2 Web Gateway to Directory URLs

Users and developers should use GDS web interface to access the directory. The DoD411 interface can be used to obtain encryption certificates and e-mail addresses for other users. It is available only to users with a DoD PKI certificate. The "crl" interface listed below is available to all users and can be used to retrieve a CRL issued by any of the DoD PKI CAs and their CA certificates (except for certain root CA certificates):

https://dod411.gds.disa.mil

http://crl.disa.mil or https://crl.disa.mil

B.3 Directory LDAP URLs

For most user needs, secure Web (HTTPS) access to GDS will suffice. For applications, LDAP may be the most efficient way to obtain the needed directory data. This section describes how such applications can gain access to certificates and CRLs in the DoD PKI and GDS directories.

A number of LDAP clients are available, each with a unique user interface. The developer is free to determine, from the application documentation, how to configure the particular application using the information provided below. Also, at some point in the future, LDAPS (i.e., LDAP over SSL/TLS) and a DoD certificate will be required to authenticate the client.

The section on directory structure provides information on the Base DN and the attributes maintained in the directory. The host names for the service are the same as those given for the Web interface.

B.4 RCVS URL

The URL for RCVS is:

http://ocsp.disa.mil

Note that this is the URL for the responder. The responder expects to receive OCSP requests. Entering this URL in a Web browser will result in error because there is no OCSP request.

B.5 Root CA Certificate URLs

Each DoD Root CA has a self-signed certificate that serves as the trust anchor for certificates belonging to CAs and EEs with certificates descending from the root CA. Relying parties must have an authentic root CA certificate containing the root CA's public key and must receive the certificate through trusted means. Because of security concerns, the root CA certificate must not be made available over clear, unprotected, unsecured, and non-authenticated links.

Note: The certificate for a root CA can be obtained from an appropriate source. However, being a self-signed certificate, the certificate's integrity must be verified using some trusted means. One approach is to get the thumbprint of the DoD Root CA certificate from a trusted source and verify that the thumbprint of the downloaded root CA certificate is the same as the thumbprint obtained from the trusted source. If one does not do that, the security of the applicable PKI may be compromised.

Desktop administrators within the Services and Agencies will need to ensure that all user desktops have their certificate trust stores updated. A link for a utility called InstallRoot can be used for Microsoft products (Internet Explorer, Outlook, and Internet Information Service) and can be found in the Downloads section of the PKI Enabling Web site at:

https://www.us.army.mil/suite/page/474113

Users not having CAC cards may go to the links at:

http://reg.c3pki.chamb.disa.mil/

or

http://reg.c3pki.den.disa.mil/

Clicking on the "Next" button will lead to a page with three links. One link will install certificates for the P3 Root CA and its subordinate CAs. A second link will install certificates for the new P3.1 Root CA and its subordinate CAs. The third link will install certificates for the External Certification Authority Root CA and External CertificationAuthorities.

The following hashes can be used to verify the correct roots:

Root CA 2: 8C94 1B34 EA1E A6ED 9AE2 BC54 CF68 7252 B4C9 B561

ECA Root: 3A32 EF7B 9AB8 36F8 3718 1A4C EFA3 55C6 4667 ACBF

B.6 ECA Information

Information on the ECA program is available at:

http://iase.disa.mil/pki/eca/documents.html

Appendix C Organizational Units

This appendix provides a list of the OUs that exist at Level 5 of the directory's DIT. These entries are under configuration control. No changes should occur without the approval of the DoD PKI PMO. The OUs may change occasionally. The OUs will likely change when the DoD reorganizes or the OU changes its name. Table 66 lists the PKI OUs. The *Directory Entry* column has the OU name as it appears in the directory. The *Organization* column provides the name of the organization. The *Use* column indicates the current use of the entry. A blank entry in this column indicates the OU is active; new subordinate entries may be added. A *D* in this column indicates that the entry is deprecated. Deprecated OUs have existing subordinate entries, but no new subordinate entries will be added. When any certificates belonging to the subordinate entries expire, renewed certificates will be issued under an active OU. When there are no remaining active subordinate entries, the OU will be deleted.

Table 66: PKI Organizational Units

Directory Entry	Organization	Use
DODIG	Department of Defense Inspector General	
IG[34]	Inspector General	D
JCS[35]	Joint Chiefs of Staff	D
JS	Joint Staff	
OSD	Office of the Secretary of Defense	
	Unified Combatant Commands	
AFRICOM	African Command	
CENTCOM	Central Command	
EUCOM	European Command	
JFCOM	Joint Forces Command	
NORTHCOM	Northern Command	
PACOM	Pacific Command	
SOCOM	Special Operations Command	
SOUTHCOM	Southern Command	
STRATCOM	Strategic Command	

[34] Replaced by DoD Inspector General (DODIG).

[35] Replaced by Joint Staff (JS).

Organizational Units

Directory Entry	Organization	Use
TRANSCOM	Transportation Command	
	Uniform Services	
NOAA	National Oceanic and Atmospheric Administration (non-DoD)	
USA	US Army	
USAF	US Air Force	
USCG	US Coast Guard (non-DoD)	
USMC	US Marines	
USN	US Navy	
USPHS	US Public Health Services (non-DoD)	
	Defense Agencies	
BMDO[36]	Ballistic Missile Defense Office	D
DARPA	Defense Advanced Research Projects Agency	
DCA[37]	Defense Commissary Agency	D
DCAA	Defense Contract Audit Agency	
DCMA	Defense Contract Management Agency	
DeCA	Defense Commissary Agency	
DFAS	Defense Finance and Accounting Service	
DIA	Defense Intelligence Agency	
DISA	Defense Information Systems Agency	
DLA	Defense Logistics Agency	
DLSA	Defense Legal Services Agency	
DSCA	Defense Security Cooperation Agency	
DSS	Defense Security Service	
DTRA	Defense Threat Reduction Agency	

[36] Replaced by Missile Defense Agency (MDA).

[37] OU acronym changed to DeCA.

Directory Entry	Organization	Use
MDA	Missile Defense Agency	
NIMA[38]	National Imagery and Mapping Agency	
NSA/CSS	National Security Agency/Central Security Service	
	DoD Field Activities	
AFIS	American Forces Information Service	
DEA[39]	DoD Education Activity	D
DHRA[40]	DoD Human Resources Activity	
DODEA	DoD Education Activity	
DODHRA[41]	DoD Human Resources Activity	D
DPMO	Defense Prisoner of War/Missing Personnel Office	
DTSA	Defense Technology Security Administration	
OEA	Office of Economic Adjustment	
TMA	Tricare Management Activity	
WHS	Washington Headquarters Services	
	Other Government Agencies	
CIA	Central Intelligence Agency	
DHS	Department of Homeland Security	
DNI	Director of National Intelligence	
DOE	Department of Energy	
DOJ	Department of Justice	
DOS	Department of State	
TREA	Treasury Department	

[38] Replaced by National Geospatial-Intelligence Agency (NGA).

[39] Renamed to DODEA.

[40] Older certificates may have the acronyms HRA or DODHRA.

[41] Older certificates may have the acronym HRA.

Organizational Units

Directory Entry	Organization	Use
	Other Organizational Units	
CONTRACTOR	Contractors	
CCEB	Combined Communications-Electronics Board	
OTHER	Other Organizations	

Appendix D PKI on the SIPRNet

D.1 SIPRNet PKI

The DoD PKI is available on both the Unclassified Internet Protocol Router Network (NIPRNet) and the Secret Internet Protocol Router Network (SIPRNet). The Root CAs are common to the PKI components of both networks. The remaining PKI components, such as the signing CAs, directories, and RCVS, are dedicated to one network or the other. PKI components on one network cannot access components on the other. Users and systems connected to one network do not have access to PKI components on the other network. The two PKI segments have a common architecture. Components on the different networks use the same products and have the same interface functions. Because the NIPRNet's user population is much larger than that of the SIPRNet, there are some differences in the scale of the PKI components operating on the two networks. For example, there are fewer signing CAs operating on the SIPRNet relative to the number operating on the NIPRNet.

Until this appendix, this document did not distinguish between the NIPRNet and SIPRNet components. However, specific references, such as signing CA names and URLs, referred to NIPRNet components. SIPRNet signing CAs and URLs are different from their NIPRNet counterparts. SIPRNet signing CA's CNs are identical to those for NIPRNet except that a SIPRNet CA's CN format has the acronym *SIPRNet* immediately following the acronym *DoD* in the NIPRNet CN format. URLs for SIPRNet-resident PKI components are the same as those for NIPRNet except that the SIPRNet host name portion of the URL ends in *.smil.mil* in place of just *.mil* in the corresponding NIPRNet URL.

Individuals holding SIPRNet certificates generally will also have separate NIPRNet certificates. Individual software certificates issued for use on SIPRNet assert only the *id-US-dod-medium* (software) certificate policy. CAC cards with their hardware-based keys cannot be used on the SIPRNet. A separate SIPRNet hardware token similar to but different from the CAC may be issued. This token will have the hardware certificate policy *id-US-dod-mediumHardware*.

The SIPRNet PKI only produces core DoD certificates. There are no SIPRNet counterparts for the FBCA or the ECA.

The PKI objects produced on the SIPRNet PKI are inherently Unclassified. However, because they reside on the SIPRNet, PKI objects must adhere to specific procedures for downgrading media containing the objects to ensure that there is no residual classified information on the media and that no malicious software has modified the object so that it contains classified information.

D.2 National (NSS) PKI

The SIPRNet PKI transitioned to the National Security Systems (NSS) PKI. NSS PKI supports interoperability of Secret-Collateral information and communications systems among various Federal organizations. The NSS PKI is hierarchical and will have a Root CA. Cross-certificates may be used to assist the evolution of existing agency PKIs into the unified NSS PKI. Participating agencies, including the DoD, will likely operate CAs that are subordinate to the NSS PKI Root CA. The subordinate CAs will issue certificates to other CAs and EEs that

D-2 the respective agencies operate. Separate documents will describe the NSS PKI and its DoD component interfaces.

Glossary

AIA	Authority Information Access
AKI	Authority Key Identifier
ANSI	American National Standards Institute
ARL	Authority Revocation List
ASN.1	Abstract Syntax Notation 1
BC	Basic Constraints
BCD	Binary Coded Decimal
C	Country
C/S/A	Combatant Command, Service, and Agency
CA	Certification Authority
CAC	Common Access Card
CDP	CRL Distribution Point
CertID	Certificate ID
CHUID	Cardholder Unique Identifier
CMS	Certificate Management System
CN	Common Name
CP	Certificate Policies
CPS	Certification Practice Statement
CRL	Certificate Revocation List
DC	Domain Controller
DER	Distinguished Encoding Rules
DISA	Defense Information Systems Agency
DIT	Directory Information Tree
DN	Distinguished Name
DNS	Domain Name Service
DoD	Department of Defense
DTM	Distributed Trust Model
ECA	External Certification Authority
ECC	Elliptic Curve Cryptography
EDIPI	Electronic Data Interchange-Person Identifier
EE	End Entity
EKU	Extended Key Usage
FASC-N	Federal Agency Smart Credential Number
FBCA	Federal Bridge Certification Authority
FIPS	Federal Information Processing Standard
FPKI	Federal Public Key Infrastructure
GDS	Global Directory Service
GMT	Greenwich Mean Time
GUID	Globally Unique Identifier
GZIP	GNU ZIP
HSPD-12	Homeland Security Presidential Directive 12
HTTP	HyperText Transfer Protocol
IAN	Issuer Alternative Name
IETF	Internet Engineering Task Force

Infosec	Information Security
IP	Internet Protocol
IPSec	Internet Protocol Security
IRCA	Interoperability Root CA
ISO	International Organization for Standardization
ITU	International Telecommunication Union
KU	Key Usage
LDAP	Lightweight Directory Access Protocol
LDAPS	LDAP over SSL
LRA	Local Registration Authority
NACI	National Agency Check with Inquires
NC	Name Constraints
NIPRNet	Unclassified Internet Protocol Router Network
NIST	National Institute of Standards and Technology
NPE	Non-Person Entity
NSA	National Security Agency
NSS	National Security Systems
O	Organization
OCSP	Online Certificate Status Protocol
OID	Object Identifier
OU	Organizational Unit
P3	Profile 3
P3.1	Profile 3.1
P3.2	Profile 3.2
P3.3	Profile 3.3
PC	Policy Constraints
PIV	Personnel Identification Verification
PKCS	Public Key Cryptography Standard
PKI	Public Key Infrastructure
PKIX	X.509 Public Key Infrastructure Working Group
PM	Policy Mapping
PMO	Program Management Office
RA	Registration Authority
RCVS	Robust Certificate Validation Service
RDN	Relative Distinguished Name
RFC	Request for Comments
RSA	Rivest-Shamir-Adleman
SAN	Subject Alternative Name
SCVP	Server-Based Certificate Validation Protocol
SDA	Subject Directory Attributes
SHA-1	Secure Hash Algorithm-1
SHA-256	Secure Hash Algorithm-256
SIA	Subject Information Access
SIPRNet	Secret Internet Protocol Router Network
SKI	Subject Key Identifier
SOA	Service-Oriented Architecture

SSL	Secure Sockets Layer
SSN	Social Security Number
TLS	Transport Layer Security
UID	Universal Identifier
UPN	User Principal Name
URI	Uniform Resource Identifier
URL	Uniform Resource Locator
UTC	Coordinated Universal Time
UTF8	Unicode Transformation Format-8

List of References

[ECA] External Certification Authority Homepage. *ECA Program PKI Program.* September 2, 2009. (http://iase.disa.mil/pki/eca/[accessed December 16, 2009])

[FPKI] National Institute of Standards and Technology. *Federal Public Key Infrastructure (PKI) X.509 Certificate and CRL Extensions Profile.* Gaithersburg, MD. October 12, 2005. (http://www.cio.gov/fpkipa/documents/fpki_certificate_profile.pdf)

[FBCA] Federal Bridge Certification Authority Homepage. FBCA Program. (http://www.cio.gov/fbca/)

[FBCACP] Federal Public Key Infrastructure Policy Authority. "X.509 Certificate Policy For The Federal Bridge Certification Authority (FBCA) Version 2.13." *Federal Public Key Infrastructure Architecture.* December 10, 2009. (http://www.idmanagement.gov/fpkipa/documents/FBCA_CP_RFC3647.pdf [accessed December 28, 2009])

[FIPS201] National Institute of Standards and Technology, FIPS Pub 201-1. *Personal Identity Verification (PIV) of Federal Employees and Contractors.* June 23, 2006. (http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf [accessed December 21, 2009])

[FPKICP] Federal Public Key Infrastructure Policy Authority. *X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework.* January 21, 2010. (http://www.idmanagement.gov/fpkipa/documents/CommonPolicy.pdf [accessed March 2, 2010])

[HSPD-12] HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors.* August 27, 2004.

[ISO3166] English Country Names and Code Elements. 2009. (http://www.iso.org/iso/country_codes/iso_3166_code_lists/english_country_names_and_code_elements.htm [accessed December 18, 2009])

[NSA-B] National Security Agency. *NSA Suite B Cryptography.* November 2, 2009. (http://www.nsa.gov/ia/programs/suiteb_cryptography/index.shtml [accessed December 21, 2009]).

[PKCS 1] RSA Laboratories. *PKCS #1: RSA Encryption Standard.* Version 1.5. November 1993.

[PKI-IF] Defense Information Systems Agency, *Department of Defense Class 3 Public Key Infrastructure Interface Specification, Version 2.0.* June 2007.

[RFC1738] Berners-Lee, T., L. Masinter, and M. McCahill. RFC 1738, *Uniform Resource Locators (URL).* Internet Engineering Task Force. December 1994. (http://www.ietf.org/rfc/rfc1758.txt)

[RFC2560] Myers, M., R. Ankney, A. Malpani, S. Galperin, and C. Adams. RFC 2560, *X.509 Internet Public Key Infrastructure Online Certificate Status Protocol – OCSP.* Internet Engineering Task Force. June 1999. (http://www.ietf.org/rfc/rfc2560.txt)

List of References

[RFC2585] Housley, R., P. Hoffman. RFC 2585, *Internet X.509 Public Key Infrastructure Operational Protocols: FTP and HTTP*. Internet Engineering Task Force. May 1999. (http://www.ietf.org/rfc/rfc2585.txt)

[RFC2797] Myers, M., X. Liu, J.Schaad, and J. Weinstein. RFC 2797, *Certificate Management Messages over CMS.* Internet Engineering Task Force. April 2000. (http://www.ietf.org/rfc/rfc2797.txt)

[RFC4158] Cooper, M., Y. Dzambasow, P. Hesse, S. Joseph, and R. Nicholas. RFC 4158, *Internet X.509 Public Key Infrastructure: Certification Path Building*, Internet Engineering Task Force, September 2005. (http://www.ietf.org/rfc/rfc4158.txt)

[RFC4510] Zeilenga, K. RFC 5410, *Lightweight Directory Access Protocol (LDAP): Technical Specification Road Map.* Internet Engineering Task Force, June 2006. (http://www.ietf.org/rfc/rfc4510.txt)

[RFC4523] Zeilenga, K. RFC 5423, *Lightweight Directory Access Protocol (LDAP) Schema Definitions for X.509 Certificates.* Internet Engineering Task Force, June 2006. (http://www.ietf.org/rfc/rfc4523.txt)

[RFC4809] Bonnati, C., S. Turner, G. Lebovitz. *Requirements for an IPsec Certificate Management Profile*. (http://tools.ietf.org/rfc/rfc4809 [accessed December 18, 2009]))

[RFC5276] Freeman, T., R. Housley, A. Malpani, D. Cooper, and W. Polk. RFC 5276, *Server-Based Certificate Validation Protocol (SCVP).* Internet Engineering Task Force. December 2007. (http://www.ietf.org/rfc/rfc5276.txt)

[RFC5280] Housley, R., W. Polk, W. Ford, and D. Solo, RFC 3280, *Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile*. January 1999. (http://www.ietf.org/rfc/rfc5280.txt)

[SEP] *Department of Defense (DoD) Public Key Infrastructure (PKI) Systems Engineering Plan (SEP) Milestone B Increment 1*. July 12, 2006.

[SP800-131] Barker, E., and A. Roginsky. NIST Special Publication 800-131, *Recommendation for the Transitioning of Cryptographic Algorithms and Key Sizes.* Computer Security Division, Information Technology Laboratory, National Institute of Standards and Technology. January 2010. (http://csrc.nist.gov/publications/drafts/800-131/draft-800-131_transition-paper.pdf)

[X.500] ITU-T Recommendations X.500 (1993) | ISO/IEC 9594-1:1994, *Information Technology - Open Systems Interconnection - The Directory: Overview of concepts, models and services.*

[X.509] ITU-T Recommendation X.509, *Information Technology - Open Systems Interconnection - The Directory: Authentication Framework.* International Telecommunication Union. June 1997.