

**Summary**

**Certification Practices Statement**

**for the**

**WidePoint (formerly Operational Research Consultants, Inc. (ORC))**

**Shared Service Provider (SSP)**

**Public Key Infrastructure (PKI)**

Version 4.0.2.1

Approved by: \_\_\_Denise M.B. Finnance\_\_\_\_\_\_\_ Date: September 23, 2016

Chief Executive Officer  
WidePoint Cybersecurity Solutions Corporation

11250 Waples Mill Road

South Tower, Suite 210

Fairfax, VA 22030

Notice: Operational Research Consultants, Inc. (ORC), a wholly-owned subsidiary of WidePoint Corporation, has changed its legal name to WidePoint Cybersecurity Solutions Corporation, hereafter referred to simply as WidePoint. This is a legal name change only for branding purposes with no change to ownership, corporation type or other status. Any and all references to "WidePoint" within this document refers specifically and only to WidePoint Cybersecurity Solutions Corporation, the wholly-owned subsidiary of WidePoint Corporation, and not to WidePoint Corporation as a whole. Any reference or citing of personnel within this document, such as "WidePoint CEO", refers to the CEO of WidePoint Cybersecurity Solutions Corporation and not the CEO of WidePoint Corporation.

Revision History

| **Version** | **Date** | Revision Summary |
| --- | --- | --- |
| 1.0 | 01 September 1999 | The initial ORC ACES Certificate Practice Statement (CPS) was the implementation document for the ORC ACES Program, submitted in accordance with GSA ACES: GS000T99ALD0007, under which ORC:   * Entering into an appropriate GSA ACES contract; * Documented the specific practices and procedures implement to satisfy the requirements of the ACES Certificate Policy; and * Successfully completed GSA's ACES Security Certification and Accreditation. |
| 2.0 | 10 February 2000 | This CPS version updated and replaced Version 1.0, to include contract modifications stipulated by the ACES PMO as a result of the Certification and Accreditation. |
| 2.1 | 10 May 2000 | This CPS version updated and replaced Version 2.0, to include the review and approval of Version 2.0 changes by the ACES PMO. |
| 3.0 | 20 November 2000 | This CPS version updated and replaced Version 2.0, to include updates stipulated by the ACES PMO as a result of the Federal Bridge Certificate Authority Policy. |
| 3.1 | 2 February 2001 | This CPS version updated and replaced Version 3.0, to include contract modifications stipulated by the ACES PMO as a result of the Federal Bridge Certificate Authority Policy compliance requirements. |
| 3.2 | 1 October 2004 | This CPS version updated and replaced Version 3.1, to include modifications stipulated by the Federal Bridge Certificate Authority Policy audit review. |
| 3.2.1 | 15 April 2005 | This CPS version updated and replaced Version 3.2, to include modifications necessary to comply with the U.S. Federal PKI Common Policy Framework (FPCPF). |
| 3.2.2 | 6 June 2005 | This CPS version updated and replaced Version 3.2.1, to include modifications necessary to comply with FPKI subcommittee comments. |
| 3.3 | 16 September 2005 | This CPS version updated and replaced Version 3.2.2, to include modifications necessary to comply with FPKI subcommittee comments and OCD review. |
| 3.3.1 | 9 January 2007 | This CPS version updated and replaced Version 3.3, to include modifications necessary to comply with the following Common Policy Change Proposals:  2005-03, Addition of High Assurance Policy to the Common Policy Framework, 13 September 2005  2006-01, Alignment of Common Authentication Policies with FIPS 201  And, the X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for the Shared Service Providers (SSP) Program, V1.2, 5 January 2006. |
| 3.3.2 | 4 May 2007 | Updates concerning the report from the PKI Shared Service Provider Working Group on ORC, dated 23 April 2007 |
| 4.0 | 14 Aug 2015 | Separation of Shared Service Provider CPS from ACES CPS so that both are stand-alone documents; addition of Derived PIV to SSP offering |
| 4.0.1 | 12 May 2016 | Updates and edits to address findings of FPKI review |
| 4.0.2 | 8 July 2016 | Updates and edits to address findings from Annual PKI Compliance Audit; updates in response to FPKI White Space Review; update corporate name to WidePoint. |
| 4.0.2.1 | 23 Sep 2016 | Follow-up edits addressing findings resulting from FPKI CPS to CP mapping review and white-space review |

**Table of Contents**

[1 Introduction 17](#_Toc473782851)

[1.1 Overview 18](#_Toc473782852)

[1.1.1 Certificate Policy 20](#_Toc473782853)

[1.1.2 Relationship between the CP and the CPS 20](#_Toc473782854)

[1.1.3 Scope 20](#_Toc473782855)

[1.1.4 Interoperation between FCPCA and CAs Issuing under Different Policies 20](#_Toc473782856)

[1.2 Document Name and Identification 21](#_Toc473782857)

[1.3 PKI Participants 22](#_Toc473782858)

[1.3.1 PKI Authorities 22](#_Toc473782859)

[1.3.1.1 Federal Chief Information Officers Council 22](#_Toc473782860)

[1.3.1.2 Federal PKI Policy Authority (FPKIPA) 23](#_Toc473782861)

[1.3.1.3 FPKI Management Authority (FPKIMA) 23](#_Toc473782862)

[1.3.1.4 FPKI Management Authority Program Manager 23](#_Toc473782863)

[1.3.1.5 Policy Management Authority 23](#_Toc473782864)

[1.3.1.6 Authorized WidePoint SSP CAs 24](#_Toc473782865)

[1.3.1.7 Certificate Status Servers 25](#_Toc473782866)

[1.3.2 Registration Authorities 25](#_Toc473782867)

[1.3.3 Trusted Agents 26](#_Toc473782868)

[1.3.3.1 Notary Public 26](#_Toc473782869)

[1.3.4 Subscribers 26](#_Toc473782870)

[1.3.4.1 PKI Sponsor 27](#_Toc473782871)

[1.3.5 Relying Parties 27](#_Toc473782872)

[1.3.6 Other Participants 28](#_Toc473782873)

[1.3.6.1 Certificate Management Authority(s) (CMA) 28](#_Toc473782874)

[1.3.6.2 Local Registration Authorities (LRAs) 28](#_Toc473782875)

[1.3.6.3 Service Providers 29](#_Toc473782876)

[1.4 Certificate Usage 29](#_Toc473782877)

[1.4.1 Appropriate Certificate Uses 29](#_Toc473782878)

[1.4.2 Prohibited Certificate Uses 30](#_Toc473782879)

[1.5 Policy Administration 30](#_Toc473782880)

[1.5.1 Organization Administering the Document 30](#_Toc473782881)

[1.5.2 Contact Person 31](#_Toc473782882)

[1.5.3 Person Determining CPS Suitability for the Common Policy 31](#_Toc473782883)

[1.5.4 CPS Approval Procedures 31](#_Toc473782884)

[1.6 Definitions and Acronyms 31](#_Toc473782885)

[2 Publication and Repository Responsibilities 32](#_Toc473782886)

[2.1 Repositories 32](#_Toc473782887)

[2.2 Publication of Certification Information 33](#_Toc473782888)

[2.2.1 Publication of Certificates and Certificate Status 33](#_Toc473782889)

[2.2.2 Publication of CA Information 34](#_Toc473782890)

[2.2.3 Interoperability 34](#_Toc473782891)

[2.3 Time or Frequency of Publication 34](#_Toc473782892)

[2.4 Access Controls on Repositories 34](#_Toc473782893)

[3 Identification and Authentication 36](#_Toc473782894)

[3.1 Naming 36](#_Toc473782895)

[3.1.1 Types of Names 36](#_Toc473782896)

[3.1.2 Need for Names to be Meaningful 41](#_Toc473782897)

[3.1.3 Anonymity or Pseudonymity of Subscribers 42](#_Toc473782898)

[3.1.4 Rules for Interpreting Various Name Forms 43](#_Toc473782899)

[3.1.5 Uniqueness of Names 43](#_Toc473782900)

[3.1.6 Recognition, Authentication, and Role of Trademarks 43](#_Toc473782901)

[3.2 Initial Identity Validation 44](#_Toc473782902)

[3.2.1 Method to Prove Possession of Private Key 44](#_Toc473782903)

[3.2.2 Authentication of Sponsoring Organization Identity 45](#_Toc473782904)

[3.2.3 Authentication of Individual Identity 45](#_Toc473782905)

[3.2.3.1 Authentication of Human Subscribers 46](#_Toc473782906)

[3.2.3.2 Authentication of Devices 50](#_Toc473782907)

[3.2.3.3 Authentication of Derived PIV Credentials 51](#_Toc473782908)

[3.2.4 Non-verified Subscriber Information 51](#_Toc473782909)

[3.2.5 Validation of Authority 51](#_Toc473782910)

[3.2.6 Criteria for Interoperation 52](#_Toc473782911)

[3.3 Identification and Authentication for Re-key 52](#_Toc473782912)

[3.3.1 Identification and Authentication for Routine Re-key 52](#_Toc473782913)

[3.3.2 Identification and Authentication for Re-key after Revocation 53](#_Toc473782914)

[3.4 Identification and Authentication for Revocation Request 53](#_Toc473782915)

[4 Certificate Life-Cycle Operational Requirements 55](#_Toc473782916)

[4.1 Certificate Application 55](#_Toc473782917)

[4.1.1 Who Can Submit a Certificate Application 55](#_Toc473782918)

[4.1.1.1 CA Certificates 56](#_Toc473782919)

[4.1.1.2 User Certificates 56](#_Toc473782920)

[4.1.1.3 Device Certificates 57](#_Toc473782921)

[4.1.1.4 Code Signing Certificates 58](#_Toc473782922)

[4.1.2 Enrollment Process and Responsibilities 58](#_Toc473782923)

[4.1.2.1 Non-SSP/PIV Workstation Certificate Enrollment 58](#_Toc473782924)

[4.1.2.2 SSP/PIV Workstation Certificate Enrollment 59](#_Toc473782925)

[4.1.2.3 Derived Certificate Enrollment 60](#_Toc473782926)

[4.2 Certificate Application Processing 60](#_Toc473782927)

[4.2.1 Performing Identification and Authentication Functions 60](#_Toc473782928)

[4.2.1.1 Authentication of Device Identity Certificates 63](#_Toc473782929)

[4.2.1.2 Derived PIV Certificates 64](#_Toc473782930)

[4.2.2 Approval or Rejection of Certificate Applications 64](#_Toc473782931)

[4.2.3 Time to Process Certificate Applications 64](#_Toc473782932)

[4.3 Certificate Issuance 64](#_Toc473782933)

[4.3.1 CA Actions During Certificate Issuance 64](#_Toc473782934)

[4.3.2 Notification to Subscriber by the CA of Issuance of Certificate 65](#_Toc473782935)

[4.4 Certificate Acceptance 66](#_Toc473782936)

[4.4.1 Conduct Constituting Certificate Acceptance 67](#_Toc473782937)

[4.4.2 Publication of the Certificate by the CA 68](#_Toc473782938)

[4.4.3 Notification of Certificate Issuance by the CA to Other Entities 68](#_Toc473782939)

[4.5 Key Pair and Certificate Usage 69](#_Toc473782940)

[4.5.1 Subscriber Private Key and Certificate Usage 69](#_Toc473782941)

[4.5.1.1 Individual Subscriber 69](#_Toc473782942)

[4.5.1.2 Server/Component Certificate Subscriber 70](#_Toc473782943)

[4.5.2 Relying Party Public Key and Certificate Usage 71](#_Toc473782944)

[4.6 Certificate Renewal 72](#_Toc473782945)

[4.6.1 Circumstance for Certificate Renewal 72](#_Toc473782946)

[4.6.2 Who May Request Renewal 72](#_Toc473782947)

[4.6.3 Processing Certificate Renewal Requests 72](#_Toc473782948)

[4.6.4 Notification of New Certificate Issuance to Subscriber 72](#_Toc473782949)

[4.6.5 Conduct Constituting Acceptance of a Renewal Certificate 72](#_Toc473782950)

[4.6.6 Publication of the Renewal Certificate by the CA 72](#_Toc473782951)

[4.6.7 Notification of Certificate Issuance by the CA to Other Entities 72](#_Toc473782952)

[4.7 Certificate Re-Key 73](#_Toc473782953)

[4.7.1 Circumstance for Certificate Re-key 73](#_Toc473782954)

[4.7.2 Who May Request Certification of a New Public Key 73](#_Toc473782955)

[4.7.3 Processing Certificate Re-keying Requests 73](#_Toc473782956)

[4.7.4 Notification of New Certificate Issuance to Subscriber 73](#_Toc473782957)

[4.7.5 Conduct Constituting Acceptance of a Re-keyed Certificate 74](#_Toc473782958)

[4.7.6 Publication of the Re-keyed Certificate by the CA 74](#_Toc473782959)

[4.7.7 Notification of Certificate Issuance by the CA to Other Entities 74](#_Toc473782960)

[4.8 Certificate Modification 74](#_Toc473782961)

[4.8.1 Circumstance for Certificate Modification 74](#_Toc473782962)

[4.8.2 Who May Request Certificate Modification 75](#_Toc473782963)

[4.8.3 Processing Certificate Modification Requests 75](#_Toc473782964)

[4.8.4 Notification of New Certificate Issuance to Subscriber 75](#_Toc473782965)

[4.8.5 Conduct Constituting Acceptance of Modified Certificate 75](#_Toc473782966)

[4.8.6 Publication of the Modified Certificate by the CA 75](#_Toc473782967)

[4.8.7 Notification of Certificate Issuance by the CA to Other Entities 76](#_Toc473782968)

[4.9 Certificate Revocation and Suspension 76](#_Toc473782969)

[4.9.1 Circumstances for Revocation 76](#_Toc473782970)

[4.9.2 Who Can Request Revocation 77](#_Toc473782971)

[4.9.3 Procedure for Revocation Request 78](#_Toc473782972)

[4.9.4 Revocation Request Grace Period 79](#_Toc473782973)

[4.9.5 Time within which CA must Process the Revocation Request 79](#_Toc473782974)

[4.9.6 Revocation Checking Requirements for Relying Parties 79](#_Toc473782975)

[4.9.7 CRL Issuance Frequency 80](#_Toc473782976)

[4.9.8 Maximum Latency for CRLs 80](#_Toc473782977)

[4.9.9 On-line Revocation/ Status Checking Availability 80](#_Toc473782978)

[4.9.10 On-line Revocation Checking Requirements 81](#_Toc473782979)

[4.9.11 Other Forms of Revocation Advertisements Available 82](#_Toc473782980)

[4.9.12 Special Requirements Related To Key Compromise 82](#_Toc473782981)

[4.9.13 Circumstances for Suspension 82](#_Toc473782982)

[4.9.14 Who Can Request Suspension 83](#_Toc473782983)

[4.9.15 Procedure for Suspension Request 83](#_Toc473782984)

[4.9.16 Limits on Suspension Period 83](#_Toc473782985)

[4.10 Certificate Status Services 83](#_Toc473782986)

[4.10.1 Operational Characteristics 83](#_Toc473782987)

[4.10.2 Service Availability 83](#_Toc473782988)

[4.10.3 Optional Features 83](#_Toc473782989)

[4.11 End of Subscription 83](#_Toc473782990)

[4.12 Key Escrow and Recovery 84](#_Toc473782991)

[4.12.1 Key Escrow and Recovery Policy and Practices 84](#_Toc473782992)

[4.12.2 Session Key Encapsulation and Recovery Policy and Practices 84](#_Toc473782993)

[5 Facility, Management, and Operational Controls 85](#_Toc473782994)

[5.1 Physical Controls 85](#_Toc473782995)

[5.1.1 Site Location and Construction 86](#_Toc473782996)

[5.1.2 Physical Access 87](#_Toc473782997)

[5.1.2.1 Physical Access for CA Equipment 90](#_Toc473782998)

[5.1.2.2 Physical Access for RA Equipment 90](#_Toc473782999)

[5.1.2.3 Physical Access for CSS Equipment 91](#_Toc473783000)

[5.1.3 Power and Air Conditioning 91](#_Toc473783001)

[5.1.4 Water Exposure 91](#_Toc473783002)

[5.1.5 Fire Prevention and Protection 91](#_Toc473783003)

[5.1.6 Media Storage 92](#_Toc473783004)

[5.1.7 Waste Disposal 92](#_Toc473783005)

[5.1.8 Off-Site Backup 92](#_Toc473783006)

[5.2 Procedural Controls 93](#_Toc473783007)

[5.2.1 Trusted Roles 93](#_Toc473783008)

[5.2.1.1 Administrator 94](#_Toc473783009)

[5.2.1.2 Officer 95](#_Toc473783010)

[5.2.1.3 Auditor 95](#_Toc473783011)

[5.2.1.4 Operator 95](#_Toc473783012)

[5.2.1.5 Trusted Agents 96](#_Toc473783013)

[5.2.2 Number of Persons Required Per Task 97](#_Toc473783014)

[5.2.3 Identification and Authentication for Each Role 98](#_Toc473783015)

[5.2.4 Roles Requiring Separation of Duties 98](#_Toc473783016)

[5.3 Personnel Controls 99](#_Toc473783017)

[5.3.1 Qualifications, Experience, and Clearance Requirements 99](#_Toc473783018)

[5.3.2 Background Check Procedures 100](#_Toc473783019)

[5.3.3 Training Requirements 101](#_Toc473783020)

[5.3.4 Retraining Frequency and Requirements 102](#_Toc473783021)

[5.3.5 Job Rotation Frequency and Sequence 102](#_Toc473783022)

[5.3.6 Sanctions for Unauthorized Actions 103](#_Toc473783023)

[5.3.7 Independent Contractor Requirements 103](#_Toc473783024)

[5.3.8 Documentation Supplied to Personnel 103](#_Toc473783025)

[5.4 Audit Logging Procedures 103](#_Toc473783026)

[5.4.1 Types of Events Recorded 104](#_Toc473783027)

[5.4.2 Frequency of Processing Log 112](#_Toc473783028)

[5.4.3 Retention of Audit Log 112](#_Toc473783029)

[5.4.4 Protection of Audit Log 112](#_Toc473783030)

[5.4.5 Audit Log Backup Procedures 113](#_Toc473783031)

[5.4.6 Audit Collection System (Internal vs. External) 113](#_Toc473783032)

[5.4.7 Notification to Event-Causing Subject 113](#_Toc473783033)

[5.4.8 Vulnerability Assessment 113](#_Toc473783034)

[5.5 Records Archival 114](#_Toc473783035)

[5.5.1 Types of Events Archived 114](#_Toc473783036)

[5.5.2 Retention Period for Archive 115](#_Toc473783037)

[5.5.3 Protection of Archive 116](#_Toc473783038)

[5.5.4 Archive Backup Procedures 117](#_Toc473783039)

[5.5.5 Requirements for Time-Stamping of Records 117](#_Toc473783040)

[5.5.6 Archive Collection System (Internal or External) 118](#_Toc473783041)

[5.5.7 Procedures to Obtain and Verify Archive Information 118](#_Toc473783042)

[5.6 Key Changeover 119](#_Toc473783043)

[5.7 Compromise and Disaster Recovery 119](#_Toc473783044)

[5.7.1 Incident and Compromise Handling Procedures 119](#_Toc473783045)

[5.7.2 Computing Resources, Software, and/or Data are Corrupted 120](#_Toc473783046)

[5.7.3 Entity (CA) Private Key Compromise Procedures 121](#_Toc473783047)

[5.7.4 Business Continuity Capabilities after a Disaster 122](#_Toc473783048)

[5.8 CA or RA Termination 122](#_Toc473783049)

[6 Technical Security Controls 123](#_Toc473783050)

[6.1 Key Pair Generation and Installation 123](#_Toc473783051)

[6.1.1 Key Pair Generation 123](#_Toc473783052)

[6.1.1.1 CA Key Pair Generation 123](#_Toc473783053)

[6.1.1.2 Subscriber Key Pair Generation 124](#_Toc473783054)

[6.1.1.3 CSS Key Pair Generation 124](#_Toc473783055)

[6.1.1.4 PIV Content Signing Key Pair Generation 124](#_Toc473783056)

[6.1.2 Private Key Delivery to Subscriber 124](#_Toc473783057)

[6.1.3 Public Key Delivery to Certificate Issuer 125](#_Toc473783058)

[6.1.4 CA Public Key Delivery to Relying Parties 125](#_Toc473783059)

[6.1.5 Key Sizes 126](#_Toc473783060)

[6.1.6 Public Key Parameters Generation and Quality Checking 126](#_Toc473783061)

[6.1.7 Key Usage Purposes (as per X.509 v3 Key Usage Field) 126](#_Toc473783062)

[6.2 Private Key Protection and Cryptographic Module Engineering Controls 127](#_Toc473783063)

[6.2.1 Cryptographic Module Standards and Controls 127](#_Toc473783064)

[6.2.2 Private Key (n out of m) Multi-person Control 128](#_Toc473783065)

[6.2.3 Private Key Escrow 129](#_Toc473783066)

[6.2.3.1 Escrow of CA Private Signature Key 129](#_Toc473783067)

[6.2.3.2 Escrow of CA Encryption Key 129](#_Toc473783068)

[6.2.3.3 Escrow of Subscriber Private Signature Key 129](#_Toc473783069)

[6.2.3.4 Escrow of Subscriber Private Encryption Key 129](#_Toc473783070)

[6.2.4 Private Key Backup 130](#_Toc473783071)

[6.2.4.1 Backup of CA Private Signature Key 130](#_Toc473783072)

[6.2.4.2 Backup of Subscriber Private Signature Key 130](#_Toc473783073)

[6.2.4.3 Backup of Subscriber Private Key Management Key 130](#_Toc473783074)

[6.2.4.4 Backup of CSS Private Key 130](#_Toc473783075)

[6.2.4.5 Backup of Device Private Key 130](#_Toc473783076)

[6.2.4.6 Backup of Common PIV Content Signing Key 131](#_Toc473783077)

[6.2.5 Private Key Archival 131](#_Toc473783078)

[6.2.6 Private Key Transfer into or from a Cryptographic Module 131](#_Toc473783079)

[6.2.7 Private Key Storage on Cryptographic Module 132](#_Toc473783080)

[6.2.8 Method of Activating Private Key 132](#_Toc473783081)

[6.2.9 Method of Deactivating Private Key 133](#_Toc473783082)

[6.2.10 Method of Destroying Private Key 133](#_Toc473783083)

[6.2.11 Cryptographic Module Rating 134](#_Toc473783084)

[6.3 Other Aspects of Key Pair Management 134](#_Toc473783085)

[6.3.1 Public Key Archival 134](#_Toc473783086)

[6.3.2 Certificate Operational Periods and Key Usage Periods 134](#_Toc473783087)

[6.3.3 Restrictions on CA Private Key Usage 135](#_Toc473783088)

[6.4 Activation Data 135](#_Toc473783089)

[6.4.1 Activation Data Generation and Installation 135](#_Toc473783090)

[6.4.2 Activation Data Protection 136](#_Toc473783091)

[6.4.3 Other Aspects of Activation Data 136](#_Toc473783092)

[6.5 Computer Security Controls 137](#_Toc473783093)

[6.5.1 Specific Computer Security Technical Requirements 137](#_Toc473783094)

[6.5.2 Computer Security Rating 137](#_Toc473783095)

[6.6 Life Cycle Technical Controls 138](#_Toc473783096)

[6.6.1 System Development Controls 138](#_Toc473783097)

[6.6.2 Security Management Controls 140](#_Toc473783098)

[6.6.3 Object Reuse 141](#_Toc473783099)

[6.6.4 Life Cycle Security Controls 141](#_Toc473783100)

[6.7 Network Security Controls 141](#_Toc473783101)

[6.8 Time-Stamping 143](#_Toc473783102)

[7 Certificate, CRL, and OCSP Profiles 144](#_Toc473783103)

[7.1 Certificate Profile 144](#_Toc473783104)

[7.1.1 Version Number(s) 144](#_Toc473783105)

[7.1.2 Certificate Extensions 144](#_Toc473783106)

[7.1.3 Algorithm Object Identifiers 144](#_Toc473783107)

[7.1.4 Name Forms 145](#_Toc473783108)

[7.1.5 Name Constraints 146](#_Toc473783109)

[7.1.6 Certificate Policy Object Identifiers 146](#_Toc473783110)

[7.1.7 Usage of Policy Constraints Extension 146](#_Toc473783111)

[7.1.8 Policy Qualifiers Syntax and Semantics 146](#_Toc473783112)

[7.1.9 Processing Semantics for the Critical Certificate Policies Extension 146](#_Toc473783113)

[7.2 CRL Profile 147](#_Toc473783114)

[7.2.1 Version Number(s) 147](#_Toc473783115)

[7.2.2 CRL and CRL Entry Extensions 147](#_Toc473783116)

[7.3 OCSP Profile 148](#_Toc473783117)

[7.3.1 Version Number(s) 150](#_Toc473783118)

[7.3.2 OCSP Extensions 150](#_Toc473783119)

[8 Compliance Audit and Other Assessments 151](#_Toc473783120)

[8.1 Frequency of Audit or Assessment 151](#_Toc473783121)

[8.2 Identity/ Qualifications of Assessor 151](#_Toc473783122)

[8.3 Assessor’s Relationship to Assessed Entity 152](#_Toc473783123)

[8.4 Topics Covered by Assessment 152](#_Toc473783124)

[8.5 Actions Taken as a Result of Deficiency 152](#_Toc473783125)

[8.6 Communication of Results 153](#_Toc473783126)

[9 Other Business and Legal Matters 154](#_Toc473783127)

[9.1 Fees 154](#_Toc473783128)

[9.1.1 Certificate Issuance or Renewal Fees 154](#_Toc473783129)

[9.1.2 Certificate Access Fees 154](#_Toc473783130)

[9.1.3 Revocation or Status Information Access Fees 154](#_Toc473783131)

[9.1.4 Fees for Other Services 154](#_Toc473783132)

[9.1.5 Refund Policy 155](#_Toc473783133)

[9.2 Financial Responsibility 155](#_Toc473783134)

[9.2.1 Insurance Coverage 155](#_Toc473783135)

[9.2.2 Other Assets 155](#_Toc473783136)

[9.2.3 Insurance or Warranty Coverage for End-Entities 155](#_Toc473783137)

[9.3 Confidentiality of Business Information 155](#_Toc473783138)

[9.3.1 Scope of Confidential Information 155](#_Toc473783139)

[9.3.2 Information not within the Scope of Confidential Information 155](#_Toc473783140)

[9.3.3 Responsibility to Protect Confidential Information 156](#_Toc473783141)

[9.4 Privacy of Personal Information 157](#_Toc473783142)

[9.4.1 Privacy Plan 157](#_Toc473783143)

[9.4.2 Information Treated as Private 157](#_Toc473783144)

[9.4.3 Information not Deemed Private 157](#_Toc473783145)

[9.4.4 Responsibility to Protect Private Information 158](#_Toc473783146)

[9.4.5 Notice and Consent to Use Private Information 158](#_Toc473783147)

[9.4.6 Disclosure Pursuant to Judicial or Administrative Process 158](#_Toc473783148)

[9.4.7 Other Information Disclosure Circumstances 158](#_Toc473783149)

[9.5 Intellectual Property Rights 158](#_Toc473783150)

[9.6 Representations and Warranties 159](#_Toc473783151)

[9.6.1 CA Representations and Warranties 159](#_Toc473783152)

[9.6.2 RA Representations and Warranties 160](#_Toc473783153)

[9.6.3 Subscriber Representations and Warranties 161](#_Toc473783154)

[9.6.4 Relying Party Representations and Warranties 162](#_Toc473783155)

[9.6.5 Representations and Warranties of Other Participants 163](#_Toc473783156)

[9.6.5.1 Repository Representations and Warranties 163](#_Toc473783157)

[9.6.5.2 LRA and Trusted Agent Representations and Warranties 164](#_Toc473783158)

[9.7 Disclaimers of Warranties 164](#_Toc473783159)

[9.8 Limitations of Liability 165](#_Toc473783160)

[9.8.1 Loss Limitation 165](#_Toc473783161)

[9.8.2 U.S. Federal Government Liability 165](#_Toc473783162)

[9.9 Indemnities 165](#_Toc473783163)

[9.10 Term and Termination 166](#_Toc473783164)

[9.10.1 Term 166](#_Toc473783165)

[9.10.2 Termination 166](#_Toc473783166)

[9.10.3 Effect of Termination and Survival 166](#_Toc473783167)

[9.11 Individual Notices and Communications with Participants 166](#_Toc473783168)

[9.12 Amendments 166](#_Toc473783169)

[9.12.1 Procedure for Amendment 166](#_Toc473783170)

[9.12.2 Notification Mechanism and Period 166](#_Toc473783171)

[9.12.3 Circumstances Under Which OID Must be Changed 167](#_Toc473783172)

[9.13 Dispute Resolution Provisions 167](#_Toc473783173)

[9.14 Governing Law 167](#_Toc473783174)

[9.15 Compliance with Applicable Law 167](#_Toc473783175)

[9.16 Miscellaneous Provisions 167](#_Toc473783176)

[9.16.1 Entire Agreement 167](#_Toc473783177)

[9.16.2 Assignment 167](#_Toc473783178)

[9.16.3 Severability 167](#_Toc473783179)

[9.16.4 Enforcement (Attorney’s Fees and Waiver of Rights) 168](#_Toc473783180)

[9.16.5 Force Majeure 168](#_Toc473783181)

[9.17 Other Provisions 168](#_Toc473783182)

[10 Bibliography 169](#_Toc473783183)

[11 Acronyms and Abbreviations 172](#_Toc473783184)

[12 Glossary 176](#_Toc473783185)

**List of Tables**

[Table 1: id-fpki-Common Policy OIDs 21](#_Toc473782843)

[Table 2: Common Name Attribute Criteria 41](#_Toc473782844)

[Table 3: Authorized Certificate Application Initiators 55](#_Toc473782845)

[Table 4: Sample OCSP Responder Self-Signed Certificate 81](#_Toc473782846)

[Table 5: PIV Roles 96](#_Toc473782847)

[Table 6: Auditable Events 105](#_Toc473782848)

[Table 7: OCSP Request Format 148](#_Toc473782849)

[Table 8: OCSP Response Format 149](#_Toc473782850)

**List of Figures**

[Figure 1-PIV Identification and Authentication Process Flow 61](#_Toc457973022)

[Figure 2-PIV Card Issuance Process 65](#_Toc457973023)

[Figure 3: VPN-1 SecuRemote and VPN-1 SecureClient Compatibility 104](#_Toc457973024)

[Figure 4: WidePoint Internal Time Service 118](#_Toc457973025)

# Introduction

This Certification Practices Statement (CPS) is the guiding document for the WidePoint Shared Service Provider (WidePoint SSP) public key infrastructure (PKI), which operates under the X.509 Certificate Policy for the U.S. Federal PKI Common Policy Framework (v1.24) as an authorized component of the Federal Enterprise Architecture.

Only CAs authorized to operate in accordance with the X.509 Certificate Policy for the U.S. Federal Public Key Infrastructure (FPKI) Common Policy Framework, version 1.24, dated May 7, 2015 assert the FPKI Common Policy Object Identifiers (OIDs) in any certificates (Authorized SSP CAs). WidePoint, having completed a compliance audit approved by the Federal PKI Policy Authority (FPKIPA), attained an Authority to Operate for providing public key certificate services under the Shared Services Provider (SSP) program as an Authorized Shared Services Provider.

WidePoint SSP public key certificates fall within the following nine of ten specific certificate policies (id-fpki-common-High is not supported):

* A policy for users with software cryptographic modules
* A policy for users with hardware cryptographic modules
* A policy for devices with software cryptographic modules
* A policy for devices with hardware cryptographic modules
* A user authentication policy
* A card authentication policy
* A PIV content signing policy
* A Derived-PIV authentication policy
* A Derived-PIV hardware authentication policy

Where a specific policy is not stated, the policies and procedures in this CPS apply equally to all nine policies.

The use of SHA-1 to create digital signatures is not allowed under the Common Policy after 12/31/2013.

The user policies governing WidePoint SSP certificates apply to Federal employees, contractors, and other affiliated personnel requiring PKI credentials for the purposes of authentication, signature, and confidentiality with Federal systems that have not been designated by law as national security systems. The device policy applies to devices operated by or on behalf of federal agencies.

The Common Policy requires the use of FIPS 140 validated cryptographic modules by Federal employees, contractors and other affiliated personnel for all cryptographic operations and the protection of trusted public keys. Software and hardware cryptographic mechanisms are equally acceptable under the Shared Services Provider policy framework. The policies for users with hardware cryptographic modules mandate Level 2 validation.

The WidePoint SSP PKI will provide the following security management services:

* Key generation/storage
* Certificate generation, modification, re-key, and distribution
* Certificate revocation list (CRL) generation and distribution
* Directory management of certificate related items
* Certificate token initialization/programming/management
* System management functions (e.g., security audit, configuration management, archive)

For entities associated with the Federal Common Policy Root CA (FCPCA), the Common Policy requires the use of either 2048 bit RSA keys or 256-bit elliptic curve keys along with the SHA-256 and SHA-384 hash algorithms. WidePoint SSP CAs are required to use 2048-bit RSA keys or 256-bit elliptic curve keys when signing certificates and CRLs that expire on or after December 31, 2010. WidePoint SSP CAs are required to use SHA-256 or SHA-384. WidePoint SSP subscriber authentication keys in certificates that expire on or after December 31, 2013 must be at least 2048-bit RSA keys or 256-bit elliptic curve keys.

The Common Policy and this WidePoint SSP CPS are consistent with the Internet Engineering Task Force (IETF) Public Key Infrastructure X.509 (IETF PKIX) RFC 3647 Certificate Policy and Certification Practices Framework.

The terms and provisions of these certificate policies will be interpreted under and governed by applicable Federal law.

## Overview

This WidePoint SSP CPS is the implementation document for WidePoint’s Shared Services Provider (SSP) Program (also known as the WidePoint SSP Public Key Infrastructure, “WidePoint SSP PKI”). The Federal Public Key Infrastructure Policy Authority (FPKIPA) has designated WidePoint as an SSP "Authorized Certification Authority (CA)" by:

* Reviewing the specific practices and procedures WidePoint implements to satisfy the requirements of the FPKI Common Policy in this certificate practice statement.
* Successfully completing a Security Assessment and Authorization (SA&A).
* Approving this CPS.

This CPS is applicable to Federal employees, contractors and other affiliated personnel, relying parties, and agency applications who [that] directly use these certificates, and who are responsible for applications or servers that use certificates. Certificate users include, but are not limited to, Certificate Management Authorities (CMAs), Registration Authorities (RAs), Local Registration Authorities (LRAs), subscribers, and relying parties.

In accordance with the stipulations of this CPS, the WidePoint SSP CA(s) that issue certificates asserting a FPKI Common Policy OID will be updated as required by and in accordance with the current X.509 CP for the U.S. Federal PKI Common Policy Framework, v1.24, and this CPS.

This CPS describes the operations of the WidePoint SSP PKI and the services that the WidePoint SSP PKI provides. These services include:

* Subscriber Registration: A subscriber or certificate applicant must appear in person before a WidePoint Registration Authority (RA), an approved Local Registration Authority (LRA), or a registered Notary Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions), as stipulated by the Policy Authority; present valid identification (from the list of acceptable documents included in Form I-9, OMB No. 1615-0047); sign the subscriber’s obligation; and mail the forms to WidePoint.
* Subscriber Enrollment: The WidePoint SSP system provides Federal Information Processing Standards (FIPS) 140-2 Level 3 Secure Socket Layer (SSL) connections to the certification authority. The subscriber must use a FIPS 140-2 Level 1 or 2 client for connection for enrollment.
* Enrollment Validation: The WidePoint registration process validates the subscriber enrollment information (see above).
* Certificate Issuance: When notified by an RA of a valid enrollment request, a WidePoint RA issues the requested certificate for delivery to a FIPS 140-2 Level 1 or 2 client. A FIPS 140-2 Level 1 issuance does not require a hardware token. WidePoint then notifies the subscriber of the issuance and provide instructions for receiving the certificate.
* Certificate Publishing: When a CA certificate is issued, WidePoint publishes it to a directory. The directory may be accessed via Hypertext Transfer Protocol.
* Encryption Key Storage: Optional storage (escrow) of encryption keys.
* Key Recovery: If encryption key storage (escrow) is selected.
* Certificate Status information: In the form of Certificate Revocation Lists (CRLs) distribution (via HTTP) and Online Certificate Status Protocol (OCSP) responses.

To assist in providing these services and in meeting the reporting requirements outlined in this CPS, WidePoint maintains a website, which contains instructions, online forms, a summary of this CPS, compliance audit results, and copies of certificates and CRLs. The majority of the information on the website is publicly accessible, although it incorporates SSL to promote data integrity and to allow users to validate the source of the information. Portions of the website are access controlled and require certificate authentication for access to authorized individuals.

WidePoint is periodically audited by its independent IT auditor against this CPS and operates primary and secondary secure data centers in conformance with the Department of Defense (DOD), U.S. General Services Administration (GSA), and commercial best practices.

### Certificate Policy

Certificates issued by the WidePoint SSP CA contain a registered certificate policy object identifier (OID), which may be used by a Relying Party to decide whether a certificate is trusted for a particular purpose. The OID corresponds to the specific type and specific level of assurance for all WidePoint SSP certificates issued under this CPS, which are available to all Relying Parties. Each WidePoint SSP certificate issued asserts the appropriate level of assurance in the *certificatePolicies* extension.

### Relationship between the CP and the CPS

This CPS applies to X.509 Version 3 certificates with assurance levels as defined in the U.S. Federal PKI Common Policy Framework CP, Version 1.24. The policies and procedures in this CPS are applicable to individuals who manage the certificates, who directly use these certificates, and individuals who are responsible for applications or servers that rely on these certificates.

### Scope

This CPS is applicable to Federal employees, contractors and other affiliated personnel, relying parties, and agency applications who [that] directly use these certificates, and who are responsible for applications or servers that use certificates. Certificate users include, but are not limited to, Certificate Management Authorities (CMAs), Registration Authorities (RAs), Local Registration Authorities (LRAs) including Issuers, Registrars and Sponsors, subscribers, and relying parties.

### Interoperation between FCPCA and CAs Issuing under Different Policies

The FPKIPA determines the interoperability criteria for CAs operating under the X.509 U.S. Federal PKI Common Policy Framework policy (Common Policy). WidePoint SSP CA’s operate under the X.509 U.S. Federal PKI Common Policy Framework policy (Common Policy).

## Document Name and Identification

The Common Policy is registered with the Computer Security Objects Register (CSOR) at the National Institute of Standards and Technology (NIST). Certificates issued by a WidePoint SSP CA, in accordance with the Common Policy and this CPS, assert at least one of the OIDs listed in the table below. The WidePoint SSP PKI and each WidePoint SSP CA complies with the following certificate policy object identifiers (OIDs) for the SSP Certificates defined in this CPS as provided in   
Table 1.

Table : id-fpki-Common Policy OIDs

| **Description** | **Policy OID** |
| --- | --- |
| id-fpki-common-policy | ::= {2 16 840 1 101 3 2 1 3 6} |
| id-fpki-common-hardware | ::= {2 16 840 1 101 3 2 1 3 7} |
| id-fpki-common-devices | ::= {2 16 840 1 101 3 2 1 3 8} |
| Id-fpki-common-devicesHardware | ::= {2 16 840 1 101 3 2 1 3 36} |
| id-fpki-common-authentication | ::= {2 16 840 1 101 3 2 1 3 13} |
| id-fpki-common-cardAuth | ::= {2 16 840 1 101 3 2 1 3 17} |
| id-fpki-common-piv-contentSigning | ::= {2 16 840 1 101 3 2 1 3 39} |
| id-fpki-common-derived-pivAuth | ::= {2 16 840 1 101 3 2 1 3 40} |
| id-fpki-common-derived-pivAuth-hardware | ::= {2 16 840 1 101 3 2 1 3 41} |

Certificates issued to users, other than devices, asserting an OID to support digitally signed documents or key management, contain either the id-fpki-common-policy or id-fpki-common-hardware. Certificates issued to devices under this policy that use FIPS 140 Level 2 or higher cryptographic modules include either id-fpki-common-devicesHardware, id-fpki-common-devices, or both. Subscriber certificates issued to devices under this policy using software cryptographic modules will include id-fpki-common-devices.

This CPS includes five (5) certificates specific to FIPS 201 Personal Identity Verification (PIV) for issuance to Federal employees and contractors:

* Certificates issued to users supporting authentication but not digital signature, where the corresponding private key is stored on a PIV card, contain id-fpki-common-authentication.
* Certificates issued to users supporting authentication where the private key is stored on a PIV card and can be used without user authentication contain id-fpki-common-cardAuth.
* Certificates issued to users in accordance with NIST SP800-157, supporting authentication but not digital signature, where the corresponding private key is not stored on a PIV card, contain either id-fpki-common-derived-pivAuth-hardware when issued in a manner which meets the requirements for Level 4 authentication as defined by OMB’s guidance for E-Authentication; or id-fpki-common-derived-pivAuth for Level 3.
* The id-fpki-common-piv-contentSigning policy is only asserted in certificates issued to devices that sign PIV Card objects in accordance with [FIPS 201] or [SP800-157].
* The requirements associated with id-fpki-common-piv-contentSigning are identical to id-fpki-common-devicesHardware except where specifically noted in this CPS.

WidePoint certificates issued under this CPS reference the Common Policy by including the appropriate OID, identified above, in the *Certificate Policies* field. Additionally, each WidePoint CA that issues certificates will hold a certificate signed by the Federal Common Policy Root CA (FCPCA) or an Authorized CA that holds a certificate signed by the FCPCA. WidePoint-issued certificates containing the foregoing OIDs may not be used except as specifically authorized by this CPS and the Common Policy. Unless specifically approved by the Federal PKI Policy Authority, only the OIDs identified above are used within WidePoint SSP certificates.

## PKI Participants

The following are roles relevant to the administration and operation of WidePoint SSP CAs operating under this CPS and the Common Policy.

### PKI Authorities

#### Federal Chief Information Officers Council

The Federal CIO Council comprises the Chief Information Officers of all cabinet level departments and other independent agencies. The Federal CIO Council has established the framework for the interoperable Federal PKI (FPKI) and oversees the operation of the organizations responsible for governing and promoting its use. In particular, the Common Policy was established under the authority of and with the approval of the Federal CIO Council.

#### Federal PKI Policy Authority (FPKIPA)

The Federal PKI Policy Authority (FPKIPA) is a group of U.S. Federal Government Agencies (including cabinet-level Departments) chartered by the Federal CIO Council. The FPKIPA owns the Common Policy and represents the interest of the Federal CIOs. The FPKIPA is responsible for:

* Maintaining the CP
* Approving the CPS for each CA that issues certificates under the Common Policy
* Approving the compliance audit report for each CA issuing certificates under the Common Policy
* Ensuring continued conformance of each CA that issues certificates under the Common Policy with applicable requirements as a condition for allowing continued participation

#### FPKI Management Authority (FPKIMA)

The FPKIMA is the organization that operates and maintains the Common Policy Root CA on behalf of the U.S. Government, subject to the direction of the FPKIPA.

#### FPKI Management Authority Program Manager

The Program Manager is the individual within the FPKI Management Authority who has principal responsibility for overseeing the proper operation of the Common Policy Root CA including the Common Policy Root CA repository, and selecting the FPKI Management Authority staff. The Program Manager is selected by the FPKI Management Authority and reports to the FPKIPA. The FPKI Management Authority Program Manager must hold a Top Secret security clearance.

#### Policy Management Authority

WidePoint’s Chief Executive Officer is responsible for maintaining the WidePoint Shared Service Provider (SSP) CPS and for ensuring that all SSP PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with this CPS and the Common Policy. This is referred to as the SSP PMA within this CPS.

Agencies that contract for the services of a WidePoint SSP CA under this CPS and the Common Policy shall establish a management body to manage any agency-operated components (e.g., RAs or repositories) and resolve name space collisions. This body shall be referred to as an Agency Policy Management Authority, or Agency PMA.

An Agency PMA is responsible for ensuring that all Agency-operated PKI components (e.g., CAs, CSSs, CMSs, RAs) are operated in compliance with the Common Policy and this CPS, and shall serve as the liaison for that agency to the FPKIPA and the SSP PMA.

#### Authorized WidePoint SSP CAs

A WidePoint SSP CA is the collection of hardware, software and operating personnel that create, sign, and issue public key certificates to subscribers. WidePoint is an authorized SSP CA and may issue certificates that reference the Common CP, having qualified as an Authorized SSP CA by:

1. Documenting the specific implemented practices and procedures under which WidePoint satisfies the requirements of the Common Policy in the WidePoint SSP CPS.
2. Successfully completing Security Certification and Accreditation (C&A) in accordance with Federal laws, GSA regulations, and guidelines.

WidePoint is responsible for all aspects of the issuance and management of WidePoint SSP Certificates, including:

* The certificate manufacturing process
* Publication of certificates
* Revocation of certificates
* Generation and destruction of CA signing keys
* Ensuring that all aspects of the WidePoint SSP CA services and WidePoint SSP CA operations and infrastructure related to SSP Certificates issued under the Common Policy and this CPS are performed in accordance with the requirements, representations, and warranties of the Common Policy and this CPS

WidePoint is responsible for ensuring that all work is performed under the supervision of WidePoint or designated Agency personnel, and provides assurance of the trustworthiness and competence of employees and their satisfactory performance of duties relating to provision of SSP services. Each WidePoint SSP CA or employee of WidePoint to whom information may be made available or disclosed is notified in writing by WidePoint that information so disclosed to WidePoint or WidePoint’s employees can be used only for the purposes and to the extent authorized herein.

WidePoint complies with all applicable Federal and GSA requirements, including those for the prevention and reporting of waste, fraud, and abuse.

.

#### Certificate Status Servers

WidePoint operates a Certificate Status Server (CSS) using an OCSP responder that provides revocation status and/or certificate validation responses. How to obtain revocation information is provided on the certificate request website. The WidePoint CSS practices conform to the stipulations of the Common Policy and this CPS. The CSS asserts all the policy OIDs for which it is authoritative. All WidePoint CSS practice updates, as well as any subsequent changes are updated in this CPS and submitted to the Policy Authority for conformance assessment. The CSS practices include:

* Conformance to the stipulations of the Common Policy and this CPS.
* Ensuring that certificate and revocation information is accepted only from valid CAs.
* Providing only valid and appropriate responses.
* Asserting all the policy OIDs for which it is authoritative.
* Maintaining evidence of due diligence being exercised in validating certificate status.

### Registration Authorities

Registration Authorities (RAs) for the WidePoint SSP CA(s) are human and non-human entities. WidePoint RAs (human) are approved by a WidePoint CAA or by another WidePoint RA. WidePoint RAs (non-human) are approved via the WidePoint Configuration Control Board (CCB) prior to installation.

For certificates asserting id-fpki-common-policy, id-fpki-common-contentSigning, id-fpki-common-devices, and id-fpki-common-devicesHardware, WidePoint RAs (human) are issued RA certificates for the purpose of collecting and submitting digitally signed verification of Subscriber identities and information to be entered into public key certificates. These RA certificates assert PIV Hardware certificate policy OIDs.

For certificates asserting id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-cardAuth, and id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware, WidePoint RAs (non-human CMS) are issued a connector certificate for secure authentication to the WidePoint SSP CA. The connector certificate is an RSA administrative certificate which authorizes the card management system to request certificates and certificate revocations of the CA.

WidePoint SSP RAs are responsible for:

* Control over the registration process
* The identification and authentication process

Section 5.2 of this CPS provides details regarding each of these RA roles.

### Trusted Agents

A Trusted Agent is a person who satisfies all the trustworthiness requirements for an RA and who performs identity proofing as a proxy for the RA for WidePoint SSP PIV credentials (FIPS 201) only. The Trusted Agent records information from applicants and verifies biometrics (e.g., photographs) on presented credentials when the applicant appears in-person before the Trusted Agent. Within the WidePoint SSP PKI, three roles serve as Trusted Agents:

* PIV Sponsor
* PIV Registrar
* PIV Issuer

The responsibilities of these roles are detailed in Section [5.2.1.5](#_Trusted_Agents).

### <Redacted>Subscribers

A subscriber is the End Entity (EE) whose name appears as the subject in a certificate, and who asserts that it uses its key and certificate in accordance with this CPS. Subscribers are limited to Federal employees, contractors, affiliated personnel, and devices operated by or on behalf of Federal agencies. CAs are sometimes technically considered “subscribers” in a PKI. However, the term “subscriber” as used in this document refers only to those who request certificates for uses other than signing and issuing certificates or certificate status information.

There is a subset of human subscribers who may be issued role-based certificates. These certificates will identify a specific role on behalf of which the subscriber is authorized to act, rather than the subscriber’s name, and are issued in the interest of supporting accepted business practices.

The role-based certificate can be used in situations where non-repudiation is desired. Normally, it will be issued in addition to an individual subscriber certificate. A specific role may be identified in certificates issued to multiple subscribers, however, the key pair will be unique to each individual role-based certificate (i.e. there may be four individuals carrying a certificate issued in the role of “Secretary of Commerce”; however, each of the four individual certificates will carry unique keys and certificate identifiers). Roles for which role-based certificates may be issued are limited to those that are held by a unique individual within an organization (e.g. Chief Information Officer, GSA is a unique individual whereas Program Analyst, GSA is not).

WidePoint CAs are technically a subscriber to the PKI; however, the term subscriber as used in this CPS refers only to those EEs who request certificates for uses other than signing and issuing certificates. Additionally, the WidePoint Card Management System is technically a subscriber and is responsible for managing smart card token content. The WidePoint Card Management System is only issued the PIV Content Signing certificate and a Connector Certificate and is not issued any certificates that express any other policy OID. Review of the certificate profile information contained within this CPS verifies that only the Content Signing Certificate and a Connector Certificate are issued to the WidePoint Card Management System.

Pre-production testing of cards generated by the Card Management System is performed internally using the PIV Data Model Tester (SP 800-85B Tool). The subsequent report is then reviewed to ensure compliance. If any item(s) results in a “failed” result, updates and configuration changes are made accordingly and a follow-up test is performed. This process is continued until all items return with a “passed” result. A production card, issued to a Subscriber, is then generated. The Subscriber then takes their card to the FPKI for testing. The card used for testing is a “live”, production card that the Subscriber will use as their PIV card thereafter. All equipment used for WidePoint PIV card issuance adheres to FIPS 201 and are products from the Approved Products List (APL).

#### PKI Sponsor

A PKI Sponsor fills the role of a Subscriber for non-human system components (non-FIPS 201) and organizations that are named as public key certificate subjects. The PKI Sponsor works with the WidePoint SSP RAs and/or LRAs, to register components (routers, firewalls, etc.) in accordance with Section 3.2.3.3, and is responsible for meeting the obligations of Subscribers as defined throughout this document. PKI Sponsor is not considered a trusted role.

### Relying Parties

A Relying Party is the entity that relies on the validity of the binding of the subscriber’s name to a public key. A Relying Party is an individual or organization that, by using another’s certificate can:

* Verify the integrity of a digitally signed message.
* Identify the creator of a message, or establish confidential communications with the holder of the certificate.
* Rely on the validity of the binding of the subscriber’s name to a public key.

Under the SSP program relying parties are those eligible Federal agencies and entities that enter into an agreement with GSA to accept SSP Certificates and agree to be bound by the terms of the Common Policy and this CPS.

Other eligible federal agencies and entities operating under the Common Policy include all Federal agencies, authorized federal contractors, agency-sponsored universities and laboratories, other organizations, and, if authorized by law, state, local, and tribal governments.

At one’s own risk, a relying party may use information in the certificate (such as certificate policy identifiers) to determine the suitability of the certificate for a particular use.

### Other Participants

#### Certificate Management Authority(s) (CMA)

WidePoint is responsible for the functions of manufacturing, issuance, suspension, and revocation of WidePoint SSP certificates.

The WidePoint SSP CA, RAs and LRAs are considered “Certificate Management Authorities” (CMAs). The term CMA refers to a function assigned to either CAs or RAs, or to both CAs and RAs.

Certificate Status Servers (CSSs) such as Online Certificate State Protocol (OCSP) Responders operated by WidePoint are also considered CMAs. WidePoint will operate an OCSP Responder in support of WidePoint SSP.

WidePoint is responsible for ensuring that all WidePoint SSP CMAs (i.e., the CA, CSAs, RAs, and LRAs) are in compliance with this CPS and the Common Policy.

WidePoint may subcontract CMA functions to third-party CMAs who agree to be bound by the Common Policy and this CPS, provided that GSA approves such subcontractor in advance. However, WidePoint remains responsible for the performance of those services in accordance with the Common Policy.

#### Local Registration Authorities (LRAs)

WidePoint RAs may delegate the identity proofing tasks to Local Registration Authorities (LRAs) who have been approved by a WidePoint RA. Upon performing their duties LRAs provide verification to the RA. If a WidePoint RA delegates duties to one or more LRAs, the WidePoint RA informs all other WidePoint RAs. LRAs may not designate other LRAs. Approval of certificates may only be approved by RA certificate holders of equal or higher levels of assurance. LRAs can be WidePoint employees on location at a subscriber’s agency or employees of a subscriber’s agency.

LRAs are obligated to accurately enter Applicant’s information into the system. LRAs may not designate other LRAs under this CPS. LRAs under this CPS are not authorized to assume any other CA administration functions.

## <Redacted>Certificate Usage

### Appropriate Certificate Uses

The sensitivity of the information processed or protected using certificates issued by the CA will vary significantly. Organizations must evaluate the environment and the associated threats and vulnerabilities and determine the level of risk they are willing to accept based on the sensitivity or significance of the information. This evaluation is done by each organization for each application and is not controlled by this CPS.

This section contains definitions for two levels of assurance, and guidance for certificate usage in their application. Emphasis is placed on two types of activity: integrity and access control to information considered sensitive and information related to electronic financial transactions and other e-commerce. The final selection of the security mechanisms, and level of strength and assurance, requires a risk management process that addresses the specific mission and environment. Each relying party is responsible for carrying out this risk analysis.

Credentials issued under the id-fpki-common-policy and id-fpki-common-derived-pivAuth policies are intended to meet the requirements for Level 3 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth] Credentials issued under the id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-High policies meet the requirements for Level 4 authentication, as defined by the OMB E-Authentication Guidance. [E-Auth]

Credentials issued under the id-fpki-common-piv-contentSigning policy are intended to meet the requirements in FIPS 201 and SP 800-157 as the digital signatory of the PIV Card Holder Unique IDentifier (CHUID) and associated PIV data objects.

In addition, the Common Policy and this CPS may support signature and confidentiality requirements for Federal Government processes.

### Prohibited Certificate Uses

This CPS prohibits the use of any application that does not follow approved standards for the storage and transmittal of cryptographic information. Applicable standards include:

* FIPS 140-2, Security Requirements for Cryptographic Modules
* FIPS 180-4, Secure Hash Algorithm
* FIPS 186-4, Digital Signature Standard
* PKCS #11 Hardware Format
* PKCS #12 Software Format
* X.509 v23 Information Technology – ASN.1 Encoding Rules 1994
* ANSI X9.31 American National Standard for Digital Signature using Reversible Public Key Cryptography for the Financial Service Industry

Certificates that assert id-fpki-common-cardAuth are only to be used to authenticate the hardware token containing the associated private key and are not to be interpreted as authenticating the presenter or holder of the token.

## Policy Administration

### Organization Administering the Document

The Chief Executive Officer of WidePoint administers WidePoint PKI organization. The WidePoint PKI Project Director is responsible for registration, maintenance, and interpretation of this CPS.

WidePoint PKI Project Director

11250 Waples Mill Road, South Tower, Suite 210

Fairfax, VA 22030

### Contact Person

Questions regarding this CPS are directed to the WidePoint SSP Program Manager:

Caroline Godfrey, Vice President, Programs

11250 Waples Mill Road, South Tower, Suite 210

Fairfax, Virginia 22030

godfreyc@orc.com

### Person Determining CPS Suitability for the Common Policy

The Government has determined the suitability of this CPS as part of the evaluation process. Any changes to this CPS made after determination of suitability will be transmitted to the Government for approval prior to incorporation.

The FPKIPA approves the CPS for each CA that issues certificates under the FPKI Common Policy.

### CPS Approval Procedures

CAs issuing certificates under the FPKI Common Policy are required to meet all facets of the policy. The FPKIPA will not issue waivers.

The CA and RA must meet all requirements of this approved CPS before commencing operations. The FPKIPA makes the determination that this CPS complies with the policy, and issues a “decision letter” to WidePoint stating WidePoint has met the requirements and complies with the policy. In some cases, the FPKIPA may require the additional approval of an authorized agency. The FPKIPA will make this determination based on the nature of the system function, the type of communications, or the operating environment.

In each case, the determination of suitability will be based on an independent compliance auditor’s results and recommendations. See Section 8 for further details.

## Definitions and Acronyms

See Sections 11 and 12.

# Publication and Repository Responsibilities

## Repositories

WidePoint maintains a master directory protected by a firewall and accessible through the Internet. Information in WidePoint SSP repositories is protected in accordance with the Privacy Act of 1974 as set forth in WidePoint’s Privacy Policy and Procedures documents.

Updating the repository is restricted only to authorized individuals using certificate authenticated access control over SSL. The directory is configured by the CAA to recognize WidePoint RAs and CAAs as authorized to make changes. WidePoint protects any and all repository information not intended for public dissemination or modification.

The WidePoint Repository is responsible for:

* Maintaining a secure system for storing and retrieving Certificates.
* Maintaining a current copy of this CPS.
* Maintaining other information relevant to Certificates.
* Providing information regarding the status of Certificates as valid or invalid that can be determined by a relying party.

WidePoint posts CA Certificates at the following location, accessible via HTTP:

* http://crl-server.orc.com/caCerts/ORC<CA Name>.p7c

WidePoint posts CRLs at the following location, accessible via HTTP:

* http://crl-server.orc.com/CRLs/ORC<CA Name>.crl

WidePoint posts certificates and CRL information in a repository established by the WidePoint SSP PKI. Only information contained in the certificate(s) is posted in this directory to ensure compliance with the Privacy Act. CA Cert information access is available via:

* https://www.orc.com/ssp/repository/

The certificate repository meets the following obligations:

* To list all un-expired CA certificates issued by or to the CA
* To contain an accurate and current CRL for the respective CAs for use by relying parties
* To be publicly accessible
* To be physically accessible, via certificate-authenticated access control over SSL, for authorized requests coordinated with the WidePoint Point of Contact (POC) during normal business hours for the operating organization
* To be maintained in accordance with the practices specified in this CPS
* To meet or exceed the requirement of 99% availability for all components within the control of the operating organization

Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

WidePoint maintains a copy of at least all certificates and CRLs WidePoint issues and makes this information available to the sponsoring agency for archiving, if requested. WidePoint provides this information on a certificate accessed web server posted no later than 10 days after the end of the collection of the data.

## Publication of Certification Information

### Publication of Certificates and Certificate Status

WidePoint maintains a publicly accessible repository that is available to subscribers and relying parties that contains:

* A listing of all current signature and encryption certificates signed by the WidePoint SSP CAs
* Current, complete, and accurate CRLs
* WidePoint SSP certificates for signing keys
* WidePoint SSP certificates for CRL signing keys
* A copy or link to the current Common Policy
* A summary of this approved CPS

The repository is located at https://www.orc.com/ssp/repository/. WidePoint’s SSP publicly accessible repository system has been designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually. The certificate status server (CSS) has also been designed and implemented so as to provide 99% availability overall and limit scheduled down-time to 0.5% annually.

### Publication of CA Information

The FPKI Common Policy document is publicly available on the FPKIPA website (see https://www.idmanagement.gov/IDM/s/). The WidePoint CPS for the WidePoint SSP CA will not be published; a redacted version of this CPS will be publicly available from the WidePoint SSP website (see https://www.orc.com/ssp/repository/).

### Interoperability

CA certificates and CRLs issued under this CPS are published as specified and in compliance with the Shared Service Provider Repository Service Requirements [SSP-REP].

## Time or Frequency of Publication

CA certificates are published to a repository at the time of issuance and remain accessible from the repository following subscriber acceptance. CRL publication is in accordance with Section [4.9](#_Certificate_Revocation_and). Frequency of CRL publication is in accordance with Section [4.9.7](#_CRL_Issuance_Frequency).

## Access Controls on Repositories

Access to SSP Certificates and SSP Certificate status information is in accordance with this CPS and the Common Policy. Access controls include:

* Physical access to WidePoint CAs and OCSP server(s) are controlled by job requirements and authentication, as stipulated in Section 5.1.2.
* WidePoint employees are only able to access those resources that they require to accomplish the tasks they are assigned, as stipulated in this CPS (access rights are assigned by resource [server, computer, share, volume, printer, etc.]).
* User authentication is via certificate authentication (or UserID and password when appropriate) and data encryption is used, as stipulated in this CPS.
* WidePoint employees are assigned access rights before accessing any electronic resources.
* The WidePoint Corporate Security Auditor determines and periodically reviews user access rights.

The CAA and SA are notified of any changes that affect employee access rights.

There are no access controls on the reading of the CPS summary, any supplemental policy information, or any supplemental practice information published by WidePoint. WidePoint SSP CA Certificate(s) and CRL information are publicly available.

These policies are elaborated upon in the WidePoint Systems Security Plan (SSP).

# Identification and Authentication

## Naming

### Types of Names

All certificates issued by the WidePoint SSP CAs conform to the X.500 Distinguished Name (DN) format for subject and issuer name fields and conform to the format specified in the Common Policy.

For WidePoint SSP certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-High, id-fpki-common-devices and id-fpki-common-devicesHardware the WidePoint SSP CA will assign X.500 distinguished names to all subscribers. These distinguished names may be in either of two forms: a geo-political name or an Internet domain component name.

All geo-political distinguished names assigned to federal employees will be in the following directory information tree:

* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container]

The organizational units department and agency appear when applicable and are used to specify the federal entity that employs the subscriber. At least one of these organizational units must appear in the DN. The additional organizational unit *structural\_container* is permitted to support local directory requirements, such as differentiation between human subscribers and devices. This organizational unit may not be employed to further differentiate between subcomponents within an agency.

The distinguished name of the federal employee subscriber will be one of the three following forms:

* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<nickname lastname>
* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<firstname initial. lastname>
* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<firstname middlename lastname>

In the first name form, nickname may be the subscriber's first name, a form of the first name, middle name, or pseudonym (e.g., Buck) by which the subscriber is generally known. A generational qualifier, such as "Sr." or "III", may be appended to any of the common name forms specified above.

Distinguished names assigned to federal contractors and other affiliated persons will be within the same directory information tree. The distinguished name of the federal contractor subscribers and affiliate subscribers will take one of the three following forms:

* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<nickname lastname> (affiliate)
* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<firstname initial. lastname> (affiliate)
* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<firstname middlename lastname> (affiliate)

For names assigned to federal contractors and other affiliated persons, generational qualifiers may be inserted between lastname and "(affiliate)".

WidePoint coordinates with the Customer agency to determine which one of the aforementioned name definitions is used.

Certificates issued under id-fpki-common-authentication include a subject alternative name. The subject alternative name extension includes the pivFASC-N name type. The value for this name is the FASC-N of the subject’s PIV card. The subject alternative name extension includes the UUID from the GUID data element of the CHUID. The UUID is included as a URI as specified in section 3 of RFC 4122.

Certificates issued under id-fpki-common-cardAuth include the UUID from the GUID data element of the CHUID. The UUID is included as a URI as specified in section 3 of RFC 4122. Certificates issued under id-fpki-common-cardAuth will not include any other name in the subject alternative name extension but may include a non-NULL name in the subject field. If included, the subject distinguished name shall take one of the following forms:

* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], serialNumber=FASC-N
* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], serialNumber=FASC-N
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], serialNumber=FASC-N
* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], serialNumber=UUID
* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], serialNumber=UUID
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], serialNumber=UUID

Practice Note: The FASC-N [PACS] consists of 40 decimal digits that are encoded as a 25-byte binary value. This 25-byte binary value may be encoded directly into the pivFASC-N name type in the subject alternative name extension, but when included in the subject field the FASC-N must be encoded as a PrintableString that is at most 64 characters long. This policy does not mandate any particular method for encoding the FASC-N within the serial number attribute as long as the same encoding method is used for all certificates issued by a CA. Acceptable methods for encoding the FASC-N within the serial number attribute include encoding the 25-byte binary value as 50 bytes of ASCII HEX or encoding the 40 decimal digits as 40 bytes of ASCII decimal.

Practice Note: When the UUID appears in the subjectAltName extension of a certificate, it must be encoded as a uniformResourceIdentifier as specified in Section 3 of [RFC 4122]. An example of a UUID encoded as a URI, from RFC 4122, is “urn:uuid:f81d4fae-7dec11d0-a765-00a0c91e6bf6”. This policy does not mandate any particular method for encoding the UUID within the serial number attribute as long as the same encoding method is used for all certificates issued by the CA and it is encoded as a PrintableString that is at most 64 characters long, however, it is recommended that the string representation from Section 3 of [RFC 4122] be used. An example would be “f81d4fae7dec-11d0-a765-00a0c91e6bf6”.

Distinguished names based on Internet domain component names shall be in the following directory information trees:

* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container]
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container]

The default Internet domain name for the agency [orgN.]…[org0].gov or [orgN.]…[org0].mil, will be used to determine DNs. The first domain component of the DN will either be dc=gov or dc=mil. At a minimum, the org0 domain component must appear in the DN. The org1 to orgN domain components appear, in order, when applicable and are used to specify the federal entity that employs the subscriber.

Distinguished names for federal employee Subscribers will take one of the following forms when their agency’s Internet domain name ends in .gov:

* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<nickname lastname>
* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname initial. lastname>
* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname middlename lastname>

Distinguished names for federal employee Subscribers will take one of the following forms when their agency’s Internet domain name ends in .mil:

* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<nickname lastname>
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname initial. lastname>
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname middlename lastname>

Distinguished names for federal contractors and affiliated persons will take one of the following forms when their agency’s Internet domain name ends in .gov:

* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<nickname lastname> (affiliate)
* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname initial. lastname> (affiliate)
* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname middlename lastname> (affiliate)

Distinguished names for federal contractors and affiliated persons will take one of the following forms when their agency’s Internet domain name ends in .mil:

* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<nickname lastname> (affiliate)
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname initial. lastname> (affiliate)
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<firstname middlename lastname> (affiliate)

Signature certificates issued under id-fpki-common-hardware may be issued with a common name that specifies an organizational role, such as the head of an agency, as follows:

* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<role [, department/agency]>
* dc=gov, dc= …., [ou=structural\_container], cn=<role [, department/agency]>

The combination of organizational role and agency must unambiguously identify a single person.

Where the [department/agency] is implicit in the role (e.g., Secretary of Commerce), it should be omitted. Where the role alone is ambiguous (e.g., Chief Information Officer) the department/agency must be present in the common name. The organizational information in the common name must match that in the organizational unit attributes.

For subscriber certificates asserting the following OID, id-fpki-common-piv-contentsigning, the distinguished name will take the following form:

* C=US, O=ORC PKI, OU=ORC, CN=<PIV Content Signer>
  + in the case which WidePoint administers the card management system for the Customer agency;
* C=US, O=U.S. Government, [OU=department], [ou=agency], CN=[organization] [ID] PIV Content Signer
  + in the case which the card management system is administered by the Customer agency

Where “ID” equals unique qualifier assigned by organization (e.g. CN=EPA 1 PIV Content Signer; CN=EPA 2 PIV Content Signer).

Devices that are the subject of certificates issued under this policy shall be assigned either a geo political name or an Internet domain component name. Device names shall take one of the following forms where device name is a descriptive name for the device:

* C=US, o=U.S. Government, [ou=department], [ou=agency], [ou=structural\_container], cn=<device name>
* dc=gov, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<device name>
* dc=mil, dc=org0, [dc=org1], …, [dc=orgN], [ou=structural\_container], cn=<device name>

Where a device is fully described by the Internet domain name, the common name attribute is optional as shown in Table 2. When the device has an Internet domain name, WidePoint confirms it resolves. For non-Internet domain names, the Letter of Authorization serves as authentication.

Table : Common Name Attribute Criteria

|  |  |
| --- | --- |
| **Security Level** | **Name Format** |
| Basic | Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical |
| Medium | Non-Null Subject Name, and optional Subject Alternative Name if marked non-critical |
| PIV Card Authentication | Non-Null Subject Name, and Subject Alternative Name |

This CPS does not restrict the directory information tree for names of CAs and CSSs. However, CAs that issue certificates under this CPS must have distinguished names. CA and CSS distinguished names may be either a geo-political name or an Internet domain component name. CA and CSS geo-political distinguished names will be composed of any combination of the following attributes:

* country; organization;
* organizational unit; and
* common name (e.g., WidePoint SSP <number>).

Internet domain component names are composed of the following attributes:

* domain component;
* organizational unit; and
* common name (e.g., SSP<#>.eva.orc.com).

For certificates issued under id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth, in order to maintain logical access requirements between the PIV Authentication certificate and the Derived PIV Authentication certificate, the primary credential (PIV Authentication) DN string is used for the Derived PIV DN string. During issuance of the Derived PIV, a unique UUID is created and stored in the Subject Alternate Name. This unique UUID is generated independent of the UUID created for the primary credential.

### Need for Names to be Meaningful

Names used in certificates issued by the WidePoint SSP CA(s) identify in a meaningful way the subscriber to which they are assigned.

The common name in the DN represents the subscriber in a way that is easily understandable for humans. For people, this will typically be a legal name, such that the preferred common name form is:

* cn=firstname initial.lastname

Common Names are meaningful as individual names, as actual server Uniform Resource Locators (URLs) or Internet Protocol (IP) addresses. Names identify the person or object to which they are assigned. WidePoint ensures that an affiliation exists between the subscriber and any organization that is identified by any component of any name in its certificate.

The common name used represents the subscriber in a way that is easily understandable for humans. For people, this is typically a legal name. For equipment, this may be a model name and serial number, or an application process (e.g., Organization X Mail List or Organization Y Multifunction Interpreter).

In the case of all Digital Signature and Encryption Certificates asserting Common Policy OIDs issued to federal employees naming variations will be one of the following:

CN = Nickname Smith; or

CN = John J. Smith; or

CN = John Jay Smith

In the case of all Digital Signature and Encryption Certificates asserting Common Policy OIDs issued to federal contractors and other affiliates designated by a sponsoring agency:

CN = Nickname Smith (affiliate); or

CN = John J. Smith (affiliate); or

CN = John Jay Smith (affiliate)

While the WidePoint SSP name in CA certificates is not generally interpreted by relying parties, the Common Policy still requires use of meaningful names by WidePoint SSP CAs issuing under the Common Policy and this CPS. If included, the common name will describe the WidePoint SSP CA, as such:

cn=ORC SSP <CA#>

The subject name in CA certificates matches the issuer name in certificates issued by the WidePoint SSP CA, as required by RFC 3280.

### Anonymity or Pseudonymity of Subscribers

WidePoint SSP does not issue anonymous or pseudonymous certificates.

### Rules for Interpreting Various Name Forms

Rules for interpreting name forms are specified in X.501. Rules for interpreting e-mail addresses are specified in [RFC 2822].

Rules for interpreting the PIV FASC-N name type are specified in [PACS].

### Uniqueness of Names

WidePoint complies with uniqueness of names; including X.500 DNs. The WidePoint SSP CA(s) share a single public directory information tree for the publication of certificates (please refer to Section 3.1.1 for method of naming assignment). WidePoint enforces name uniqueness, as described in Sections 3.1.1 and 3.1.2.

WidePoint ensures the following for subscriber names:

* The name contains the subscriber identity and organization affiliation (if applicable) that is meaningful to humans.
* The naming convention is described in this CPS (see Section 3.1.1).
* WidePoint complies with the Policy Authority for the naming convention.

This does not prevent devices from sharing a Fully Qualified Domain Name (FQDN) as CN.

### Recognition, Authentication, and Role of Trademarks

A corporate entity is not guaranteed that its Common Name will contain a trademark if requested. WidePoint will not issue that name to the rightful owner if it has already issued one sufficient for identification. WidePoint will not issue a certificate knowing that it infringes the trademark of another.

The use of trademarks in a name form or as any part of a name form is discouraged. Trademarks will not be used as a name form or as a part of the name form for certificates issued to government employees unless U.S. Government personnel hold them or devices have a legitimate right to their use. The holder of the trademark will only use trademarks in certificates issued to contractors, contractor-owned servers, foreign nationals, or organizations with specific permission.

## Initial Identity Validation

### Method to Prove Possession of Private Key

In all cases where the subscriber generates key pairs, the subscriber is required to prove, to a WidePoint SSP CA, possession of the private key that corresponds to the public key in the certificate request. Subscribers are required to use a FIPS 140-2 validated cryptographic module for generation of keys. PIV certificates are issued on a PIV card via a GSA FIPS-201 approved Card Management System (CMS); refer to FIPS 201 Evaluation Program Approved Product List.

The subscriber is in possession and control of the private key from time of generation or benign transfer. The WidePoint SSP CAs authenticate the subscriber with a Proof of Possession (POP) test when requesting and retrieving a certificate by requiring the subscriber to perform a private key operation and verifying that the public key presented by the subscriber matches the private key. WidePoint supports multiple enrollment protocols which support POP including:

* KEYGEN/SPAC, CRMF/CMMF, PKCS #10 and CMC

To affect POP, the CA supplies a random challenge string to the browser as part of the KEYGEN tag. The public key generated by the browser and the challenge string supplied by the CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base 64 encoded and sent to the CA as part of the certificate request; the CA verifies the signature using the included public key, thus proving possession by the browser of the private key corresponding to that public key.

The public key and challenge strings are DER encoded as PublicKeyAndChallenge and then digitally signed with the private key to produce a SignedPublicKeyAndChallenge. The SignedPublicKeyAndChallenge is base64 encoded, and the ASCII data is finally submitted to the server as the value of a name-value pair, where the name is specified by the NAME attribute of the KEYGEN tag. When retrieving the completed certificate the browser also checks before importing the certificate into its database, to verify that the public key in the certificate being installed matches the private key it originally generated.

An additional out-of-band check is performed by requiring the requestor to print the base 64 of the DER encoded certificate request and present it in person during the validation process. The RA validates both the person’s identity and their possession of a certificate request corresponding to their private key.

For id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices, id-fpki-common-devicesHardware, id-fpki-common-piv-contentSigning certificates, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware; the Subscriber generates a key pair (private/public) using the device’s associated Cryptographic Service Provider (CSP) and creates a signed PKCS10 object. For id-fpki-common-devices, the key pair is generated in a software CSP, at a minimum. For id-fpki-common-piv-contentSigning, the key pair is generated in a hardware CSP. For id-fpki-common-devices and id-fpki-common-piv-contentSigning, the PKI Sponsor submits the PKCS10 object to the WidePoint SSP PKI CA for certificate processing.

In all cases, RAs may request additional information or verification from an RA or LRA if deemed necessary by the RA to confirm the requestor’s identity.

### Authentication of Sponsoring Organization Identity

When an applicant requests an SSP Certificate, in addition to verifying the applicant’s authorization to represent the Sponsoring Organization, WidePoint verifies the Sponsoring Organization's current operating status and that said organization conducts business at the address listed in the SSP Certificate application. WidePoint provides validation of information concerning the Sponsoring Organization, such as legal company name, type of entity, year of formation, names of directors and officers, address (number and street, city, ZIP code), and telephone number. All applicants are notified, on the website application process, that the process is secure.

Users will provide proof of their relationship to the company/organization they work for. This proof can be accomplished by:

* Applicant requesting a certificate accompanied by a U.S. Government sponsor
* Applicant presenting a government-issued photo ID badge including the applicants company affiliation
* Applicant providing a signed letter on company or agency letterhead from an authorized organization official attesting to the relationship (this is the only method approved for server certificate requests)
* Applicant presenting an un-expired photo ID badge issued by the organization

In all cases, in order to issue a certificate asserting a Common Policy OID, the applicant will obtain, from an authorized organization official, approval to hold a Common Policy certificate.

### Authentication of Individual Identity

WidePoint allows a certificate to be issued only to a single entity. Certificates are not issued that contain a public key whose associated private key is shared.

#### Authentication of Human Subscribers

Verification of an applicant’s identity will be performed prior to certificate issuance and the applicant’s identity must be verified no more than 30 days before initial certificate issuance. For medium assurance certificates the applicant’s in-person identity verification may be performed by an RA or LRA. All applicants for medium hardware assurance certificates are required to appear in person before an RA or LRA.

For id-fpki-common-authentication, id-fpki-common-cardAuth, and id-fpki-common-hardware, identity-proofing is performed in accordance with section 2.7, PIV Identity Proofing and Registration Requirements, of FIPS 201-2.

Applicants for medium assurance and medium hardware assurance certificates are required to present two (2) official photo credentials along with other application information, identified below, and the applicant form generated during the certificate request process containing the public key.

Minors and others not competent to perform face-to-face registration alone are not supported under this CPS.

The RA or LRA will archive a copy of all information used in the verification process. At a minimum, authentication procedures for WidePoint SSP certificate Federal employee applicants must include the following steps:

1. Verify that a request for certificate issuance to the applicant was submitted by agency management.
2. Verify Applicant’s employment through use of official agency records.
3. Establish applicant's identity by in-person proofing before the RA or LRA, based on either of the following processes:
   1. Process #1:
      1. The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
      2. The RA or LRA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
      3. The credential presented in Step 3) a) i) above is verified by the RA or LRA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying a database maintained by the organization that issued the credential, but other equivalent methods may be used.
   2. Process #2:
      1. The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
      2. The RA or LRA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
      3. The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in Step 3) b) i) above is verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).

Practice Note: This may be accomplished by querying a database maintained by the organization that issued the financial instrument or through use of a commercial credit database. In some instances, commercial credit card databases will validate name and address of current cardholders on-line; this validation is acceptable if the card is presented to the RA or LRA. Other methods may be accepted.

1. Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

For contractors and other affiliated personnel, the authentication procedures must include the following steps:

1. Verify that a request for certificate issuance to the applicant was submitted by an authorized sponsoring agency employee (e.g., contracting officer or contracting officer’s technical representative).
2. Verify sponsoring agency employee's identity and employment through either one of the following methods:
3. A digitally signed request from the sponsoring agency employee, verified by a currently valid employee signature certificate issued by an agency CA, may be accepted as proof of both employment and identity,
4. Authentication of the sponsoring agency employee with a valid employee PIV-authentication certificate issued by the agency may be accepted as proof of both employment and identity, or
5. In-person identity proofing of the sponsoring agency employee may be established before the registration authority as specified in employee authentication above and employment validated through use of the official agency records.
6. Establish applicant's identity by in-person proofing before the registration authority, based on either of the following processes:
   1. Process #1:
      1. The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
      2. The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
      3. The credential presented in Step 3) a) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid). Typically this is accomplished by querying official records maintained by the organization that issued the credential.
   2. Process #2:
      1. The applicant presents a government-issued form of identification (e.g., an Agency ID badge, a passport, or driver's license) as proof of identity, and
      2. The RA examines the presented credential for biometric data that can be linked to the applicant (e.g., a photograph on the credential itself or a securely linked photograph of applicant), and
      3. The applicant presents current corroborating information (e.g., current credit card bill or recent utility bill) to the RA. The identifying information (e.g., name and address) on the credential presented in Step 3) b) i) above shall be verified by the RA for currency and legitimacy (e.g., the agency ID is verified as valid).
7. Record and maintain a biometric of the applicant (e.g., a photograph or fingerprint) by the RA or CA. (Handwritten signatures and other behavioral characteristics are not accepted as biometrics for the purposes of this policy.) This establishes an audit trail for dispute resolution.

In all cases, RA or LRA records the following information:

* The Identity of the person performing the validation process
* Applicant’s name as it appears in the certificate Common Name field
* A signed declaration by the identity-verifying agent that they verified the identity of the applicant, using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury)
* Method of application (i.e., online, in-person)
* The method used to authenticate the applicant’s identity, including identification type and unique number or alphanumeric identifier on the ID
* A biometric of the applicant (facial image, fingerprint, etc.)
* The date and time of verification
* A handwritten signature by the applicant in the presence of the person performing the identity verification using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury)

For each data element accepted for proofing, including electronic forms:

* Name of document presented for identity proofing
* For PIV certificates the identity source documents must come from the list of acceptable documents included in Form I-9, OMB No. 1615-0047, Employment Eligibility Verification.
* Issuing authority
* Date of issuance
* Date of expiration

All fields verified:

* Source of verification (i.e., which databases used for cross-checks)
* Method of verification (i.e., online, in-person)
* Date/time of verification
* The WidePoint SSP name, including subcontractors, if any
* All associated error messages and codes
* Date/time of process completion
* Names (IDs) of WidePoint PKI processes, including subcontractors’ processes, if any.

Only for those applicants requesting id-fpki-common-policy, id-fpki-common-devices, id-fpki-common-devicesHardware, US Notaries Public may act as a Trusted Agent. These persons may validate the identity of individuals who are unable to present their identity credentials in person to an RA or Trusted Agent. In this situation, the Subscriber will be provided with a form including the Subscriber’s name, organizational affiliation (if subscriber is affiliated with an organization), and certificate request number. The Subscriber will be required to present this form, along with required IDs and credentials identifying organizational affiliation. The Notary Public will witness and certify the form.

The Subscriber will submit the notarized form and copies of the information used to establish identity via certified mail to an RA.

In all cases, WidePoint may request additional information or verification if deemed necessary to confirm the requestor’s identity.

#### Authentication of Devices

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor as described in Section 4.1.1.3. The PKI Sponsor is responsible for providing the CAA, or approved RAs, through an application form, correct information regarding:

* Equipment identification (e.g. serial number) or service name (e.g. DNS name) or unique software application name
* Equipment or software application public keys
* Equipment or software application authorizations and attributes (if any are to be included in the certificate)
* Contact information to enable WidePoint to communicate with the PKI sponsor when required

These certificates will only be issued to authorized devices under the subscribing organization’s control. In the case a human PKI Sponsor is changed, the new PKI Sponsor must review the status of each device under his/her sponsorship to ensure it is still authorized to receive certificates. See Section 9.6.3 for subscriber responsibilities.

A WidePoint RA authenticates the validity of any authorizations to be asserted in the certificate, and verifies source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by one of the following methods:

* Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested)
* In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 4.1.1.3.

#### Authentication of Derived PIV Credentials

This section applies to certificates asserting id-fpki-common-derived-pivAuth-hardware and id-fpki-common-derived-pivAuth. An RA or CAA verifies that the request for certificate issuance to the PIV Cardholder has been submitted by an authorized agency employee.

The PIV Cardholder presents his/her PIV Card for validation. The PIV Cardholder is prompted to activate the card to demonstrate they are in possession of the corresponding private key. The PIV Cardholder activates the card using either their PIN or their biometric. Using standards-compliant PKI path validation, WidePoint validates the PIV card confirming that it is neither expired nor revoked, and that it is from a trusted source. For certificates asserting id-fpki-common-derived-pivAuth-hardware, the foregoing occurs with the PIV Cardholder in the presence of the RA or CAA.

WidePoint maintains a copy of the PIV Cardholder’s PIV Authentication certificate.

For certificates asserting id-fpki-common-derived-pivAuth-hardware, applicants must appear at the RA in person to present the PIV Card and perform the PKI-AUTH authentication mechanism. The RA performs a 1:1 comparison of the PIV Cardholder, in accordance with [SP 800-76], against biometric data stored on the PIV Card. The RA records and maintains the biometric sample used to validate the PIV Cardholder. In cases where 1:1 biometric comparison is not possible, then the PIV Cardholder presents a government-issued form of identification. The RA examines this additional credential for biometric data (e.g., a photograph on the credential itself) which can be linked to the PIV Cardholder. If validation is successful using the additional credential, then the process documentation for the issuance of the certificate includes the identity of the RA, a signed declaration by the RA that he/she verified the identity of the PIV Cardholder as required by this CPS using the format set forth at 28 U.S.C. 1746 (declaration under penalty of perjury), a unique identifying number from the second form of identification or a facsimile of the ID, a biometric of the PIV Cardholder, and the date and time of the verification.

Seven days after issuing the Derived credential, WidePoint checks the revocation status of the PIV Authentication certificate (using the OCSP/CRL URL within the PIV Authentication certificate) which was recorded during the Derived PIV enrollment. This step can detect use of a compromised PIV Card to obtain a derived credential.

### Non-verified Subscriber Information

WidePoint does not include information in certificates that has not been verified.

### Validation of Authority

Before issuing certificates that assert organizational authority, WidePoint validates the individual’s authority to act in the name of the organization. This validation is performed by having the applicant complete and submit a “Proof of Organizational Affiliation” letter, made available to applicants on the WidePoint SSP website. WidePoint uses Proof of Organizational Affiliation letters for applicants attempting to obtain:

* Component/ Server certificates
* VPN IPsec Component Certificates

A specific Proof of Organizational Affiliation letter is provided for each particular type of certificate request.

WidePoint additionally requires a Proof of Organizational Affiliation for certificate requests from individuals who either do not possess a company issued photo ID badge or organizations which do not issue company photo ID badges, signed by a Duly Authorized Company Representative, stating that they are an employee of that organization.

### Criteria for Interoperation

The FPKIPA determines the interoperability criteria for CAs operating under the X.509 U.S. Federal PKI Common Policy Framework policy.

## Identification and Authentication for Re-key

### Identification and Authentication for Routine Re-key

SSP Certificate re-keying (signing and encryption) is accomplished through the limitation on certificate renewal, as in Section 3.2. The minimum in-person registration requirement for all SSP certificate re-keying described, with the exception of CA certificates, is once every 9 years from the time of initial registration (i.e., after two 3-year re-keys). WidePoint SSP subscribers must identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through initial registration process, described in Section 3.2.3.1, at least once every nine years from the time of initial registration.

For device certificates, identity may be established through the use of the device’s current signature key, the signature key of the device’s human PKI Sponsor, except that identity shall be established through the initial registration process at least once every nine years from the time of initial registration.

In addition, for re-key of subscriber certificates issued under id-fpki-common-derived-pivAuth-hardware, identity is established via mutual authentication between WidePoint and the cryptographic module containing the current key, if the new key will be stored in the same cryptographic module as the current key. The Subscriber’s identity must be established through the initial registration process if the new key will be stored in a different cryptographic module than the current key. An RA or CAA verifies that the request for certificate re-issuance to the PIV Cardholder has been submitted by an authorized agency employee.

CA certificate re-key follows the same procedure as is performed for initial CA certificate generation.

For re-key of subscriber certificates issued under id-fpki-common-derived-pivAuth and id-fpki-common-derived-pivAuth-hardware, the department or agency shall verify that the Subscriber is eligible to have a PIV Card (i.e., PIV Card is not terminated).

### Identification and Authentication for Re-key after Revocation

After a certificate has been revoked or expired, the applicant is required to go through the initial registration process as described in Section 3.2.3.1.

## Identification and Authentication for Revocation Request

Certificate revocation requests may be made using the same practices as certificate issuance requests. In addition, certificate revocation requests may be made electronically using e-mail digitally signed by a certificate of equal or greater level of assurance than that of the certificate for which the request is made. In either case, the request must include the reason for revocation. See Section 4.9 for details on certificate revocation procedures. Subscribers who are in possession of their private keys may also revoke their own certificates at any time via the WidePoint SSP website (http://www.orc.com/ssp/repository/revocation).

A subscriber may request revocation of a certificate regardless of whether or not it has been compromised. WidePoint may revoke a subscriber’s certificate for cause. The RA collects signed documentation stating the reason and circumstances for the revocation. If an RA performs this on behalf of a subscriber, a formal, signed message format known to the WidePoint RA is employed.

A WidePoint SSP Certificate revocation request that is submitted electronically may be authenticated on the basis of a digital signature using the SSP Certificate’s associated key pair. The identity of the person submitting a revocation request in any other manner is authenticated in accordance with Section 4.9 of this CPS. Revocation requests authenticated on the basis of the SSP Certificate’s associated key pair are always accepted as valid. Other revocation request authentication mechanisms for non-PIV certificates include a request in writing signed by the subscriber and sent via U.S. Postal Service first-class mail. WidePoint RAs verify the authentication mechanism and balances the need to prevent unauthorized revocation requests against the need to quickly revoke certificates. In the case of certificates asserting Common Policy OIDs, WidePoint will only accept revocation requests from the subscriber or persons authorized by each sponsoring agency to make revocation requests.

# Certificate Life-Cycle Operational Requirements

## Certificate Application

WidePoint SSP offers the certificate types as described in this CPS. The Certificate application process provides sufficient information to:

* Establish the applicant’s authorization (by the employing or sponsoring agency) to obtain a certificate (per Section 3.2.3).
* Establish and record the identity of the applicant (per Section 3.2.3).
* Obtain the applicant’s public key and verify the applicant’s possession of the private key for each certificate required (per Section 3.2.1).
* Verify any role or authorization information requested for inclusion in the certificate via documentation on company/organization letterhead or digitally signed email provided by an authorized representative of the organization.

These steps may be performed in any order that is convenient for WidePoint and the applicant, and that do not defeat security. However, all must be completed before certificate issuance.

### Who Can Submit a Certificate Application

Table 3 identifies the parties may initiate the WidePoint SSP Certificate application process.

Table : Authorized Certificate Application Initiators

| **Potential Subscriber** | **Authorized Initiator** |
| --- | --- |
| Application Server | PKI Sponsor responsible for the component receiving the certificate |
| Federal Employee | Sponsoring Organization; or potential subscriber |

The individual requiring the certificate will make a certificate request. When applicable, the subscriber’s organization is required to provide a Point of Contact (POC) for verification of any roles or authorizations to be included in the subscriber’s certificates, via signed letterhead or digitally signed e-mail. The CAAs record all such appointments in a log available to all RAs. This point of contact may be the PKI Sponsor or CSAA. A request is made from a workstation via a web interface. When making the certificate request, the applicant will submit a proposed distinguished name in accordance with local naming conventions, generate the public private key pair using FIPS 140-2 Level 1 approved software or Level 2 hardware tokens, and submit the information and the public key to the CA for disposition.

The applicant will protect the private key with a password. This password will be kept confidential and will not be recorded or given to any other parties.

In the case of medium assurance certificates, the applicant will make the request using a web browser incorporating a FIPS 140-2 Level 1 cryptographic module for generating the key pair and submitting the required information through an online form. In the case of medium hardware assurance certificates, the applicant will make the request at the RA workstation using a web browser and a FIPS 140-2 Level 2 token for generating the key pair and submitting the required information through an online form. The following instructions explain the steps necessary for an applicant to apply for a certificate:

* Connect to the WidePoint SSP web page (http://www.orc.com/ssp/repository) and follow the directions filling out the electronic and printed forms
* For encryption keys, the application process asks if the subscriber desires to escrow the encryption key and notifies subscriber upon successful completion or failure of key escrow
* Present the printed application and two photo IDs to an RA, LRA, or Notaries Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions)

Upon notification of certificate issuance by e-mail, the certificate is accepted and retrieved.

#### CA Certificates

WidePoint does not issue CA certificates outside of WidePoint.

#### User Certificates

The individuals requiring certificates will only make certificate requests for themselves. Users are not permitted to make requests on behalf of another individual. Requests for id-fpki-common-hardware, id-fpki-common-devices, Id-fpki-common-devicesHardware, id-fpki-common-derived-pivAuth, id-fpki-common-derived-pivAuth-hardware are made via a web interface. Requests for id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-piv-contentSigning are made from a card workstation connecting to the WidePoint SSP CA.

When making a certificate request via web interface, the applicant will complete an SSP Certificate application and provide requested information requested by an online form. The following steps occur during the application process:

* The applicant is presented with a screen detailing the subscriber obligations and required to accept these obligations prior to continuing
* The applicant completes the online form which includes his or her name, address, phone number, e-mail address (if available), and identifying information
* The applicant generates a public and private key pair and is required to use a password to protect the private key, as stipulated in the Subscriber Agreement. This password is stored locally and is required to be kept confidential and not be recorded or given to any other parties. An applicant should create passwords in accordance with the relevant passage in Section 6.2.8, “Method of Activating Private Key.”
* The applicant submits identifying information and the public key to the CA
* The applicant proves to the CA that the public key forms a functioning key pair with the private key via the proof of possession functionality as described in Section 4.9.3.

Upon submission of the completed application form, the applicant is provided with a request number and is required to print the form, and take it, with the appropriate identity credentials, to an authorized RA, LRA, trusted agent or member of the Notary Public to have the identity credentials verified. If the applicant goes in person to an RA, LRA or trusted agent, the application process for the applicant is completed. If the applicant has the forms notarized, the applicant is required to send the notarized form via U.S. postal service to WidePoint or personally deliver the forms to a WidePoint facility. This information is provided on the printed form.

In the case of certificates asserting a Common Policy OID, if the sponsoring agency's RPS allows applicants the option to use a notary, the applicant is required to send the notarized form via U.S. postal service to a sponsoring agency's designated RA or personally deliver the forms to a sponsoring agency's designated RA, in accordance with the stipulations of the agency RPS.

#### Device Certificates

Some computing and communications components (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the component must have a human PKI Sponsor. The PKI Sponsor is responsible for providing to the CAA, or approved RAs, through an application form, correct information regarding:

* Equipment identification
* Equipment public keys
* Equipment authorizations and attributes (if any are to be included in the certificate)
* Contact information to enable WidePoint to communicate with the PKI sponsor when required

A WidePoint RA authenticates the validity of any authorizations to be asserted in the certificate, and verifies source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by one of the following methods:

* Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested)
* In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 3.2.3.1

#### Code Signing Certificates

Not applicable. WidePoint does not support code-signing certificate for SSP.

### Enrollment Process and Responsibilities

All WidePoint SSP electronic transmissions and communications supporting application and issuance processes are authenticated and protected from modification using SSL. Where electronic communications are used, cryptographic mechanisms commensurate with the strength of the public/private key pair are used. Out-of-band communications protect the confidentiality and integrity of the data by sealing all data and only sending via trusted carriers (e.g. U.S. Postal Service, FedEx, UPS).

#### Non-SSP/PIV Workstation Certificate Enrollment

For certificates asserting id-fpki-common-policy, id-fpki-common-devices, id-fpki-common-devicesHardware, id-fpki-common-piv-contentSigning the applicant (Subscriber or Human PKI Sponsor) requiring the certificate must make the certificate request. When applicable, the applicant’s organization is required to provide a Point of Contact (POC) for verification of any roles or authorizations to be included in the subscriber’s certificates, via signed letterhead or digitally signed e-mail. This point of contact may be the PKI Sponsor. A request is made via a web interface. When making the certificate request, the applicant must submit a proposed distinguished name in accordance with local naming conventions, generate the public/private key pair using FIPS 140-2 Level 1 approved software or Level 2 hardware tokens, and submit the information and the public key to the CA for disposition. For id-fpki-common-devicesHardware a FIPS 140-2 Level 2 or higher cryptographic module must be used to generate the public/private key pair.

The applicant must protect the private key with a password. This password must be kept confidential and is not to be recorded or given to any other parties.

In the case of id-fpki-common-policy and if-fpki-common-devices certificates, the applicant makes the request electronically using a web browser incorporating a FIPS 140-2 Level 1 cryptographic module for generating the key pair and submitting the required information through an online form. The following instructions explain the steps necessary for an applicant to apply for a certificate:

* Connect to the WidePoint SSP web page and follow the directions filling out the electronic and printed forms.
* Present the printed application and two photo IDs to an RA, LRA, or Notaries Public (or a person legally empowered to witness and certify the validity of documents and to take affidavits and depositions).

Upon notification of certificate issuance by e-mail, the certificate is accepted and retrieved.

If at any time “out-of-band” communications become necessary for communication with subscribers/applicants, WidePoint will protect the confidentiality and integrity of the data by sealing all data and only sending via trusted carriers (e.g. U.S. Postal Service, FedEx, UPS).

#### SSP/PIV Workstation Certificate Enrollment

WidePoint SSP certificate requests for id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-cardAuth, begin with an agency/organization PIV Sponsor process prior to the enrollment process. The PIV Sponsor receives notification from an authorized agency/organization official to add an applicant to the agency’s/organization’s PIV site. The PIV Sponsor then creates an applicant record in the site from employment information (e.g. from the agency/organization HR, Personnel, or Security). Once the applicant’s record has been added to the site, the PIV Sponsor notifies the PIV Registrar that an applicant has been added to the site and is ready for enrollment.

The enrollment process requires the applicant to meet in-person with the PIV Registrar at the designated PIV workstation. The PIV Registrar activates the workstation site using their PIV Registrar PIV token. The PIV Registrar then reviews the applicant’s identity documents (checking expiration dates and that names match) and ensures the identity documents match the information previously entered by the PIV Sponsor. Upon confirmation of matching identity documents, the PIV Registrar captures the biometrics (fingerprints and facial image). Next, the PIV Registrar enters the applicant’s hair color, eye color, gender, height, weight, and race into the site. The PIV Registrar then confirms the applicant’s NACI status and either sets the status to “approved” in the system or “waiting for response” and selects “Card Issuance Approved”.

#### Derived Certificate Enrollment

For id-fpki-common-derived-pivAuth, the Subscriber presents id-fpki-common-authentication to the Derived Credential Enrollment (DCE) site using her PIV Card. The site challenges the Subscriber for her PIN in order to access the PIV Authentication certificate on the card. Upon receipt of the correct PIN, the site reads the card and populates a CSR form based on the data read, and generates a QR Code. The Subscriber scans the QR code using a WidePoint Certificate on Device ® mobile app. A mobile enrollment code is generated. The Subscriber validates the CSR by entering the mobile enrollment code at the DCE site.

## Certificate Application Processing

Information in certificate applications is verified as being accurate before certificates are issued. This section describes WidePoint procedures to verify information in certificate applications.

### Performing Identification and Authentication Functions

The applicant’s identity will be established in-person. Information provided is checked to ensure its legitimacy. Federal Government-issued Photo I.D Credentials are required. The applicant’s identity must be personally verified prior to the certificate being issued. The applicant will appear personally before either:

* A WidePoint authorized RA or LRA
* A Trusted Agent approved by the WidePoint or appointed in writing by name by WidePoint
* A person certified by a State or Federal Government as being authorized to confirm identities (such as Notaries Public), that use a stamp, or seal to authenticate their identity confirmation

The WidePoint SSP RA, LRA or trusted agent will verify:

* That the applicant is a duly authorized representative of the Sponsoring Organization as an employee, partner, member, agent, or other association, in good standing.
* The Sponsoring Organization’s identity as specified in Section 3.2.3.1.

The process documentation and authentication requirements will include the following:

* Identity of the person performing the identification.
* A signed declaration by that person that he or she verified the identity of the subscriber as required by the applicable certificate policy which may be met by establishing how the applicant is known to the verifier as required by this certificate policy.
* A unique identifying number from the ID of the verifier and from the ID of the applicant.
* The date and time of the verification.
* A declaration of identity signed by the applicant using a handwritten signature. This will be performed in the presence of the person performing the identity authentication.

The applicant will personally appear before one of the required identity verifiers at any time prior to application of a WidePoint SSP CA’s signature to the applicant’s certificate. Alternatively, when private keys are delivered to subscribers via hardware tokens, the subscribers will personally appear before the WidePoint SSP RA, LRA or Trusted Agent to obtain their tokens or token activation data.



Figure -PIV Identification and Authentication Process Flow

The RA or LRA will archive a copy of all information used in the verification process. In all cases, the agency/organization records the following information:

* The Identity of the person performing the validation process
* Applicant’s name as it appears in the certificate Common Name field
* A signed declaration by the identity-verifying agent that they verified the identity of the applicant
* Method of application (i.e., online, in-person)
* The method used to authenticate the applicant’s identity, including identification type and unique number or alphanumeric identifier on the ID
* The date of verification
* A handwritten signature by the applicant in the presence of the person performing the identity verification

The following elements are present for each data element accepted for proofing, including electronic forms:

* Name of document presented for identity proofing
* Issuing authority
* Date of issuance
* Date of expiration
* All fields verified
* Source of verification (i.e., which databases used for cross-checks)
* Method of verification (i.e., online, in-person)
* Date/time of verification
* The WidePoint SSP name, including subcontractors, if any
* All associated error messages and codes
* Date/time of process completion
* Names (IDs) of WidePoint PKI processes, including subcontractors’ processes, if any.

Alternately, certificate requests may be validated and authenticated on the basis of electronically authenticated subscriber requests using a current, valid PKI signature certificate issued by a WidePoint SSP CA and associated private key. The following restrictions apply:

* The assurance level of the new certificate will be the same or lower than the certificate used as the authentication credential.
* The DN of the new certificate will be identical to the DN of the certificate used as the authentication credential.
* Information in the new certificate that could be used for authorization will be identical to that of the certificate used as the authentication credential.
* The expiration date of the new certificate will be no later than the next required in-person authentication date associated with the certificate used as the authentication credential.
* The validity period of the new certificate will not be greater than the maximum validity period requirements of the Common Policy for that particular type of certificate.
* The in-person authentication date associated with the new certificate will be no later than the in-person authentication date associated with the certificate used for authentication.

In all cases, WidePoint may request additional information or verification if deemed necessary to confirm the requestor’s identity.

#### Authentication of Device Identity Certificates

Some computing and communications devices (web servers, routers, firewalls, etc.) may be named as certificate subjects. In such cases, the device must have a human PKI Sponsor as described in Section 4.1.1.3. The PKI Sponsor is responsible for providing the WidePoint SSP approved RA’s, through an application form, correct information regarding:

* Equipment identification
* Equipment public keys
* Equipment authorizations and attributes (if any are to be included in the certificate)
* Contact information to enable the WidePoint to communicate with the PKI sponsor when required

A WidePoint SSP RA will authenticate the validity of any authorizations to be asserted in the certificate, and will verify source and integrity of the data collected to an assurance level commensurate with the certificate level being requested. Authentication and integrity checking is accomplished by one of the following methods:

* Verification of digitally signed messages sent from PKI sponsors (using certificates of equivalent or greater assurance than that being requested).
* In person registration by the PKI Sponsor, with the identity of the PKI Sponsor confirmed in accordance with the requirements of Section 4.1.1.3.

#### Derived PIV Certificates

For id-fpki-common-derived-pivAuth, a WidePoint RA accesses the DCE site using a certificate of equal or greater assurance than the certificate to be issued to the Subscriber. This RA validates the information provided as described in section 3.2.3.3, “Authentication of Derived PIV Credentials”.

### Approval or Rejection of Certificate Applications

Upon successful completion of the subscriber identification and authentication process, WidePoint creates the requested SSP Certificate, notifies the applicant thereof, and makes the SSP Certificate available to the applicant. If the applicant provided an e-mail address, WidePoint sends the notification message via e-mail. If no e-mail address was provided, WidePoint sends the notification to the U.S. postal address provided.

If verification is not successful or the application is otherwise rejected, WidePoint notifies the applicant of the verification failure or rejection via an out-of-band notification process linked to the certificate applicant’s physical postal address. This notification includes the steps required by the applicant to resume processing of the certificate request.

### Time to Process Certificate Applications

The entire process from applicant appearing before one of the required identity verifiers to certificate issuance will take no more than 30 days.

## Certificate Issuance

### CA Actions During Certificate Issuance

For issuance of id-fpki-common-authentication and id-fpki-common-cardAuth certificates, interaction with the CA at the time of certificate issuance is conducted by the RA (PIV Issuer) using his/her RA (PIV Issuer) PIV card to authenticate to the PIV card issuing station, as shown in Figure 1, below . The PIV card issuing station authenticates to the CA via the Certificate Management Server, which securely connects to the CA. Upon receiving the approval from the PIV Registrar, who has conducted in-person identity verification in accordance with section 3.2.1.3, the RA (PIV Issuer) will:

* Verify the identity of the applicant via in-person identity-proofing and verify the integrity of the information in the certificate request,
* Print the PIV card

The applicant, via the PIV card issuing/activation station, will then activate the PIV card via biometric 1:1 authentication, which was captured during registration. The applicant generates a PIN for the PIV card. A request is then generated to the CA to build and sign a certificate, if all certificate requirements have been met. Once the certificates have been written to the PIV card, the applicant, now a Subscriber, formally acknowledges their obligations as described in section 9.6.3, via the PIV card issuing station using his/her PIV card and associated PIN.



Figure -PIV Card Issuance Process

For id-fpki-common-devices, Id-fpki-common-devicesHardware, id-fpki-common-piv-contentSigning,id-fpki-common-derived-pivAuth, id-fpki-common-derived-pivAuth-hardware, upon successful completion of the subscriber identification and authentication process in accordance with section 3.2.3, Authentication of Individual Identity, of this CPS, WidePoint creates the requested certificate, notifies the applicant thereof, and, after ensuring that the Subscriber has formally acknowledged his/her obligations in accordance with section 9.6.3, Subscriber Representations and Warranties, makes the certificate available to the applicant.

For id-fpki-common-derived-pivAuth, a WidePoint RA issues the certificate by clicking on a button at the Derived Credential Enrollment (DCE) site.

WidePoint SSP does not accept or allow for additional authorization or attribute information from Applicants for inclusion in certificates.

### Notification to Subscriber by the CA of Issuance of Certificate

If the applicant provided an e-mail address, WidePoint sends the notification message via e-mail. If no e-mail address was provided, WidePoint sends the notification to the U.S. postal address provided.

The notification informs the applicant of the creation of a certificate, states a URL for use by the applicant for retrieving the certificate, contain a unique serial number, and reaffirms the subscriber’s responsibilities as explained in the application process. For device certificates, the notification is sent to the human PKI Sponsor associated with the device certificate. The notification also obligates the subscriber to:

* Accurately represent themselves in all communications with the WidePoint PKI.
* Protect the private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures.
* Notify WidePoint, in a timely manner, of the suspicion that his or her private key(s) is compromised or lost. Such notification through mechanisms consistent with this CPS.
* Abide by all the terms, conditions, and restrictions levied upon the use of his or her private key(s) and certificate(s).

Upon issuance of an SSP Certificate, WidePoint warrants to all program participants that:

* WidePoint has issued, and manages, the SSP Certificate in accordance with the requirements in this CPS.
* WidePoint has complied with all requirements in this CPS when identifying the subscriber and issuing the SSP Certificate.
* There are no misrepresentations of fact in the SSP Certificate known to WidePoint and that WidePoint has verified the information in the SSP Certificate.
* Information provided by the subscriber for inclusion in the SSP Certificate has been accurately transcribed to the SSP Certificate.
* The SSP Certificate meets the material requirements of this CPS.

For id-fpki-common-derived-pivAuth, e-mail notification is sent from the DCE site.

## Certificate Acceptance

As described in this CPS, a condition to issuing an SSP Certificate is that the subscriber will indicate acceptance or rejection of the WidePoint SSP Certificate to WidePoint and acknowledge the subscriber obligations. By accepting the WidePoint SSP Certificate, the subscriber is warranting that all information and representations made by the subscriber that are included in the WidePoint SSP Certificate are true.

WidePoint notifies the certificate applicant of certificate issuance through e-mail. The notification includes the URL that the applicant uses to receive the approved certificate. WidePoint verifies possession of the subscriber’s private key at the time the applicant accepts the issued certificate.

The notification informs the subscriber of the creation of the certificate, contents of the certificate and reaffirms the subscriber’s responsibilities as explained in the application process. The notification informs the subscriber if the private key has been escrowed.

The subscriber agreement includes the following subscriber obligations. The subscriber will:

* Accurately represent themselves in all communications with the WidePoint.
* Protect their private keys at all times, in accordance with this policy, as stipulated in their certificate acceptance agreements, and local procedures.
* Notify WidePoint, in a timely manner, of the suspicion that their private keys are compromised or lost. Such notification will be made directly or indirectly through mechanisms consistent with this CPS.
* Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.
* Formally accept the certificate at the designated WidePoint web page during certificate retrieval. (Failure to do so will result in revocation of the certificate.)

The subscriber has already agreed to the obligations during the request phase (as stipulated in the Subscriber Agreement), and the certificate can only be accepted during a Proof of Possession (POP) of private key test. WidePoint logs the acceptance of the certificate.

A subscriber who does not provide this verification notice within 30 calendar days of receiving notification that his or her approved certificate is available for downloading, or who is found to have acted in a manner counter to these obligations will have his or her certificate revoked, and will forfeit all claims he or she may have against the WidePoint SSP PKI in the event of a dispute arising from the failure to fulfill the obligations above.

### Conduct Constituting Certificate Acceptance

The subscriber is in possession and control of the private key from time of generation or benign transfer. The WidePoint SSP CAs authenticate the subscriber with a POP test when requesting and retrieving a certificate by requiring the subscriber to perform a private key operation and verifying that the public key presented by the subscriber matches the private key. WidePoint supports multiple enrollment protocols which support POP including: KEYGEN/SPAC, CRMF/CMMF, PKCS #10 and CMC.

To affect POP the CA supplies a random challenge string to the browser as part of the KEYGEN tag. The public key generated by the browser and the challenge string supplied by the CA are DER (Distinguished Encoding Rules) encoded together, and the resulting PublicKeyAndChallenge value is then digitally signed with the private key to produce a SignedPublicKeyAndChallenge value. This signed value is then base 64 encoded and sent to the CA as part of the certificate request; the CA verifies the signature using the included public key, thus proving possession by the browser of the private key corresponding to that public key.

The public key and challenge strings are DER encoded as PublicKeyAndChallenge and then digitally signed with the private key to produce a SignedPublicKeyAndChallenge. The SignedPublicKeyAndChallenge is base64 encoded, and the ASCII data is finally submitted to the server as the value of a name-value pair, where the name is specified by the NAME-attribute of the KEYGEN tag. When retrieving the completed certificate the browser also checks before importing the certificate into its database, to verify that the public key in the certificate being installed matches the private key it originally generated.

For id-fpki-common-derived-pivAuth, the Subscriber launches the WidePoint Certificate on Device ® mobile app and clicks on the download certificate button.

Failure to object to a properly requested certificate or its contents constitutes acceptance of the certificate.

In all cases, RAs may request additional information or verification from an RA or LRA if deemed necessary by the RA to confirm the requestor’s identity.

### Publication of the Certificate by the CA

As part of the SSP Certificate application process, the subscriber’s public key is transferred to the WidePoint SSP CAs in a way that ensures:

* It has not been changed during transit
* The sender possesses the private key that corresponds to the transferred public key
* The sender of the public key is the legitimate user claimed in the certificate application

Public keys are delivered to the certificate issuer in a PKCS#10 or Certificate Request Message Format (CRMF) certificate request.

WidePoint SSP PKI CA certificates are published to the appropriate repositories.

### Notification of Certificate Issuance by the CA to Other Entities

WidePoint will notify Federal PKI Policy Authority any time a WidePoint SSP CA issues a CA certificate to any entity outside of WidePoint.

## Key Pair and Certificate Usage

WidePoint certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all certificates and is always marked critical in order to limit the use of a public key certificate for its intended purpose, as stipulated in the X.509 Certificate and CRL Extensions Profile [CCP-PROF].

### Subscriber Private Key and Certificate Usage

Certificates asserting the id-fpki-common-authentication will include a critical key usage extension, asserting only the digitalSignature value.

#### Individual Subscriber

When requesting and using a certificate issued under this CPS, a subscriber accepts the following obligations:

* To accurately represent themselves in all communications with the PKI.
* To protect the certificate private key from unauthorized access in accordance with Section 6.2, as stipulated in their certificate acceptance agreements, and local procedures.
* To immediately report to the appropriate RA or LRA and request certificate revocation if private key compromise is suspected.
* To use the certificate only for authorized applications which have met the requirements of this CPS.
* To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension.
* To report any changes to information contained in the certificate to the appropriate RA or LRA for certificate reissue.
* Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.
* Subscribers leaving the organizations that sponsored their participation in the PKI will surrender to their organization's PKI POC (through any accountable mechanism, defined in an agency’s Registrations Practice Statement (RPS) in the case of FPFCF) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization.

These obligations are provided to the subscriber during the registration process in the form of a Subscriber Agreement that the subscriber must read and agree to prior to completing registration. Theft, compromise or misuse of the private key may cause the subscriber, relying party and their organization legal consequences.

#### Server/Component Certificate Subscriber

When requesting, renewing and using a server certificate or VPN IPSec issued under this CPS, the applicant agency or company and their PKI Sponsor accept the following obligations:

* To accurately represent themselves in all communications with the PKI and abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s).
* To protect the certificate private key from unauthorized access in accordance with Section 6.2.
* To immediately report to the appropriate RA and request certificate revocation if private key compromise is suspected.
* In the event of a PKI sponsor change, due to the verified individual having left the employ of the subscribing company or no longer being assigned as the PKI sponsor for the certificate, the applicant company must designate a new PKI sponsor and the new PKI sponsor must complete a new identity verification.
* When renewing the server certificate, the PKI sponsor must complete a new identity verification.
* Confirm that you are a current employee of the applying company and that you are authorized to obtain server certificates for the company by completing and submitting the “Proof of Organizational Affiliation” letter.
* The server designated in the certificate request is the only system on which the certificate is to be installed.
* To use the certificate only for authorized applications that has met the requirements of this CPS.
* To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension.
* To report any changes to information contained in the certificate to the appropriate RA for certificate reissue processing.

### Relying Party Public Key and Certificate Usage

This CPS is binding on each Qualified Relying Party by virtue of the relying party’s acceptance of certificates issued by WidePoint SSP as trusted, and governs its performance with respect to its application for, use of, and reliance on SSP Certificates.

WidePoint publicly posts a summary of this CPS on the WidePoint website (SSP.orc.com) to provide the relying party information regarding the expectation of the WidePoint systems. When accepting a certificate issued under this CPS, a relying party accepts the following obligations:

* Perform a risk analysis to decide whether the level of assurance provided by the certificate is adequate to protect the relying party based upon the intended use.
* To ensure that the certificate is being used for an appropriate approved purpose.
* To check for certificate revocation prior to reliance.
* To use the certificate for the purpose for which it was issued, as indicated in the certificate information (e.g., the key usage extension).
* To verify the digital signature of the WidePoint CA that issued the certificate being relied upon as stipulated in the Common Policy.
* To establish trust in the WidePoint SSP PKI by verifying the chain of CA certificates starting from a trust anchor of the relying party in accordance with the guidelines set by the X.509 Version 3 Amendment:
  + For WidePoint certificates asserting a Common Policy OID, this trust anchor is the FCPCA Self-signed CA with no additional chaining.
* To acknowledge all warranty and liability limitations.
* Preserve original signed data, the applications necessary to read and process that data, and the cryptographic applications needed to verify the digital signatures on that data for as long as it may be necessary to verify the signature on that data.
* To abide by all the terms, conditions and restrictions levied upon the use of the issued private key(s) and certificate(s) as stipulated in the Common Policy.

Data format changes associated with application upgrades may invalidate digital signatures and will be avoided.

Relying parties that do not abide by these obligations assume all risks associated with the certificates upon which they are relying.

## Certificate Renewal

WidePoint does not renew SSP certificates, and therefore does not accept requests for renewal. Any use of the term “renewal” within this CPS refers to rekeying. At the end of the life of a certificate, WidePoint provides subscribers with the ability to obtain a new certificate via rekey, with a different public key and new serial number (and, when applicable, on a new card) while retaining the rest of the subscriber’s information from the expiring certificate (e.g. name, email address, etc.). The process for rekeying a Subscriber’s certificate is described in Section 3.3.1, above. Although true renewal is not available under this CPS, WidePoint does use the term “Renewal” when interacting with Subscribers for simplification of Customer understanding.

### Circumstance for Certificate Renewal

Renewal does not apply within the WidePoint SSP PKI. See section 4.6.

### Who May Request Renewal

Renewal does not apply within the WidePoint SSP PKI. See section 4.6.

### Processing Certificate Renewal Requests

Renewal does not apply within the WidePoint SSP PKI. See section 4.6.

### Notification of New Certificate Issuance to Subscriber

Renewal does not apply within the WidePoint SSP PKI. See section 4.6.

### Conduct Constituting Acceptance of a Renewal Certificate

Renewal does not apply within the WidePoint SSP PKI. See section 4.6.

### Publication of the Renewal Certificate by the CA

Renewal does not apply within the WidePoint SSP PKI. See section 4.6.

### Notification of Certificate Issuance by the CA to Other Entities

Renewal does not apply within the WidePoint SSP PKI. See section 4.6.

## Certificate Re-Key

WidePoint SSP Certificate re-keying (signing and encryption) is accomplished through the limitation on certificate renewal, see Section 3.2.3. The minimum requirement for all SSP certificate re-keying, with the exception of CA certificates, is once every 8 years from the time of initial registration (i.e., after three 2-year renewals) Following the last renewal, the certificate must not be further re-keyed, renewed or modified. WidePoint SSP subscribers will identify themselves for the purpose of re-keying through use of their current signature key, except that identity will be established through the initial registration process described in Section 3.2.3.1.

### Circumstance for Certificate Re-key

A certificate will be re-keyed when it can no longer be renewed.

A revoked certificate will not be re-keyed.

Requirements for CA re-key are described in Section 5.6.

### Who May Request Certification of a New Public Key

The Subscriber or RA may request the re-key of a Subscriber certificate. If an applicant/subscriber’s initial valid certificate (public/private key) needs to be re-keyed, the RA will send an RA-approved re-issuance email to the RAs with comments/remarks on what needs to be modified/updated. The RA will also send an RA-approved revocation request email to the RAs with the applicant/subscriber’s initial certificate request ID#(s) for revocation. In the case of device certificates, the human PKI sponsor of the device may request certification of a new public key for the device. An RA will take the appropriate actions.

### Processing Certificate Re-keying Requests

The re-key process will be in accordance with the certificate issuance process described in Section 3.2. Identity validation may be in accordance with Section 3.3. The Subscriber or RA with a valid certificate may request the modification of a Subscriber certificate. The CA or RA will validate any changes in the subscriber authorizations reflected in the certificate. For device certificates, the human PKI Sponsor of the device may request certificate modification for the device.

### Notification of New Certificate Issuance to Subscriber

Authorized SSP CAs will notify subscribers of new SSP certificate issuance in accordance with the notification processes specified in Section 4.3.2.

### Conduct Constituting Acceptance of a Re-keyed Certificate

Conduct constituting acceptance of a re-keyed certificate will be in accordance with the processes specified in Section 4.4.1.

### Publication of the Re-keyed Certificate by the CA

When a WidePoint SSP CA private signature key is updated, and thus generates a new public key, WidePoint notifies all CAAs, RAs, LRAs, and subscribers that rely on the CA’s certificate that it has been changed.

CA and OCSP responder certificates may be renewed.

### Notification of Certificate Issuance by the CA to Other Entities

When a WidePoint SSP CA private signature key is updated, and thus generates a new public key, WidePoint notifies all CAAs, RAs, LRAs, and subscribers that rely on the CA’s certificate that it has been changed.

## Certificate Modification

Modifying a certificate means creating a new certificate that has the same or a different key, a different serial number, and differs in one or more other fields, from the old certificate. For example, the WidePoint SSP may choose to update a certificate of a Subscriber who gains an authorization. The old certificate may or may not be revoked, but must not be further re-keyed, renewed, or updated.

WidePoint will authenticate the validity of any authorizations using the same means as for the initial authorization or means of equal or greater security and assurance.

When a WidePoint SSP CA updates its private signature key and thus generates a new public key, the WidePoint SSP will obtain a new certificate from the parent CA in accordance with the requirement of Section 4.1.

### Circumstance for Certificate Modification

A WidePoint SSP CA may modify a CA or OCSP responder certificate whose characteristics have changed (e.g. assert new policy OID). The new certificate will have a different subject public key.

A WidePoint SSP certificate may be modified if some of the information other than the DN, such as the e-mail address or authorizations, has changed.

If the Subscriber’s name has changed, the Subscriber must undergo the initial registration process.

### Who May Request Certificate Modification

The Subscriber or RA with a valid certificate may request the modification of a Subscriber certificate. The CA or RA will validate any changes in the subscriber authorizations reflected in the certificate. For device certificates, the human PKI Sponsor of the device may request certificate modification.

### Processing Certificate Modification Requests

The certificate modification process will be in accordance with the certificate issuance process described in Section 3.2. Identity validation must be in accordance with this CPS. In addition, the CA or RA validates any changes in the subscriber authorizations reflected in the certificate. Proof of all subject information changes must be provided to the RA or other designated agent and verified before the modified certificate is issued. The RA exercises due diligence in validating the requested change of information and/or authorizations (e.g. applicant/subscriber’s Common Name, Affiliation, and/or email address). The RA will send an RA-approved issuance or Re-issuance email to the RAs with comments/remarks on what needs to be modified/ updated before issuance. If an individual’s name changes (e.g., due to marriage), then proof of the name change must be provided to the RA or other designated agent in order for a certificate with the new name to be issued. If the subscriber’s authorizations have decreased, the existing certificate will be revoked and the subscriber will be required to obtain a new certificate following the initial registration process of new subscribers.

### Notification of New Certificate Issuance to Subscriber

WidePoint CAs will notify subscribers of new certificate issuance in accordance with the notification processes specified in Section 4.3.2.

### Conduct Constituting Acceptance of Modified Certificate

Conduct constituting acceptance of a certificate shall be in accordance with the processes specified in Section 4.4.1.

### Publication of the Modified Certificate by the CA

WidePoint makes no stipulation regarding publication of subscriber certificates, except as noted in Section 9.4.3.

### Notification of Certificate Issuance by the CA to Other Entities

WidePoint makes not stipulation regarding notification of certificate issuance by the CA to other entities, except as noted in Section 2.2, Publication of Certification Information.

## Certificate Revocation and Suspension

Revocation requests must be authenticated. The individual making the request will either digitally sign requests for certificate revocation, or the individual will present the request in person to an RA.

WidePoint CAs operating under this CPS will issue CRLs covering all unexpired certificates issued under this CPS, except for OCSP responder certificates that include the id-pkix-ocsp-nocheck extension.

WidePoint CAs operating under this CPS will make public a description of how to obtain revocation information for the certificates WidePoint publishes, and an explanation of the consequences of using dated revocation information. This information is given to subscribers during certificate request or issuance, and is readily available to any potential relying party.

Certificate suspension for WidePoint CA certificates is not allowed.

### Circumstances for Revocation

Whenever any of the circumstances below occur, the associated certificate will be revoked and placed on the CRL, except for OCSP Responder certificates that include the id-pkix-ocsp-nocheck extension. In addition, if it is determined, subsequent to issuance of new certificates, that a private key used to sign requests for one or more additional certificates may have been compromised at the time the requests for additional certificates were made, all certificates authorized by directly or indirectly chaining back to that compromised key will be revoked. Certificates will remain on the CRL until they expire. They will be removed after they expire, but must at least appear in one CRL.

A Subscriber or a Sponsoring Organization (where applicable), is responsible for promptly requesting revocation of an WidePoint SSP certificate:

* When the private key, or the media holding the private key, associated with the WidePoint SSP Certificate is, or is suspected of having been, compromised
* When the individual named in the certificate no longer represents, or is no longer affiliated with, the Sponsoring Organization.
* If WidePoint learns, or reasonably suspects, that the subscriber’s private key has been compromised or the subscriber has failed to meet their responsibilities.
* If WidePoint determines that the WidePoint SSP Certificate was not properly issued in accordance with this CPS.
* If the certificate holder requests that the certificate be revoked.
* If the certificate holder can be shown to have violated the subscriber obligations, including payment of any required fees.
* If the certificate holder is no longer authorized to hold the certificate (e.g. termination of employment or change in responsibilities).
* If the information in the certificate is no longer accurate so that identifying information needs to be changed (e.g. change of name or privilege attributes asserted in the subscriber’s certificate are reduced).
* The subscriber’s employer or organization requests revocation.
* The certificate was obtained by fraud or mistake.
* The certificate was not correctly requested, issued or accepted.
* The certificate contains incorrect information, is defective or creates a possibility of incorrect reliance or usage.
* Certificate private key compromise is suspected.
* The certificate holder fails to make a payment or other contractual obligations related to the certificate.

WidePoint reserves the right to revoke any WidePoint SSP issued certificate at its discretion.

WidePoint provides for the revocation of certificates when requested, at any time for any reason. If the Government provided RA functions, or if WidePoint has delegated revocation functions to subcontractor RAs, all information is transmitted via a network between WidePoint and/or subcontractors and/or government RAs using mutual authentication.

### Who Can Request Revocation

WidePoint may summarily revoke certificates within WidePoint’s domain at its discretion. A written notice and brief explanation for the revocation will subsequently be provided to the subscriber. The RA can request the revocation of a subscriber’s certificate on behalf of any authorized party, as specified herein. A subscriber may request revocation of his/her/its WidePoint SSP Certificate at any time for any reason. A Sponsoring Organization may request revocation of an SSP Certificate issued to its authorized representatives (agency employees and/or contractors) at any time for any reason. If the Government provided RA functions, or if WidePoint has delegated revocation functions to subcontractor RAs, all information is transmitted via a network between WidePoint and/or subcontractors and/or government RAs using mutual authentication.

WidePoint reserves the right to revoke any WidePoint SSP-issued certificate at its discretion.

### Procedure for Revocation Request

When a revocation request with a stated reason from revocation comes from an agency designated person authorized to request revocation of certificates and is digitally or manually signed with identity credentials at least to the same assurance level as the certificate to be revoked, WidePoint will revoke the certificate immediately.

If a WidePoint CMA or RA is making the request, the reason for the revocation request is documented. If an LRA is requesting the revocation, the reason will be sent to an RA via a digitally signed e-mail message for revocation, who investigates the request, document the reason for the revocation request and archive. Upon disposition, the CMA or RA sends the reason for revocation and confirm that it was vetted to the RA via a digitally signed e-mail message for revocation.

Where subscribers use hardware tokens, revocation is optional if all the following conditions are met:

* the revocation request was not for key compromise;
* the hardware token does not permit the user to export the signature private key;
* the subscriber surrendered the token to the PKI;
* the token was zeroized or destroyed promptly upon surrender;
* the token has been protected from malicious use between surrender and zeroization or destruction.

In all other cases, revocation of the certificates is mandatory. Even where all the above conditions have been met, revocation of the associated certificates will be executed.

WidePoint will revoke the certificate by placing its serial number and identifying information on a CRL. WidePoint will also remove the certificate from any repositories containing that certificate.

The subscriber is notified of the revocation request, reason for the request, and status of the request. If appropriate, the subscriber is provided information on obtaining a new certificate and a list of all certificates issued.

If a WidePoint CMA is choosing to revoke a certificate because of sufficient evidence of noncompliance with this CPS, a WidePoint RA documents the reason for certificate revocation and notifies the subscriber of the revocation.

Subscribers leaving the organizations that sponsored their participation in the PKI will surrender to their organization’s PKI POC (through any accountable mechanism, defined in the RPS) all cryptographic hardware tokens that were issued, under the sponsoring organization, prior to leaving the organization. The PKI POC will zero (refer to Section 6.2.7) or destroy the token promptly upon surrender and will protect the token from malicious use from the time of surrender. In all cases, whether software or hardware tokens are involved, the organization will promptly notify a WidePoint RA to revoke the certificate and attest to the disposition of the token, via a digitally signed e-mail.

### Revocation Request Grace Period

Certificates are revoked upon request as soon as the need can be verified. There is no grace period. The subscriber, or sponsoring organization, must request revocation from WidePoint as soon as the need for revocation has been determined.

### Time within which CA must Process the Revocation Request

WidePoint CAs will revoke certificates as quickly as practical upon receipt of a proper revocation request. RAs receive revocation requests via email request or revocation letters on company letter head. Once an RA receives a revocation request email from an RA the revocation is conducted immediately. Revocation requests will be processed before the next CRL is published, excepting those requests received within two hours of CRL issuance. Revocation requests received within two hours of CRL issuance will be processed before the following CRL is published.

Certificates are revoked upon request as soon as the need can be verified. There is no grace period. The subscriber, or sponsoring organization, must request revocation from WidePoint as soon as the need for revocation has been determined.

### Revocation Checking Requirements for Relying Parties

WidePoint makes no stipulation regarding Relying Parties’ checking of revocation information.

Practice note: Use of revoked certificates could have damaging or catastrophic consequences. The matter of how often new revocation data should be obtained is a determination to be made by the relying party, considering the risk, responsibility, and consequences for using a certificate whose revocation status cannot be guaranteed.

### CRL Issuance Frequency

The WidePoint SSP CAs issue CRLs every 6 hours with a validity period of 48 hours. The CMS.cfg file is configured to ensure the frequency of the nextUpdate, where the parameters for 6-hour frequency and 48-hour validity are maintained. New CRLs are issued four times per day even if there are no changes or updates to be made, and certificate status information is published not later than the next scheduled update.

When a revocation request is granted for the reason of key compromise, the revocation information will be posted on the next CRL, except that, if the revocation request is made within 2 hours of the next schedule CRL, the revocation information may be posted on the very next CRL. All superseded CRLs are removed from the repository upon posting of the latest CRL.

When a CA certificate or subscriber certificate is revoked because of compromise, or suspected compromise, of a private key, a CRL is issued immediately as stipulated in Section 4.9.12.

WidePoint SSP CRLs may be obtained from:

http://wwworc.com/ssp/repository

Each CRL is published no later than the time specified in the “nextUpdate” field of the previously issued CRL for the same scope.

### Maximum Latency for CRLs

The CRL will be posted upon generation, but within no more than 4 hours after generation. Furthermore, each CRL will be published no later than the time specified in the nextUpdate field of the previously issued CRL for the same scope.

### On-line Revocation/ Status Checking Availability

WidePoint validates online and near-real-time the status (Valid, Invalid or Suspended) and signature of the SSP Certificate indicated in an SSP Certificate Validation Request message. The CA returns in the Certificate Status Response message a signed message.

The WidePoint WAN OCSP Responder (CSP) is located at: ssp<CA #>.eva.orc.com.

WidePoint supports online status checking via OCSP [RFC 6960] for end entity certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices, id-fpki-common-devicesHardware, id-fpki-common-authentication, id-fpki-common-cardAuth, id-fpki-common-piv-contentSigning, id-fpki-common-derived-pivAuth, and id-fpki-common-derived-pivAuth-hardware. Status information maintained by the OCSP server is configured to be updated and available to relying parties within 6 hours.

However, because some relying parties cannot accommodate on-line communications, WidePoint SSP CAs make CRLs available, as stated in Section 4.9.7.

### On-line Revocation Checking Requirements

Each Qualified Relying Party will validate every SSP Certificate it receives in connection with a transaction. Any self-signed OCSP responder used for verifying certificates asserting a policy OID from this CPS are required to meet the certificate profile stipulated in the X.509 Certificate and CRL Extensions Profile [CCP-PROF] (refer to sample profile below) and ensure that:

* Certificates indicated as being valid have a chain of valid certificates (valid as defined by [X.509]) linking back to a “trusted Root CA.”
* Each certificate in the certificate chain used to validate the certificate whose status is being requested is checked for revocation, such that the relying party need not check more than one responder to validate a subscriber certificate.
* Certificate status responses provide authentication and integrity services commensurate with the assurance level of the certificate being verified.
* It is made clear in the certificate status response the attributes (other than certificate subject name [e.g., citizenship, clearance authorizations, etc.]) being authenticated by the responder.
* Accurate and up-to-date CRLs, from the WidePoint CAs, are used to provide the revocation status.
* Revocation status responses provide authentication and integrity services commensurate with the assurance level of the certificate being checked.

Table 3 presents a sample OCSP Responder Self-Signed Certificate.

Table : Sample OCSP Responder Self-Signed Certificate

| **Field** | **Value** |
| --- | --- |
| Version | V3 (2) |
| Serial Number | Must be unique |
| Issuer Signature Algorithm | Sha256WithRSAEncryption { 1 2 840 113549 1 1 11} |
| Issuer Distinguished Name | cn=<Host URL | IP Address | Host Name>, ou=<OCSP Responder Name>, o=<Organization>, c=US | *optional: e=*[*admin@mail.com*](mailto:admin@mail.com)*, l=locality, s=state* | |
| Validity Period | Not more than 6 years from date of issue in Generalized Time format |
| Subject Distinguished Name | cn=<Host URL | IP Address | Host Name>, ou=<OCSP Responder Name>, o=<Organization>, c=US | *optional: e=*[*admin@mail.com*](mailto:admin@mail.com)*, l=locality, s=state* | |
| Subject Public Key Information | 2048 bit RSA key modulus, rsaEncryption {1 2 840 113549 1 1 11} |
| Issuer Unique Identifier | Not Present |
| Subject Unique Identifier | Not Present |
| Issuer’s Signature | Sha256WithRSAEncryption {1 2 840 113549 1 1 11} |
| Extensions | Not Present |

WidePoint disclaims any liability for loss due to use of any validation information relied upon by any party that does not comply with this stipulation, in accordance with this CPS.

### Other Forms of Revocation Advertisements Available

WidePoint does not make available any other methods to publicize revoked certificates.

### Special Requirements Related To Key Compromise

If a WidePoint SSP certificate is revoked because of suspicion of private key compromise, the following additional requirements apply in addition to requirements specified above.

If a WidePoint SSP CA certificate is revoked, a CRL will be issued <redacted>

WidePoint issues new CRLs <redacted>, through website posting, any relying parties that download the CRL that a certificate has been revoked because of key compromise, and the date that the suspected compromise occurred.

If the compromised certificate was an RA certificate, the RA revalidates any subscriber certificates validated after the date of the suspected compromise, and revokes any certificates not revalidated.

WidePoint uses reason codes and has the ability to transition any reason code to compromise.

### Circumstances for Suspension

At no time does WidePoint ORC suspend a CA certificate. Certificates may be suspended by a PIV Card management system as a result of a failure in the issuance process.

### Who Can Request Suspension

The PIV Card management system may request suspension as a result of a failure in the issuance process.

### Procedure for Suspension Request

The PIV Card management system submits a request for suspension to the CA.

### Limits on Suspension Period

Certificates are suspended for no more than 30 days after which they are revoked by a WidePoint SSP CAA.

## Certificate Status Services

The WidePoint Certificate Status Authority (CSA) operating under this CPS is subject to no stipulations.

### Operational Characteristics

The CSA provides OCSP responses to subscribers and is responsible for:

* Providing certificate revocation status and/or complete certification path validation (including revocation checking) to the Relying Parties upon request.
* Ensuring that the status and validation responses contain authentication and integrity services commensurate with the assurance level of the certificate being checked.

<redacted>.

### Service Availability

WidePoint makes no stipulations regarding service availability, except those detailed in Section 4.9.7 and 4.9.9.

### Optional Features

None.

## End of Subscription

WidePoint makes no stipulation regarding subscription, other than a subscription ends when the certificate expires or is revoked.

## Key Escrow and Recovery

Under no circumstances is a signature key escrowed. WidePoint does not require private key escrow for confidentiality keys. However, WidePoint recommends to EEs that they locally escrow a copy of the confidentiality private key.

For some purposes (such as data recovery), some organizations may desire key archival and key retrieval for the private component of the encryption certificate key pair. To facilitate this, WidePoint offers a key escrow and recovery capability.

CA private keys are never escrowed.

### Key Escrow and Recovery Policy and Practices

The method, procedures and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protection and destruction of the requested copy of an escrowed key are described in a Key Recovery Practice Statement (KRPS). To date, there has been no customer requirement for Key Escrow. Therefore, WidePoint does not have a KRPS in place for the SSP program. If/when a customer requirement arises for key escrow, WidePoint will develop and implement a KRPS. Escrowed keys are protected at no less than the level of security in which they were generated, delivered, and protected by the subscriber.

Under no circumstances is a subscriber signature key allowed to be held in trust by a third party.

### Session Key Encapsulation and Recovery Policy and Practices

WidePoint SSP does not support key escrow and recovery using key encapsulation techniques.

# Facility, Management, and Operational Controls

The security controls in-place for the WidePoint SSP system are commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of information within the WidePoint SSP system. This includes assuring that systems and applications used by the Government operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.

All users of WidePoint SSP, including Federal employees granted access to the SSP Program, by agreeing to adhere to this CPS, shall comply with GSA Order CIO 2100.1D.

For each system, the WidePoint CAA serves as the focal point for assuring there is adequate security within the system, including ways to prevent, detect, and recover from security problems. The responsibility for security is assigned in writing to the CAA and that individual is trained in the technology used in the system and in providing security for such technology including the management of security controls such as user identification and authentication.

## Physical Controls

WidePoint’s SSP CA equipment is dedicated to the CA function. RA workstations and RA hardware tokens are dedicated to the use of issuing certificates. LRAs use general-purpose workstations and medium hardware assurance certificates dedicated to the SSP certificate application process.

The CA, RA, Certificate Management System, and CSA equipment consists of equipment dedicated to the CA, RA, Certificate Management System, and CSA functions, and do not perform non-related functions. The equipment includes, but is not limited to, the system running the CA, RA, Certificate Management System, and CSA software, hardware cryptographic modules, and databases and directories located on the equipment. In addition, databases and directories located on the equipment are not accessible to the subscribers and Relying Parties.

Unauthorized use of CA, RA, Certificate Management System, and CSA equipment is forbidden. Physical security controls are implemented that protect the hardware and software from unauthorized use. WidePoint SSP CA equipment is protected from unauthorized access while the cryptographic module is installed and activated via multi-party control. WidePoint implements multi-level physical access controls to reduce the risk of equipment tampering even when the cryptographic module is not installed and activated. Cryptographic modules and the CA cryptographic tokens are protected against theft, loss, and unauthorized use through multi-level physical security and multi-party management.

<redacted>.

### Site Location and Construction

Redacted.

### Physical Access

Physical access to CA, RA and CSA hardware, including the firewall server, and any external cryptographic hardware tokens, is limited to those personnel performing one of the roles identified in Section 5.2. Access to any media containing CA, RA or CSA information is also physically protected and access restricted to authorized personnel.

<redacted>.

#### Physical Access for CA Equipment

<redacted>.

#### Physical Access for RA Equipment

<redacted>.

#### Physical Access for CSS Equipment

<redacted>.

### Power and Air Conditioning

<redacted>.

### Water Exposure

<redacted>.

### Fire Prevention and Protection

<redacted>.

### Media Storage

<redacted>.

### Waste Disposal

<redacted>.

### Off-Site Backup

<redacted>.

## Procedural Controls

The SSP system is controlled in accordance with National Institute of Standards and Technology (NIST) Special Publication 800-53, as well as DOD, and GSA for certification authority operations.

### Trusted Roles

A trusted role is one whose incumbent performs functions that can introduce security problems if not carried out properly, whether accidentally or maliciously. The people selected to fill these roles have proven to be diligent and trustworthy as described in the next section. The functions performed in these roles form the basis of trust in the entire PKI. WidePoint uses two approaches to increase the likelihood that these roles can be successfully carried out. The first approach is to ensure that the persons filling the roles are trustworthy and properly trained. The second is to distribute the functions of the role among several people, so that any malicious activity requires collusion.

The trusted roles are the CAA, the SA, RA, and the Certificate Status Authority Administrator. <redacted>.

#### Administrator

WidePoint refers to the role of Administrator as a Certificate Authority Administrator (CAA). Any WidePoint CAA who operates a CA that asserts a certificate policy OID defined in this document is subject to the stipulations of this CPS.

#### <redacted>Officer

WidePoint refers to the role of Officer as a Registration Authority (RA). RAs, at the discretion of the CAA, can assume the responsibility of issuing and revoking certificates. <redacted>

#### Auditor

The WidePoint Corporate Security Auditor is a distinct individual who is not in the direct reporting chain of the Information Technology or Operations departments and does not perform any additional trusted roles. <redacted>.

#### Operator

#### WidePoint refers to the Operator as the System Administrator (SA). The SA is primarily responsible for administration of the CA, RA, and CSA host computers and operating systems<redacted>Trusted Agents

In keeping with the goal of maintaining the trustworthiness of WidePoint’s SSP credentials, a separation of roles has been implemented for the operation of the WidePoint SSP card workstation(s). <redacted>

### Number of Persons Required Per Task

WidePoint implements commercially reasonable practices that ensure that one person acting alone cannot circumvent safeguards. To increase the likelihood that these roles can be successfully carried out the functions are distributed among more than one person, so that any malicious activity would require collusion. <redacted>.

### Identification and Authentication for Each Role

All persons fulfilling one of the CMA roles defined in this CPS must prove capable of identifying and authenticating themselves with two forms of picture identification.

### Roles Requiring Separation of Duties

WidePoint implements commercially reasonable practices that ensure that one person acting alone cannot circumvent safeguards. To increase the likelihood that these roles can be successfully carried out the functions of CAA, SA, and RA are distributed among more than one person, so that any malicious activity would require collusion.

<redacted>.

## Personnel Controls

### Qualifications, Experience, and Clearance Requirements

All personnel performing one of the roles identified in Section 5.2.1 are required to have a personal security investigation that has been favorably adjudicated in order to be assigned to sensitive positions. An active secret clearance is sufficient to meet this requirement. For individuals who do not have an active clearance, WidePoint requests the individual to provide references and sign a background verification disclosure and authorization and release. All personnel in a trusted role go through a background check, performed by a qualified investigator, as described in Section 5.3.2.

WidePoint <redacted>will:

* Be of unquestionable loyalty, trustworthiness, and integrity.
* Have demonstrated security consciousness and awareness in all daily activities.
* Have a strong background in information technology resource administration and technical administration in computer operations, system software, and/or application software totaling 12 months.
* Not be assigned other duties that would interfere with their <redacted>duties and responsibilities.
* Not knowingly have been previously relieved of a past assignment for reasons of negligence or non-performance of duties.
* Be U.S. citizens.
* Have demonstrated financial stability.
* Have valid personal security investigations favorably adjudicated and be assigned to sensitive positions.
* Have received proper training in the performance of roles and duties. <redacted>.

In addition, <redacted>have a technical understanding of the CA system and the responsibilities of <redacted>that system.

<redacted>will go through a thorough background check performed by a qualified investigator, including, but not limited to:

* Criminal history check that shows no misdemeanor or felony convictions.
* Civil lawsuit history checks and a social security number trace to confirm valid number.
* Personal, financial, and work/job reference checks which show that the subject of the check is competent, reliable, and trustworthy.
* Financial status check showing that the subject of the check has not committed any fraud or is otherwise financially trustworthy.
* Education verification of highest or most relevant degree.
* DMV records will demonstrate no pattern of violations.
* A residence check to demonstrate that the person is a trustworthy neighbor.

An active secret clearance is sufficient to meet this requirement. The results of these checks will not be released except as required by the Common Policy.

### Background Check Procedures

<redacted>will either hold a US security clearance or go through a thorough background check covering:

* Criminal history check that shows no misdemeanor or felony convictions.
* Civil lawsuit history checks and a social security number trace to confirm valid number.
* Personal, financial, and work/job reference checks which show that the subject of the check is competent, reliable and trustworthy.
* Financial status check showing that the subject of the check has not committed any fraud or is otherwise financially trustworthy.
* Education verification of highest or most relevant degree.
* DMV records will demonstrate no pattern of violations.
* A residence check to demonstrate that the person is a trustworthy neighbor.
* Social Security trace will show that the person has a valid social security number.

The period of investigation must cover <redacted>for each area, excepting the residence check which must cover at least the last three years. Regardless of the date of award, the highest educational degree must be verified.

An active secret clearance will be sufficient to meet this requirement. The results of these checks will not be released except as required by [Section 9.4.4](#_Responsibility_to_Protect) of the Common Policy.

A competent adjudication authority (e.g. OPM, DSS) using a process consistent with Executive Order 12968 August 1995 or equivalent will have performed adjudication of the background investigation. Re-screening is performed when required, as determined by the requirements of the initial investigation <redacted>. The WidePoint Facility Security Officer is responsible for maintaining and stewardship of clearance data.

### Training Requirements

### All personnel, and contractors located or working on-site or accessing U.S. Government IT resources receive information systems security awareness training annually. Additionally, periodic refresher training is provided to all personnel. <redacted>Retraining Frequency and Requirements

Those involved in filling trusted roles are made aware of changes in a WidePoint -authorized CA operation by way of notifications and training <redacted>.

### Job Rotation Frequency and Sequence

### <redacted>Sanctions for Unauthorized Actions

Any unauthorized actions resulting in irreparable damage to the SSP system such as compromising the private key will be prosecuted to the fullest extent of the law. The responsible individuals may be prosecuted to the maximum of extent that the law affords, both criminal and civil.

Any unauthorized actions by an RA will result in the immediate revocation of the RA certificate and the removal of that individual from the RA role. Certificates issued by that RA might also be revoked. The RA may be prosecuted for any damages caused to the WidePoint SSP system.

Any unauthorized actions by an RA or LRA will result in the immediate revocation of the RA/ LRA certificate and the removal of that individual from the RA/ LRA role. Certificates validated by that RA/ LRA might also be revoked. The RA/ LRA may be prosecuted for any damages caused to the WidePoint SSP system.

### Independent Contractor Requirements

Any company subcontracting to provide services for any CMA role with regards to the WidePoint SSP system is required to establish procedures, which are reviewed and approved by WidePoint. The subcontractor will require all employees delivering such services to be in accordance with this CPS and the Common Policy, and subject to the compliance audit requirements of this CPS.

### Documentation Supplied to Personnel

Operations and maintenance documentation is supplied to authorized individuals performing the roles of CAA and SA. Operations manuals for systems and CA administration are written and managed for each logical instance of the WidePoint SSP system and each physical instance of an WidePoint SSP system.

Documentation is provided to personnel as required for fulfilling the requirements of each role.

## Audit Logging Procedures

<redacted>

## Records Archival

<redacted>.

## Key Changeover

<redacted>.

## Compromise and Disaster Recovery

### Incident and Compromise Handling Procedures

Compromise or disaster notification and recovery procedures are employed by WidePoint to ensure a secure state. <redacted>.

### Computing Resources, Software, and/or Data are Corrupted

<redacted>CA data, <redacted>, are backed up <redacted>

### Entity (CA) Private Key Compromise Procedures

<redacted>.

### Business Continuity Capabilities after a Disaster

<redacted>.

## CA or RA Termination

* <redacted>.

# Technical Security Controls

## Key Pair Generation and Installation

### Key Pair Generation

<redacted>.

#### CA Key Pair Generation

#### WidePoint’s CA certificate-signing keys are generated in FIPS 140-2 Level 3 validated cryptographic Hardware Security Modules (HSM) <redacted>Subscriber Key Pair Generation

Subscribers are required to use a FIPS 140-2 validated cryptographic module for generation of keys. The WidePoint SSP CAs only allows compliant key pair generation. In the case of a Level 1 cryptographic module used for software generation, the WidePoint SSP CA(s) performs a browser check prior to registration to ensure compliance against a list of FIPS 140-2 Level 1 browsers and upon submitting a registration request.

For the id‑fpki-common-hardware, id-fpki-common-authentication, and id-fpki-common-cardAuth policies, subscriber keys are generated in FIPS 140 Level 2 hardware cryptographic modules and the certificates are issued on a PIV card via a GSA FIPS-201 approved Card Management System (CMS) (refer to FIPS 201 Evaluation Program Approved Product List). For id-fpki-common-derived-pivAuth-hardware, subscriber key pairs are generated in FIPS 140 Level 2 hardware cryptographic modules. Any pseudo-random numbers used for key generation material will be generated by a FIPS-approved method. Symmetric keys may be generated by means of either software or hardware mechanisms.

#### CSS Key Pair Generation

The WidePoint SSP CSS (OCSP responder) certificate signing keys will be generated in a FIPS 140-2 Level 2 (or higher) validated cryptographic HSM in accordance with FIPS 186-2 <redacted>

#### PIV Content Signing Key Pair Generation

For WidePoint SSP CMS which issues PIV Content-Signing certificates, the keys will be generated using a FIPS 140-2 (or higher) HSM for the CMS. The WidePoint SSP does not support issuance of id-fpki-common-High.

<redacted>.

### Private Key Delivery to Subscriber

The WidePoint SSP subscriber’s private key is generated directly on the subscriber’s token or in a key generator that benignly transfers the key to the subscriber’s token. The subscriber is in possession and control of the private key from the time of generation or benign transfer. WidePoint does not allow for key generation on behalf of the subscriber.

### Public Key Delivery to Certificate Issuer

* <redacted>.

Public keys are delivered to the certificate issuer in a PKCS#10 or Certificate Request Message Format (CRMF) certificate request.

### CA Public Key Delivery to Relying Parties

WidePoint supports delivery of the WidePoint SSP CA and trust anchor public keys (including the FCPCA trust anchor) via a web interface to a protected server using SSL. The public key is stored such that it is unalterable and not subject to substitution. Relying Parties must contact the help desk to receive the official certificate hashes to compare them with the certificates downloaded from the site.

In the case of the FCPCA trust anchor, information will be provided to the certificate subject through one of the following secure processes (that will be identified in the sponsoring agencies RPS):

* Government RA provides the trust anchor to the certificate subject during in person identity proofing.
* Government RA provides a hash of the trust anchor information (a.k.a., a “fingerprint”) to the certificate subject during in-person identity proofing; the certificate subject downloads the trust anchor information from the WidePoint SSP website and verifies the “fingerprint”. The WidePoint SSP website includes instructions to the certificate subject on how to verify the “fingerprint”.
* The certificate subject obtains the trust anchor information from the WidePoint SSP website (or other Government sponsored web server) and calculates the “fingerprint”. The WidePoint SSP website includes instructions to the certificate subject on how to calculate the “fingerprint”. The subject confirms the fingerprint against a value obtained through a secure independent process, such as a letter sent through first class mail from a Government RA or WidePoint RA.

### Key Sizes

WidePoint-issued Rivest, Shamir, Adleman (RSA) keys, including CA keys, <redacted> <redacted>. WidePoint does not support elliptic curve certificates.

<redacted>.

### Public Key Parameters Generation and Quality Checking

Public key parameters for use with the RSA algorithm defined in PKCS#-1 are generated and checked in accordance with PKCS#-1.

### Key Usage Purposes (as per X.509 v3 Key Usage Field)

WidePoint certifies keys for use in signing or encrypting, but not both. The use of a specific key is determined by the key usage extension. The key usage extension is included in all certificates and is always marked critical in order to limit the use of public key certificate for its intended purpose, as stipulated in the X.509 Certificate and CRL Extensions Profile [CCP-PROF].

## <redacted>Private Key Protection and Cryptographic Module Engineering Controls

### Cryptographic Module Standards and Controls

The relevant standard for cryptographic modules is Security Requirements for Cryptographic Modules [current version of FIPS140]. Cryptographic modules are validated to the FIPS 140 Level identified in this section.

Subscribers will use cryptographic modules that have been validated to meet at least the criteria specified for FIPS 140 Level 1 for all cryptographic operations. FIPS 140 Level 2 must be used to receive a Medium Hardware Assurance certificate, including PIV. WidePoint SSP Subscribers issued certificates under the hardware user’s policy (id-fpki-common-hardware or id-fpki-common-devicesHardware) or one of the hardware authentication policies (id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, or id-fpki-common-cardAuth) must use a FIPS 140 Level 2 or higher validated hardware cryptographic module for all private key operations.

<redacted>.

### Private Key (n out of m) Multi-person Control

<redacted>.

### Private Key Escrow

Under no circumstances is a WidePoint CA signature key used to sign certificates or CRLs escrowed.

Under no circumstances will a signature key be escrowed. WidePoint does not require private key escrow for confidentiality keys. However, WidePoint recommends to EEs that they locally escrow a copy of the confidentiality private key.

For some purposes (such as data recovery), some organizations may desire key archival and key retrieval for the private component of the encryption certificate key pair. To facilitate this, WidePoint offers a key escrow and recovery capability.

The method, procedures and controls which apply to the storage, request for, extraction and/or retrieval, delivery, protection and destruction of the requested copy of an escrowed key are described in the WidePoint KRPS. <redacted>.

### Private Key Backup

#### Backup of CA Private Signature Key

WidePoint may back up the CA private key on a separate cryptographic module in order to alleviate the need to re-key in the case of cryptographic module failure. At least one copy of the private signature key will be stored off-site. The backup module is an HSM that meets FIPS 140 Level 3 requirements and Level 3 key management requirements. In the event a CA private key requires back-up, the procedure is performed under the same multi-person control as the generation of the original signature key. The module is under the protection of the CAA and the SA under lock and key at all times, in accordance with this CPS. When WidePoint re-keys, the private key in the backup module is zeroed or otherwise destroyed.

#### Backup of Subscriber Private Signature Key

WidePoint recommends to users that they make backup copies of software based encryption private keys and provides recommended procedures on the SSP website. Backup of private signature keys for the sole purpose of key recovery will not be made. Backup copies must be stored in an encrypted form and protected by a password from unauthorized access. The Subscriber (PKI Sponsor for Component) is responsible for ensuring that all copies of private keys, including those that might be embedded in component backups, are protected. This includes protecting any workstation on which any of its private keys reside. Storage must ensure security controls consistent with the protection provided by the subscriber’s cryptographic module.

<redacted>.

### Private Key Archival

Under no circumstances are WidePoint SSP CA private signature keys, subscriber private signatures keys, non-repudiation signature or authentication keys archived. <redacted>.

### Private Key Transfer into or from a Cryptographic Module

<redacted>.

Private keys are generated by and in a cryptographic module. <redacted>.

### Private Key Storage on Cryptographic Module

WidePoint makes no stipulations regarding private key storage on cryptographic modules beyond that specified in FIPS 140.

### Method of Activating Private Key

A passphrase/PIN/biometric will be used to activate the private key for RA, LRA, subscriber medium assurance and medium hardware assurance (e.g. PIV). Passwords will be generated by the subscriber and entered at the time of key generation (at the RA/LRA workstation in the case of medium hardware assurance) and managed according to the FIPS 140-2 guidance for strong passwords in accordance with the subscriber obligation agreement. Entry of activation data will be protected from disclosure. <redacted>.

### Method of Deactivating Private Key

<redacted>.

### Method of Destroying Private Key

<redacted>.

### Cryptographic Module Rating

See Section 6.2.1.

## Other Aspects of Key Pair Management

### Public Key Archival

Archival of public keys is achieved via certificate archival.

### Certificate Operational Periods and Key Usage Periods

<redacted>The validity period of a WidePoint SSP end entity certificate is up to three (3) years, with a maximum of two (2) renewals before requiring re-key.

<redacted>.

### Restrictions on CA Private Key Usage

<redacted>.

Under no circumstances will the WidePoint SSP CA signature keys used to support non-repudiation services be escrowed by a third party.

## Activation Data

### Activation Data Generation and Installation

The <redacted>end entities will use passwords to protect access to private keys. <redacted>.

### Activation Data Protection

<redacted>.

### Other Aspects of Activation Data

All WidePoint CMA personnel are required to change their individual token passwords no less than once every 3 months and log this action in the audit notebook.

<redacted>.

## Computer Security Controls

<redacted>

## Life Cycle Technical Controls

### System Development Controls

Individuals filling trusted roles within the WidePoint facility use security management tools and procedures to ensure that the operational systems and networks adhere to the security requirements that check the integrity of the system data, software, discretionary access controls, audit profiles, firmware, and hardware to ensure secure operation.

Security management control includes the execution of tools and procedures to ensure that the operational system and network adhere to configured security. <redacted>.

### Security Management Controls

<redacted>.

### Object Reuse

<redacted>.

### Life Cycle Security Controls

See Section 6.6.1.

## Network Security Controls

<redacted>.

## Time-Stamping

The WidePoint SSP system provides time stamps for use in audit record generation. <redacted>.

# Certificate, CRL, and OCSP Profiles

## Certificate Profile

WidePoint SSP Certificates contain public keys used for authenticating the sender and receiver of an electronic message and verifying the integrity of such messages, i.e., public keys used for digital signature verification.

WidePoint creates and maintains SSP Certificates that conform to the ITU-T Recommendation X.509, *“The Directory: Authentication Framework,”* June 1997*.*

All WidePoint SSP Certificates include a reference to an OID for this CPS within the appropriate field, and contain the required certificate fields according to this CPS.

Complete certificate profile information, including key generation methods, for WidePoint certificates can be found in the X.509 Certificate and CRL Extensions Profile for the Common Policy [CCP-PROF] and the applicable WidePoint CA build document.

### Version Number(s)

WidePoint SSP CAs are configured to issue X.509 v3 SSP certificates (populate version field with integer 2).

### Certificate Extensions

WidePoint SSP certificate profiles are in accordance with the requirements of the certificate profiles described in the Common Policy and the applicable WidePoint CA build document. In the case of certificates issued under this CPS and asserting a Common Policy OID, profiles are in accordance with the requirements of the certificate profiles described in the X.509 Certificate and CRL Extensions Profile [CCP-PROF] and the applicable WidePoint CA build document.

Access control information may be carried in the subjectDirectoryAttributes non-critical extension. The syntax is defined in detail in [SDN702].

### Algorithm Object Identifiers

WidePoint SSP CAs are configured to issue certificates that use the following OIDs for signatures.

|  |  |
| --- | --- |
| Sha256WithRSAEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs‑1(1) 11} |

Certificates under this Policy use the following OIDs for identifying the algorithm for which the subject key was generated.

|  |  |
| --- | --- |
| rsaEncryption | {iso(1) member-body(2) us(840) rsadsi(113549) pkcs(1) pkcs-1(1) 1} |

WidePoint certifies only public keys associated with the crypto-algorithms identified above, and only uses the signature crypto-algorithms described above to sign certificates, certificate revocation lists and WidePoint’s OCSP responses.

WidePoint does not generate elliptic curve public keys or implement RSA with PSS padding.

### Name Forms

X.500 Distinguished Names (DNs) are used by all WidePoint CAs in the issuer and subject fields of the certificates, with the attribute type as further constrained by RFC 3280.

X.500 Directories use the DN for lookups. All Relying Parties will have the ability to process DNs. If communities request to use other names, for example certificates used to implement a hardware protocol, where device addresses are most useful and certificate lookup is not performed, WidePoint will define alternate name forms to be included in the subjectAltName extension and provide the alternative name form to the Policy Authority. Any name form, defining General Name [ISO9594-8] is used, in accordance with the required profile (Section 3.1).

The subject field in certificates issued under id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-authentication, id-fpki-common-derived-pivAuth-hardware, id-fpki-common-derived-pivAuth, id-fpki-common-devicesHardware, id-fpki-common-piv-contentSigning and id-fpki-common-devices is populated with an X.500 distinguished name as specified in Section 3.1.1, Types of Names.

The issuer fields of certificates are populated with a non-empty X.500 Distinguished Name as specified in Section 3.1.1, Types of Names.

The subject alternative name extension is present and includes the pivFASC-N name type in certificates issued under id-fpki-common-authentication and id-fpki-common-cardAuth.

The subject alternative name extension is present and includes a UUID, encoded as a URI, in certificates issued under id-fpi-common-authentication, id-fpki-common-cardAuth, id-fpki-common-derived-pivAuth-hardware, and id-fpki-common-derived-pivAuth.

### Name Constraints

The WidePoint SSP CAs may assert name constraints in CA certificates.

### Certificate Policy Object Identifiers

Certificates issued by the WidePoint CAs assert the OID appropriate to the level of assurance with which it was issued. Certificates issued under this CPS assert at least one of the following OIDs in the certificate policies extension, as appropriate:

id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}

id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}

id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}

id-fpki-common-devicesHardware ::= {2 16 840 1 101 3 2 1 3 36}

id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}

id-fpki-common-derived-pivAuth ::= {2 16 840 1 101 3 2 1 3 40}

id-fpki-common-derived-pivAuth-hardware ::= {2 16 840 1 101 3 2 1 3 41}

id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}

id-fpki-common-piv-contentSigning ::= {2 16 840 1 101 3 2 1 3 39}

Certificates that express the id-fpki-common-piv-contentSigning policy OID will not express any other policy OIDs.

### Usage of Policy Constraints Extension

Policy constraints may be asserted in WidePoint SSP CA certificates.

### Policy Qualifiers Syntax and Semantics

The certificates issued under this CPS will not contain policy qualifiers.

### Processing Semantics for the Critical Certificate Policies Extension

WidePoint SSP CAs are configured to not set the certificate policies extension to be critical. Relying Parties whose client software does not process this extension operate in this regard at their own risk. Processing semantics for the critical certificate policy extension used by WidePoint conforms to [CCP-PROF].

## CRL Profile

WidePoint CRL profiles addressing the use of each extension are provided in and conform to the X.509 Certificate and CRL Extensions Profile [CCP-PROF] and the applicable WidePoint CA build document.

### Version Number(s)

CRLs issued under this CPS assert a version number as described in the X.509 standard [ISO9594-8], CRLs assert Version 2.

### CRL and CRL Entry Extensions

Detailed CRL profiles covering the use of each extension are available and described in the X.509 Certificate and CRL Extensions Profile [CCP-PROF] and are in accordance with the Common Policy CRL profile. The CA supports CRL Distribution Points (CRL DP) in all EE certificates. The CRL DP is as follows:

* [http://SSP](http://aces).orc.com/CRLs/ORC<CA Name>.crl

In the case of subordinate CAs:

* [http://SSP](http://aces).orc.com/CRLs/ORC<CA Name>.crl

## OCSP Profile

Certificate status authorities (CSAs) operated under this CPS sign responses using algorithms designated for CRL signing, as shown below. OCSP requests are not required to be signed (refer to RFC6960 for detailed syntax). OCSP requests and responses contain the following formats as shown in Table 7 below.

Table : OCSP Request Format

| **Field** | **Expected Value** |
| --- | --- |
| Version | V3 (2) |
| Requester Name | Not Required |
| Request List | List of certificates – generally this should be the list of two certificates: WidePoint certificate and end entity certificate |
| Signature | Not Required |
| Extensions | Not Required |

Table 8 lists which fields are populated by a WidePoint OCSP Responder:

Table : OCSP Response Format

| **Field** | **Expected Value** |
| --- | --- |
| Response Status | Successful | Malformed Request | Internal Error | Try Later |
| Response Type | id-pkix-ocsp-basic {1 3 6 1 5 5 7 48 1 1} |
| Version | V1 (0) |
| Responder ID | Hash of Responder public key |
| Produced At | Generalized Time |
| List of Responses | Each response will contain certificate id; certificate status[[1]](#footnote-2), thisUpdate, nextUpdate[[2]](#footnote-3), |
| Extension |  |
| Nonce | Will be present if nonce extension is present in the request |
| Signature Algorithm | Sha256WithRSAEncryption {1 2 840 113549 1 1 11} |
| Signature | Present |
| Certificates | Applicable certificates issued to the OCSP Responder |

### Version Number(s)

The Certificate Status Authority operated under this CPS uses OCSP Version 1.

### OCSP Extensions

Critical OCSP extensions are not used.

# Compliance Audit and Other Assessments

WidePoint conducts an annual compliance audit, or earlier if requested, to ensure that the requirements of this CPS are being implemented and enforced. The WidePoint SSP PMA is responsible for ensuring audits are conducted for all PKI functions regardless of how or by whom the PKI components are managed and operated. No particular assessment methodology is required.

## Frequency of Audit or Assessment

The WidePoint SSP systems are periodically, but at a minimum annually, independently audited for conformance to the appropriate policies and procedures, as well as the “Compliance Audit Requirements” document. WidePoint operates primary and secondary (backup) secure data centers in conformance with FISMA and commercial practices. The WidePoint SSP systems conform to FISMA requirements, as stipulated for Moderate systems.

WidePoint has developed Certification, accreditation, and security assessment policies and procedures that are at a minimum reviewed and updated annually, in accordance with NIST SP 800-53.

Security controls are reviewed, at a minimum, annually and updated accordingly for the purpose of determining the extent to which controls are correctly implemented and operating, and meeting the system’s security needs.

The completion of the most recent security assessment is cited in the WidePoint System Security Plan.

## Identity/ Qualifications of Assessor

The auditor must demonstrate competence in the field of compliance audits, and must be thoroughly familiar with the CA’s CPS and the Common Policy. The compliance auditor must perform such compliance audits as a regular ongoing business activity. In addition to the previous requirements, the auditor must be a certified information system auditor (CISA) or IT security specialist, and a PKI subject matter specialist who can offer input regarding acceptable risks, mitigation strategies, and industry best practices.

A certified IT auditing firm (approved by the SSP PMO) audits WidePoint annually, in accordance with FISMA for compliance. WidePoint has an independent internal department that performs weekly procedures in order to attest to WidePoint compliance with this CPS. Audit and inspection is accomplished in accordance with the NIST SP 800-53.

## Assessor’s Relationship to Assessed Entity

The compliance auditor either will be a private firm that is independent from the entities (CA and RAs) being audited, or it will be sufficiently organizationally separated from those entities to provide an unbiased, independent evaluation. An example of the latter situation may be an Agency inspector general. To insure independence and objectivity, the compliance auditor may not have served in developing or maintaining the WidePoint’s CA Facility or certification practices statement. The FPKIPA will determine whether a compliance auditor meets this requirement.

The Agency PMA is responsible for identifying and engaging a qualified auditor of agency operations implementing aspects of this CPS and providing WidePoint with a copy of the audit report letter as evidence of completion of an annual audit.

WidePoint relies upon the combined efforts of an independent external IT auditor, which is an entity separate from WidePoint, and an internal audit capability that is sufficiently organizationally separated from those entities operating the CA, so as to provide an unbiased, independent evaluation. WidePoint performs internal audits of SSP CSA and RA facilities, as defined herein.

## Topics Covered by Assessment

The purpose of WidePoint SSP compliance audits is to verify that WidePoint and its recognized trusted roles comply with all the requirements of the current versions of the CP and this CPS. All aspects of the WidePoint SSP operation are subject to compliance audit inspections. Components other than WidePoint SSP CAs may be audited fully or by using a representative sample. If the auditor uses statistical sampling, all PKI components, PKI component managers and operators must be considered in the sample. The samples must vary on an annual basis.

## Actions Taken as a Result of Deficiency

When a compliance auditor finds a discrepancy between a WidePoint CMA’s operation and the stipulations of this CPS, the following actions will occur:

1. The compliance auditor will note the discrepancy.
2. The compliance auditor will notify the parties, identified in Section 8.6, of the discrepancy and determine what further notifications or actions are necessary.
3. WidePoint will propose a remedy, including expected time for completion, to the FPKIPA and each WidePoint SSP Agency PMA.

Any remedy may include permanent or temporary WidePoint SSP cessation or termination of WidePoint SSP operation to revoke a certificate issued by the CA, or take other actions deemed appropriate. However, several factors must be considered in this decision, including the severity of the discrepancy and the risks it imposes, and the disruption to the certificate using community.

Remedies will be defined by the FPKIPA and communicated to WidePoint as soon as possible to limit the risks created. The FPKIPA and WidePoint will determine a time for completion. The implementation of remedies will be coordinated between the FPKIPA-affected Agency and WidePoint, and subsequently communicated to the FPKIPA. A special audit may be required to confirm the implementation and effectiveness of the remedy.

## Communication of Results

On an annual basis, an Auditor Letter of Compliance, prepared in accordance with the FPKI Compliance Audit Requirements document, on behalf of an Agency PMA and its management, and operation of RA and/or LRA equipment and systems on-site at the Agency’s facility must be provided to WidePoint.

On an annual basis, WidePoint submits an audit compliance package to the FPKIPA. This package is prepared in accordance with the FPKI Compliance Audit Requirements document and includes an assertion from WidePoint that all PKI components have been audited – including any components that may be separately managed and operated. The report shall identify the versions of the CP and this CPS used in the assessment. Additionally, where necessary, the results will be communicated as set forth in Section 8.5 above.

Required remedies will be defined and communicated by the auditor to WidePoint as soon as possible to limit the risks created. A special audit may be required to confirm the implementation and effectiveness of the remedy.

If a CMA entity is found not to be in compliance with this CPS, or the Common Policy, WidePoint will notify the FPKIPA immediately upon completion of the audit.

# Other Business and Legal Matters

## Fees

Fees are either published on the WidePoint website or established contractually.

### Certificate Issuance or Renewal Fees

A fee per validity year, unless otherwise negotiated, is levied by WidePoint to issue Identity and Encryption certificates. A fee per year, unless otherwise negotiated, is levied by WidePoint to issue Server certificates. Likewise, a fee per each additional year, unless otherwise negotiated, is levied by WidePoint to renew a WidePoint SSP certificate. A fee per encryption certificate is levied for the escrowing of encryption keys.

A fee, unless otherwise negotiated, is levied by WidePoint for the replacement of certificates and or tokens when the subscriber’s private key has not been compromised and there are no changes to the certificate.

Fees for tokens are separate from Certificate Issuance, Renewal, and Replacement Fees.

### Certificate Access Fees

WidePoint does not impose any certificate access fees on subscribers with respect to its own SSP Certificate(s) or the status of such Certificate(s). No fee is levied by WidePoint for access to information about any certificate issued by WidePoint that is requested under a court order. WidePoint assesses a fee from subscribers and Relying Parties for recovering archived certificates.

### Revocation or Status Information Access Fees

Fees may be assessed for certificate validation services. WidePoint CSA services are priced separate from certificate issuance services, on a transaction and subscription basis.

### Fees for Other Services

No fee is levied for online access to policy information. A reasonable fee to cover media reproduction and distribution costs may be levied for a physical media copy of this policy information. A consulting fee per hour is levied for certificate support required in addition to the detailed instructions delivered with the notification of subscriber certificate issuance. This additional support includes documentation, telephone and on-site support.

### Refund Policy

Refunds may be negotiated on a case-by-case basis. As described in Section 4.4.1, the subscriber is in possession and control of the private key at the time of issuance. Once issuance has occurred, there will be no refund.

## Financial Responsibility

WidePoint does not limit the use of certificates issued by WidePoint SSP CAs under this CPS. Rather, entities, acting as relying parties, must determine what financial limits, if any, they wish to impose for certificates used to consummate a transaction.

### Insurance Coverage

WidePoint maintains reasonable levels of business insurance.

### Other Assets

Not applicable.

### Insurance or Warranty Coverage for End-Entities

Not applicable.

## Confidentiality of Business Information

CA information not requiring protection is made publicly available. Public access to WidePoint organizational information will be determined at the sole discretion of WidePoint.

### Scope of Confidential Information

WidePoint will keep the following information confidential at all times:

* Private signing and client authentication keys
* Personal or non-public information about Subscribers
* WidePoint security mechanisms

### Information not within the Scope of Confidential Information

Information deemed not within the scope of confidential information will include:

* Information included in Certificates
* WidePoint SSP CA public certificates
* Information contained in the WidePoint CPS Summary document
* Any certificate status or certificate revocation reason code

### Responsibility to Protect Confidential Information

Except as required to support the audits performed by WidePoint’s independent external auditor, confidential information will not be released to third parties unless required by law or requested by a court with jurisdiction over the WidePoint SSP CA.

## Privacy of Personal Information

Each Authorized WidePoint SSP CA that maintains an SSP system of records establishes appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to its security or integrity which could result in substantial harm, embarrassment, inconvenience, or unfairness to any individual on whom information is maintained in accordance with Title 5, U.S.C., Sec. 552a. A Privacy Impact Analysis (PIA) is conducted on the WidePoint SSP system, and a copy of the results is retained by GSA.

### Privacy Plan

WidePoint conducts a Privacy Impact Assessment for the WidePoint SSP systems, in compliance with FISMA and NIST SP 800-53. If deemed necessary, WidePoint will have a Privacy Plan to protect personally identifying information from unauthorized disclosure. WidePoint protects all Subscriber identifying information. All Subscriber identifying information will be maintained in accordance with applicable laws.

### Information Treated as Private

Information requested from individuals during the certificate issuance process other than that information which is specifically included in the certificate, is withheld from release. This information may include personal information as described in Section 3.1 and is subject to the Privacy Act. All information in the WidePoint SSP record (not repository) is handled as SBU, and access will be restricted to those with official needs. The contents of the archives maintained by WidePoint SSP CAs operating under the CP and this CPS will not be released except as required by law.

Certificate private keys are considered sensitive and access will be restricted to the certificate owner, except as stipulated with regard to escrow and/or recovery of encryption certificates. Private keys held by the WidePoint SSP will be held in strictest confidence. Under no circumstances will any private key appear unencrypted outside the WidePoint SSP hardware. Private keys held by the WidePoint SSP will be released only to a trusted authority in accordance with this CPS, or law enforcement official, in accordance with U.S. law, the Common Policy, and this CPS (see Section 2.8.2).

Audit logs and transaction records as a whole are considered sensitive and will not be made available publicly.

### Information not Deemed Private

No sensitive information will be held in certificates, as certificate information is publicly available in repositories. Information not considered sensitive includes the subscriber’s name, electronic mail address, certificate public key, and certificate validity period. However, certificates which contain the FASC-N in the subject alternative name extension will not be made publicly available, but will be held in secure repositories and only made available via LDAP/S or HTTP/S protocols.

### Responsibility to Protect Private Information

WidePoint will not disclose certificate-related information to any third party unless authorized by the FPKIMA or Agency PMA, required by law, government rule or regulation, or order of a court of competent jurisdiction. WidePoint will authenticate any request for release of information. Sensitive But Unclassified (SBU) information pertaining to the WidePoint SSP program will be securely stored at either WidePoint’s facility or WidePoint’s off-site location. This does not prevent WidePoint from disclosing the certificate and certificate status information (e.g., CRL, OCSP Requests and Responses, etc.).

### Notice and Consent to Use Private Information

The WidePoint SSP PMA or Agency PMA is not required to provide any notice or obtain the consent of the subscriber or Authorized Agency Personnel in order to release private information in accordance with other stipulations of Section 9.4. All notices will be in accordance with the applicable laws.

### Disclosure Pursuant to Judicial or Administrative Process

Sensitive data will be released to law enforcement officials only under a proper court order. The WidePoint SSP will not disclose certificate or certificate-related information to any third party unless expressly authorized by the FPKIMA or Agency PMA, required by criminal law, government rule or regulation, or order of a criminal court with jurisdiction. WidePoint will authenticate such requests prior to disclosure. External requests must be made via the subscriber’s organization, unless under court order.

### Other Information Disclosure Circumstances

None.

## Intellectual Property Rights

Unless otherwise agreed, property interests in the following security-related information materials and data are regarded as the property of the parties indicated below:

* Certificates and CRLs are the property of WidePoint. Permission is granted to reproduce and distribute certificates issued by the WidePoint SSP on a nonexclusive, royalty-free basis, provided that they are reproduced and distributed in full. CA certificates and CRLs will not be published in any publicly accessible repository or directory without the express written permission of WidePoint.
* This CPS is the sole property of Widepoint.
* Private keys are the personal property of the subscribers who rightfully use or are capable of using them (or their employer or principal), regardless of the physical medium within which they are stored and protected.
* Public keys are the personal property of subscribers (or their employer or principal), regardless of the physical medium within which they are stored and protected.
* WidePoint SSP Certificates, including WidePoint SSP public keys, are the property of WidePoint. WidePoint licenses relying parties to use such keys only in conjunction with FIPS 140-2 validated encryption modules.

Distinguished names are the property of the individuals named or their employer.

## Representations and Warranties

Agencies contracting with WidePoint for SSP services and certificates under this CPS are required to ensure that their respective Agency Policy Management Authorities perform the following:

* Review periodic compliance audits to ensure that RAs and other components operated by the agency are operating in compliance with this CPS; and
* Review name space control procedures to ensure that distinguished names are uniquely assigned within their agency.

### CA Representations and Warranties

WidePoint warrants that its procedures are implemented in accordance with this CPS, and that any issued certificates that assert the policy OIDs identified in Section 1.2, are issued in accordance with the stipulations of this CPS. WidePoint warrants that CRLs issued and keys generated by WidePoint are in conformance with this CPS.

WidePoint warrants that any RA, LRA, or designated authority will operate in accordance with the applicable sections of this CPS.

Subscriber (applicant) Agencies that authorize and employ PKI Sponsor(s), CSAA(s), or LRA(s) warrant that:

* The PKI Sponsor(s), CSAA(s), LRA(s) procedures are implemented in accordance with the Common Policy and this CPS.
* All PKI Sponsor(s), CSAA(s), and/or LRA (sanctions are accomplished in accordance with this CPS.
* The PKI Sponsor(s), CSAA(s), and/or LRA(s) operate in accordance with the applicable sections of this CPS.
* The PKI Sponsor(s), CSAA(s), and/or LRA(s) meet the personnel and training requirements stipulated in this CPS.
* The applicant organization will cooperate and assist WidePoint in monitoring and auditing that authorized PKI Sponsor(s), CSAA(s), and/or LRA(s), are operating in accordance with the applicable sections of this CPS.
* Network security controls to the PKI Sponsor(s), CSAA(s), and/or LRA(s) equipment are in accordance with the applicable sections of this CPS.

### RA Representations and Warranties

RAs are obligated to accurately represent the information prepared for the WidePoint SSP and to process requests and responses in a timely and secure manner. RAs may designate LRAs; however, LRAs may not designate other LRAs under this CPS. An RA that performs registration functions as described in this CPS must comply with the stipulations of the CP, and comply with this CPS, which has been approved by the FPKIPA for use with the CP. RAs under this CPS are not authorized to assume any other SSP administration functions.

An RA supporting the WidePoint SSP PKI, and this CPS, is obligated to conform to the stipulations of this document, including:

* Maintaining its operations in conformance to the stipulations of this CPS.
* Including only valid and appropriate information in certificate requests, and maintaining evidence that due diligence was exercised in validating the information contained in the certificate.
* Ensuring that obligations are imposed on subscribers in accordance with Section 9.6.3, and that Subscribers are informed of the consequences of not complying with those obligations.

When validating subscriber requests for certificates issued under this CPS, an RA accepts the following obligations:

* To validate the accuracy of all information contained in the subscriber’s certificate request.
* To validate that the named subscriber actually requested the certificate.
* To verify to the RA that the certificate request originated from the named subscriber and that the information contained in the certificate request is accurate.
* To use the RA certificate only for purposes associated with the RA function.
* To use private keys only on the machines that are protected and managed using commercial best practices.
* To request revocation and verify reissue requirements of a subscriber’s certificate upon notification of changes to information contained in the certificate.
* To request revocation of the certificates of subscribers found to have acted in a manner counter to subscriber obligations.
* To inform subscribers and the RA of any changes in the RA’s status.
* To protect the RA certificate private keys from unauthorized access.
* To immediately revoke his/her own RA certificate and report to the RA if private key compromise is suspected.
* To ensure that obligations are imposed on subscribers in accordance with Section 2.1.6.
* To inform subscribers of the consequences of not complying with those obligations.

An RA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of RA responsibilities.

### Subscriber Representations and Warranties

Each subscriber (or human PKI Sponsor for device certificates) obtaining a certificate from the WidePoint SSP PKI is required to sign (either digitally sign or wet signature) a document containing the requirements he/she must meet pertaining to the protection of the private key and use of the certificate, before being issued the certificate. Wherever possible, subscriber documents will be digitally signed.

When requesting and using a certificate issued under this CPS, a subscriber (or human PKI Sponsor for device certificates) accepts the following obligations:

* To accurately represent themselves in all communications with WidePoint and the PKI.
* To protect the certificate private key from unauthorized access in accordance with Section 6.2, as stipulated in their certificate acceptance agreements, and local procedures.
* To immediately report to an RA or LRA and request certificate revocation if private key compromise is suspected.
* To use the certificate only for authorized applications which have met the requirements of the Common Policy and this CPS.
* To use the certificate only for the purpose for which it was issued, as indicated in the key usage extension.
* To use private keys only on the machines that are protected and managed using commercial best practices.
* To report any changes to information contained in the certificate to the appropriate RA or LRA for certificate reissue processing.
* Abide by all the terms, conditions, and restrictions levied upon the use of their private keys and certificates.

These obligations are provided to the subscriber during the registration process in the form of a Subscriber Agreement that the subscriber must read and agree to prior to completing registration. Theft, compromise or misuse of the private key may cause the subscriber, relying party and their organization legal consequences.

If the human PKI Sponsor for a device is not physically located near the sponsored device, and/or does not have sufficient administrative privileges on the sponsored device to protect the device’s private key and ensure that the device’s certificate is only used for authorized purposes, the device PKI Sponsor may delegate these responsibilities to an authorized administrator for the device. The delegation must be documented and signed by both the device PKI Sponsor and the authorized administrator for the device. Delegation does not relieve the device PKI Sponsor of his or her accountability for these responsibilities. In the case where a human PKI Sponsor changes, either the departing or new PKI Sponsor must notify WidePoint via digitally signed email of the change, listing the status of each certificate under his/her sponsorship.

### Relying Party Representations and Warranties

This CPS does not specify the steps which a relying party should take to determine whether to rely upon a certificate. The relying party decides, pursuant to its own policies, what steps to take. WidePoint SSP merely provides the tools (i.e., certificates and CRLs) needed to perform the trust path creation and certificate validation which the relying party may wish to employ in its determination.

### Representations and Warranties of Other Participants

#### Repository Representations and Warranties

WidePoint warrants that the WidePoint SSP procedures are implemented in accordance with this CPS and the Common Policy, and that any certificates issued that assert the policy OIDs identified in this CPS are issued in accordance with the stipulations of the Common Policy.

WidePoint warrants that WidePoint RAs or Trusted Agents operate in accordance with the applicable sections of this CPS and the Common Policy.

WidePoint posts SSP certificates and CRL information in a directory established by the WidePoint SSP. Only information contained in the certificate will be posted in this directory to ensure compliance with the Privacy Act. Access is available via Hypertext Transfer Protocol (HTTP) through a directory gateway interface. The WidePoint SSP directory sub-tree identifies the identifier ou=ORC. The WidePoint SSP directory gateway is located at:

* <https://SSP>.orc.com/dsgw/bin/csearch?context=dsgw.

The certificate repository meets the following obligations:

* To list all un-expired certificates for the WidePoint SSP to relying parties.
* To contain an accurate and current CRL for the WidePoint SSP for use by relying parties.
* To be publicly accessible through a web server gateway using HTTPS and FIPS 140-2 approved encryption.
* To be physically accessible, via certificate authenticated access control over SSL, for authorized requests coordinated with the CA point of contact during normal business hours for the operating organization.
* To be maintained in accordance with the practices specified in this CPS.
* To meet or exceed the requirement of 99% availability for all components within the control of the operating organization. NOTE: Communication failures as a result of Internet problems external to the operating organization will not count against this availability requirement.

WidePoint maintains a copy of at least all certificates and CRLs it issues and provides this information to the US Government for archiving. WidePoint provides this information on a certificate accessed web server posted no later than 10 days after the end of the collection of the data. If desired, the archive information can be delivered to the US Government on CDROM or other FPKIPA approved media.

#### LRA and Trusted Agent Representations and Warranties

LRAs and Trusted Agents will perform Subscriber identity verification in accordance with this CPS and in accordance with the Common Policy.

When validating subscriber requests for certificates issued under this CPS, an LRA accepts the following obligations:

* To validate that the named subscriber actually requested the certificate
* To use the LRA certificate only for purposes associated with the LRA function
* To request revocation and verify reissue requirements of a subscriber’s certificate upon notification of changes to information contained in the certificate
* To request revocation of the certificates of subscribers found to have acted in a manner counter to subscriber obligations
* To inform subscribers and an RA of any changes in LRA status
* To protect the LRA certificate private keys from unauthorized access
* To immediately request revocation of the LRA certificate and report to the RA if private key compromise is suspected
* To ensure that obligations are imposed on subscribers in accordance with Section 2.1.5
* To inform subscribers of the consequences of not complying with those obligations

An LRA who is found to have acted in a manner inconsistent with these obligations is subject to revocation of LRA responsibilities.

## Disclaimers of Warranties

Without limiting other subscriber obligations stated in this CPS, all subscribers are liable for any misrepresentations they make in certificates to third parties who, having verified one or more digital signatures with the certificate, reasonably rely on the representations contained therein.

WidePoint disclaims all warranties and obligations of any type other than those listed herein or in the Common Policy.

## Limitations of Liability

### Loss Limitation

WidePoint disclaims any liability for loss due to use of certificates issued by the WidePoint SSP provided that the certificate was issued in accordance with the Common Policy and this CPS and that the relying party has used validation information that complies with the Common Policy and this CPS. WidePoint acknowledges professional liability with respect to the WidePoint SSP, WidePoint CMAs, and/ or the WidePoint RAs and WidePoint LRAs.

The limit for losses per transaction due to improper actions by the WidePoint SSP or and WidePoint CMA is limited to $1,000 (U.S. Dollars). The limit for losses per incident due to improper actions by the WidePoint SSP or a WidePoint CMA is $1 million (U.S. Dollars).

### U.S. Federal Government Liability

In accordance with the Common Policy, Subscribers and Relying Parties will have no claim against the US Federal Government arising from use of the Subscriber’s certificate or an WidePoint SSP CMA determination to terminate (revoke) a certificate. In no event will the Government be liable for any losses, including direct or indirect, incidental, consequential, special, or punitive damages, arising out of or relating to any certificate issued or revoked by the WidePoint SSP under this CPS.

WidePoint will have no claim for loss against the FPKIPA, including but not limited to the revocation of the WidePoint SSP certificate.

Subscribers and Relying Parties will have no claim against the US Federal Government arising from erroneous certificate status information provided by the servers and services operated by the WidePoint SSP, CSA, and by the US Federal Government.

## Indemnities

Agents of the WidePoint SSP (e.g., RA, Trusted Agents, etc.) assume no financial responsibility for certificates improperly used.

## Term and Termination

### Term

This CPS will remain in effect until an updated WidePoint SSP CPS supplants this CPS, or the SSP PKI is terminated.

### Termination

This CPS will survive any termination of the CA. The requirements of this CPS remain in effect through the end of the archive period for the last certificate issued. Termination of the Common Policy is at the discretion of the FPKIPA.

### Effect of Termination and Survival

The responsibilities for protecting business confidential and personal information, and for protecting the Government’s intellectual property rights will survive termination of this CPS.

Intellectual property rights will survive this CPS, in accordance with the IP laws of the United States. The requirements of this CPS remain in effect through the end of the archive period for the last certificate issued.

## Individual Notices and Communications with Participants

WidePoint will use commercially reasonable methods to communicate with all parties.

## Amendments

### Procedure for Amendment

The FPKIPA will review the Common Policy at least once every year. Corrections, updates, or changes to the CP will be made publicly available either by posting a copy of the CP or a link to the CP’s location on the WidePoint website. Suggested changes to the CP will be communicated to the contact in Section 1.5.2; such communication must include a description of the change, a change justification, and contact information for the person requesting the change.

WidePoint will update this CPS is accordance with changes to the Common Policy. This redacted version of the CPS will be made available via the WidePoint website.

### Notification Mechanism and Period

WidePoint will publish information (including the currently approved CPS, with sensitive data redacted) on a web site.

### Circumstances Under Which OID Must be Changed

The policy OIDs will only change if the FPKIPA determines that a change in the CP reduces the level of assurance provided.

## Dispute Resolution Provisions

The FPKIPA will be the sole arbiter of disputes over the interpretation or applicability of the Common Policy.

With respect to Subscriber or Relying Party Agreements or Obligations made by an entity by purchasing the services associated with this CPS, disputes as to operational or policy issues will use the procedure set forth in the *Shared Service Provider Roadmap*.

## Governing Law

The laws of the United States of America will govern the enforceability, construction, interpretation, and validity of this CPS with respect to the Common Policy

## Compliance with Applicable Law

Operation of the WidePoint CA(s) is required to comply with applicable law.

## Miscellaneous Provisions

### Entire Agreement

None.

### Assignment

None.

### Severability

All contracts negotiated, for the purpose of providing WidePoint SSP services under the policy, will contain clauses that ensure continuity and stability of the WidePoint SSP operation.

Should it be determined that one section of this policy is incorrect or invalid, the other sections will remain in effect until the policy is updated. Requirements for updating this policy are described in Section 9.12. Responsibilities, requirements, and privileges of this document are transferred to the newer edition upon release of that newer edition.

### Enforcement (Attorney’s Fees and Waiver of Rights)

Failure by any person to enforce a provision of this CPS will not be deemed a waiver of future enforcement of that or any other provision.

### Force Majeure

WidePoint will not be responsible for any breach of warranty, delay, or failure in performance under this CPS that results from events beyond its control including, but not limited to, acts of God, acts of war, epidemics, power outages, fire, earthquakes, and other disasters.

## Other Provisions

None.

# Bibliography

The following documents were used in part to either directly or indirectly develop this CPS:

| **Common Name or Acronym** | **Information and Location** |
| --- | --- |
| ABADSG | Digital Signature Guidelines, 1996-08-01. <http://www>.abanet.org/scitech/ec/isc/dsgfree.html. |
| CIMC | Certificate Issuing and Management Components Family of Protection Profiles, version 1.0, October 31, 2001. |
| FIPS 140-2 | Security Requirements for Cryptographic Modules May 25, 2001. <http://csrc>.nist.gov/publications/fips/fips140-2/fips1402.pdf |
| FIPS 186-2 | Digital Signature Standard, January 27, 2000. <http://csrc>.nist.gov/publications/fips/fips186-2/fips186-2-change1.pdf |
| FIPS 201 | Personal Identity Verification (PIV) of Federal Employees and Contractors <http://csrc>.nist.gov/publications/fips/fips201-1/FIPS-201-1-chng1.pdf |
| FOIACT | 5 U.S.C. 552, Freedom of Information Act. <http://www>4.law.cornell.edu/uscode/5/552.html |
| FPKI-E | Federal PKI Version 1 Technical Specifications: Part E-X.509 Certificate and CRL Extensions Profile, 7 July 1997 <http://csrs>.nist.gov/pki/FPKI7-10.DOC |
| FPKI-Prof | Federal PKI X.509 Certificate and CRL Extensions Profile |
| ISO9594-8 | Information Technology-Open Systems Interconnection-The Directory: Authentication Framework, 1997. |
| ITMRA | 40 U.S.C. 1452, Information Technology Management Reform Act of 1996. <http://www>4.law.cornell.edu/uscode/40/1452.html |
| NAG69C | Information System Security Policy and Certification Practice Statement for Certification Authorities, rev C, November 1999. |
| NIST SP 800-73 | Interfaces for Personal Identity Verification (4 Parts) <http://csrc>.nist.gov/publications/PubsSPs.html |
| NIST SP 800-76 | Biometric Data Specification for Personal Identity Verification <http://csrc>.nist.gov/publications/nistpubs/800-76-1/SP800-76-1\_012407.pdf |
| NIST SP 800-78 | Cryptographic Algorithms and Key Sizes for Personal Identification Verification (PIV) <http://csrc>.nist.gov/publications/nistpubs/800-78-2/sp800-78-2.pdf |
| NIST SP 800-157 | Guidelines for Derived Personal Identity Verification (PIV) Credentials <http://nvlpubs>.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-157.pdf |
| NSD42 | National Policy for the Security of National Security Telecom and Information Systems, 5 Jul 1990. <http://snyside>.sunnyside.com/cpsr/privacy/computer\_security/nsd\_42.txt (redacted version) |
| NS4005 | NSTISSI 4005, Safeguarding COMSEC Facilities and Material, August 1997. |
| NS4009 | NSTISSI 4009, National Information Systems Security Glossary, January 1999. |
| PIV Profile | X.509 Certificate and Certificate Revocation List (CRL) Extensions Profile for Personal Identity Verification (PIV) Cards, Date: April 23 2010, Reference Link: <http://www>.idmanagement.gov/fpkipa/documents/pivi\_certificate\_crl\_profile.pdf |
| PKCS#12 | Personal Information Exchange Syntax Standard, April 1997. <ftp://ftp>.rsasecurity.com/pub/pkcs/pkcs-12/pkcs-12v1.pdf |
| RFC 2510 | Certificate Management Protocol, Adams and Farrell, March 1999. |
| RFC 3647 | Certificate Policy and Certification Practices Framework, Chokhani and Ford, Sabett, Merrill, and Wu, November 2003. |

# Acronyms and Abbreviations

|  |  |
| --- | --- |
| AID | Application Identifier |
| CA | Certification Authority |
| CARL | Certificate Authority Revocation List |
| CCB | Configuration Control Board |
| CMS | Card Management System |
| COMSEC | Communications Security |
| CP | Certificate Policy; also Common Policy |
| CPS | Certification Practice Statement |
| CRL | Certificate Revocation List |
| CSOR | Computer Security Object Registry |
| DOD | Department of Defense |
| DN | Distinguished Name |
| DPCI | Derived PIV Credential Issuer |
| DSA | Digital Signature Algorithm |
| DSS | Digital Signature Standard |
| ERC | Enhanced Reliability Check |
| FAR | Federal Acquisition Regulations |
| FBCA | Federal Bridge Certification Authority |
| FQDN | Fully Qualified Domain Name |
| FPCPF | U.S. Federal PKI Common Policy Framework |
| FPKI MA | Federal Public Key Infrastructure Management Authority |
| FED-STD | Federal Standard |
| FIPS PUB | (US) Federal Information Processing Standard Publication |
| FPKI | Federal Public Key Infrastructure |
| FPKI-E | Federal PKI Version 1 Technical Specifications: Part E – X.509 Certificate and CRL Extensions Profile |
| FPKISC | Federal PKI Steering Committee |
| FPKIPA | Federal PKI Policy Authority |
| GPEA | Government Paperwork Elimination Act of 1998 |
| GSA | General Services Administration |
| HTTP | HyperText Transfer Protocol |
| HSM | Hardware Security Module |
| IETF | Internet Engineering Task Force |
| ISO | International Organization for Standardization |
| ISSO | Information Systems Security Officer |
| ITU | International Telecommunications Union |
| ITU-T | International Telecommunications Union – Telecommunications Sector |
| ITU-TSS | International Telecommunications Union – Telecommunications System Sector |
| LDAP | Lightweight Directory Access Protocol |
| NII | National Information Infrastructure |
| NIST | National Institute of Standards and Technology |
| NSA | National Security Agency |
| NSTISSI | National Security Telecommunications and Information Systems Security Instruction |
| OCSP | Online Certificate Status Protocol |
| OID | Object Identifier |
| PIN | Personal Identification Number |
| PIV | Personal Identity Verification |
| PKCS | Public Key Certificate Standard |
| PKI | Public Key Infrastructure |
| PKIX | Public Key Infrastructure X.509 |
| POC | Point of Contact |
| RA | Registration Authority |
| RFC | Request For Comments |
| RSA | Rivest-Shamir-Adleman (encryption algorithm) |
| SHA-1 | Secure Hash Algorithm, Version 1 |
| S/MIME | Secure Multipurpose Internet Mail Extension |
| SNOC | Secure Network Operations Center |
| SSL | Secure Sockets Layer |
| TSDM | Trusted Software Development Methodology |
| UPN | User Principal Name |
| UPS | Uninterrupted Power Supply |
| URL | Uniform Resource Locator |
| U.S.C. | United States Code |
| UUID | Universally Unique Identifier (defined by RFC 4122) |
| WWW | World Wide Web |

# Glossary

| **Term** | **Definition** |
| --- | --- |
| Access | Ability to make use of any information system (IS) resource. [NS4009] |
| Access Control | Process of granting access to information system resources only to authorized users, programs, processes, or other systems. [NS4009] |
| Accreditation | Formal declaration by a Designated Approving Authority that an Information System is approved to operate in a particular security mode using a prescribed set of safeguards at an acceptable level of risk. [NS4009] |
| Activation Data | Private data, other than keys, that are required to access cryptographic modules (i.e., unlock private keys for signing or decryption events). |
| Affiliated Organization | Organizations that authorize affiliation with Subscribers of PIV certificates. |
| Applicant | The subscriber is sometimes also called an "applicant" after applying to a certification authority for a certificate, but before the certificate issuance procedure is completed. [ABADSG footnote 32] |
| Archive | Long-term, physically separate storage. |
| Attribute Authority | An entity, recognized by the FPKIPA or comparable Entity body as having the authority to verify the association of attributes to an identity. |
| Audit | Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures. [NS4009] |
| Audit Data | Chronological record of system activities to enable the reconstruction and examination of the sequence of events and changes in an event. [NS4009, "audit trail"] |
| Authenticate | To confirm the identity of an entity when that identity is presented. |
| Authentication | Security measure designed to establish the validity of a transmission, message, or originator, or a means of verifying an individual's authorization to receive specific categories of information. [NS4009] |
| Backup | Copy of files and programs made to facilitate recovery if necessary. [NS4009] |
| Binding | Process of associating two related elements of information. [NS4009] |
| Biometric | A physical or behavioral characteristic of a human being. |
| Certificate | A digital representation of information which at least (1) identifies the certification authority issuing it, (2) names or identifies its subscriber, (3) contains the subscriber's public key, (4) identifies its operational period, and (5) is digitally signed by the certification authority issuing it. [ABADSG]. As used in this CPS, the term “Certificate” refers to certificates that expressly reference the OID(s) of this CPS in the “Certificate Policies” field of an X.509 v.3 certificate. |
| Certification Authority (CA) | An authority trusted by one or more users to issue and manage X.509 Public Key Certificates and CARLs or CRLs. |
| Certification Authority Revocation List (CARL) | A signed, time-stamped list of serial numbers of CA public key certificates, including cross-certificates, that have been revoked. |
| CA Facility | The collection of equipment, personnel, procedures and structures that are used by a Certification Authority to perform certificate issuance and revocation. |
| Certificate Management Authority (CMA) | A Certification Authority or a Registration Authority. |
| Certification Authority Software | Key Management and cryptographic software used to manage certificates issued to subscribers. |
| Certificate Policy (CP) | A Certificate Policy is a specialized form of administrative policy tuned to electronic transactions performed during certificate management. A Certificate Policy addresses all aspects associated with the generation, production, distribution, accounting, compromise recovery and administration of digital certificates. Indirectly, a certificate policy can also govern the transactions conducted using a communications system protected by a certificate-based security system. By controlling critical certificate extensions, such policies and associated enforcement technology can support provision of the security services required by particular applications. |
| Certification Practice Statement (CPS) | A statement of the practices that a CA employs in issuing, suspending, revoking and renewing certificates and providing access to them, in accordance with specific requirements (i.e., requirements specified in this CP, or requirements specified in a contract for services). |
| Certificate-Related Information | Information, such as a subscriber's postal address, that is not included in a certificate. May be used by a CA managing certificates. |
| Certificate Revocation List (CRL) | A list maintained by a Certification Authority of the certificates that it has issued that are revoked prior to their stated expiration date. |
| Certificate Status Authority | A trusted entity that provides on-line verification to a Relying Party of a subject certificate's trustworthiness, and may also provide additional attribute information for the subject certificate. |
| Client (application) | A system entity, usually a computer process acting on behalf of a human user that makes use of a service provided by a server. |
| Common Criteria | A set of internationally accepted semantic tools and constructs for describing the security needs of customers and the security attributes of products. |
| Compromise | Disclosure of information to unauthorized persons, or a violation of the security policy of a system in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object may have occurred. [NS4009] |
| Computer Security Objects Registry (CSOR) | Computer Security Objects Registry operated by the National Institute of Standards and Technology. |
| Confidentiality | Assurance that information is not disclosed to unauthorized entities or processes. [NS4009] |
| Cross-Certificate | A certificate used to establish a trust relationship between two Certification Authorities. |
| Cryptographic Module | The set of hardware, software, firmware, or some combination thereof that implements cryptographic logic or processes, including cryptographic algorithms, and is contained within the cryptographic boundary of the module. [FIPS1401] |
| Crypto period | Time span during which each key setting remains in effect. [NS4009] |
| Data Integrity | Assurance that the data are unchanged from creation to reception. |
| Digital Signature | The result of a transformation of a message by means of a cryptographic system using keys such that a Relying Party can determine: (1) whether the transformation was created using the private key that corresponds to the public key in the signer’s digital certificate; and (2) whether the message has been altered since the transformation was made. |
| Dual Use Certificate | A certificate that is intended for use with both digital signature and data encryption services. |
| Duration | A field within a certificate which is composed of two subfields; “date of issue” and “date of next issue”. |
| E-commerce | The use of network technology (especially the internet) to buy or sell goods and services. |
| Encrypted Network | A network that is protected from outside access by NSA-approved high-grade (Type I) cryptography. Examples are SIPRNET and TOP SECRET networks. |
| Encryption Certificate | A certificate containing a public key that is used to encrypt electronic messages, files, documents, or data transmissions, or to establish or exchange a session key for these same purposes. |
| End-entity | Relying Parties and Subscribers |
| Entity | For the purposes of this document, “Entity” refers to an organization, corporation, community of interest, or government agency with operational control of a CA. |
| Entity CA | A CA that acts on behalf of an Entity, and is under the operational control of an Entity. The Entity may be an organization, corporation, or community of interest. For the Federal Government, an Entity may be any department, subordinate element of a department, or independent organizational entity that is statutorily or constitutionally recognized as being part of the Federal Government. |
| FBCA Management Authority (FPKI MA) | The Federal Public Key Infrastructure Management Authority is the organization selected by the Federal Public Key Infrastructure Policy Authority to be responsible for operating the Federal Bridge Certification Authority. |
| Federal Public Key Infrastructure Policy Authority (FPKI PA) | The FPKIPA is a federal government body responsible for setting, implementing, and administering policy decisions regarding inter-Entity PKI interoperability that uses the FBCA. |
| Firewall | Gateway that limits access between networks in accordance with local security policy. [NS4009] |
| High Assurance Guard (HAG) | An enclave boundary protection device that controls access between a local area network that an enterprise system has a requirement to protect, and an external network that is outside the control of the enterprise system, with a high degree of assurance. |
| Information System Security Officer (ISSO) | Person responsible to the designated approving authority for ensuring the security of an information system throughout its lifecycle, from design through disposal. [NS4009] |
| Inside threat | An entity with authorized access that has the potential to harm an information system through destruction, disclosure, modification of data, and/or denial of service. |
| Integrity | Protection against unauthorized modification or destruction of information. [NS4009]. A state in which information has remained unaltered from the point it was produced by a source, during transmission, storage, and eventual receipt by the destination. |
| Intellectual Property | Useful artistic, technical, and/or industrial information, knowledge or ideas that convey ownership and control of tangible or virtual usage and/or representation. |
| Intermediate CA | A CA that is subordinate to another CA, and has a CA subordinate to itself. |
| Key Escrow | A deposit of the private key of a subscriber and other pertinent information pursuant to an escrow agreement or similar contract binding upon the subscriber, the terms of which require one or more agents to hold the subscriber's private key for the benefit of the subscriber, an employer, or other party, upon provisions set forth in the agreement. [adapted from ABADSG, "Commercial key escrow service"] |
| Key Exchange | The process of exchanging public keys in order to establish secure communications. |
| Key Generation Material | Random numbers, pseudo-random numbers, and cryptographic parameters used in generating cryptographic keys. |
| Key Pair | Two mathematically related keys having the properties that (1) one key can be used to encrypt a message that can only be decrypted using the other key, and (ii) even knowing one key, it is computationally infeasible to discover the other key. |
| Local Registration Authority (LRA) | A Registration Authority with responsibility for a local community. |
| Mission Support Information | Information that is important to the support of deployed and contingency forces. |
| Mutual Authentication | Occurs when parties at both ends of a communication activity authenticate each other (see authentication). |
| Naming Authority | An organizational entity responsible for assigning distinguished names (DNs) and for assuring that each DN is meaningful and unique within its domain. |
| National Security System | Any telecommunications or information system operated by the United States Government, the function, operation, or use of which involves intelligence activities; involves cryptologic activities related to national security; involves command and control of military forces; involves equipment that is an integral part of a weapon or weapons system; or is critical to the direct fulfillment of military or intelligence missions, but does not include a system that is to be used for routine administrative and business applications (including payroll, finance, logistics, and personnel management applications). [ITMRA] |
| Non-Repudiation | Assurance that the sender is provided with proof of delivery and that the recipient is provided with proof of the sender's identity so that neither can later deny having processed the data. [NS4009] Technical non-repudiation refers to the assurance a Relying Party has that if a public key is used to validate a digital signature, that signature had to have been made by the corresponding private signature key. Legal non-repudiation refers to how well possession or control of the private signature key can be established. |
| Object Identifier (OID) | A specialized formatted number that is registered with an internationally recognized standards organization. The unique alphanumeric/numeric identifier registered under the ISO registration standard to reference a specific object or object class. In the federal government PKI they are used to uniquely identify each of the seven policies and cryptographic algorithms supported. |
| Out-of-Band | Communication between parties utilizing a means or method that differs from the current method of communication (e.g., one party uses U.S. Postal Service mail to communicate with another party where current communication is occurring online). |
| Outside Threat | An unauthorized entity from outside the domain perimeter that has the potential to harm an Information System through destruction, disclosure, modification of data, and/or denial of service. |
| Physically Isolated Network | A network that is not connected to entities or systems outside a physically controlled space. |
| PKI Sponsor | Fills the role of a Subscriber for non-human system components that are named as public key certificate subjects, and is responsible for meeting the obligations of subscribers as defined throughout this CPS. |
| Policy Management Authority (PMA) | Body established to oversee the creation and update of Certificate Policies, review Certification Practice Statements, review the results of CA audits for policy compliance, evaluate non-domain policies for acceptance within the domain, and generally oversee and manage the PKI certificate policies. For the FBCA, the PMA is the FPKIPA. |
| Principal CA | The Principal CA is a CA designated by an Entity to interoperate with the FBCA. An Entity may designate multiple Principal CAs to interoperate with the FBCA. |
| Privacy | Restricting access to Subscriber or Relying Party information in accordance with Federal law and Entity policy. |
| Private Key | (1) The key of a signature key pair used to create a digital signature. (2) The key of an encryption key pair that is used to decrypt confidential information. In both cases, this key must be kept secret. |
| Public Key | (1) The key of a signature key pair used to validate a digital signature. (2) The key of an encryption key pair that is used to encrypt confidential information. In both cases, this key is made publicly available normally in the form of a digital certificate. |
| Public Key Infrastructure (PKI) | A set of policies, processes, server platforms, software and workstations used for the purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates. |
| Registration Authority (RA) | An entity that is responsible for identification and authentication of certificate subjects, but that does not sign or issue certificates (i.e., a Registration Authority is delegated certain tasks on behalf of an authorized CA). |
| Re-key (a certificate) | To change the value of a cryptographic key that is being used in a cryptographic system application; this normally entails issuing a new certificate on the new public key. |
| Relying Party | A person or Entity who has received information that includes a certificate and a digital signature verifiable with reference to a public key listed in the certificate, and is in a position to rely on them. |
| Renew (a certificate) | The act or process of extending the validity of the data binding asserted by a public key certificate by issuing a new certificate. |
| Repository | A database containing information and data relating to certificates as specified in this CPS; may also be referred to as a directory. |
| Responsible Individual | A trustworthy person designated by a sponsoring organization to authenticate individual applicants seeking certificates on the basis of their affiliation with the sponsor. |
| Revoke a Certificate | To prematurely end the operational period of a certificate effective at a specific date and time. |
| Risk | An expectation of loss expressed as the probability that a particular threat will exploit a particular vulnerability with a particular harmful result. |
| Risk Tolerance | The level of risk an entity is willing to assume in order to achieve a potential desired result. |
| Root CA | In a hierarchical PKI, the CA whose public key serves as the most trusted datum (i.e., the beginning of trust paths) for a security domain. |
| Server | A system entity that provides a service in response to requests from clients. |
| Signature Certificate | A public key certificate that contains a public key intended for verifying digital signatures rather than encrypting data or performing any other cryptographic functions. |
| Subordinate CA | In a hierarchical PKI, a CA whose certificate signature key is certified by another CA, and whose activities are constrained by that other CA. (See superior CA). |
| Subscriber | A Subscriber is an entity that (1) is the subject named or identified in a certificate issued to that entity, (2) holds a private key that corresponds to the public key listed in the certificate, and (3) does not itself issue certificates to another party. This includes, but is not limited to, an individual or network device. |
| Superior CA | In a hierarchical PKI, a CA who has certified the certificate signature key of another CA, and who constrains the activities of that CA. (See subordinate CA). |
| System Equipment Configuration | A comprehensive accounting of all system hardware and software types and settings. |
| System High | The highest security level supported by an information system. [NS4009] |
| Technical non-repudiation | The contribution public key mechanisms to the provision of technical evidence supporting a non-repudiation security service. |
| Threat | Any circumstance or event with the potential to cause harm to an information system in the form of destruction, disclosure, adverse modification of data, and/or denial of service. [NS4009] |
| Trust List | Collection of trusted certificates used by Relying Parties to authenticate other certificates. |
| Trusted Agent | Entity authorized to act as a representative of an Entity in confirming Subscriber identification during the registration process. Trusted Agents do not have automated interfaces with Certification Authorities. |
| Trusted Certificate | A certificate that is trusted by the Relying Party on the basis of secure and authenticated delivery. The public keys included in trusted certificates are used to start certification paths. Also known as a "trust anchor". |
| Trusted Timestamp | A digitally signed assertion by a trusted authority that a specific digital object existed at a particular time. |
| Trustworthy System | Computer hardware, software and procedures that: (1) are reasonably secure from intrusion and misuse; (2) provide a reasonable level of availability, reliability, and correct operation; (3) are reasonably suited to performing their intended functions; and (4) adhere to generally accepted security procedures. |
| Two-Person Control | Continuous surveillance and control of positive control material at all times by a minimum of two authorized individuals, each capable of detecting incorrect and/or unauthorized procedures with respect to the task being performed, and each familiar with established security and safety requirements. [NS4009] |
| Update (a certificate) | The act or process by which data items bound in an existing public key certificate, especially authorizations granted to the subject, are changed by issuing a new certificate. |
| Zeroize | A method of erasing electronically stored data by altering the contents of the data storage so as to prevent the recovery of the data. [FIPS1401] |

# 

1. If the certificate is revoked, the OCSP Responder will provide revocation time and revocation reason from CRL entry and CRL entry extension. [↑](#footnote-ref-2)
2. The OCSP Responder will use thisUpdate and nextUpdate from CA CRL. [↑](#footnote-ref-3)