Department of Defense
Public Key Infrastructure

DoD Approved External PKIs
Master Document

Version 11.1

July 16, 2024

Prepared for:

DoD PKI Program Management Office
9800 Savage Road
Suite 6738
Fort George G. Meade, MD 20755-6718

Prepared by:

Booz Allen Hamilton
8283 Greensboro Drive
McLean, Virginia 22102

Revision Page

Date	Version	Change Description
6/7/2011	1.0	Release 1.0
8/18/2011	1.1	Updated Treasury and ORC SSP sections, updated Department of State assurance level section, incorporated text comments, added additional VeriSign ECA CA, and added VeriSign NFI and ActivIdentity, Inc. NFI as a DoD approved PKIs.
10/05/2011	1.2	Added Citi NFI PKI and new DOD CAs 27-30 and DOD EMAIL CAs 27-30.
11/04/2011	1.3	Added Entrust NFI PKI as a DoD Approved External PKI
01/05/2012	2.0	Added Verizon Business NFI PKI as a DoD Approved External PKI Removed expired DoD [EMAIL] CAs 11,12,14
04/27/2012	2.1	Added ORC NFI PKI as a DoD Approved External PKI Removed expired DoD [EMAIL] CA 13 Removed expired Treasury Root CA and 3 Issuing CAs (OCIO, Fiscal, Treasury Public)
06/22/2012	2.2	Added new SHA-256 Dept. of State CA and updated Assurance Level information Added Boeing PKI as a DoD Approved External PKI Removed expired DoD [EMAIL] CA 15-18 and expired Entrust SSP SHA-1 chains
08/01/2012	2.3	Removed ActivIdentity NFI PKI as a DoD Approved External PKI Updated VeriSign NFI SHA-256 chain with US Senate and Millennium PIV-I CAs
02/13/2013	2.4	Added content for DoD [EMAIL] CA 31-32 and NPE CA 1-2 Updated VeriSign NFI PKI SHA-256 chain with Booz Allen and CSC SHA-256 PIV-I CAs Replaced expired Exostar FIS Certificate Authority
03/25/2013	2.5	Added Netherlands Ministry of Defence PKI as a DoD Approved External PKI
05/28/2013	3.0	Added Australian Defence Organisation (ADO) PKI as a DoD Approved External PKI Added content for DoD CCEB Interoperability Root CA 1
07/01/2013	3.1	Removed Citi NFI PKI as a DoD Approved External PKI Added content for Exostar FIS Signing CA 2 Issuing CA
09/05/2013	3.2	Renamed VeriSign NFI and SSP to Symantec NFI and SSP Updated Symantec NFI PKI SHA-256 chain with Eid Passport – RAPIDGate PIV-I CA
11/06/2013	3.3	Added content for HHS Intermediate CA under Entrust SSP Added content for Veterans Affairs Issuing CA under Treasury SSP Removed expired Treasury OCIO Issuing CA
01/01/2014	4.0	Removed expired SHA-1 content from ORC SSP and Symantec NFI/SSP PKIs.
02/20/2014	4.1	Added content for IdenTrust ECA 4
03/24/2014	4.2	Added content for Symantec Client ECA – G4 Added new Federal PKI Policy OID: id-fpki-common-piv-contentSigning
05/06/2014	4.3	Removed expired CAs: DoD [EMAIL] CA 19-20 and IdenTrust ECA 2. Updated CCEB IRCA 1 > ADOCA03 cross certificate Added content for additional Raytheon SHA-1 trust chain
06/10/2014	4.4	Added content for ORC ECA HW 5, ORC ECA SW 5, and ADOCA016 Removed expired content for ORC ECA HW 3 and ORC ECA SW 3

Revision Page (continued)

Date	Version	Change Description
07/01/2014	4.5	Added Exostar SHA-256 PKI as a DoD Approved External PKI, Removed expired content for VeriSign Client ECA – G2 Removed FPKI SHA-1 Authentication and CardAuth OIDs Removed SHA-1 OIDs from Symantec NFI and SSP, and Verizon Business SSP
08/01/2014	4.6	Added Cassidian NFI PKI as a DoD Approved External PKI Removed Exostar SHA-1 PKI as a DoD Approved External PKI Replaced ORC Root 2 with the Federal Common Policy CA (FCPCA) as trust anchor for ORC SSP Removed ORC SSP Inherited Policies from ORC Root 2
08/22/2014	4.6.1	Added Eid Passport – RAPIDGate Premier Issuing CA (Symantec NFI)
02/02/2015	4.7	Removed expired CAs: DoD [EMAIL] CA 21-24 and ADOCA014
06/01/2015	5.0	Added content for DoD Root CA 3 and ECA Root CA 4 Added Northrop Grumman SHA-256 PKI as DoD Approved External PKI Added content for NRC Issuing CA (Symantec SSP) Added new FPKI OIDs: id-fpki-common-pivAuth-derived and id-fpki-common-pivAuth-derived-hardware Removed expired Raytheon trust chain
07/01/2015	5.1	Added content for re-keyed Treasury issuing CAs (DHS, NASA, OCIO, SSA)
09/04/2015	5.2	Added content for Raytheon SHA-256 PKI
11/13/2015	5.3	Added content for DoD [ID | SW] [EMAIL] CAs 33-38 and ORC ECA 6. Removed content for Cassidian/Airbus (decommissioned)
12/04/2015	5.4	Added content for DoD [ID] [EMAIL] CAs 39-44
01/12/2016	5.5	Added content for Carillon Federal Services PKI Removed expired content for DoD [EMAIL] CA 25-26
01/26/2016	5.6	Added content for re-keyed Entrust SSP PKI chain
03/16/2016	5.7	Added content for DoD ID SW CAs 45-46 and IndenTrust NFI (IdenTrust Root and Booz Allen PIV-I CAs)
04/18/2016	5.8	Added content for DoD Root CA 4, DoD ID SW CAs 47-48, and IndenTrust ECA 5. Updated Lockheed Martin Assurance Level section.
05/18/2016	5.9	Added content for Lockheed Martin SHA-256, CSRA (Symantec NFI), Treasury Fiscal Service Issuing CA (re-keyed), IdenTrust ECA S21, and ORC NFI 3. Removed expired Treasury Fiscal Service Issuing CA. Added TSCP SHA-256 Assurance Levels.
07/21/2016	6.0	Added content for DoD Root CA 5, IdenTrust ECA Component S21 and CSRA Device CA. Updated ORC NFI PKI assurance levels.
01/18/2017	6.1	Added content for DoD CAs 49-58, DoD CCEB Interoperability Root CA 2, Boeing SecureBadge Medium-G2, and Carillon Federal Services PIV-I CA 2. Updated ADOCA03 > ADOCA016 cross cert. Removed DoD Intermediate CA 1-2 (decommissioned) and NASA Operational CA-serial 0x443EA7E9 (expired)
04/25/2017	6.2	Added SureID Issuing CA (Symantec NFI). Updated CCEB Interoperability Root CA 1 → ADOCA03 cross certificate. Removed expired IdenTrust ECA 3, NASA Operational CA-(serial 0x45F94AB5), and SSA Issuing CA serial 0x45F94AA3)

Revision Page (continued)

Date	Version	Change Description
03/05/2018	6.3	Updated content for Lockheed Martin SHA-256 (CertiPath Bridge). Added content for ADO SHA-256 PKI. Removed expired DoD [EMAIL] CA 27-30, ORC ECA HW4, ORC ECA SW4, Verisign ECA-G3, Lockheed Martin SHA-1, Millennium Challenge Corp, ICF International, DHS CA-4, Dept. of Transportation G3, Naval Reactors G2, and HHS SSP CA B7. Removed Symantec ECA G4 (no longer an approved ECA vendor)
09/17/2018	6.4	Added WidePoint ORC ECA 7 and Senate PIV-I CA G4. Updated CCEB IRCA 2 → ADO Interop CA cross certificate. Removed expired NRC SSP Agency CA G2, Veterans Affairs User CA B1, Executive Office of the President CA-B4, Senate PIV-I CA G2 (SHA-1), and Northrop Grumman Corporation SHA-1 chain. Removed decommissioned DoD NPE CAs 1-2. Updated table in Section 5.1. Updated assurance levels for ORC NFI.
11/28/2018	6.5	Added re-keyed U.S. Department State AD Root and HA CAs, and the new PIV CA2. Other minor edits.
01/22/2019	6.6	Added DoT SSP Agency CA Trust Chain which includes previously unapproved Symantec SSP intermediate CA – G4. Removed expired DoD [EMAIL] CAs 31-32, Verizon Business issuing CA (CN=CT-GEN-MSO-CA-B1), ADO SHA-1 chain, U.S. Treasury Fiscal Service CA (serial 0x46EACEA1), and Boeing SecureBadge Medium G2 (serial 0x611EEB96000000000006)
04/25/2019	7.0	Removed links that no longer work. Updated link for DoD Certificate Policy URL. Added content for re-keyed Entrust SSP HHS-FPKI Intermediate CA-E1 (serial 0x44809a90). Removed expired CN=ORC NFI CA 2 certificate (serial 0xEE7CAF3AC34501FD7E415A88A0C4BF51) Removed expired Entrust SSP PKI Trust Chain 2 Adding CN=Veterans Affairs User CA B1 Trust Chain (serial 0x251ea36536cfebb0e9d1334d0cb96102bab16589) Added content for re-keyed Entrust Managed Services NFI Trust Chain #2 (serial 0x4aa8a60d and 0x4aa8b9ea) Updated information for DoD Root CA 5 Added content for DoD [ID | EMAIL | SW] CAs 59-61 Added PIV Content Signing OIDs for Verizon Business SSP
06/10/2019	7.1	Added content for IdenTrust ECA Component S22 and IdenTrust ECA S22C
08/07/2019	7.2	Added content for Boeing SHA-256 Trust Chain Removed expired Symantec NFI CA certs: RAPIDGate PIV-I Agency CA, CSC CA-2, Booz Allen Hamilton CA 02. These certificates were not renewed. Updated all IASE links to new Cyber Exchange website
08/27/2019	7.3	Added NASA chain Updated DoD Assurance Levels Table Updated Symantec SSP PKI Asserted Policies Table Removed expired Entrust NFI Medium Assurance SSP CA and Fiscal Service CA (Treasury SSP PKI)

Revision Page (continued)

Date	Version	Change Description
12/23/2019	8.0	Removed SHA-1 content, including assurance level information since DoD no longer is accepting SHA-1 certificates as of November 15, 2019. Removed expired U.S. Department of State PIV CA Removed expired Entrust Managed Service NFI Root CA Updated SSP and NFI names to match the official FPKI listings Removed Verizon Business NFI CA Updated Rekeyed Entrust Managed Services Root and SSP CA
05/22/2020	8.1	Added content for new Netherlands Ministry of Defence PKI-G3 (NL MoD PKI-G3). Moved NL MoD PKI to Category III since DoD CIO determined the PKI is an "Other Mission Partner PKI," as defined in DoDI 8520.02. Added content for new VA and DHS Issuing CAs (Treasury SSP) and Dept. of State PIV CA2 issuing CA. Remove expired NL MoD PKI-G2 chain. Updated Assurance Levels for Dept. of State, Treasury SSP, and NL MoD.
08/24/2020	8.2	Updated ADO Interoperability CA → ADO Public Identity and Public Device CA cross certificates
09/10/2020	8.3	Re-adding Entrust SSP Issuing CA – Rekey #2 to Trust Chain #1
10/06/2020	8.4	Added new WidePoint NFI trust chain
01/22/2021	8.5	Added DoD DERILITY CA-1 (DoD Root CA 3) Removed the following expired certificates: ORC SSP3 (WidePoint Federal SSP), DHS CA4 (Treasury Trust Chain 1), NASA Operational CA (Treasury Trust Chain 1), OCIO CA (Treasury Trust Chain 1), Fiscal Service CA (Treasury Trust Chain 1), Treasury Public CA (Treasury Trust Chain 1), DigiCert NFI PKI Trust Chain 1, Verizon/Cybertrust Federal SSP Trust Chain 1. Removed deprecated DoD PIV-Auth OIDs from DoD Assurance Level section. Added PIV-Auth-derived OIDs to Federal PKI Assurance Level Section
04/20/2021	8.6	Added DoD ID CA-63 (DoD Root CA 3), Exostar Federated Identity Service Signing CA 4, and Raytheon Class 3 G3 Trust Chain
05/24/2021	8.7	Removing ORC reference in section 4.2. Replaced Federal Common Policy CA G2 trust anchor for WidePoint SSP, DigiCert SSP, Symantec SSP, and Verizon SSP.
06/15/2021	9.0	Added DoD EMAIL 62-65, DoD ID 62, 64-65 and DoD SW 66-67 (DoD Root CA 3)
07/08/2021	9.1	Added WidePoint ECA 8 Added PIV-Auth and PIV-Auth-2048 back to DoD Assurance Levels section. Although OIDs are to be deprecated, DoD CP v10.7 has not been approved at the time this document was published. Corrected Assurance Levels sections for Entrust SSP, Dept of State, Treasury, DigiCert SSP to accurately reflect DoD approved OIDs

Revision Page (continued)

Date	Version	Change Description
11/19/2021	9.2	Added WidePoint ORC NFI 4, U.S. Department of Transportation Agency CA G5, and Carillon Federal Services PKI PIV-I CA 1 (Trust Chain 1) and Carillon PKI Services (Trust Chain 2) Updated DoD CCEB Interoperability Root CA-2 → Australian Defence Interoperability CA cross certificate. Removed the following CAs since they have expired: DoD SW CAs 37-38, DoD [ID | EMAIL] CAs 41-44, WidePoint ORC ECA 6, and ORC NFI CA 3 (issued by ORC Root 2). Removed ORC Root 2 since it's no longer cross certified with FBCA-G4 and has no active subordinate CAs. Updated Assurance Levels for Raytheon, DigiCert Federal SSP, and Carillion Federal Services
05/10/2022	9.3	Updated Assurance Levels for DigiCert NFI and Australia Defence Organisation Removed the following CAs since they have expired: DoD ID SW CAs 45-48, IdenTrust ECA S21, and US Dept. of State High Assurance CA (Trust Chain 1) Added new content for IdenTrust ECA 23 and ECA Component S23
6/23/2022	9.4	Added new content for DigiCert NFI PKI Trust Chain 2 Removed expired IdenTrust ECA Component S23
7/29/2022	9.4.1	Added Raytheon SHA-2 arc OIDs
10/18/2022	9.5	Added new content for Australian Defence Public Identity G2 CAs
01/18/2023	9.6	Added content for DoD [ID|EMAIL] CA 71 and SW CAs 68, 69, 75 Removed retired/expired DoD CAs 49-58 Renamed Carillon Federal Service – Trust Chain 2 to Carillon Information Security PKI Added content for Lockheed Martin PKI Trust Chain 2 Identified Public Key and Signature Algorithms for all CA certificates
03/01/2023	10.0	Added content for DoD Root CA 6 Separated Carillon Federal Services and Information Security PKI Assurance Levels into separate sections Other minor edits

Revision Page (continued)

Date	Version	Change Description
07/24/2023	10.1	Added/updated content for the following CAs: • DoD Root CA 5 - DoD SW CAs 76-77 • DoD Root CA 6 – DoD [ID|EMAIL] CAs 70, 72, 73 and DoD SW CA 74 • Northrop Grumman Corporate Root CA (RSA4096/SHA-384) • Northrop Grumman Corporate Signing CA (RSA3072/SHA-384) • ADO Interoperability CA → ADO Public Identity and Public Device CA cross certificates Removed content for the following expired CAs • WidePoint NFI PKI - ORC NFI CA 3 • Raytheon PKI, Trust Chain 1 – Raytheon Root CA-G2, Raytheon Class 3 MASCA (**NOTE:** Although Raytheon Root CA-G2 is not expired, there are no active issuing CAs and Raytheon Root CA-G3 is now the preferred Root CA)
10/18/2023	10.2	Added content for DOD DERILITY CA 3-4 (DoD Root CA 6) and U.S. Senate PIV-I CA G6 (WidePoint NFI)
05/13/02024	11.0	Added content for the following CAs: • ECA Root CA 5 • WidePoint ECA 9 (ECA RSA4096/SHA-384 Subordinate CAs) Removed content for the following expired CA: • Exostar Federated Identity Service Signing CA 3
07/16/2024	11.1	Replaced legacy PKI categories with the new 6 PKI types Removed expired WidePoint ORC ECA 7 Added/updated content for the following: • DoD CCEB Interoperability Root CA-2 → Australian Defence Interoperability CA cross certificate. • WidePoint SSP Intermediate CA • U.S. Department of Transportation Agency CA G6 • Rekeyed Entrust Managed Services Root and SSP CA (Trust Chain 3)

Table of Contents

1.0 Introduction

This document provides Certification Authority (CA) certificate trust chain and assurance level information for all Department of Defense (DoD) approved Public Key Infrastructures (PKIs). DoD Chief Information Officer (CIO) is the governing authority for DoD approved external PKIs. Prior to 2008, the only DoD approved external PKI was the DoD-managed External Certification Authority (ECA) program PKI. On May 24, 2011, DoD CIO released Department of Defense Instruction (DoDI) 8520.02 authorizing PKI interoperability with DoD approved external PKIs The DoD External Interoperability Plan describes the criteria and process for DoD approved external PKIs and is available on the DoD authoritative external Interoperability site https://cyber.mil/pki-pke/interoperability. DoD approved PKIs must conform to all criteria stated in the DoD External Interoperability Plan to include cross certification with the Federal PKI (FPKI) at Federal Bridge Certification Authority (FBCA) medium hardware assurance level or higher and successful completion of Joint Interoperability Test Command (JITC) testing[1]. DoD organizations that wish to interoperate with DoD approved external PKIs must comply with DoD Instruction 8520.02.[2] DoD relying parties may interoperate using cross-certificate trust or direct trust. If interoperating using direct trust, DoD relying parties must ensure that they are only accepting PKI credentials that meet the FBCA medium hardware assurance level restriction.[3] In addition to PKI authentication and validation, administrators should ensure that DoD information systems are performing access control.[4]

[1] The DoD Partner PKI Interoperability test plan is located on the external interoperability site at https://dl.cyber.mil/pki-pke/pdf/unclass-jitc_partner_pki_evaluation_test_plan_v2.pdf
[2] DoDI 8520.02 is available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852002p.pdf
[3] For more information on Assurance Levels, see Section 5.
[4] DoDI 8520.03 is available at https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/852003p.pdf

2.0 DoD PKI Trust Chains

DoD PKI began as a medium assurance pilot in 1998 and has since evolved to a heavily operationalized PKI with over 4.5 million subscribers. DoD currently has over 30 issuing CAs that issues both hardware and software certificates at various assurance levels. DoD most commonly distributes CA certificates with the PKE InstallRoot utility.[5] It also has CA certificates which support cross-certificate interoperability with its Federal, industry, and international partners which are not included in the base InstallRoot package.

2.1 DoD Trust Anchors

2.1.1 DoD Root CA 3

DoD Root CA 3 is the primary RSA2048/SHA-256 DoD trust anchor for which all DoD SHA-256 end entity and issuing CA certificates should be validated against. This trust anchor has issued DoD CAs 59-60, 62-67, 71, 75,and DoD DERILITY CA-1.

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Mar 20 18:46:41 2012 GMT
Valid To	Dec 30 18:46:41 2029 GMT
SHA-1 Print	D7:3C:A9:11:02:A2:20:4A:36:45:9E:D3:22:13:B4:67:D7:CE:97:FB

2.1.2 DoD Root CA 4

DoD Root CA 4 is the primary ECC p256/SHA-256 DoD trust anchor for which all DoD ECC p256/SHA-256 end entity and issuing CA certificates should be validated against. Currently, there are no active subordinate CA certificates.

TRUST ANCHOR (ECC-p256/SHA256)	
Issuer	CN=DoD Root CA 4,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Root CA 4,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Jul 30 19:48:23 2012 GMT
Valid To	Jul 25 19:48:23 2032 GMT
SHA-1 Print	B8:26:9F:25:DB:D9:37:EC:AF:D4:C3:5A:98:38:57:17:23:F2:D0:26

2.1.3 DoD Root CA 5

DoD Root CA 5 is the primary ECC p384/SHA-384 DoD trust anchor for which all DoD ECC p384/SHA-384 end entity and intermediate CA certificates should be validated against. This trust anchor has issued DoD SW CAs 61, 68, 69, 76, and 77.

TRUST ANCHOR (ECC-p384/SHA384)	
Issuer	CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0F
Valid From	Jun 14 17:17:27 2016 GMT
Valid To	Jun 14 17:17:27 2041 GMT
SHA-1 Print	4E:CB:5C:C3:09:56:70:45:4D:A1:CB:D4:10:FC:92:1F:46:B8:56:4B

[5] InstallRoot is available on the Cyber Exchange PKE site at https://cyber.mil/pki-pke/tools-configuration-files/

2.1.4 DoD Root CA 6

DoD Root CA 6 is the primary RSA4096/SHA-384 DoD trust anchor for which all DoD SHA-384 end entity and issuing CA certificates should be validated against. This trust anchor has issued DoD [ID|EMAIL] CAs 70, 72, 73, DoD SW CA 74, and DoD DERILITY CAs 3-4.

TRUST ANCHOR (RSA4096/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Jan 24 16:36:17 2023 GMT
Valid To	Jan 24 16:36:17 2053 GMT
SHA-1 Print	D3:7E:CF:61:C0:B4:ED:88:68:1E:F3:63:0C:4E:2F:C7:87:B3:7A:EF

2.1.5 DoD Interoperability Root CA 2

DoD Interoperability Root CA 2 is the RSA2048/SHA-256 DoD trust anchor for cross-certificate trust with SHA-256 Federal and Industry partner PKIs. For applications that do not support cross-certificate trust, the direct trust chains will also be posted. However, application owners that interoperate using direct trust will need to implement separate checks to ensure that only certificates with DoD approved PKI certificate policy OIDs are accepted for authentication. Additionally, direct trust application owners will need to remove the partner PKI trust anchors in the event of a compromise since they will be unable to rely upon a revocation by DoD.

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=DoD Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DoD Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Nov 29 14:25:10 2010 GMT
Valid To	Nov 24 14:25:10 2030 GMT
SHA-1 Print	52:2E:1B:F5:BE:15:2F:A9:8B:ED:4F:01:AA:44:1D:01:09:2D:5A:31

2.1.6 DoD CCEB Interoperability Root CA 2

US DoD CCEB Interoperability Root CA 2 is the RSA2048/SHA-256 DoD trust anchor for cross-certificate trust with the SHA-256 Combined Communications-Electronics Board (CCEB) partner National Defense PKIs. Since the preferred method of certificate path processing is cross-certificate trust, cross certificate trust chains will be published. Additionally, for applications that do not support cross-certificate trust, the direct trust chains will also be posted. However, application owners that interoperate using direct trust will need to ensure extra precautions are in place to ensure that only certificates with DoD approved PKI certificate policy OIDs are accepted for authentication. Additionally, direct trust application owners will need to remove the CCEB partner PKI trust anchors in the event of a compromise since they will be unable to rely upon a revocation by DoD. Since CCEB is a Category III PKI, the trust chains will be listed in Section 5.4, *Foreign, Allied, or Coalition Partner PKIs or other PKIs*.

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=US DoD CCEB Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=US DoD CCEB Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Aug 23 13:57:10 2016 GMT
Valid To	Dec 30 13:57:10 2030 GMT
SHA-1 Print	73:A7:1C:9F:68:03:BA:8C:0E:2B:7A:28:A5:C4:8F:87:2C:67:97:E2

2.2 DoD Subordinate/Issuing CAs

DoD Intermediate and Subordinate CA certificates are a part of the PKE InstallRoot utility. Additionally, they are hosted in Global Directory Service (GDS).

2.2.1 DoD RSA2048/SHA-256 Subordinate CAs

Subordinate CA certificates will be issued by DoD Root CA 3.

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-59,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0304
Valid From	Apr 2 13:37:25 2019 GMT
Valid To	Apr 2 13:37:25 2025 GMT
SHA-1 Print	53:FD:E0:F4:06:38:BD:1A:68:A6:8D:1E:91:08:90:09:B3:3B:AE:5E

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-59,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0305
Valid From	Apr 2 13:38:32 2019 GMT
Valid To	Apr 2 13:38:32 2025 GMT
SHA-1 Print	19:07:FC:2B:22:3E:E0:30:1B:45:74:5B:DB:59:AA:D9:0F:E7:C5:D7

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-60,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0303
Valid From	Apr 2 13:34:49 2019 GMT
Valid To	Apr 2 13:34:49 2025 GMT
SHA-1 Print	5D:FF:DA:B6:58:91:5F:A6:B0:DB:4E:0B:CF:70:D5:BB:1B:84:25:FC

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-62,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x054A
Valid From	Jun 1 14:07:31 2021 GMT
Valid To	Jun 2 14:07:31 2027 GMT
SHA-1	14:F4:CF:D8:36:44:12:A6:A2:7E:5B:BA:82:C5:34:2F:F9:B3:37:A7

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-62,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x055D
Valid From	Jun 8 13:51:38 2021 GMT
Valid To	Jun 9 13:51:38 2027 GMT
SHA-1	CC:04:A4:F7:33:B7:67:76:1D:E8:93:5D:4C:74:5E:B2:55:24:B5:05

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-63,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x050F
Valid From	Apr 6 13:55:54 2021 GMT
Valid To	Apr 7 13:55:54 2027 GMT
SHA-1 Print	67:B7:51:60:BD:82:99:E2:34:2F:46:CC:8A:C6:34:B2:AF:B3:37:68

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-63,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x0548
Valid From	Jun 1 14:02:21 2021 GMT
Valid To	Jun 2 14:02:21 2027 GMT
SHA-1	1B:97:7E:31:04:F2:7C:D4:AF:B4:7D:50:2E:09:03:7A:95:6A:B1:26

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-64,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x054B
Valid From	Jun 1 14:09:37 2021 GMT
Valid To	Jun 2 14:09:37 2027 GMT
SHA-1	D9:99:1B:D1:E8:9A:E5:A8:B1:14:3C:3C:37:F0:11:03:77:9B:8D:B7

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-64,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x0549
Valid From	Jun 1 14:05:19 2021 GMT
Valid To	Jun 2 14:05:19 2027 GMT
SHA-1	8C:A4:FC:F4:D1:18:6F:52:E2:43:BE:7B:8C:CC:FE:B0:EC:7D:4F:4E

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-65,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x054C
Valid From	Jun 1 14:11:23 2021 GMT
Valid To	Jun 2 14:11:23 2027 GMT
SHA-1	28:38:D2:5A:E3:51:65:4A:09:4F:00:34:8F:4B:D0:EA:31:78:D8:71

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-65,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x055E
Valid From	Jun 8 13:55:26 2021 GMT
Valid To	Jun 9 13:55:26 2027 GMT
SHA-1	67:12:88:D3:AD:BB:59:09:AA:28:58:E3:F8:64:98:DE:D6:FD:85:A0

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-66,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x055F
Valid From	Jun 8 13:57:18 2021 GMT
Valid To	Jun 9 13:57:18 2027 GMT
SHA-1	8F:9D:91:C3:3D:4B:4E:4E:6F:D7:69:0C:05:30:48:A7:AA:BB:D3:A2

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-67,OU=PKI,OU=DoD,O=U.S. Government,C=US
S/N	0x0560
Valid From	Jun 8 13:58:25 2021 GMT
Valid To	Jun 9 13:58:25 2027 GMT
SHA-1	7B:38:AA:22:D6:F7:6A:8F:F4:8B:23:D2:48:5E:7D:25:20:F9:9C:AB

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD DERILITY CA-1,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x04C2
Valid From	Jan 19 14:55:37 2021 GMT
Valid To	Jan 20 14:55:37 2027 GMT
SHA-1 Print	6B:25:06:83:B9:96:E2:58:16:96:F4:99:06:1B:55:81:A7:86:7C:89

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-71,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x070B
Valid From	Dec 6 17:10:24 2022 GMT
Valid To	Dec 6 17:10:24 2028 GMT
SHA-1 Print	73:7B:EA:A4:D4:56:3E:18:6D:6B:4C:45:53:30:57:9F:A0:85:A3:BF

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-71,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x070C
Valid From	Dec 6 17:12:15 2022 GMT
Valid To	Dec 6 17:12:15 2028 GMT
SHA-1 Print	D3:98:C9:F7:09:EA:78:7F:46:AF:B2:B3:1C:BD:96:46:28:AF:A3:D4

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DoD Root CA 3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-75,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x070D
Valid From	Dec 6 17:13:49 2022 GMT
Valid To	Dec 6 17:13:49 2028 GMT
SHA-1 Print	DE:C1:3E:9A:63:02:C3:D0:A0:E0:AF:81:5D:6B:4E:79:F2:AF:8A:54

2.2.2 DoD RSA2048/3072/4096/SHA-384 Subordinate CAs

Subordinate CA certificates will be issued by DoD Root CA 6.

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-70,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x47
Valid From	May 16 16:00:08 2023 GMT
Valid To	May 15 16:00:08 2029 GMT
SHA-1 Print	60:05:F7:E3:9B:D4:75:CE:11:DD:4B:74:BC:85:B9:C7:18:2B:9A:53

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-70,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x44
Valid From	May 16 15:51:56 2023 GMT
Valid To	May 15 15:51:56 2029 GMT
SHA-1 Print	D9:E0:EE:F2:ED:4C:A1:89:EA:CE:25:35:E4:76:52:67:A5:C3:68:D0

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-72,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x48
Valid From	May 16 16:02:26 2023 GMT
Valid To	May 15 16:02:26 2029 GMT
SHA-1 Print	CE:68:B2:5F:A5:32:D9:59:93:5A:EB:2C:29:E1:35:85:31:90:35:35

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-72,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x45
Valid From	May 16 15:54:35 2023 GMT
Valid To	May 15 15:54:35 2029 GMT
SHA-1 Print	8C:16:E4:E3:99:88:E2:95:B8:4F:29:F8:0D:16:09:4E:E4:27:9C:47

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD ID CA-73,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x49
Valid From	May 16 16:03:49 2023 GMT
Valid To	May 15 16:03:49 2029 GMT
SHA-1 Print	D7:0C:59:5B:AC:C3:1B:5A:29:48:EB:9C:F2:59:CA:F9:D0:49:D2:1F

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD EMAIL CA-73,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x46
Valid From	May 16 15:58:04 2023 GMT
Valid To	May 15 15:58:04 2029 GMT
SHA-1 Print	E1:A5:23:71:2E:D8:A5:C5:81:CE:5F:A6:FE:F6:46:CD:1D:AF:0B:46

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-74,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x4A
Valid From	May 16 16:05:29 2023 GMT
Valid To	May 15 16:05:29 2029 GMT
SHA-1 Print	29:41:EF:E0:F6:52:1F:18:6D:00:69:31:EF:DA:11:0B:97:DC:82:48

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD DERILITY CA-3,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0X93
Valid From	Sep 26 15:37:49 2023 GMT
Valid To	Sep 25 15:37:49 2029 GMT
SHA-1 Print	C1:72:FF:63:8F:79:8F:FA:BA:6B:3E:B0:0D:C3:27:C5:BD:63:6E:17

ISSUING CA (RSA2048/SHA384)	
Issuer	CN=DoD Root CA 6,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD DERILITY CA-4,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x94
Valid From	Sep 26 15:40:52 2023 GMT
Valid To	Sep 25 15:40:52 2029 GMT
SHA-1 Print	AA:B2:82:81:0D:12:B5:81:74:EE:B2:7F:E3:45:B5:EB:6F:73:3E:D3

2.2.3 DoD ECC p256/SHA-256 Subordinate CAs

Subordinate CA certificates will be issued by DoD Root CA 4. Currently, there are no active DoD ECC p256/SHA-256 Subordinate CAs

2.2.4 DoD ECC p384/SHA-384 Subordinate CAs

Subordinate CA certificates will be issued by DoD Root CA 5 .

ISSUING CA (ECC-p384/SHA384)	
Issuer	CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-61,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0xC2
Valid From	Apr 2 13:41:24 2019 GMT
Valid To	Mar 31 13:41:24 2025 GMT
SHA-1 Print	5F:55:5A:B8:A8:7D:D1:46:31:41:71:62:12:45:CF:72:0B:F5:3B:8A

ISSUING CA (ECC-p384/SHA384)	
Issuer	CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-68,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0333
Valid From	Jul 20 13:56:48 2021 GMT
Valid To	Jul 19 13:56:48 2027 GMT
SHA-1 Print	C8:35:4A:83:6F:A5:28:BE:9B:55:8D:60:20:95:96:42:63:38:AE:0A

ISSUING CA (ECC-p384/SHA384)	
Issuer	CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-69,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0334
Valid From	Jul 20 13:59:26 2021 GMT
Valid To	Jul 19 13:59:26 2027 GMT
SHA-1 Print	2F:06:AD:B1:1C:CC:5D:A2:BE:D0:3F:30:AF:84:32:CC:B8:DD:8C:AF

ISSUING CA (ECC-p384/SHA384)	
Issuer	CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-76,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0537
Valid From	May 16 15:44:56 2023 GMT
Valid To	May 14 15:44:56 2029 GMT
SHA-1 Print	0F:DA:32:D7:7C:8A:9E:75:83:59:DA:5E:46:B3:41:BD:0D:97:66:42

ISSUING CA (ECC-p384/SHA384)	
Issuer	CN=DoD Root CA 5,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=DOD SW CA-77,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x0538
Valid From	May 16 15:48:18 2023 GMT
Valid To	May 14 15:48:18 2029 GMT
SHA-1 Print	93:DF:1A:4C:47:43:A5:A9:1F:3C:16:34:85:FC:C2:63:6C:8B:8D:59

3.0 ECA PKI Trust Chains

The DoD sponsored External Certification Authority (ECA) program was the first DoD approved external PKI. Prior to the 2008 CIO memorandum, *Approval of External Public Key Infrastructures,* it was the only means for DoD partners to interoperate with DoD users and servers. The ECA program is managed by the DoD PKI PMO and has four types of certificates and three different assurance levels. The ECA certificates are included in InstallRoot and GDS hosts the ECA CA information to include CA certificates, cross-certificate content, and Certificate Revocation Lists (CRLs). The DoD Robust Certificate Validation Service (RCVS) provides Online Certificate Status Protocol (OCSP) responses for ECA Subordinate CA certificates. More information can be found on the ECA homepage, https://public.cyber.mil/eca/. DoD users and systems that choose to trust ECA PKI, should implement direct trust by installing the appropriate trust chain into the application or system trust store. Please note that for servers, this provides the capability to authenticate ECA PKI certificates and a separate access control decision to determine need-to-know should be made before providing access to DoD information systems.

3.1 ECA Trust Anchors

3.1.1 ECA Root CA 4

ECA Root CA 4 is the RSA2048/SHA-256 ECA trust anchor. ECA Root CA 4 has a one-way cross-certificate relationship with DoD Interoperability Root CA 2 which is cross certified with the Federal Bridge CA. This will allow DoD partners to validate ECA SHA-256 certificates against their own PKI trust anchors.

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Serial #	0x01
Valid From	Mar 20 16:13:04 2012 GMT
Valid To	Dec 30 16:13:04 2029 GMT
SHA-1 Print	73:E8:BB:08:E3:37:D6:A5:A6:AE:F9:0C:FF:DD:97:D9:17:6C:B5:82

3.1.2 ECA Root CA 5

ECA Root CA 5 is the RSA4096/SHA-384 ECA trust anchor. ECA Root CA 5 has a one-way cross-certificate relationship with DoD Interoperability Root CA 2 which is cross certified with the Federal Bridge CA. This will allow DoD partners to validate ECA SHA-384 certificates against their own PKI trust anchors.

TRUST ANCHOR (RSA4096/SHA384)	
Issuer	CN=ECA Root CA 5,OU=ECA,O=U.S. Government,C=US
Subject	CN=ECA Root CA 5,OU=ECA,O=U.S. Government,C=US
Serial #	0x01
Valid From	Mar 12 15:34:56 2024 GMT
Valid To	Mar 12 15:34:56 2050 GMT
SHA-1 Print	DB:00:E5:B7:CC:93:93:03:1F:E8:A6:1D:F6:6C:65:7C:74:62:BB:21

3.2 ECA Subordinate/Issuing CAs

There are currently two ECA vendors which operate ECA subordinate CAs: IdenTrust and WidePoint (formerly ORC).

3.2.1 ECA RSA2048/SHA-256 Subordinate CAs[6]

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=WidePoint ECA 8,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x054F
Valid From	Jul 6 14:55:56 2021 GMT
Valid To	Jul 7 14:55:56 2027 GMT
SHA-1 Print	33:47:07:68:4F:E4:BC:CF:B4:DB:F5:0E:D3:C4:63:ED:9E:A7:74:67

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA S22,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x02F5
Valid From	May 7 12:55:28 2019 GMT
Valid To	May 7 12:55:28 2025 GMT
SHA-1 Print	A7:BC:FC:00:C8:18:D2:69:7D:49:C9:40:7A:5C:7C:2E:EE:25:0F:00

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA S22C,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x02F6
Valid From	May 7 12:57:36 2019 GMT
Valid To	May 7 12:57:36 2025 GMT
SHA-1 Print	85:81:69:08:02:68:C6:47:3E:C5:92:93:A4:12:22:46:59:F1:AC:7B

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA Component S23,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x0626
Valid From	Apr 5 15:38:24 2022 GMT
Valid To	Apr 5 15:38:24 2028 GMT
SHA-1 Print	4B:07:4F:52:86:88:0E:7B:40:26:ED:B7:B6:3F:1A:C0:28:2E:F2:02

[6] All issuing CAs off ECA Root CA 4 can also be pulled from http://crl.disa.mil/issuedby/ECAROOTCA4_IB.p7c or https://crl.disa.mil

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=ECA Root CA 4,OU=ECA,O=U.S. Government,C=US
Subject	CN=IdenTrust ECA S23,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x0627
Valid From	Apr 5 15:41:42 2022 GMT
Valid To	Apr 5 15:41:42 2028 GMT
SHA-1 Print	89:CB:C3:2B:7D:B1:0E:7D:0A:70:06:99:69:C3:78:4A:BA:29:BF:D9

3.2.2 ECA RSA4096/SHA-384 Subordinate CAs[7]

ISSUING CA (RSA4096/SHA384)	
Issuer	CN=ECA Root CA 5,OU=ECA,O=U.S. Government,C=US
Subject	CN=WidePoint ECA 9,OU=Certification Authorities,OU=ECA,O=U.S. Government,C=US
Serial #	0x08
Valid From	May 7 15:01:03 2024 GMT
Valid To	May 6 15:01:03 2034 GMT
SHA-1 Print	25:9D:0E:DD:9B:3D:87:B8:EC:DD:C9:05:3E:0F:C8:C2:53:BA:C9:E8

[7] All issuing CAs off ECA Root CA 5 can also be pulled from http://crl.disa.mil/issuedby/ECAROOTCA5_IB.p7c or https://crl.disa.mil

4.0 DoD Approved External PKI Trust Chains

In addition to the DoD and ECA PKI, the external PKIs listed in this section are approved for use within DoD at the Federal PKI medium hardware assurance level or higher (although many PKIs have multiple assurance levels).[8] Some of the partners listed in this section maintain their own PKI, referred to within the Federal PKI community as "Legacy PKIs", and many obtain their PKI certificates through Shared Service Providers (SSPs) or other commercial Non-Federal Issuers (NFIs).

The DoD External Interoperability Plan (EIP) defines six types of PKIs:[9]

Type 1: Federal Executive Branch Department and Agency PIV PKIs
Type 2: Federal Executive Branch Shared Service Provider (SSP) PIV PKIs
Type 3: Commercial Medium Hardware PKIs
Type 4: Commercial Personal Identity Verification-Interoperable (PIV-I) PKIs
Type 5: Combined Communication-Electronics Board (CCEB) Partner PKIs
Type 6: Other Mission Partner PKIs on Unclassified DoD Networks

4.1 DoD Approved External PKI Summary

Type	PKI	Highest Assurance Level	Date Tested	Date Retested
DoD Sponsored	**DoD External Certification Authority (ECA) Program**	PIV-I	N/A	
Type 1	**Department of State PKI**	PIV	Sep-08	May-20
Type 2	**Entrust Federal SSP PKI** *Agencies include, but are not limited to:*	PIV	Feb-10	Jul-24
	Department of Energy			
	Department of Justice			
	National Institute of Standards and Technology			
	Health and Human Services	PIV	Oct-13	
Type 2	**WidePoint Federal SSP (formerly ORC SSP)** *Agencies include, but are not limited to:*	PIV	Dec-08	Jul-14
	Department of Transportation/Federal Aviation Administration	PIV	Jun-24	

[8] See Section 5.0 for more details on assurance levels.
[9] The DoD External Interoperability Plan is available on the DoD authoritative External PKI Interoperability site at https://dl.cyber.mil/pki-pke/pdf/unclass-fouo-dod_external_interoperability_plan_26aug2010.pdf

Type	PKI	Highest Assurance Level	Date Tested	Date Retested
Type 2	**DigiCert Federal SSP PKI (formerly Symantec SSP PKI, VeriSign SSP PKI)** *Agencies include, but are not limited to:*	PIV	Nov-08	
	Department of Transportation/Federal Aviation Administration	PIV		Oct-21
Type 2	**U.S. Treasury SSP PKI** *Agencies include:*	PIV	Sep-08	
	Department of Homeland Security	PIV	Mar-09	Mar-20
	Fiscal Service	PIV	Mar-09	
	National Aeronautics and Space Administration	PIV	Mar-09	Jun 19
	Social Security Administration	PIV	Jan-09	
	U.S. Treasury Department – OCIO	PIV	Sep-08	
	Department of Veteran Affairs	PIV	Mar-20	
Type 2	**Verizon/Cybertrust Federal SSP PKI** *Agencies include:*	PIV	Oct-09	
	Department of Veteran Affairs	PIV		Apr-19
Type 3	**Boeing PKI**	Medium Hardware	May-12	Jul-19
Type 3	**Exostar LLC PKI**	Medium Hardware	Sep-09	Mar-21
Type 3	**Lockheed Martin PKI**	Medium Hardware	Mar-09	Dec-22
Type 3	**Raytheon PKI**	Medium Hardware	Mar-09	Mar-21
Type 4	**Carillon Federal Services PKI**	PIV-I	Dec-15	Sep-21
Type 4	**Carillon Information Security PKI**	PIV-I	Sep-21	
Type 4	**Entrust Managed Services NFI PKI**	PIV-I	Oct-11	Apr-19
Type 4	**IdenTrust NFI**	PIV-I	Mar-16	
Type 4	**Northrop Grumman PKI**	PIV-I	Nov-08	Jun-23
Type 4	**WidePoint NFI PKI (formerly ORC NFI PKI)** *Organizations include:*	PIV-I	Mar-12	Jul-21
	U.S. Senate	PIV-I	Jul-23	
Type 4	**DigiCert NFI PKI (formerly Symantec NFI PKI, VeriSign NFI PKI)** *Organizations include:*	PIV-I	Apr-11	
	CSRA (formerly Computer Sciences Corporation)	Medium Hardware	Jan-13	Jul-16
	Eid Passport	PIV-I	Feb-13	Aug-14
	SureID	PIV-I	Mar-17	
	U.S. Senate	PIV-I	Sep-18	Jan-22
Type 5	**Australian Defence Organisation**	Medium Hardware	Jun-13	Oct-22
Type 6	**Netherlands Ministry of Defence**	Medium Hardware	Sep-12	Feb-20

4.2 Federal Agencies (Type 1 and 2 PKIs)

Federal Agency PKIs are defined in the DoD External Interoperability Plan as Type 1 and 2 PKIs and must adhere to FIPS 201 and the Personal Identity Verification (PIV) standard.[10] Although the Type 1 and 2 PKIs have PIV certificates, some have other non-PIV certificates at varying assurance levels. All PIV certificates issued after December 31, 2010 must be SHA-256. DoD application owners should ensure their systems are patched or upgraded as applicable to support validation of SHA-256 certificates.

4.2.1 Entrust Federal SSP PKI (GSA MSO)

The General Services Administration Managed Service Office (GSA MSO) provides PIV credentials to a number of Federal agencies as a Shared Service Provider (SSP). The GSA MSO established the USAccess program to offer federal agencies a managed, shared service solution to simplify the process of procuring and maintaining PIV credentials. Currently GSA MSO credentials are provided solely by the Entrust Federal SSP. DoD approved U.S. Federal Agencies that receive certificates from the Entrust Federal SSP PKI include but not limited to Department of Energy, Department of Justice, and National Institute of Standards and Technology. Entrust Federal SSP PKI has one trust chain as shown below.

4.2.1.1 Trust Chain 1

ENTRUST SSP TRUST ANCHOR- KEY UPDATE #2 (CERTS ISSUED 7/23/15-PRESENT - RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x448062F4
Valid From	Jul 23 16:06:36 2015 GMT
Valid To	Jul 23 16:36:36 2025 GMT
SHA-1 Print	59:C3:01:37:60:A6:A9:67:99:F0:6D:95:BE:92:E2:1D:B1:93:89:6F

ENTRUST SSP ISSUING CA-KEY UPDATE #2 (CERTS ISSUED 7/23/15-PRESENT - RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services SSP CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x448063D5
Valid From	Jul 30 16:37:44 2015 GMT
Valid To	Jul 23 16:36:36 2025 GMT
SHA-1 Print	DE:C0:1B:F4:0C:15:3F:BC:38:BF:2C:A7:66:B0:4F:9D:FB:DA:30:64

HEALTH AND HUMAN SERVICES INTERMEDIATE CA-KEY UPDATE #2 (CERTS ISSUED 12/20/2016-PRESENT - RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	CN=HHS-FPKI-Intermediate-CA-E1,OU=Certification Authorities,OU=HHS,O=U.S. Government,C=US
Serial #	0x44809A90
Valid From	Dec 20 15:40:39 2016 GMT
Valid To	Jul 20 16:10:39 2025 GMT
SHA-1 Print	D5:E3:11:40:64:37:C3:5A:79:BC:02:3C:2B:BB:57:04:9F:5D:8F:77

[10] Details on FIPS 201 and PIV can be found at http://csrc.nist.gov/groups/SNS/piv/index.html

4.2.1.2 Trust Chain 2

ENTRUST SSP TRUST ANCHOR- KEY UPDATE #3 (CERTS ISSUED 8/13/19-PRESENT - RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x4481077A
Valid From	Aug 13 13:50:38 2019 GMT
Valid To	Aug 13 14:20:38 2029 GMT
SHA-1 Print	AF:B1:A1:66:B3:CF:53:A0:DE:E2:DF:C6:E2:27:BB:26:55:92:F1:13

ENTRUST SSP ISSUING CA-KEY UPDATE #3 (CERTS ISSUED 8/13/19-PRESENT - RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services SSP CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x448107B6
Valid From	Aug 13 15:46:29 2019 GMT
Valid To	Jul 13 16:16:29 2029 GMT
SHA-1 Print	72:2E:8A:BB:E6:B6:6E:47:D1:BC:EC:3C:7E:C4:7A:A5:BB:E4:D3:C5

4.2.1.3 Trust Chain 3

ENTRUST SSP TRUST ANCHOR- KEY UPDATE #4 (CERTS ISSUED7/11/23-PRESENT - RSA2048/SHA384)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x4481B22B
Valid From	Jul 11 20:48:46 2023 GMT
Valid To	Dec 11 21:18:46 2030 GMT
SHA-1 Print	57:A5:16:B7:02:F3:17:CF:83:46:25:A7:AD:68:C4:F1:33:57:08:86

ENTRUST SSP ISSUING CA-KEY UPDATE #4 (CERTS ISSUED 7/11/23-PRESENT - RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services SSP CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x4481B22F
Valid From	Jul 11 21:33:31 2023 GMT
Valid To	Nov 11 22:03:31 2030 GMT
SHA-1 Print	19:FE:A4:9C:46:87:60:ED:CE:96:00:A9:DA:96:57:B4:84:73:4D:24

4.2.1.4 End Entity Information

Entrust Federal SSP PKI issues RSA2048/SHA-256 end entity certificates.

4.2.2 WidePoint Federal SSP PKI (Formerly ORC SSP PKI)

WidePoint Federal SSP PKI provides PIV credentials to federal agencies including the DoD approved Department of Transportation. WidePoint Federal SSP PKI has one trust chain as shown below.

4.2.2.1 Trust Chain

TRUST ANCHOR (RSA4096/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Serial #	0x21E5B9A0CC956DE278CA012BA8FDC58A98B3FBEA
Valid From	Oct 14 13:35:12 2020 GMT
Valid To	Oct 14 13:35:12 2040 GMT
SHA-1 Print	99:B4:25:1E:2E:EE:05:D8:29:2E:83:97:A9:01:65:29:3D:11:60:28

INTERMEDIATE CA (RSA4096/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=WidePoint SSP Intermediate CA,O=ORC PKI,C=US
Serial #	0x28F49A629440B3FDF097AC0FD46DBD9735379187
Valid From	Apr 3 13:51:38 2023 GMT
Valid To	Mar 15 13:51:38 2033 GMT
SHA-1 Print	EE:F5:18:0A:85:2B:04:44:83:A1:38:BC:B3:0A:D9:54:84:63:E0:9B

ISSUING CA (RSA4096/SHA384)	
Issuer	CN=WidePoint SSP Intermediate CA,O=ORC PKI,C=US
Subject	CN=U.S. Department of Transportation Agency CA G6,OU=U.S. Department of Transportation,O=U.S. Government,C=US
Serial #	0x309B986D8A7FB52A7EA7DC858693C5E06E7AE33A
Valid From	May 4 19:13:56 2023 GMT
Valid To	Mar 8 00:17:04 2033 GMT
SHA-1 Print	7B:6D:CB:34:AB:28:4E:C8:97:F0:FF:E1:A2:F8:F9:50:82:F0:9C:74

4.2.2.2 End Entity Information

Since WidePoint Federal PKI does not have any approved issuing CAs, the public key and hashing algorithm of end entity certificates are unknown.

4.2.3 Department of State PKI

The Department of State maintains its own PKI and has two trust chains as shown below: U.S. Department of State AD High Assurance CAs issue user signature and encryption certificates as well as SSL certificates; and U.S. Department of State PIV CA2 issues PIV authentication certificates.

4.2.3.1 Trust Chain 1

DEPARTMENT OF STATE TRUST ANCHOR (KEY 1 – RSA2048/SHA1)	
Issuer	CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Subject	CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Serial #	0x40D9CA01
Valid From	Jun 23 17:50:55 2004 GMT
Valid To	Jun 23 18:20:55 2034 GMT
SHA-1 Print	31:8F:93:37:82:A2:80:88:11:5A:CE:0F:D9:62:EB:EC:8D:3D:EB:FA

PIV ISSUING CA (KEY 1 - RSA2048/SHA256)	
Issuer	CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Subject	OU=U.S. Department of State PIV CA2,OU=Certification Authorities,OU=PIV,OU=Department of State,O=U.S. Government,C=US
Serial #	0x51B02402
Valid From	Aug 3 16:13:25 2016 GMT
Valid To	Aug 3 16:43:25 2026 GMT
SHA-1 Print	FF:E0:7F:B4:28:BC:EF:4B:F3:8E:BB:FA:E1:E4:23:39:E0:3E:77:56

4.2.3.2 Trust Chain 2

DEPARTMENT OF STATE TRUST ANCHOR (REKEY 2 - RSA4096/SHA256)	
Issuer	CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Subject	CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Serial #	0x51B052E7
Valid From	Aug 30 14:03:08 2017 GMT
Valid To	Dec 30 14:33:08 2037 GMT
SHA-1 Print	84:6D:D1:25:59:E7:EC:1F:40:51:71:8E:32:4B:CE:7C:1E:31:2F:83

SSL/SIGNATURE/ENCRYPTION ISSUING CA (REKEY 3 - RSA4096/SHA256)	
Issuer	CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Subject	CN=U.S. Department of State AD High Assurance CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Serial #	0x51B069FA
Valid From	Mar 6 21:24:54 2018 GMT
Valid To	Mar 6 21:54:54 2028 GMT
SHA-1 Print	18:9C:0E:90:53:10:26:44:21:81:16:88:EC:CC:5E:51:3D:0F:3C:91

PIV ISSUING CA (REKEY 2 – RSA3072/SHA256)	
Issuer	CN=U.S. Department of State AD Root CA,CN=AIA,CN=Public Key Services,CN=Services,CN=Configuration,DC=state,DC=sbu
Subject	OU=U.S. Department of State PIV CA2,OU=Certification Authorities,OU=PIV,OU=Department of State,O=U.S. Government,C=US
Serial #	0x51B0B97F
Valid From	Jan 24 23:34:08 2020 GMT
Valid To	Jan 25 00:04:08 2030 GMT
SHA-1 Print	68:A4:E9:AB:7A:1F:B8:FB:85:31:6A:77:0F:F9:CA:87:4C:02:07:24

4.2.3.3 End Entity Information

The Department of State PKI issues RSA2048/SHA-256 end entity certificates.

4.2.4 U.S. Treasury SSP PKI[11][12]

U.S. Treasury operates a SSP PKI which provides PIV credentials to Treasury, Department of Homeland Security, Social Security Administration, and National Aeronautics and Space Administration. Treasury SSP PKI has one Root CA with separate issuing CAs for each agency. All revocation data from each CA is SHA-256. The addition of the SHA-256 issuing CAs occurred at the end of 2010.

[11] U.S. Treasury SSP PKI certificates can be obtained from http://pki.treas.gov/root_sia.p7c

[12] CAs that have been identified as "CRLs only" do not issue new certificates and only issue CRLs. Certificates previously issued from these CAs are still valid.

4.2.4.1 Trust Chain 1

TREASURY SSP TRUST ANCHOR – CURRENT (RSA2048/SHA1)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x443EA73A
Valid From	Aug 5 14:16:30 2006 GMT
Valid To	Aug 5 14:46:30 2026 GMT
SHA-1 Print	02:FF:F6:B3:FC:81:5C:57:E6:83:2D:FC:38:61:85:13:33:B0:C3:0B

DHS ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=DHS CA4,OU=Certification Authorities,OU=Department of Homeland Security,O=U.S. Government,C=US
Serial #	0x4E398128
Valid From	Jun 13 14:35:04 2015 GMT
Valid To	Jun 13 15:05:04 2025 GMT
SHA-1 Print	A3:1A:5D:F2:F1:C1:01:9B:9C:F5:B7:CA:4E:3B:26:65:0B:9C:A9:3F

TREASURY FISCAL SERVICE ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Fiscal Service,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4E398167
Valid From	Oct 17 13:37:26 2015 GMT
Valid To	Oct 17 14:07:26 2025 GMT
SHA-1 Print	ED:3F:B3:16:11:82:57:A4:4E:A1:1A:49:3D:A1:41:5B:EB:30:12:D7

NASA ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=NASA Operational CA,OU=Certification Authorities,OU=NASA,O=U.S. Government,C=US
Serial #	0x4E398116
Valid From	Jun 13 14:24:52 2015 GMT
Valid To	Jun 13 14:54:52 2025 GMT
SHA-1 Print	FE:75:72:BB:DE:7B:7F:44:15:2A:CC:8E:17:15:C1:87:14:DC:9D:63

TREASURY OCIO ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=OCIO CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x4E398101
Valid From	Apr 19 15:17:45 2015 GMT
Valid To	Apr 19 15:47:45 2025 GMT
SHA-1 Print	5A:D2:54:C3:EC:EB:B5:B7:E1:08:CA:A0:CC:80:30:59:8A:7B:77:09

SSA ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Social Security Administration Certification Authority,OU=SSA,O=U.S. Government,C=US
Serial #	0x4E3980EF
Valid From	Apr 19 15:04:29 2015 GMT
Valid To	Apr 19 15:34:29 2025 GMT
SHA-1 Print	BB:6C:62:E6:48:D5:03:F1:BE:AB:75:EF:5F:69:B1:72:56:17:59:93

4.2.4.2 Trust Chain 2

TREASURY SSP TRUST ANCHOR – CURRENT (RSA4096/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Serial #	0x570D2BFF
Valid From	Jul 13 13:03:26 2016 GMT
Valid To	Jul 13 13:33:26 2036 GMT
SHA-1 Print	CA:0B:69:14:2A:89:7F:07:5B:D9:DA:22:95:34:AD:73:BA:36:06:A8

NASA ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=NASA Operational CA,OU=Certification Authorities,OU=NASA,O=U.S. Government,C=US
Serial #	0x5CCB3196
Valid From	May 4 12:40:55 2019 GMT
Valid To	May 4 13:10:55 2029 GMT
SHA-1 Print	F5:04:01:2B:1F:E5:7B:43:81:E3:BF:5B:A9:F4:91:14:4E:D7:6E:E1

VETERANS AFFAIRS ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=Department of Veterans Affairs CA,OU=Certification Authorities,OU=Department of Veterans Affairs,O=U.S. Government,C=US
Serial #	0x5CCB3215
Valid From	Jun 22 13:23:22 2019 GMT
Valid To	Jun 22 13:53:22 2029 GMT
SHA-1 Print	76:CC:89:8F:03:EB:0F:C7:E0:87:7A:AC:30:A0:C1:34:0B:B3:48:79

DHS ISSUING CA – CURRENT (RSA2048/SHA256)	
Issuer	OU=US Treasury Root CA,OU=Certification Authorities,OU=Department of the Treasury,O=U.S. Government,C=US
Subject	OU=DHS CA4,OU=Certification Authorities,OU=Department of Homeland Security,O=U.S. Government,C=US
Serial #	0x5CCB31CA
Valid From	Jun 6 11:11:16 2019 GMT
Valid To	Jun 6 11:41:16 2029 GMT
SHA-1 Print	58:08:5A:64:E1:81:57:3F:4F:D9:17:C5:C0:21:EB:1C:F3:44:DD:5F

4.2.4.3 End Entity Information

U.S. Treasury SSP PKI issues RSA2048/SHA-256 end entity certificates.

4.2.5 DigiCert Federal SSP PKI (formerly Symantec SSP PKI, VeriSign SSP PKI)

DigiCert Federal SSP PKI provides SHA-256 Personal Identity Verification (PIV) credentials to Federal agencies. DigiCert Federal SSP has one SHA-256 trust chain as shown below. The trust chain shares a Root and Intermediate CA with different issuing CAs for each agency. DigiCert Federal SSP PKI also has device Issuing CA certificates which are currently not included because they don't meet the medium hardware assurance level requirement. DigiCert Federal SSP SHA-2 PKI is subordinate to Federal Common Policy CA G2.

4.2.5.1 Trust Chain 1

TRUST ANCHOR (RSA4096/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Serial #	0x21E5B9A0CC956DE278CA012BA8FDC58A98B3FBEA
Valid From	Oct 14 13:35:12 2020 GMT
Valid To	Oct 14 13:35:12 2040 GMT
SHA-1 Print	99:B4:25:1E:2E:EE:05:D8:29:2E:83:97:A9:01:65:29:3D:11:60:28

INTERMEDIATE CA (RSA2048/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Symantec SSP Intermediate CA - G4,O= Symantec Corporation,C=US
Serial #	0x262BD1F025C8AF37334545666EA6C9EA946C2C34
Valid From	Nov 18 14:42:41 2020 GMT
Valid To	Nov 12 14:42:41 2024 GMT
SHA-1 Print	4C:40:F6:2B:5C:3F:13:53:3A:8F:8A:1D:44:F8:B0:27:AA:A0:FD:3D

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=Symantec SSP Intermediate CA - G4,O=Symantec Corporation,C=US
Subject	CN=U.S. Department of Transportation Agency CA G4,OU=U.S. Department of Transportation,O=U.S. Government,C=US
Serial #	0x61A90F3E5FF532F9FE6209D931279A82
Valid From	Dec 11 00:00:00 2014 GMT
Valid To	Nov 11 23:59:59 2024 GMT
SHA-1 Print	DC:5B:59:08:00:76:58:64:58:79:02:AF:98:3C:21:A7:20:9B:E3:20

4.2.5.2 Trust Chain 2

TRUST ANCHOR (RSA4096/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Serial #	0x21E5B9A0CC956DE278CA012BA8FDC58A98B3FBEA
Valid From	Oct 14 13:35:12 2020 GMT
Valid To	Oct 14 13:35:12 2040 GMT
SHA-1 Print	99:B4:25:1E:2E:EE:05:D8:29:2E:83:97:A9:01:65:29:3D:11:60:28

INTERMEDIATE CA (RSA2048/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=DigiCert Federal SSP Intermediate CA - G5,O=DigiCert\, Inc.,C=US
Serial #	24BC168F9CCB30CFCEF8F0A58F26F10181869266
Valid From	Nov 18 16:34:38 2020 GMT
Valid To	Dec 13 16:34:38 2028 GMT
SHA-1 Print	9A:EC:FB:E2:DE:8A:EA:49:D2:20:BB:F7:99:17:2C:00:52:7F:E7:56

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=DigiCert Federal SSP Intermediate CA - G5,O=DigiCert\, Inc.,C=US
Subject	CN=U.S. Department of Transportation Agency CA G5,OU=U.S. Department of Transportation,O=U.S. Government,C=US
Serial #	0x0ED81C303EA3566787FACA36899A931A
Valid From	Mar 5 00:00:00 2019 GMT
Valid To	Dec 12 23:59:59 2028 GMT
SHA-1 Print	B1:D0:5E:5B:9E:02:5E:A4:B3:B3:E3:0D:C3:F4:5A:19:F9:EC:51:F6

4.2.5.3 End Entity Information

DigiCert Federal SSP PKI issues RSA2048/SHA-256 end entity certificates.

4.2.6 Verizon/Cybertrust Federal SSP PKI

Verizon/Cybertrust Federal SSP PKI provides PIV credentials to federal agencies. Verizon/Cybertrust Federal SSP PKI has the same Root with separate intermediate and issuing CAs for each agency. DoD relying parties who interoperate with Verizon/Cybertrust Federal SSP PKI certificates must ensure they can support SHA-256. Verizon/Cybertrust Federal SSP PKI is subordinate to Federal Common Policy CA.

4.2.6.1 Trust Chain

TRUST ANCHOR (RSA4096/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Serial #	0x21E5B9A0CC956DE278CA012BA8FDC58A98B3FBEA
Valid From	Oct 14 13:35:12 2020 GMT
Valid To	Oct 14 13:35:12 2040 GMT
SHA-1 Print	99:B4:25:1E:2E:EE:05:D8:29:2E:83:97:A9:01:65:29:3D:11:60:28

INTERMEDIATE CA (RSA2048/SHA384)	
Issuer	CN=Federal Common Policy CA G2,OU=FPKI,O=U.S. Government,C=US
Subject	CN=Verizon SSP CA A2,OU=SSP,O=Verizon,C=US
Serial #	0x25FCA834ADA24A4455A2DB0FF4CEF7C411198E3A
Valid From	Nov 18 14:56:18 2020 GMT
Valid To	Dec 6 14:56:18 2026 GMT
SHA-1 Print	B2:16:7F:D3:8F:F4:7B:B9:10:D8:DC:C3:2F:CC:3B:7B:63:A0:9F:F7

DEPARTMENT OF VETERANS AFFAIRS ISSUING CA (RSA2048/SHA256)	
Issuer	CN=Verizon SSP CA A2,OU=SSP,O=Verizon,C=US
Subject	CN=Veterans Affairs User CA B1,OU=PKI,OU=Services,DC=va,DC=gov
Serial #	0x251EA36536CFEBB0E9D1334D0CB96102BAB16589
Valid From	Jan 25 04:59:15 2017 GMT
Valid To	Jan 25 04:59:15 2027 GMT
SHA-1 Print	67:14:61:94:8B:8E:F7:65:FE:5E:12:48:22:2A:F3:FC:DD:45:75:64

4.2.6.2 End Entity Information

Verizon/Cybertrust Federal SSP PKI issues RSA2048/SHA-256 end entity certificates.

4.3 Industry Partners (Type 3 and 4 PKIs)

Industry Partners are classified in the DoD External Interoperability Plan as Type 3 and 4 PKIs and in addition to meeting the technical requirements and successfully completing JITC testing, must sign a Memorandum of Agreement (MOA), and be sponsored by a DoD relying party. Industry partners can be approved at PIV-I or Medium Hardware and often have additional assurance levels.[13] PIV-I certificates must be SHA-256. Application owners that need to validate PIV-I certificates should ensure that their applications are patched or upgraded as necessary to be able to validate SHA-256 signed certificates.

[13] For more information on assurance levels, see Section 5.0.

4.3.1 Boeing PKI

Boeing PKI is an Aero Defense partner through CertiPath and has a SHA-256 infrastructure.

4.3.1.1 Trust Chain

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=Boeing PCA G3,OU=certservers,O=Boeing,C=US
Subject	CN=Boeing PCA G3,OU=certservers,O=Boeing,C=US
Serial #	0x436F7A9D4C0BA5BA4ABB757EAB10CA0A
Valid From	Mar 29 17:13:58 2013 GMT
Valid To	Nov 29 17:20:01 2030 GMT
SHA-1 Print	71:87:DF:F9:26:99:2C:90:E6:48:43:92:32:4E:30:36:A5:61:F2:48

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=Boeing PCA G3,OU=certservers,O=Boeing,C=US
Subject	CN=Boeing Medium Assurance Hardware Issuing CA G3,OU=CertServers,O=Boeing,C=US
Serial #	0x61DA556400000000000F
Valid From	Aug 29 01:55:57 2017 GMT
Valid To	Aug 29 02:05:57 2027 GMT
SHA-1 Print	D7:1B:3A:FF:15:6C:6E:54:28:42:99:75:88:4D:9A:5E:A6:F6:55:4D

4.3.1.2 End Entity Information

Boeing currently issues RSA2048/SHA-256 end entity certificates.

4.3.2 Carillon Federal Services PKI

Carillon Federal Services PKI issues PIV-I credentials to Federal, State & Local Agencies as well as private companies that provide products and services to the DoD. The PKI has two SHA-256 Trust Chain as shown below. DoD relying parties that wish to interoperate with Carillon should ensure their applications support SHA-256.

4.3.2.1 Trust Chain

TRUST ANCHOR (RSA4096/SHA256)	
Issuer	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Subject	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Serial #	0x014325B6A074
Valid From	Jun 12 18:46:31 2015 GMT
Valid To	Jun 12 18:46:31 2035 GMT
SHA-1 Print	55:E9:A9:43:49:CD:45:19:0D:C0:FE:ED:B2:2C:B7:C9:71:5C:28:98

ISSUING CA (RSA4096/SHA256)	
Issuer	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Subject	CN=Carillon Federal Services PIV-I CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Serial #	0x0BB34DC334FF
Valid From	Jun 12 19:01:13 2015 GMT
Valid To	Jun 12 19:01:13 2028 GMT
SHA-1 Print	DC:78:C9:7B:02:19:E4:9F:93:81:33:44:5E:18:2D:FA:AC:7C:C8:76

ISSUING CA (RSA4096/SHA256)	
Issuer	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Subject	CN=Carillon Federal Services PIV-I CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Serial #	0x7CFB6F1184C8
Valid From	Jun 21 18:32:16 2018 GMT
Valid To	Apr 30 18:32:16 2028 GMT
SHA-1 Print	EB:D9:CC:57:A8:77:0A:C6:D8:EB:37:74:3E:79:C5:F5:77:80:63:3E

ISSUING CA (RSA4096/SHA256)	
Issuer	CN=Carillon Federal Services NFI Root CA1,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Subject	CN=Carillon Federal Services PIV-I CA2,OU=Certification Authorities,O=Carillon Federal Services Inc.,C=US
Serial #	0x0649D6143BAF
Valid From	Apr 29 14:54:33 2016 GMT
Valid To	Apr 30 14:54:33 2028 GMT
SHA-1 Print	0B:6F:1D:20:C7:90:00:E1:16:E8:62:D5:EA:E3:E5:F9:3B:C7:79:8A

4.3.2.2 End Entity Information

Carillon Federal Services PKI issues RSA2048/SHA-256 end entity certificates.

4.3.3 Carillon Information Security PKI

Carillon Information Security PKI issues PIV-I credentials to Federal, State & Local Agencies as well as private companies that provide products and services to the DoD. The PKI has one SHA-256 Trust Chain as shown below. DoD relying parties that wish to interoperate with Carillon should ensure their applications support SHA-256.

4.3.3.1 Trust Chain

TRUST ANCHOR (RSA4096/SHA256)	
Issuer	CN=Carillon PKI Services G2 Root CA 2,OU=Certification Authorities,O=Carillon Information Security Inc.,C=CA
Subject	CN=Carillon PKI Services G2 Root CA 2,OU=Certification Authorities,O=Carillon Information Security Inc.,C=CA
Serial #	0x64BF302590F7
Valid From	Jan 20 19:50:42 2020 GMT
Valid To	Jan 20 19:50:42 2040 GMT
SHA-1 Print	93:81:08:67:92:2D:10:B4:F2:95:63:0E:84:45:3C:48:CF:11:07:83

ISSUING CA (RSA4096/SHA256)	
Issuer	CN=Carillon PKI Services G2 Root CA 2,OU=Certification Authorities,O=Carillon Information Security Inc.,C=CA
Subject	CN=Carillon PKI Services CA 2,OU=Certification Authorities,O=Carillon Information Security Inc.,C=CA
Serial #	0x0CF61C00DBB4
Valid From	Apr 20 16:09:36 2021 GMT
Valid To	Jan 20 16:09:36 2030 GMT
SHA-1 Print	0E:1C:B4:D3:D7:63:4F:83:30:FC:A4:CB:8F:9A:F8:82:1F:44:6E:9D

4.3.3.2 End Entity Information

Carillon Information Security PKI issues RSA2048/SHA-256 end entity certificates.

4.3.4 Entrust Managed Services NFI PKI

Entrust Managed Services NFI PKI issues PIV-I credentials to non-DoD entities and personnel desiring to use those certificates to interact with DoD Relying Parties. Entrust NFI PKI has one SHA-256 Trust Chain as shown below. DoD relying parties that wish to interoperate with Entrust NFI PKI should ensure their applications support SHA-256.

4.3.4.1 Trust Chain

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services NFI Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust Managed Services NFI Root CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x4AA8A60D
Valid From	Nov 16 16:31:04 2016 GMT
Valid To	Dec 16 17:01:04 2027 GMT
SHA-1 Print	47:E3:19:E1:99:5F:79:F8:83:3C:57:94:65:D9:31:EA:24:8E:E7:B5

ISSUING CA (RSA2048/SHA256)	
Issuer	OU=Entrust Managed Services NFI Root CA,OU=Certification Authorities,O=Entrust,C=US
Subject	OU=Entrust NFI Medium Assurance SSP CA,OU=Certification Authorities,O=Entrust,C=US
Serial #	0x4AA8B9EA
Valid From	May 16 14:31:35 2017 GMT
Valid To	Nov 16 15:01:35 2027 GMT
SHA-1 Print	4B:88:18:ED:C7:5E:69:83:90:4E:E7:15:13:C8:5E:16:5F:2D:89:7C

4.3.4.2 End Entity Information

Entrust NFI PKI issues RSA2048/SHA-256 end entity certificates.

4.3.5 Exostar, LLC.

Exostar, LLC PKI is a SHA-256 Federal Bridge partner andhas one SHA-256 trust chain as shown below.

4.3.5.1 Trust Chain

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=Exostar Federated Identity Service Root CA 2,OU=Certification Authorities,O=Exostar LLC,C=US
Subject	CN=Exostar Federated Identity Service Root CA 2,OU=Certification Authorities,O=Exostar LLC,C=US
Serial #	0x315A18EF287EEE924ED386C42DB24B17
Valid From	Jan 25 15:23:41 2013 GMT
Valid To	Jan 25 15:30:19 2030 GMT
SHA-1 Print	C6:B4:F6:D0:B8:6E:EE:2C:02:96:0C:EA:8A:F4:29:37:E8:66:87:EC

ISSUING CA 1 (RSA2048/SHA256)	
Issuer	CN=Exostar Federated Identity Service Root CA 2,OU=Certification Authorities,O=Exostar LLC,C=US
Subject	CN=Exostar Federated Identity Service Signing CA 4,DC=evincible,DC=com
Serial #	0x2E000000070C47ED3776B35FC0000000000007
Valid From	Sep 30 22:48:00 2020 GMT
Valid To	Jan 25 15:30:19 2030 GMT
SHA-1 Print	D5:F1:80:DB:66:4E:C8:0B:E7:7D:9B:FD:54:84:A5:0C:EC:E5:A5:8D

4.3.5.2 End Entity Information

Exostar currently issues RSA2048/SHA-256 end entity certificates only.

4.3.6 IdenTrust NFI PKI

The IdenTrust Global Common PKI (IdenTrust NFI) issues PIV-I credentials to U.S. Federal agencies, contractors and other entities requiring U.S. Federal reliance or interoperability. IdenTrust NFI has one SHA-256 trust chain as shown below.

4.3.6.1 Trust Chain

TRUST ANCHOR (RSA4096/SHA256)	
Issuer	CN=IdenTrust Global Common Root CA 1,O=IdenTrust,C=US
Subject	CN=IdenTrust Global Common Root CA 1,O=IdenTrust,C=US
Serial #	0x0A0142800000014523CD7FD000000002
Valid From	Jan 16 18:05:05 2014 GMT
Valid To	Jan 16 18:05:05 2034 GMT
SHA-1 Print	AD:00:62:E2:90:97:D8:AA:FE:5B:47:CA:62:B3:57:D9:88:32:E6:A6

ISSUING CA 1 (RSA2048/SHA256)	
Issuer	CN=IdenTrust Global Common Root CA 1,O=IdenTrust,C=US
Subject	CN=Booz Allen Hamilton PIVi CA 01,OU=IdenTrust Global Common,O=IdenTrust,C=US
Serial #	0x14A35B824AF8D58C710CCB3D8FEA0CA8
Valid From	Aug 28 17:16:27 2015 GMT
Valid To	Aug 28 17:16:27 2025 GMT
SHA-1 Print	5C:EE:B1:8E:44:50:75:05:9A:00:BB:CC:B4:FB:D1:67:73:7B:69:37

4.3.6.2 End Entity Information

IdenTrust NFI PKI currently issues RSA2048/SHA-256 end entity certificates.

4.3.7 Lockheed Martin

Lockheed Martin PKI is an Aero Defense partner PKI and has a SHA-256 and SHA-384 infrastructure. Lockheed Martin has two trust chains as shown below.

4.3.7.1 Trust Chain 1

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=Lockheed Martin Root Certification Authority 2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Root Certification Authority 2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Serial #	0x7ACE2BC80B3F3791479C8B9E6623875B
Valid From	Jun 19 05:18:34 2013 GMT
Valid To	Jun 19 05:24:38 2030 GMT
SHA-1 Print	C5:FD:5D:D4:37:93:36:07:DE:60:F8:4C:E5:A2:A4:65:21:35:16:18

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=Lockheed Martin Root Certification Authority 2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Certification Authority 4 G2,OU=Certification Authorities,O=Lockheed Martin Corporation,C=US
Serial #	0x611952440000000000006
Valid From	Apr 11 20:13:50 2017 GMT
Valid To	Feb 11 20:23:50 2025 GMT
SHA-1 Print	E2:A9:EE:10:63:DE:F7:0B:C0:95:BA:EE:02:15:C6:FD:0B:20:E4:CE

ISSUING CA (CRLS ONLY - RSA2048/SHA256)	
Issuer	CN=Lockheed Martin Root Certification Authority 2,OU=Certification Authorities,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Certification Authority 4 G2,OU=Certification Authorities,O=Lockheed Martin Corporation,C=US
Serial #	0x114890820000000000004
Valid From	Sep 9 23:36:58 2015 GMT
Valid To	Sep 9 23:46:58 2025 GMT
SHA-1 Print	EA:44:FB:F1:CC:3B:5E:24:97:22:86:04:FD:EE:60:4B:F1:85:65:E4

4.3.7.2 Trust Chain 2

TRUST ANCHOR (RSA4098/SHA384)	
Issuer	CN=Lockheed Martin Root Certification Authority 6,OU=Certification Authority,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Root Certification Authority 6,OU=Certification Authority,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Serial #	0x3A2CC796F13329A84623284249C564F8
Valid From	Aug 3 16:50:59 2022 GMT
Valid To	Aug 3 16:58:44 2042 GMT
SHA-1 Print	72:D0:A6:A7:65:E5:A4:68:57:92:CB:EF:6E:AE:1D:22:CF:86:79:1B

ISSUING CA (RSA3072/SHA384)	
Issuer	CN=Lockheed Martin Root Certification Authority 6,OU=Certification Authority,O=Lockheed Martin Corporation,L=Denver,ST=Colorado,C=US
Subject	CN=Lockheed Martin Certification Authority 6 G3,OU=Certification Authorities,O=Lockheed Martin Corporation,C=US
Serial #	0x5000000002C6157508039D8381000000000002
Valid From	Aug 3 17:50:08 2022 GMT
Valid To	Aug 3 18:00:08 2032 GMT
SHA-1 Print	49:AB:03:AF:3C:85:8E:08:F8:4D:CD:45:65:60:EC:A8:EF:47:07:0B

4.3.7.3 End Entity Information

Lockheed currently issues RSA2048/SHA-256 end entity certificates.

4.3.8 Northrop Grumman

Northrop Grumman PKI is an Aero Defense partner through CertiPath and has one trust chain as shown below.

4.3.8.1 Trust Chain 1

TRUST ANCHOR (RSA3072/SHA256)	
Issuer	CN=Northrop Grumman Corporate Root CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporate Root CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Serial #	0x32ADA9B80CB58EAC43DC76F8AD0C0CFB
Valid From	Oct 11 16:07:09 2013 GMT
Valid To	Oct 11 16:07:09 2033 GMT
SHA-1 Print	41:16:57:F7:83:2C:26:2F:37:3D:8F:9E:09:A1:AF:C4:D0:A1:0A:6A

ISSUING CA (RSA3072/SHA256)	
Issuer	CN=Northrop Grumman Corporate Root CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporate Signing CA-G2,OU=Northrop Grumman Information Technology,O=Northrop Grumman Corporation,C=US
Serial #	0x61848400000000000002
Valid From	Oct 11 18:56:36 2013 GMT
Valid To	Oct 11 19:06:36 2026 GMT
SHA-1 Print	E4:54:AC:18:FC:9A:E0:17:3C:36:5E:87:67:B6:79:CF:E0:36:E6:3F

4.3.8.2 Trust Chain 2

TRUST ANCHOR (RSA4096/SHA384)	
Issuer	CN=Northrop Grumman Corporate Root CA-384,OU=Northrop Grumman Enterprise Services,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporate Root CA-384,OU=Northrop Grumman Enterprise Services,O=Northrop Grumman Corporation,C=US
Serial #	0x35255D5782331E9F415C55C40D4352D8
Valid From	Dec 20 16:14:30 2022 GMT
Valid To	Dec 20 16:14:30 2042 GMT
SHA-1 Print	8A:CC:AD:F0:9E:AE:E2:35:B3:E7:16:DD:F8:DD:5C:A1:F9:D6:60:C4

ISSUING CA (RSA3072/SHA384)	
Issuer	CN=Northrop Grumman Corporate Root CA-384,OU=Northrop Grumman Enterprise Services,O=Northrop Grumman Corporation,C=US
Subject	CN=Northrop Grumman Corporate Signing CA-384,OU=Northrop Grumman Enterprise Services,O=Northrop Grumman Corporation,C=US
Serial #	0x44000000062F35CB73B872F525000000000006
Valid From	Mar 1 17:55:08 2023 GMT
Valid To	Mar 1 18:05:08 2036 GMT
SHA-1 Print	23:9D:14:21:72:13:B7:DE:F0:BE:4A:2E:36:07:22:7E:83:A6:94:98

4.3.8.3 End Entity Information

Northrop currently issues RSA2048/SHA-256/SHA-384 end entity certificates.

4.3.9 WidePoint NFI PKI (formerly ORC NFI PKI)

WidePoint NFI PKI provides PIV-I credentials to federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, and, if authorized by law, state, local, and tribal governments. WidePoint NFI PKI has one SHA-256 trust chain as shown below.

4.3.9.1 Trust Chain

TRUST ANCHOR (RSA4096/SHA256)	
Issuer	CN=WidePoint NFI Root 2,OU=Certification Authorities,O=WidePoint,C=US
Subject	CN=WidePoint NFI Root 2,OU=Certification Authorities,O=WidePoint,C=US
Serial #	0x3F4A18DA6A75B9794D6C9875B9BD5B6DEE028674
Valid From	Jan 16 20:47:31 2020 GMT
Valid To	Jan 9 20:47:31 2045 GMT
SHA-1 Print	20:B0:8D:30:52:66:20:F1:9F:BD:F7:2E:A9:1A:42:A9:FA:A7:71:11

ISSUING CA (RSA4096/SHA256)	
Issuer	CN=WidePoint NFI Root 2,OU=Certification Authorities,O=WidePoint,C=US
Subject	CN=WidePoint ORC NFI 4,OU=Certification Authorities,O=WidePoint,C=US
Serial #	0x3581750BD6E26757BCB9E0A4513DA84946587EBF
Valid From	Feb 18 19:33:40 2020 GMT
Valid To	Feb 18 19:33:40 2030 GMT
SHA-1 Print	5A:95:AE:A9:90:A7:AE:C4:92:13:4A:5B:43:7C:F3:32:4F:26:07:93

ISSUING CA (RSA2048/SHA256)	
Issuer	CN=WidePoint NFI Root 2,OU=Certification Authorities,O=WidePoint,C=US
Subject	CN=WidePoint NFI CA 5,O=ORC PKI,C=US
Serial #	0x671B355A39B72FDDF67723F142ED726D4E0307B4
Valid From	Apr 17 19:29:38 2020 GMT
Valid To	Apr 18 19:29:38 2030 GMT
SHA-1 Print	52:A2:B8:99:34:A8:F5:37:19:D6:20:69:74:96:A6:EB:82:A0:6E:13

ISSUING CA (RSA4096/SHA256)	
Issuer	CN=WidePoint NFI Root 2,OU=Certification Authorities,O=WidePoint,C=US
Subject	CN=Senate PIV-I CA G6,OU=Office of the Sergeant at Arms,OU=U.S. Senate,O=U.S. Government,C=US
Serial #	0x68B3A082D2817AB76183E371219642AA20E7816A
Valid From	May 5 17:03:00 2023 GMT
Valid To	Dec 31 23:45:00 2030 GMT
SHA-1 Print	1D:94:6C:2A:17:24:ED:57:6E:43:66:04:F0:2D:BF:C3:F2:DC:CF:F0

4.3.9.2 End Entity Information

WidePoint NFI PKI issues RSA2048/SHA-256 end entity certificates.

4.3.10 Raytheon

Raytheon is an Aero Defense partner through CertiPath. They maintain infrastructure details at http://www.raytheon.com/pki.

4.3.10.1 Trust Chain

TRUST ANCHOR (RSA4096/SHA256)	
Issuer	CN=Raytheon Technologies Root CA,OU=Root-G3,O=CAs,DC=rtx,DC=com
Subject	CN=Raytheon Technologies Root CA,OU=Root-G3,O=CAs,DC=rtx,DC=com
Serial #	0x5F874B3E
Valid From	Oct 14 18:33:50 2020 GMT
Valid To	Oct 14 19:03:50 2040 GMT
SHA-1 Print	1D:75:38:E9:FE:23:B2:18:EC:16:BC:4A:7A:9D:B9:7B:91:20:50:28

ISSUING CA (RSA3072/SHA256)	
Issuer	CN=Raytheon Technologies Root CA,OU=Root-G3,O=CAs,DC=rtx,DC=com
Subject	CN=Raytheon Technologies Medium Assurance CA,OU=Class3-G3,O=CAs,DC=rtx,DC=com
Serial #	0x5F874BA8
Valid From	Oct 15 14:10:03 2020 GMT
Valid To	Oct 15 14:40:03 2030 GMT
SHA-1 Print	57:3C:DF:0B:F2:59:19:5F:90:1E:05:9F:04:28:A2:AA:77:EB:C2:F0

4.3.10.2 End Entity Information

Raytheon currently issues RSA2048/SHA-256 end entity certificates only.

4.3.11 DigiCert NFI PKI (formerly Symantec NFI PKI, VeriSign NFI PKI)

DigiCert Non-Federal Issuer (NFI) PKI provides PKI credentials to state and local Government as well as contractors. DigiCert NFI issues two types of DoD approved certificates: PIV-Interoperable (PIV-I) certificates and Medium Hardware certificates. In addition to installing the proper trust chain, DoD relying parties that interoperate with DigiCert NFI certificates must ensure that their applications support SHA-256. DigiCert NFI PKI also has device Issuing CA certificates which are currently not included because they don't meet the medium hardware assurance level requirement.

4.3.11.1 Trust Chain 1

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Serial #	0x401AC46421B31321030EBBE4121AC51D
Valid From	Apr 2 00:00:00 2008 GMT
Valid To	Dec 1 23:59:59 2037 GMT
SHA-1 Print	36:79:CA:35:66:87:72:30:4D:30:A5:FB:87:3B:0F:A7:7B:B7:0D:54

INTERMEDIATE CA (RSA2048/SHA256)	
Issuer	CN=VeriSign Universal Root Certification Authority,OU=(c) 2008 VeriSign, Inc. - For authorized use only,OU=VeriSign Trust Network,O=VeriSign, Inc.,C=US
Subject	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Serial #	0x45B1BEB5F3D47BFBC145F4D9179E22F2
Valid From	Sep 30 00:00:00 2014 GMT
Valid To	Sep 29 23:59:59 2024 GMT
SHA-1 Print	55:DB:7B:0B:02:A0:CD:64:4E:2B:B7:62:45:F8:F0:89:3A:E9:F9:A9

EID PASSPORT – LRA 2 ISSUING CA (USER CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Subject	CN=Eid Passport LRA 2 CA,OU=Eid Passport PIV-I LRA Network,O=Eid Passport, Inc.,C=US
Serial #	0x74FA80B580B11F82CDE84EF3AD8E36A4
Valid From	Mar 10 00:00:00 2015 GMT
Valid To	Sep 28 23:59:59 2024 GMT
SHA-1 Print	03:35:E3:67:01:06:DA:48:DB:61:E0:06:65:FA:16:F8:D8:C1:10:AE

CSRA ISSUING CA (USER CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Subject	CN=CSRA FBCA C3 CA,OU=CSRA FBCA MedHW,O=CSC Government Solutions LLC,C=US
Serial #	0x48B53C25944E6ED645339ECF1079FD37
Valid From	Dec 17 00:00:00 2015 GMT
Valid To	Sep 28 23:59:59 2024 GMT
SHA-1 Print	FA:ED:5B:3A:A8:5B:FE:A0:BA:8B:A8:84:68:97:06:04:4D:FC:0E:C9

CSRA ISSUING CA (DEVICE CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Subject	CN=CSRA FBCA C3 Device CA,OU=CSRA FBCA Devices,O=CSC Government Solutions LLC,C=US
Serial #	0x45AABDFFDAE1621D52B260DAF7EF3BD7
Valid From	Dec 17 00:00:00 2015 GMT
Valid To	Sep 28 23:59:59 2024 GMT
SHA-1 Print	CF:92:29:CB:50:BF:5D:C2:5C:15:6C:4F:82:5A:67:E2:96:42:36:C8

SURE ID ISSUING CA (USER CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Subject	CN=SureID Inc. CA1,OU=SureID PIV-I,O=SureID, Inc.,C=US
Serial #	0x6353433BC55FBF2E550AB0594D6CE5C3
Valid From	Jan 19 00:00:00 2016 GMT
Valid To	Sep 28 23:59:59 2024 GMT
SHA-1 Print	80:64:02:25:2C:DE:85:44:33:38:48:04:CA:F0:53:F1:52:FF:48:3F

U.S. SENATE ISSUING CA (USER CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Symantec Class 3 SSP Intermediate CA - G3,OU=Symantec Trust Network,O=Symantec Corporation,C=US
Subject	CN=Senate PIV-I CA G4,OU=Office of the Sergeant at Arms,OU=U.S. Senate,O=U.S. Government,C=US
Serial #	0x52C8B762E38B30212288790964B7AB2C
Valid From	Aug 2 00:00:00 2016 GMT
Valid To	Sep 28 23:59:59 2024 GMT
SHA-1 Print	3C:9D:0B:C4:63:DD:1A:C0:F9:10:12:B4:40:E9:BD:C1:CD:CD:0E:FF

4.3.11.2 Trust Chain 2

TRUST ANCHOR (RSA4096/SHA256)	
Issuer	CN=DigiCert Non Federal SSP Private Root CA - G2,O=DigiCert\, Inc.,C=US
Subject	CN=DigiCert Non Federal SSP Private Root CA - G2,O=DigiCert\, Inc.,C=US
Serial #	0x15633C7CA8C2573D11288E40D2D04D98
Valid From	Aug 20 00:00:00 2020 GMT
Valid To	Aug 19 23:59:59 2040 GMT
SHA-1 Print	C7:90:34:78:94:59:8D:5A:C2:05:BF:E9:B5:CA:DD:88:7E:44:96:32

INTERMEDIATE CA (RSA2048/SHA256)	
Issuer	CN=DigiCert Non Federal SSP Private Root CA - G2,O=DigiCert\, Inc.,C=US
Subject	CN=DigiCert Class 3 SSP Intermediate CA - G4,O=DigiCert\, Inc.,C=US
Serial #	0x5225C7EC937C8B6BC170A0CBEB4EACAB
Valid From	Aug 20 00:00:00 2020 GMT
Valid To	Aug 19 23:59:59 2030 GMT
SHA-1 Print	31:DF:53:34:5E:65:EA:E1:5A:CD:55:BC:82:BC:EF:84:7C:62:EE:3F

U.S. SENATE ISSUING CA (USER CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=DigiCert Class 3 SSP Intermediate CA - G4,O=DigiCert\, Inc.,C=US
Subject	CN=Senate PIV-I CA G5 PROD,OU=Office of the Sergeant at Arms,OU=U.S. Senate,O=U.S. Government,C=US
Serial #	0x2EEC611F22944F9D462A5A8BBEE06485
Valid From	Mar 25 00:00:00 2021 GMT
Valid To	Aug 18 23:59:59 2030 GMT
SHA-1 Print	81:6A:2C:18:DB:2E:56:73:20:5D:17:A9:8D:0F:FF:EF:8B:F4:77:7E

4.3.11.3 End Entity Information

DigiCert NFI PKI issues RSA2048/SHA-256 end entity certificates.

4.4 Foreign, Allied, or Coalition Partner PKIs or other PKIs (Type 5 and 6 PKIs)

Foreign, Allied, Coalition Partners, or other PKIs are classified in the DoD External Interoperability Plan as Type 5 and 6 PKIs. In addition to meeting the technical requirements and successfully completing JITC testing, Type 5 and 6 PKIs must sign a Cross Certification Arrangement (CCA). The Category III PKI Certificate Policy will be mapped to the DoD PKI Certificate Policy in accordance with DoD PKI policy. With respect to CCEB, the CCA will comply with Allied Communications Publication (ACP) 185 which is the framework for PKI Interoperability between CCEB partner nations. Type 5 and 6 partners can be approved at Medium Hardware or Device and often have additional assurance levels. For applications that cannot perform cross-certificate path validation, direct trust may be used with additional consideration. DoD users and systems that choose to directly trust a Type 5 and 6 PKI should install the appropriate trust chain into the application or system trust store and ensure that the application is inspecting the certificate to ensure it asserts a DoD approved certificate policy OID. For more information DoD approved OIDs, refer to Section 5, Assurance Levels.

4.4.1 Australian Defence Organisation (ADO) PKI

The Australian Defence Organisation (ADO) PKI provides PKI credentials to military and civilian personnel. Subscribers include any individual that has been approved as having a requirement to be authenticated as affiliated with ADO. Subscribers include:

- Defence personnel (permanent and reserve members of the Australian Defence Force (ADF), and Australian Public Service (APS) employees)
- Members of the ADF Cadets
- Contractors, Consultants and Professional Service Providers (individuals)
- Other individuals approved by ADO as having a requirement for an ADO Certificate.
- Secure Communications Resource Certificates are only issued to non-person entities (NPE), not individuals

ADO PKI has two RSA2048/SHA-256 Trust Chains as shown below. ADO has a two-way trust relationship with US DoD CCEB Interoperability Root CA 2 (SHA-256). DoD relying parties that wish to interoperate with ADO cross-certificates should ensure their applications support cross certificate path processing.

4.4.1.1 Cross-Certificate Trust Chain – US to Australia

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=US DoD CCEB Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=US DoD CCEB Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Serial #	0x01
Valid From	Aug 23 13:57:10 2016 GMT
Valid To	Dec 30 13:57:10 2030 GMT
SHA-1 Print	73:A7:1C:9F:68:03:BA:8C:0E:2B:7A:28:A5:C4:8F:87:2C:67:97:E2

US DOD CCEB INTEROPERABILITY ROOT CA 2-ADO INTEROPERABILITY CA CROSS CERTIFICATE (RSA2048/SHA256)	
Issuer	CN=US DoD CCEB Interoperability Root CA 2,OU=PKI,OU=DoD,O=U.S. Government,C=US
Subject	CN=Australian Defence Interoperability CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x0765
Valid From	Jun 25 14:59:15 2024 GMT
Valid To	Jun 25 14:59:15 2027 GMT
SHA-1 Print	80:10:95:89:00:3B:11:D6:EE:1C:25:7C:49:49:04:1C:F0:0C:CE:A9

ADO INTEROPERABILITY CA- ADO PUBLIC INDENTITY CA CROSS CERTIFICATE (RSA2048/SHA256)	
Issuer	CN=Australian Defence Interoperability CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Identity CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x07FFE5B0197DEB4D88FDB737A4011043ED69C695
Valid From	Jul 11 04:20:03 2023 GMT
Valid To	Jul 11 04:20:03 2026 GMT
SHA-1 Print	DF:C7:B7:36:44:40:39:5E:CD:29:E0:F7:4E:B6:C2:9C:A3:7A:FA:B0

ADO INTEROPERABILITY CA- ADO PUBLIC INDENTITY CA G2 CROSS CERTIFICATE (RSA2048/SHA256)	
Issuer	CN=Australian Defence Interoperability CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Identity CA G2,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x3AAAB6534A4274B4A2666D496AA83439D38E42E5
Valid From	Aug 5 01:27:46 2021 GMT
Valid To	Aug 5 01:27:46 2024 GMT
SHA-1 Print	99:62:0E:78:80:2E:B7:43:AD:51:3B:31:84:49:B1:A8:38:24:EE:8C

ADO INTEROPERABILITY CA- ADO PUBLIC INDENTITY CA AUTOENROL G2 CROSS CERTIFICATE (RSA2048/SHA256)	
Issuer	CN=Australian Defence Interoperability CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Identity CA AutoEnrol G2,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x5D2C6AF7E7C19DA9AB6CAC4A3F4AD8F4BAB1101A
Valid From	Aug 5 01:46:47 2021 GMT
Valid To	Aug 5 01:46:47 2024 GMT
SHA-1 Print	21:78:FC:A3:CD:2B:5E:77:85:86:A1:DE:16:7C:AC:C6:BC:18:1B:23

ADO INTEROPERABILITY CA- ADO PUBLIC DEVICE CA CROSS CERTIFICATE (RSA2048/SHA256)	
Issuer	CN=Australian Defence Interoperability CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Device CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x32A3898AACD9EB24B57BBB09DDC800C8EA9EAE72
Valid From	Jul 11 05:01:40 2023 GMT
Valid To	Jul 11 05:01:40 2026 GMT
SHA-1 Print	63:A8:6A:B5:34:0C:C4:1C:13:CA:D6:8F:3F:AB:75:AB:D8:1D:F8:3B

4.4.1.2 Direct Trust Chain

TRUST ANCHOR (RSA2048/SHA256)	
Issuer	CN=Australian Defence Public Root CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Root CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x29EB9233464F3241FF831900A9ADC4D9F8E3E27F
Valid From	Nov 28 22:25:28 2016 GMT
Valid To	Nov 28 22:13:48 2036 GMT
SHA-1 Print	A9:CA:FE:9D:FD:67:F4:14:5A:D3:97:D0:E2:F3:05:0D:19:8D:E6:EE

ADO PUBLIC IDENTITY ISSUING CA (USER CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Australian Defence Public Root CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Identity CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x465E48F8D5E2EC398F9636EF05283028266E1EBF
Valid From	Nov 28 23:10:31 2016 GMT
Valid To	Nov 28 23:10:31 2026 GMT
SHA-1 Print	74:E5:D1:56:04:B5:4D:E5:D5:F8:47:E7:06:73:26:1E:2F:8E:21:6B

ADO PUBLIC IDENTITY ISSUING CA G2 (USER CERTIFICATES ONLY RSA2048/SHA256)	
Issuer	CN=Australian Defence Public Root CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Identity CA G2,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0X562A6459B4455AF46F735D2B85D6288DE2DB7559
Valid From	May 6 05:00:47 2021 GMT
Valid To	May 6 04:59:08 2031 GMT
SHA-1 Print	92:F7:F1:17:6F:95:7C:51:F4:95:EB:04:BB:0A:25:36:17:FB:E5:96

ADO PUBLIC IDENTITY ISSUING CA AUTOENROL G2 (USER CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Australian Defence Public Root CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Identity CA AutoEnrol G2,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Serial #	0x52274CE24C63571A52D2788F844494161E21C854
Valid From	May 6 05:14:08 2021 GMT
Valid To	May 6 05:13:50 2031 GMT
SHA-1 Print	EF:74:E7:BD:2B:80:04:69:EB:90:EA:3A:EC:01:B2:C2:4F:A3:51:8D

ADO PUBLIC DEVICE ISSUING CA (DEVICE CERTIFICATES ONLY - RSA2048/SHA256)	
Issuer	CN=Australian Defence Public Root CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=AU
Subject	CN=Australian Defence Public Device CA,OU=CAs,OU=PKI,OU=DoD,O=GOV,C=A
Serial #	0x6A82BB0C9A0A4D178708995809AF63D29E6BE39D
Valid From	Nov 28 23:32:46 2016 GMT
Valid To	Nov 28 23:32:46 2026 GMT
SHA-1 Print	CC:D8:00:76:F6:A4:70:99:BB:F6:8F:02:8C:F0:96:9E:DF:6F:F2:26

4.4.1.3 End Entity Information

ADO PKI currently issues RSA2048/SHA-256 end entity certificates only.

4.4.2 Netherlands Ministry of Defence PKI

The Netherlands Ministry of Defence (NL MoD) operates a PKI to provide defense employees with a capability for secure communications with reliable authentication. It is an implementation of the Dutch Law for electronic signatures and is subordinate to the Dutch government PKI Policy. The NL MoD PKI primarily issues certificates to defense employees and affiliates. NL MoD is a foreign PKI, therefore they are classified as a Category III PKI since they are an "Other Mission Partner PKI," as specified in DoDI 8520.02. The CertiPath Policy Management Authority (PMA) is responsible for setting, implementing, and administering policy decisions related to the CertiPath Bridge and the related CAs that are cross certified with the CertiPath Bridge.

NL MoD PKI has one SHA-256 Trust Chain as shown below. DoD relying parties that wish to interoperate with NL MoD should ensure their applications support SHA-256.

4.4.2.1 SHA-256 Trust Chain

TRUST ANCHOR (RSA4096/SHA256)	
Issuer	CN=Staat der Nederlanden Root CA - G3,O=Staat der Nederlanden,C=NL
Subject	CN=Staat der Nederlanden Root CA - G3,O=Staat der Nederlanden,C=NL
Serial #	0x98A239
Valid From	Nov 14 11:28:42 2013 GMT
Valid To	Nov 13 23:00:00 2028 GMT
SHA-1 Print	D8:EB:6B:41:51:92:59:E0:F3:E7:85:00:C0:3D:B6:88:97:C9:EE:FC

INTERMEDIATE CA (RSA4096/SHA256)	
Issuer	CN=Staat der Nederlanden Root CA - G3,O=Staat der Nederlanden,C=NL
Subject	CN=Staat der Nederlanden Organisatie Persoon CA - G3,O=Staat der Nederlanden,C=NL
Serial #	0x98A246
Valid From	Nov 14 15:09:37 2013 GMT
Valid To	Nov 12 23:00:00 2028 GMT
SHA-1 Print	4F:F6:F8:A7:12:D7:3E:15:E5:19:41:CC:B3:9E:F2:DE:8E:F9:83:72

ISSUING CA (RSA4096/SHA256)	
Issuer	CN=Staat der Nederlanden Organisatie Persoon CA - G3,O=Staat der Nederlanden,C=NL
Subject	CN=Ministerie van Defensie PKIoverheid Organisatie Persoon CA - G3,2.5.4.97=#0C0E4E54524E4C2D3237333730393835,O=Ministerie van Defensie,C=NL
Serial #	0x2A41257774A0AC234977FE3A77B9E67E79F57D4D
Valid From	Jun 27 08:49:06 2019 GMT
Valid To	Nov 12 00:00:00 2028 GMT
SHA-1 Print	58:38:A2:CB:26:5E:0A:EB:ED:FF:30:69:CF:AB:3F:88:48:71:95:AD

4.4.2.2 End Entity Information

NL MoD issues RSA2048/SHA-256 end entity certificates.

5.0 Assurance Levels[14]

Assurance levels are represented by Certificate Policy Object Identifiers (OIDs) which are asserted in the *Certificate Policies* x509 certificate extension.[15] Every PKI has its own certificate policy OIDs which are registered uniquely to the organization and are defined in the PKI's certificate policy. Since each PKI has different certificate policy OIDs which are separately defined, it is easier to speak in terms of relative Federal PKI (FPKI) assurance levels. This especially works well since part of the cross certification process includes mapping equivalent policies. In the cross certification trust model, a PKI can enforce a set of acceptable certificate policies through policy mappings. *Policy Mappings* is an x509 certificate extension used in cross-certificates. In DoD, policy mappings are defined in the cross-certificate issued by the Interoperability Root CAs. DoD PKI only maps to FBCA medium hardware assurance level or higher, which causes all lower assurance levels to be invalid according to the standard. In the direct trust model, the responsibility is on the data owner to enforce the DoD allowable set of policies. This can be done through defining an initial-policy-set for applications that support it or through some other means of certificate policy OID restriction or filtering. Some commercial applications such as the Trust Anchor Constraints Tool (TACT) and Webcullis support this functionality.[16]

DoD PKI and ECA PKI, software certificates are allowed as an approved form of identity credential per DoD instruction 8520.03. However, DoD Instruction 8520.02, Enclosure 3 Paragraph 1c states: "While DoD medium assurance (software) certificates are acceptable for use within the DoD, they are primarily intended for use in servers and other non-person entities (e.g., SSL certificates), and their use for identifying people (i.e., issuance of an identity certificate for a person) should be minimized".

5.1 DoD Assurance Levels

All DoD assurance levels are permitted for use within DoD. Although some DoD relying parties may wish to further restrict the set of acceptable DoD policies. For instance, some application owners may require hardware certificates and not accept software certificates which have a lower assurance level. The DoD certificate policy OIDs are shown below. More information is provided in the DoD Certificate Policy.[17]

CERTIFICATE POLICY OID	DESCRIPTIVE NAME
2.16.840.1.101.2.1.11.5 *	id-US-dod-medium
2.16.840.1.101.2.1.11.9 *	id-US-dod-mediumhardware
2.16.840.1.101.2.1.11.10	id-US-dod-PIV-Auth[18]
2.16.840.1.101.2.1.11.17 *	id-US-dod-mediumNPE
2.16.840.1.101.2.1.11.18 *	id-US-dod-medium-2048
2.16.840.1.101.2.1.11.19 *	id-US-dod-mediumHardware-2048
2.16.840.1.101.2.1.11.20	id-US-dod-PIV-Auth-2048[19]
2.16.840.1.101.2.1.11.31	id-US-dod-peerInterop[20]

[14] For more information on assurance levels, see NIST 800-63, Digital Identity Guidelines https://pages.nist.gov/800-63-3

[15] RFC 5280 can be found at http://www.ietf.org/rfc/rfc5280.txt

[16] Webcullis can be found at http://pkif.sourceforge.net/webcullis.html

[17] The DoD Certificate Policy can be found at https://dl.cyber.mil/pki-pke/pdf/unclass-dod_cp.pdf

[18] id-US-dod-PIV-Auth is not used operationally within DoD.

[19] id-US-dod-PIV-Auth-2048 is not used operationally within DoD.

[20] The Peer Interop OID is only used for cross-certificates issued to external PKIs that cannot demonstrate comparability to one or more requirements of Medium Assurance and the DoD determines that there is a need for interoperation and

CERTIFICATE POLICY OID	DESCRIPTIVE NAME
2.16.840.1.101.2.1.11.36	id-US-dod-mediumNPE-112
2.16.840.1.101.2.1.11.37	id-US-dod-mediumNPE-128
2.16.840.1.101.2.1.11.38	id-US-dod-mediumNPE-192
2.16.840.1.101.2.1.11.39	id-US-dod-medium-112
2.16.840.1.101.2.1.11.40	id-US-dod-medium-128
2.16.840.1.101.2.1.11.41	id-US-dod-medium-192
2.16.840.1.101.2.1.11.42	id-US-dod-mediumHardware-112
2.16.840.1.101.2.1.11.43	id-US-dod-mediumHardware-128
2.16.840.1.101.2.1.11.44	id-US-dod-mediumHardware-192
2.16.840.1.101.2.1.11.59	id-US-dod-admin
2.16.840.1.101.2.1.11.60	id-US-dod-internalNPE-112
2.16.840.1.101.2.1.11.61	id-US-dod-internalNPE-128
2.16.840.1.101.2.1.11.62	id-US-dod-internalNPE-192

* These policy OIDs are included for historical purposes and are no longer authorized for use in end entity certificates issued under this CP. The terms Medium, Medium NPE, and Medium-Hardware are still used throughout this CP to refer to groups of policy OIDs with the same requirements as described below.

5.2 ECA PKI Assurance Levels

All ECA PKI assurance levels are permitted for use within DoD. Although some relying parties may wish to further restrict the set of acceptable ECA policies. For instance, some application owners may require hardware certificates and not accept software certificates which have a lower assurance level. The ECA certificate policy OIDs are shown below. More information is provided in the ECA Certificate Policy.[21]

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.12.1	id-eca-medium	Yes. All ECA Certificate Policies are allowed per DoD policy
2.16.840.1.101.3.2.1.12.2	id-eca-medium-hardware	
2.16.840.1.101.3.2.1.12.3	id-eca-medium-token	
2.16.840.1.101.3.2.1.12.4	id-eca-medium-sha256	
2.16.840.1.101.3.2.1.12.5	id-eca-medium-token-sha256	
2.16.840.1.101.3.2.1.12.6	id-eca-medium-hardware-pivi	
2.16.840.1.101.3.2.1.12.7	id-eca-cardauth-pivi	
2.16.840.1.101.3.2.1.12.8	id-eca-contentsigning-pivi[22]	
2.16.840.1.101.3.2.1.12.9	id-eca-medium-device-sha256	
2.16.840.1.101.3.2.1.12.10	id-eca-medium-hardware-sha256	

5.3 Federal PKI (FPKI) Assurance Levels

All DoD approved external PKIs are cross certified with FPKI, either directly or through an SSP or another bridge. Part of the cross certification process includes mapping organizational certificate policy OIDs to equivalent FPKI policy OIDs. DoD currently has cross-certificate relationships with the Federal Bridge CA to support cross-certificate trust with our SHA-256 partners. DoD enforces RFC 5280 constraints in its cross-certificates and only maps to FPKI policies which are at a hardware assurance level or higher, causing all lower assurance certificate policies to be considered invalid by policy. Application owners that interoperate using direct trust will be responsible for ensuring that only certificates at DoD allowed assurance levels are accepted by their applications. In order to comply with NIST cryptographic guidance, FPKI introduced a significant

acceptance of certificates issued by the external PKIs. Relying Parties need to ensure that it is appropriate to use the certificate issued by a PKI that maps to Peer Interop before enabling systems to accept these certificates.

[21] The ECA CP can be found at https://dl.cyber.mil/pki-pke/pdf/unclass-eca_cp_v4-6_final_signed.pdf

[22] All contentsigning OIDs are intended only for use in digitally signing data objects on a PIV-I smart card and shall not be used for any other purpose. Content Signing PIV-I certificates shall only be issued to Card Management Systems.

architectural redesign in 2015[23]. The redesign introduced two new SHA-256 FPKI systems: Federal Bridge CA and Federal Common Policy CA. FPKI has decommissioned the legacy FBCA (ou=Entrust), SHA-1 Federal Root CA, Common Policy systems.

5.3.1 Federal PKI Assurance Levels

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance	No
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance	No
2.16.840.1.101.3.2.1.3.3	id-fpki-certpcy-mediumAssurance	No
2.16.840.1.101.3.2.1.3.4	id-fpki-certpcy-highAssurance	Yes
2.16.840.1.101.3.2.1.3.5	fpki-certpcy-testAssurance	No
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	No
2.16.840.1.101.3.2.1.3.9	id-eGov-Level1	No
2.16.840.1.101.3.2.1.3.10	id-eGov-Level2	No
2.16.840.1.101.3.2.1.3.11	id-eGov-Applications	No
2.16.840.1.101.3.2.1.3.12	id-fpki-certpcy-mediumHardware	Yes
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes
2.16.840.1.101.3.2.1.3.14	id-fpki-certpcy-medium-CBP	No
2.16.840.1.101.3.2.1.3.15	id-fpki-certpcy-mediumHW-CBP	No
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-Physical access only
2.16.840.1.101.3.2.1.3.18	id-fpki-certpcy-pivi-hardware	Yes
2.16.840.1.101.3.2.1.3.19	id-fpki-certpcy-pivi-cardAuth	Yes-Physical access only
2.16.840.1.101.3.2.1.3.20	id-fpki-certpcy-pivi-contentSigning	Yes
2.16.840.1.101.3.2.1.3.28	id-eGov-Level1-IdP	No
2.16.840.1.101.3.2.1.3.29	id-eGov-Level2-IdP	No
2.16.840.1.101.3.2.1.3.30	id-eGov-Level3-IdP	No
2.16.840.1.101.3.2.1.3.31	id-eGov-Level4-IdP	No
2.16.840.1.101.3.2.1.3.32	id-eGov-BAE-Broker	No
2.16.840.1.101.3.2.1.3.33	id-eGov-RelyingParty	No
2.16.840.1.101.3.2.1.3.34	id-eGov-MetaSigner	No
2.16.840.1.101.3.2.1.3.35	id-eGov-MetaSigner-Hardware	No
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes
2.16.840.1.101.3.2.1.3.37	id-fpki-certpcy-mediumDevice	No. Currently under consideration.
2.16.840.1.101.3.2.1.3.38	id-fpki-certpcy-mediumDeviceHardware	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	Yes

5.4 Entrust Federal SSP PKI Assurance Levels

Entrust Federal SSP PKI currently has a one-way cross-certificate relationship with Federal Common Policy CA G2. The Federal Common Policy CA G2 issued a certificate to Entrust Managed Services Root CA, but there is no reverse certificate. Entrust Federal SSP PKI currently asserts the following certificate policies in its certificates, five of which are permitted by DoD policy:

[23] NIST Special Publication 800-78-4 can be found at http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-78-4.pdf

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes-asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes-asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	Yes-asserted	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	Yes-asserted	Yes

5.5 WidePoint Federal SSP PKI Assurance Levels

WidePoint Federal SSP PKI has a one-way cross-certificate relationship with FPKI, with cross certificates issued from Federal Common Policy CA G2 to ORC SSP 4 and WidePoint ORC SSP 5.

5.5.1 WidePoint Federal SSP PKI Asserted Policies

WidePoint Federal SSP PKI currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes-asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes-asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes-asserted	Yes

5.6 Department of State PKI Assurance Levels

Department of State currently has a two-way cross-certificate relationship with Federal Common Policy CA. It currently asserts the following certificate policies in its certificates, six of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.6.1	state-basic	Yes. Mapped	No
2.16.840.1.101.3.2.1.6.2	state-low	Yes. Mapped	No
2.16.840.1.101.3.2.1.6.3	state-moderate	Yes. Mapped	No
2.16.840.1.101.3.2.1.6.4	state-high	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.6.12	state-medHW	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.16	id-fpki-common-high	Yes. Asserted	Yes

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-pivContentSigning	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	Yes. Asserted	Yes

5.7 U.S. Treasury SSP PKI Assurance Levels

U.S Treasury Root CA currently has a two-way cross-certificate relationship with Federal Common Policy CA. U.S. Treasury SSP PKI currently asserts the following certificate policies in its certificates, six of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.5.2	id-treasury-certpcy-rudimentary	Yes. Mapped	No
2.16.840.1.101.3.2.1.5.3	id-treasury-certpcy-basicindividual	Yes. Mapped	No
2.16.840.1.101.3.2.1.5.4	id-treasury-certpcy-mediumhardware	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.5.5	id-treasury-certpcy-high	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.5.7	id-treasury-certpcy-medium	Yes. Mapped	No
2.16.840.1.101.3.2.1.5.8	id-treasury-certpcy-basicorganizational	No	No
2.16.840.1.101.3.2.1.5.10	id-treasury-pivi-hardware	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.5.11	id-treasury-pivi-cardAuth	Yes. Mapped	Yes-Physical access only
2.16.840.1.101.3.2.1.5.12	id-treasury-pivi-contentSigning	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.16	id-fpki-common-high	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	Yes. Asserted	Yes

5.8 DigiCert Federal SSP PKI Assurance Levels

DigiCert Federal SSP SHA-2 PKI is subordinate to Federal Common Policy CA G2 which has a two-way cross-certificate with FBCA and several legacy PKIs. Federal Common Policy is also the trust anchor for the other SSPs.

5.8.1 DigiCert Federal SSP PKI Asserted Policies

DigiCert Federal SSP PKI currently asserts the following certificate policies in its certificates, four of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes. Asserted & Mapped	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes. Asserted	Yes

5.8.2 DigiCert Federal SSP PKI Inherited Policies

Although DigiCert Federal SSP PKI only asserts the certificate policies in section 5.8.1, the parent of its SHA-256 PKI, Federal Common Policy CA, has issued subordinate CA certificates to each SSP as well as cross-certificates to Department of State and Federal Bridge CA. Federal Common Policy CA G2 asserts the following certificate policies in its cross-certificate to FBCA, extending trust to the entire FBCA community at many assurance levels.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.3	id-fpki-certpcy-mediumAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.4	id-fpki-certpcy-highAssurance	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Mapped	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.12	id-fpki-certpcy-mediumHardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.14	id-fpki-certpcy-medium-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.15	id-fpki-certpcy-mediumHW-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.18	id-fpki-certpcy-pivi-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.19	id-fpki-certpcy-pivi-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.20	id-fpki-certpcy-pivi-contentSigning	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.36	id-fpki-common-devicesHardware	Yes. Asserted & Mapped	Yes
2.16.840.1.101.3.2.1.3.37	id-fpki-certpcy-mediumDevice	Yes. Asserted	No. Currently under consideration.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.38	id-fpki-certpcy-mediumDeviceHardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.39	id-fpki-common-piv-contentSigning	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.40	id-fpki-common-pivAuth-derived	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.41	id-fpki-common-pivAuth-derived-hardware	Yes. Asserted	Yes

5.9 Verizon/Cybertrust Federal SSP PKI Assurance Levels

Verizon/Cybertrust Federal SSP PKI is subordinate to Federal Common Policy CA G2 which has a two-way cross-certificate with FBCA and several legacy PKIs. Federal Common Policy is also the trust anchor for the other SSPs.

5.9.1 Verizon/Cybertrust Federal SSP PKI Asserted Policies

Verizon/Cybertrust Federal SSP PKI currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes-asserted	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes-asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes-asserted	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes-asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.39	id-fpki-common-pivcontentsigning	Yes-asserted	Yes

5.9.2 Verizon/Cybertrust Federal SSP PKI Inherited Policies

Although Verizon/Cybertrust Federal SSP PKI only asserts the certificate policies in section 5.9.1, its parent, Federal Common Policy CA G2, has issued subordinate CA certificates to each SSP as well as cross-certificates to Department of Veteran Affairs and FBCA. Federal Common Policy CA G2 asserts the following certificate policies in its cross-certificate to FBCA, extending trust to the entire FBCA community at many assurance levels.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.1	id-fpki-certpcy-rudimentaryAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.2	id-fpki-certpcy-basicAssurance	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.6	id-fpki-common-policy	Yes. Mapped	No
2.16.840.1.101.3.2.1.3.7	id-fpki-common-hardware	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.8	id-fpki-common-devices	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.13	id-fpki-common-authentication	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.14	id-fpki-certpcy-medium-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.15	id-fpki-certpcy-mediumHW-CBP	Yes. Asserted	No
2.16.840.1.101.3.2.1.3.16	id-fpki-common-High	Yes. Mapped	Yes
2.16.840.1.101.3.2.1.3.17	id-fpki-common-cardAuth	Yes. Asserted	Yes-Physical access only

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.101.3.2.1.3.18	id-fpki-certpcy-pivi-hardware	Yes. Asserted	Yes
2.16.840.1.101.3.2.1.3.19	id-fpki-certpcy-pivi-cardAuth	Yes. Asserted	Yes-Physical access only
2.16.840.1.101.3.2.1.3.20	id-fpki-certpcy-pivi-contentSigning	Yes. Asserted	Yes

5.10 Boeing PKI Assurance Levels

Boeing currently has a two-way cross-certificate relationship with the SHA-1 CertiPath Bridge CA. The SHA-1 CertiPath Bridge CA has a two-way cross-certificate relationship with the SHA-1 Federal Root CA. Boeing currently asserts the following certificate policies in its certificates, one of which is permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.73.15.3.1.4	id-mediumSoftware-SHA-1	No	No
1.3.6.1.4.1.73.15.3.1.5	id-mediumHardware-SHA-1	No	No
1.3.6.1.4.1.73.15.3.1.8	id-mediumCBPSoftware-SHA-1	No	No
1.3.6.1.4.1.73.15.3.1.9	id-mediumCBPHardware-SHA-1	No	No
1.3.6.1.4.1.73.15.3.1.10	id-mediumHardware-cardAuthentication-SHA1	No	No
1.3.6.1.4.1.73.15.3.1.11	id-mediumSoftware-SHA256	Yes	No
1.3.6.1.4.1.73.15.3.1.12	id-mediumHardware-SHA256	Yes	Yes
1.3.6.1.4.1.73.15.3.1.13	id-mediumCBPSoftware-SHA256	No	No
1.3.6.1.4.1.73.15.3.1.14	id-mediumCBPHardware-SHA256	No	No
1.3.6.1.4.1.73.15.3.1.15	id-mediumHardware-cardAuthentication-SHA256	Yes	Yes – Physical Access Only
1.3.6.1.4.1.73.15.3.1.16	id-mediumHardware-contentSigning-SHA1	Yes	No
1.3.6.1.4.1.73.15.3.1.17	id-mediumHardware-contentSigning-SHA256	Yes	Yes

5.11 Carillon Federal Services PKI Assurance Levels[24]

Carillon Federal Services PKI currently has a two-way cross-certificate relationship with the CertiPath Bridge CA – G2. It currently asserts the following certificate policies in its certificates, four of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.45606.3.1.1	id-CFSINFRASTRUCTURE	No	No
1.3.6.1.4.1.45606.3.1.2	id-CFSINFRASTRUCTURE-256	No	No
1.3.6.1.4.1.45606.3.1.3	id-basicSoftware	No	No
1.3.6.1.4.1.45606.3.1.4	id-basicHardware	No	No
1.3.6.1.4.1.45606.3.1.7	id-mediumSoftware	No	No
1.3.6.1.4.1.45606.3.1.8	id-mediumHardware	No	No
1.3.6.1.4.1.45606.3.1.9	id-basicSoftware-256	No	No
1.3.6.1.4.1.45606.3.1.10	id-basicHardware-256	No	No
1.3.6.1.4.1.45606.3.1.11	id-mediumSoftware-256	No	No
1.3.6.1.4.1.45606.3.1.12	id-mediumHardware-256	Yes	Yes
1.3.6.1.4.1.45606.3.1.20	id-AIVHardware	Yes	Yes
1.3.6.1.4.1.45606.3.1.21	id-AIVCardAuth	Yes	Yes – Physical Access Only
1.3.6.1.4.1.45606.3.1.22	id-AIVContentSigning	Yes	Yes

[24] Carillon Federal Services Inc. Public Key Infrastructure Certificate Policy, CFS-POL-007, https://pub.carillon.ca/CertificatePolicy.pdf December 7, 2017.

NOTE: AIV (Advanced Identity Verification) enables the issuance of smart cards that are technically interoperable with United States Federal Government Personal Identity Verification (PIV) Card readers and applications as well as PIV-Interoperable (PIV-I) card readers and applications. AIV fully maps to PIV-I specification as defined by the U.S. Federal Government.

5.12 Carillon Information Security PKI Assurance Levels[25]

Carillon Information Security PKI currently has a two-way cross-certificate relationship with the CertiPath Bridge CA – G2. It currently asserts the following certificate policies in its certificates, six of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.25054.3.1.3	id-basicSoftware	No	No
1.3.6.1.4.1.25054.3.1.4	id-basicHardware	No	No
1.3.6.1.4.1.25054.3.1.5	id-mediumSoftwareCBP	No	No
1.3.6.1.4.1.25054.3.1.6	id-mediumHardwareCBP	No	No
1.3.6.1.4.1.25054.3.1.7	id-mediumSoftware	No	No
1.3.6.1.4.1.25054.3.1.8	id-mediumHardware	No	No
1.3.6.1.4.1.25054.3.1.9	id-basicSoftware-256	No	No
1.3.6.1.4.1.25054.3.1.10	id-basicHardware-256	No	No
1.3.6.1.4.1.25054.3.1.11	id-mediumSoftware-256	Yes	Yes – Email Encryption Only
1.3.6.1.4.1.25054.3.1.12	id-mediumHardware-256	Yes	Yes
1.3.6.1.4.1.25054.3.1.13	id-mediumDeviceSoftware-256	Yes	No
1.3.6.1.4.1.25054.3.1.14	id-mediumDeviceHardware-256	Yes	Yes
1.3.6.1.4.1.25054.3.1.15	id-mediumAeroSoftware-256	No	No
1.3.6.1.4.1.25054.3.1.16	id-mediumAeroHardware-256	No	No
1.3.6.1.4.1.25054.3.1.17	id-basicDeviceSoftware-256	No	No
1.3.6.1.4.1.25054.3.1.18	id-basicDeviceHardware-256	No	No
1.3.6.1.4.1.25054.3.1.20	id-iceCAPHardware	Yes	Yes
1.3.6.1.4.1.25054.3.1.21	id-iceCAPCardAuth	Yes	Yes – Physical Access Only
1.3.6.1.4.1.25054.3.1.22	id-iceCAPContentSigning	Yes	Yes
1.3.6.1.4.1.25054.3.1.30	id-mediumSoftwareCBP-256	Yes	No
1.3.6.1.4.1.25054.3.1.31	id-mediumHardwareCBP-256	Yes	No

5.13 CertiPath Bridge Assurance Levels[26]

CertiPath an organization that provides bridge services and has two bridge CAs that are cross certified with Federal PKI. They have the SHA-256 CertiPath Bridge CA – G2 which is cross certified with Federal Bridge CA. CertiPath vets and cross-certifies commercial and Aero/Defense partners to include PIV-Interoperable (PIV-I) partners.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.24019.1.1.1.1	id-mediumSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.2	id-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.3	id-highHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.4	id-mediumCBPSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.5	id-mediumCBPHardware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.6	id-highCBPHardware	No.	No

[25] Carillon Information Security Inc, Publik Key Infrastructure Certificate Policy, CIS, POL-007

[26] CertiPath has additional OIDs that are obsolete, reserved, or used for test purposes. CertiPath lists the entire arc here: - https://certipath.com/services/federated-trust/policy-management-authority/

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.24019.1.1.1.7	id-IceCAP-hardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.8	id-IceCAP-cardAuth	Yes. Mapped	Yes-Physical access only
1.3.6.1.4.1.24019.1.1.1.9	id-IceCAP-contentSigning	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.17	id-variant-mediumSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.18	id-variant-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.19	id-variant-highHardware	Yes. Mapped	Yes
1.3.6.1.4.1.24019.1.1.1.20	id-variant-mediumCBPSoftware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.21	id-variant-mediumCBPHardware	Yes. Mapped	No
1.3.6.1.4.1.24019.1.1.1.22	id-variant-highCBPHardware	Yes. Mapped	No

5.14 Entrust Managed Services NFI PKI Assurance Levels

Entrust NFI PKI currently has a two-way cross-certificate relationship with the SHA-256 FBCA. It currently asserts the following certificate policies in its certificates, five of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.114027.200.3.10.7.1	id-emspki-nfssp-medium-policy	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.2	id-emspki-nfssp-medium-hardware	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.7.3	id-emspki-nfssp-medium-devices	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.4	id-emspki-nfssp-mediumauthentication	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.7.5	id-emspki-nfssp-medium-cardAuth	No	No
2.16.840.1.114027.200.3.10.7.6	id-emspki-nfssp-pivi-hardware	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.7.7	id-emspki-nfssp-basic-policy	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.8	id-emspki-nfssp-rudimentary-policy	Yes. Mapped	No
2.16.840.1.114027.200.3.10.7.9	id-emspki-nfssp-pivi-contentsigning	Yes. Mapped	Yes
2.16.840.1.114027.200.3.10.7.10	id-emspki-nfssp-contentsigning	Yes	No
2.16.840.1.114027.200.3.10.7.11	id-emspki-nfssp-cardauth	Yes	No
2.16.840.1.114027.200.3.10.7.12	id-emspki-nfssp-derived-credential	Yes	No
2.16.840.1.114027.200.3.10.7.13	id-emspki-nfssp-pivi-cardAuth	Yes	Yes
2.16.840.1.114027.200.3.10.7.14	id-emspki-nfssp-medium-CBP	Yes	No
2.16.840.1.114027.200.3.10.7.15	id-emspki-nfssp-mediumHW-CBP	Yes	No
2.16.840.1.114027.200.3.10.7.16	id-emspki-nfssp-medium-devicesHW	Yes	Yes

5.15 Exostar Assurance Levels

Exostar Federated Identity Service Root CA 2 currently has a two-way cross-certificate relationship with the SHA-256 Federal Bridge CA. It currently asserts the following certificate policies in its certificates, one of which is permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.13948.1.1.1.5	id-mediumSoftware-sha2	Yes. Mapped	No
1.3.6.1.4.1.13948.1.1.1.6	id-mediumHardware-sha2	Yes. Mapped	Yes
1.3.6.1.4.1.13948.1.1.1.8	id-basic-sha2	Yes. Mapped	No

5.16 IdenTrust NFI PKI Assurance Levels

IdenTrust Global Common Root CA currently has a two-way cross-certificate relationship with the SHA-256 Federal Bridge CA. It currently asserts the following certificate policies in its certificates, seven of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.113839.0.100.2.1	id-igc-BasicSoftware-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.2.2	id-igc-BasicSoftware-Encryption Certificate	Yes. Mapped	No
2.16.840.1.113839.0.100.3.1	id-igc-MediumSoftware-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.3.2	id-igc-MediumSoftware-EncryptionCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.12.1	id-igc-MediumHardware-SigningCertificate	Yes. Mapped	Yes
2.16.840.1.113839.0.100.12.2	id-igc-MediumHardware-EncryptionCertificate	Yes. Mapped	Yes
2.16.840.1.113839.0.100.14.1	id-igc-MediumCommercialBestPractices-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.14.2	id-igc-MediumCommercialBest Practices-EncryptionCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.15.1	id-igc-MediumHardwareCommercialBestPractices-SigningCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.15.2	id-igc-MediumHardwareCommercialBestPractices-EncryptionCertificate	Yes. Mapped	No
2.16.840.1.113839.0.100.18.0	id-igc-pivi-hardware-identity	Yes. Mapped	Yes
2.16.840.1.113839.0.100.18.1	id-igc-pivi-hardware-signing	Yes. Mapped	Yes
2.16.840.1.113839.0.100.18.2	id-igc-pivi-hardware-encryption	Yes. Mapped	Yes
2.16.840.1.113839.0.100.19.1	id-igc-pivi-CardAuthentication	Yes. Mapped	Yes – Physical access only
2.16.840.1.113839.0.100.20.1	id-igc-pivi-contentSigning	Yes. Mapped	Yes
2.16.840.1.113839.0.100.37.1	id-igc-MediumDeviceSoftware-DeviceCertificate	No	No
2.16.840.1.113839.0.100.37.2	id-igc-MediumDeviceSoftware-SSLcertificate	No	No
2.16.840.1.113839.0.100.38.1	id-igc-MediumDeviceHardware-DeviceCertificate	No	No

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.113839.0.100.38.2	id-igc-MediumDeviceHardware-SSLcertificate	No	No

5.17 Lockheed Martin Assurance Levels

Lockheed Martin currently has a two-way cross-certificate relationship with the SHA-256 CertiPath Bridge CA. The SHA-256 CertiPath Bridge CA has a two-way cross-certificate relationship with the Federal Bridge CA. Lockheed Martin currently asserts the following certificate policies in its certificates, one of which is permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.103.100.1.1.3.3	Medium Assurance Hardware Certificate	Yes. Mapped	Yes
1.3.6.1.4.1.103.100.1.1.3.4	Medium Assurance Software Certificate	Yes. Mapped	No
1.3.6.1.4.1.103.100.1.1.3.3	Medium Assurance Derived Certificate	Yes. Mapped	No
1.3.6.1.4.1.103.100.1.1.3.4	Medium Assurance Hardware Device Certificate	Yes. Mapped	No

5.18 Netherlands Ministry of Defence PKI Assurance Levels

The Netherlands Ministry of Defence PKI currently has a two-way cross-certificate relationship with the CertiPath Bridge CA – G3 (SHA-256). It currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.528.1.1003.1.2.3.1	Citizen - Authenticity	No	No
2.16.528.1.1003.1.2.3.2	Citizen - Non repudiation	No	No
2.16.528.1.1003.1.2.3.3	Citizen - Confidentiality	No	No
2.16.528.1.1003.1.2.5.1	Authenticity	Yes. Mapped	Yes
2.16.528.1.1003.1.2.5.2	Irrefutability/signature	Yes. Mapped	Yes
2.16.528.1.1003.1.2.5.3	Confidentiality	Yes. Mapped	Yes
2.16.528.1.1003.1.2.5.4	Services - Authenticity	No	No
2.16.528.1.1003.1.2.5.5	Services - Confidentiality	No	No
2.16.528.1.1003.1.2.5.6	Services - Server	No	No
2.16.528.1.1003.1.2.5.7	Services – Non-repudiation	No	No
2.16.528.1.1003.1.2.6.1	Autonomous Devices - Authenticity	No	No
2.16.528.1.1003.1.2.6.2	Autonomous Devices – Confidentiality	No	No
2.16.528.1.1003.1.2.6.3	Autonomous Devices - Combination	No	No

5.19 Northrop Grumman PKI Assurance Levels

Northrop Grumman Corporation Root CAs currently has a two-way cross-certificate relationship with the SHA-256 CertiPath Bridge CA – G2. It currently asserts the following certificate policies in its certificates, five of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.16334.509.2.7	Medium Assurance-256 Software Certificate	Yes. Mapped	No
1.3.6.1.4.1.16334.509.2.8	Medium Assurance-256 Hardware Token	Yes. Mapped	Yes
1.3.6.1.4.1.16334.509.2.9	PIV-I Assurance-256 Hardware Token	Yes. Mapped	Yes
1.3.6.1.4.1.16334.509.2.10	PIV-I Assurance-256 Card Authentication	Yes. Mapped	Yes. Physical Access Only
1.3.6.1.4.1.16334.509.2.11	PIV-I Assurance-256 Content Signing	Yes. Mapped	Yes
1.3.6.1.4.1.16334.509.2.13	Medium Assurance-384 Software Certificate	Yes. Mapped	No
1.3.6.1.4.1.16334.509.2.14	Medium Assurance-384 Hardware Token	Yes. Mapped	Yes

5.20 WidePoint NFI PKI Assurance Levels

WidePoint's ORC NFI CA 3 has a two-way cross-certificate relationship with the Federal Bridge CA. ORC NFI CA 3 currently asserts the following certificate policies in its certificates, four of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.3922.1.1.1.3	id-orc-nfissp-medium	Yes. Mapped	No
1.3.6.1.4.1.3922.1.1.1.12	id-orc-nfissp-mediumhardware	Yes. Mapped	Yes
1.3.6.1.4.1.3922.1.1.1.18	id-orc-nfissp-pivi-hardware	Yes. Mapped	Yes
1.3.6.1.4.1.3922.1.1.1.19	id-orc-nfissp-pivi-cardAuth	Yes. Mapped	Yes – Physical Access Only
1.3.6.1.4.1.3922.1.1.1.20	id-orc-nfissp-pivi-contentSigning	Yes. Mapped	Yes
1.3.6.1.4.1.3922.1.1.1.37	id-orc-nfissp-mediumDevices	Yes. Mapped	No
1.3.6.1.4.1.3922.1.1.1.38	id-orc-nfissp-mediumDeviceHardware	Yes. Mapped	Yes

5.21 Raytheon PKI Assurance Levels

Raytheon currently has a two-way cross-certificate relationship with the SHA-256 CertiPath Bridge CA. It has multiple assurance levels defined below. It currently asserts the following certificate policies in its certificates, two of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.1569.10.1.12	id-raytheon-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.1569.10.1.13	id-raytheon-mediumSoftware	Yes	No
1.3.6.1.4.1.1569.10.1.14	id-raytheon-mediumCBPHardware	Yes	No
1.3.6.1.4.1.1569.10.1.15	id-raytheon-mediumCBPSoftware	Yes	No
1.3.6.1.4.1.1569.10.1.18	id-raytheon-medium-device-Hardware	Yes	Yes
1.3.6.1.4.1.1569.10.1.19	id-raytheon-medium-device-Software	Yes	No
1.3.6.1.4.1.26769.10.1.12	id-raytheon-SHA2-mediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.26769.10.1.13	id-raytheon-SHA2-mediumSoftware	Yes	No
1.3.6.1.4.1.26769.10.1.14	id-raytheon-SHA2-mediumCBPHardware	Yes	No
1.3.6.1.4.1.26769.10.1.15	id-raytheon-SHA2-mediumCBPSoftware	Yes	No

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.26769.10.1.18	id-raytheon-SHA2-medium-device-Hardware	Yes	Yes
1.3.6.1.4.1.26769.10.1.19	id-raytheon-SHA2-medium-device-Software	Yes	No

5.22 DigiCert NFI PKI Assurance Levels

DigiCert NFI PKI currently has a two-way cross-certificate relationship with the SHA-256 FBCA. DigiCert NFI PKI currently asserts the following certificate policies in its certificates, six of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
2.16.840.1.113733.1.7.23.3.1.6	Non-Federal SSP Medium	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.7	Non-Federal SSP MediumHardware	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.8	Non-Federal SSP Devices	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.13 (no longer issued, found in legacy certificates only)	Non-Federal SSP Auth	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.14	Non-Federal SSP Medium CBP	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.15	Non-Federal SSP MediumHardware CBP	Yes. Mapped	No
2.16.840.1.113733.1.7.23.3.1.17	Non-Federal SSP PIV-I cardAuth	Yes. Mapped	Yes – Physical Access Only
2.16.840.1.113733.1.7.23.3.1.18	Non-Federal SSP PIV-I Hardware	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.20	Non-Federal SSP PIV-I contentSigning	Yes. Mapped	Yes
2.16.840.1.113733.1.7.23.3.1.36	Non-Federal SSP mediumDevicesHardware	Yes. Mapped	Yes

5.23 TSCP SHA-256 Bridge Assurance Levels

TSCP is an organization that provides bridge services and has one bridge CA that is cross certified with the Federal Bridge CA. TSCP vets and cross-certifies commercial and Aero/Defense partners to include PIV-Interoperable (PIV-I) partners.

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO FBCA (Y/N)	ALLOWABLE PER POLICY (Y/N)
1.3.6.1.4.1.38099.1.1.1.1	id-Medium	No	No
1.3.6.1.4.1.38099.1.1.1.2	id-MediumHardware	Yes. Mapped	Yes
1.3.6.1.4.1.38099.1.1.1.3	id-Medium-CBP	No	No
1.3.6.1.4.1.38099.1.1.1.4	id-MediumHardware-CBP	No	No
1.3.6.1.4.1.38099.1.1.1.5	id-PIVI	Yes. Mapped	Yes
1.3.6.1.4.1.38099.1.1.1.6	id-PIVI-CardAuth	Yes. Mapped	Yes – Physical access only
1.3.6.1.4.1.38099.1.1.1.7	id-PIVI-ContentSigning	Yes. Mapped	Yes
1.3.6.1.4.1.38099.1.1.1.8	id-SHA1-Medium	No	No
1.3.6.1.4.1.38099.1.1.1.9	id-SHA1-MediumHardware	No	No
1.3.6.1.4.1.38099.1.1.1.10	id-SHA1-Medium-CBP	No	No
1.3.6.1.4.1.38099.1.1.1.11	id-SHA1-MediumHardware-CBP	No	No

5.24 Australian Defence Organisation (ADO) PKI Assurance Levels

ADO currently has a two-way cross-certificate relationship with the US DoD CCEB Interoperability Root CA 2 (SHA-256). It currently asserts the following certificate policies in its certificates, three of which are permitted by DoD policy:

CERTIFICATE POLICY OID	DESCRIPTIVE NAME	MAPPED BACK TO DoD (Y/N)	ALLOWABLE PER CCA (Y/N)
1.2.36.1.334.1.2.1.1	ADO Individual Low Assurance	No	No
1.2.36.1.334.1.2.1.2	ADO Individual Medium Assurance	Yes. Mapped	Yes
1.2.36.1.334.1.2.1.3	ADO Individual High Assurance	Yes. Mapped	Yes
1.2.36.1.334.1.2.1.4	ADO Individual Very High Assurance	No	No
1.2.36.1.334.1.2.2.1	ADO Resource Low Assurance	No	No
1.2.36.1.334.1.2.2.2	ADO Resource Medium Assurance	Yes. Mapped	Yes
1.2.36.1.334.1.2.2.3	ADO Resource High Assurance	No	No

Glossary of Terms[27]

Access Control	The process of granting or denying specific requests: 1) for obtaining and using information and related information processing services; and 2) to enter specific physical facilities (e.g., Federal buildings, military establishments, and border crossing entrances).
Access Control mechanism	Security safeguards (i.e., hardware and software features, physical controls, operating procedures, management procedures, and various combinations of these) designed to detect and deny unauthorized access and permit authorized access to an information system.
Assurance	Measure of confidence that the security features, practices, procedures, and architecture of an information system accurately mediates and enforces the security policy.
Assurance Level	The level of assurance refers to the strength of the binding between the public key and the individual whose subject name is cited in the certificate, the mechanisms used to control the use of the private key, and the security provided by the PKI itself.[28] In the context of this document, assurance levels are represented by Certificate Policy Object Identifiers (OIDs) which translate back to defined controls specified in corresponding organizational or Federal PKI Certificate Policy documents.
Authenticate	To verify the identity of a user, user device, or other entity.
Authentication	Hardware or software-based algorithm that forces users, devices, or processes to prove their identity before accessing data on an information system.
Authorization	Access privileges granted to a user, program, or process or the act of granting those privileges.
Certification Authority	A trusted third party that issues digital certificates and verifies the identity of the holder of the digital certificate.
Certificate	A digitally signed representation of information that 1) identifies the authority issuing it, 2) identifies the subscriber, 3) identifies its valid operational period (date issued / expiration date).

[27] Definitions were largely taken directly from the National Information Assurance Glossary, CNSS- 4009 https://www.cnss.gov/CNSS/issuances/Instructions.cfm. Some definitions were taken from CIO Council *Personal Identity Verification (PIV) Interoperability For Non-Federal Issuers* document. Full text and requirements are available here: https://www.idmanagement.gov/docs/archived/fpki-pivi-for-issuers.pdf

[28] Assurance level definition taken from FBCA Certificate Policy document, https://www.idmanagement.gov/docs/fpki-x509-cert-policy-fbca.pdf

Certificate Policy (CP)	A specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery, and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications.
Certificate Revocation List (CRL)	A list of revoked public key certificates created and digitally signed by a Certification Authority.
Credential	Evidence or testimonials that support a claim of identity or assertion of an attribute and usually are intended to be used more than once.
Credential Service Provider (CSP)	A trusted entity that issues or registers subscriber tokens and issues electronic credentials to subscribers. The CSP may encompass registration authorities and verifiers that it operates. A CSP may be an independent third party, or may issue credentials for its own use.
Cross-certificate	A certificate used to establish a trust relationship between two Certification Authorities.
Digital Signature	Cryptographic process used to assure data object originator authenticity, data integrity, and time stamping for prevention of replay.
Direct Trust	Method of PKI trust where the relying party directly installs the trust anchor of another PKI. (Note: this does not mean cross-certificate trust is not inherited via transitive trust)
Distinguished Name (DN)	A unique name or character string that unambiguously identifies an entity according to the hierarchical naming conventions of X.500 directory service.
DoD CIO	Office of the Department of Defense (DoD) Chief Information Officer (CIO). Governing authority for DoD approved external PKIs.
Cross-certificate trust	Method of PKI trust where the relying party installs an internal trust anchor and inherits trust through issued cross-certificates.
Federal Bridge Certification Authority (FBCA)	See Federal PKI.
External Certification Authority (ECA)	DoD program to support the issuance of DoD-approved certificates to industry partners and other external entities and organizations.
Federal Information Processing Standard (FIPS)	A standard for adoption and use by Federal agencies that has been developed within the Information Technology Laboratory and published by the National Institute of Standards and Technology, a part of the U.S. Department of Commerce. A FIPS covers some topic in information technology in order to achieve a common level of quality or some level of interoperability.

Federal Public Key Infrastructure (Federal PKI or FPKI)	The Federal PKI consists of a collection of Public Key Infrastructure components (Certificate Authorities, Directories, Certificate Policies and Certificate Practice Statements) that are used to provide peer-to-peer interoperability and a Federal Trust Anchor for SSP PKIs. In the context of this document there are five specific FPKI systems. 1. Legacy FBCA (ou=Entrust). Legacy FBCA system that is being decommissioned on 6/30/11. 2. Legacy Common Policy. The old Federal trust anchor and former parent for Shared Service Provider PKIs. It is to be decommissioned on 6/30/11. 3. SHA-1 Federal Root CA. This system is the new SHA-1 trust anchor and bridge CA that cross certifies other SHA-1 bridge member CAs and provides a Federal trust anchor for some SHA-1 legacy SSP PKIs. 4. Federal Bridge CA (FBCA). New SHA-256 FBCA system that cross certifies with other SHA-256 bridge member CAs. 5. Federal Common Policy CA. SHA-256 trust anchor for most of the Federal Government to include SSP PKIs. It also issues cross-certificates to some legacy PKIs.
Federal PKI Policy Authority (FPKI PA)	The Federal Public Key Infrastructure (FPKI) Policy Authority is an interagency body set up under the CIO Council to enforce digital certificate standards for trusted identity authentication across the federal agencies and between federal agencies and outside bodies, such as universities, state and local governments and commercial entities.
Global Directory Service (GDS)	DoD directory service that hosts all CA information to include CA certificates, cross-certificate content, and CRLs. GDS provides both a web and directory service. GDS hosts CA information at via HTTP/HTTPS at crl.disa.mil and via LDAP at crl.gds.disa.mil. GDS also hosts user encryption certificates at https://dod411.gds.disa.mil.
Legacy PKI	Agency-operated PKI that was in existence prior to Jan 1, 2008.[29]
Memorandum of Agreement (MOA)	Binding agreement between DoD Policy Management Authority and the External PKI. Required for Category I or Category II PKIs.
Non-Federal Issuer	A PKI or Card issuer that is not a Federal PIV issuer.
Online Certificate Status Protocol (OCSP)	Online Certificate Status Protocol (OCSP) is an Internet protocol used for obtaining the revocation status of an X.509 digital certificate and is described in RFC 2560.

[29] FIPS 201 describes Legacy PKI requirements and is available at http://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.201-2.pdf

Personal Identity Verification (PIV)	The process of creating and using a government-wide secure and reliable form of identification for Federal employees and contractors, in support of HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*.
Personal Identity Verification (PIV) Card	A government-issued credit card-sized identification that contains a contact and contactless chip. The holder's facial image will be printed on the card, along with other identifying information and security features. The contact chip will store a PKI certificate, the Cardholder Unique Identifier (CHUID), and a fingerprint biometric, all of which can be used to authenticate the user for physical access to federally controlled facilities and logical access to federally-controlled information systems. A PIV Card is fully conformant with federal PIV standards (i.e., Federal Information Processing Standard (FIPS) 201 and related documentation). Only cards issued by federal entities can be fully conformant. Federal standards ensure the PIV Cards are interoperable with and trusted by all Federal government relying parties.
PIV-Interoperable (PIV-I)	The process of creating and using a secure and reliable form of identification that is interoperable with the Federal government PIV process.[30]
PIV Interoperable (PIV-I) Card	A PIV-I (Personal Identity Verification – Interoperable) Card meets the PIV technical specifications to work with Federal PIV infrastructure elements such as card readers, and is issued in a manner that allows Federal government Relying Parties to trust the card. The PIV-I Card is suitable for level of assurance 4 as defined in OMB Memorandum M-04-04 and NIST SP 800-63, as well as multi-factor authentication as defined in NIST SP 800-116. A PIV-I card differs from a PIV card in that it does not meet all the requirements of FIPS-201.
Public Key	A cryptographic key that may be widely published and is used to enable the operation of an asymmetric cryptography scheme. This key is mathematically linked with a corresponding private key. Typically, a public key can be used to encrypt, but not decrypt, or to validate a signature, but not to sign.
Public Key Enabling (PKE)	The incorporation of the use of PKI certificates for security services such as authentication, confidentiality, data integrity, and non-repudiation.
Public Key Infrastructure (PKI)	The framework and services that provide for the generation, production, distribution, control, accounting and destruction of public key certificates. Components include the personnel, policies, processes, server platforms, software, and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, recover, and revoke public key certificates.
Relying party	An entity that relies upon the subscriber's credentials, typically to process a transaction or grant access to information or a system
Robust Certificate Validation Service (RCVS)	DoD service that provides certificate validation information to DoD PKI relying parties to include OCSP responses.

[30] The PIV-I certification process is detailed at https://www.idmanagement.gov/docs/fpki-test-req-guide.pdf

Root Certification Authority	In a hierarchical Public Key Infrastructure, the Certification Authority whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain.
Shared Service Provider[31]	Entity authorized by Federal PKI PA to perform CA services for Agencies.
Subordinate Certification Authority	In a hierarchal PKI, a Certification Authority whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA.
Subscriber	A party who receives a credential or token from a Credentials Service Provider (CSP) and becomes a claimant in an authentication protocol.
Transitive Trust	Term used to describe trust inherited from direct trust implementations. An implementation example would be installing another PKI trust anchor which has issued a cross-certificate outside its own PKI.
Trust Anchor	An established point of trust (usually based on the authority of some person, office, or organization) from which an entity begins the validation of an authorized process or authorized (signed) package. A "trust anchor" is sometimes defined as just a public key used for different purposes (e.g., validating a Certification Authority, validating a signed software package or key, validating the process (or person) loading the signed software or key).
Type 1 PKI	Federal Executive Branch Department and Agency PIV PKIs
Type 2 PKI	Federal Executive Branch Shared Service Provider (SSP) PIV PKIs
Type 3 PKI	Commercial Medium Hardware PKIs
Type 4 PKI	Commercial Personal Identity Verification-Interoperable (PIV-I) PKIs
Type 5 PKI	Combined Communication-Electronics Board (CCEB) Partner PKIs
Type 6 PKI	Other Mission Partner PKIs on Unclassified DoD Network
Unclassified	Information that has not been determined pursuant to E.O. 12958, as amended, or any predecessor order, to require protection against unauthorized disclosure and that is not designated as classified.
User	Individual, or (system) process acting on behalf of an individual, authorized to access an information system
Validation	Confirmation (through the provision of strong, sound, objective evidence) that requirements for a specific intended use or application have been fulfilled (e.g., a trustworthy credential has been presented, or data or information has been formatted in accordance with a defined set of rules, or a specific process has demonstrated that an entity under consideration meets, in all respects, its defined attributes or requirements).
X.509 Public Key Certificate	The public key for a user (or device) and a name for the user (or device), together with some other information, rendered unforgeable by the digital signature of the certification authority that issued the certificate, encoded in the format defined in the ISO/ITU-T X.509 standard. Also known as X.509 Certificate.

[31] Official list of certified Shared Service Providers is available at https://www.idmanagement.gov/trust-services