Privacy Office Contact Information

Please send any questions by email to gsa.privacyact@gsa.gov or by U.S. Mail to:
General Services Administration
Chief Privacy Officer
1800 F Street NW
Washington, DC 20405

Document Purpose

This document contains important details about a GSA managed System, Application, or Project (identified below by the Authorization Package name). To accomplish its mission the GSA Office it supports must, in the course of business operations, collect personally identifiable information (PII) about the people who use such products and services. PII is any information [1] that can be used to distinguish or trace an individual's identity like a name, address, or place and date of birth.

GSA uses Privacy Impact Assessments (PIAs) to explain how it collects, maintains, disseminates, uses, secures, and destroys information in ways that protect privacy. This PIA comprises sections that reflect GSA's privacy policy and program goals. The sections also align to the Fair Information Practice Principles (FIPPs), a set of eight precepts codified in the Privacy Act of 1974.[2]

[1]OMB Memorandum Preparing for and Responding to the Breach of Personally Identifiable Information (OMB M-17-12) defines PII as: "information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual." The memorandum notes that "because there are many different types of information that can be used to distinguish or trace an individual's identity, the term PII is necessarily broad."

[2] Privacy Act of 1974, 5 U.S.C. § 552a, as amended.

General Information

PIA Identifier: 410
System Name: WidePoint PKI Shared Service Provider (WPPKI SSP)
CPO Approval Date: 3/29/2023
PIA Expiration Date: 3/28/2026

Information System Security Manager (ISSM) Approval

Arpan Patel

System Owner/Program Manager Approval

Cheryl Jenkins

Chief Privacy Officer (CPO) Approval

Richard Speidel

PIA Overview

A: System, Application, or Project Name:
WidePoint PKI Shared Service Provider (WPPKI SSP)

B: System, application, or project includes information about:
WidePoint operates as a Federal Personal Identity Verification (PIV) Shared Service Provider, hereafter referred to as The WidePoint PIV SSP, for federal agencies to issue PIV credentials and digital certificates that identify individuals

and devices for use with electronic authorizations such as digital signing, smart card logon to networks, access to websites and applications as well as physical access authorizations. The WidePoint PIV SSP operates a certification authority infrastructure that issues digital certificates contained on HSPD-12 PIV credentials issued to federal agencies and their contractors. Additionally, the WidePoint PIV SSP manages the life cycle of those issued credentials and certificates to include revocation, renewal, and expiration. In order to issue digital certificates and PIV credentials that identify a human or a device digitally, identification information is collected to ensure that human or device that the certificate or credential represents is who they say they are. The WidePoint PIV SSP digital certificate credentials are utilized to provide secure authentication and trusted transactions for federal employees and contractors, and their devices (including web services and domain authentication). These credentials can be used to: - authenticate to government and organization websites - contract for the purchase of goods or services - verify the identity of electronic mail correspondents - verify the identity of web/application servers and devices - verify the identity of individuals and devices accessing data servers - verify the identity of individuals for physical access

C: For the categories listed above, how many records are there for each?
5000

D: System, application, or project includes these data elements:
* Name and other biographic, demographic or biometric information (date of birth, age, gender, race, height, fingerprints, photos);
* Contact information (address, telephone number, email address);
* Identification numbers: Social Security Number (SSN) in the case where no other identification could be provided, Driver’s license number, passport number, or other government-issued identifiers or images of documents, etc that are part of the I-9 list.

Overview:

The purpose of the systems and system components governed by this document is to facilitate issuance of public key infrastructure digital certificates and certificate life-cycle services (i.e. expiration, revocation, validation) for the programs identified in Section 1 of this document. These programs are authorized by various federal entities to issue certificates to federal employees and their contractors, department of defense contractors and commercial entities that wish to do business with federal or state and local governments., Digital certificate credentials are issued to human and device subscribers and can be used to:
Authenticate to government and organization websites;
Contract for the purchase of goods or services;
Verify the identity of electronic mail correspondents;
Verify the identity of web/application servers and devices;
Verify the identity of individuals and devices accessing data servers; and,
Verify the identity of individuals for physical access.

1.0 Purpose of Collection

1.1: What legal authority and/or agreements allow GSA to collect, maintain, use, or disseminate the information?
The WidePoint PIV SSP is approved by the Federal PKI Policy Authority to issue certificates under the Federal PKI Common Policy Framework, hereafter referred to as FPCPF see here - https://www.idmanagement.gov/topics/fpki/#certificate-policies. The WidePoint PIV SSP has been an approved provider of credentials under the FPCPF since 2007. WidePoint's most recent Memorandum of Agreement (MOA) with the Federal PKI Policy Authority can be found in APPENDIX A.

1.2: Is the information searchable by a personal identifier, for example a name or Social Security number?
Yes

1.2a: If so, what Privacy Act System of Records Notice(s) (SORN(s) applies to the information being collected?
SORN not required

1.2: System of Records Notice(s) (Legacy Text): What System of Records Notice(s) apply/applies to the information?
In accordance with Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors published August 2013, hereafter referred to as FIPS 201-2, the WidePoint PIV SSP does collect information that is personally identifiable in order to issue a PIV credential to a Federal Employee or a Contractor. The types of Personally Identifiable Information, hereafter referred to as PII, is detailed by Section 2 of FIPS 201-2, in particular Section 2.4 Biometric Data Collection for PIV Card, and Section 2.6 Chain of Trust which describes the data captured to tie an individual to the biometric data captured as described in Section 2.4. Individual agencies are responsible for creating their own System of Records Notice(s), hereafter referred to as SORNs.

1.2b: Explain why a SORN is not required.
Individual agencies are responsible for creating their own System of Records Notice(s).

1.3: Has an information collection request (ICR) been submitted to or approved by the Office of Management and Budget (OMB)?

1.3: Information Collection Request: Provide the relevant names, OMB control numbers, and expiration dates.

1.4: What is the records retention schedule for the information systems(s)? Explain how long and for what reason the information is kept.
In accordance with FPCPF Section 5.5 – Records Archival and Section 5.5.2 - Retention Period for Archive and the WidePoint PIV SSP Certification Practice Statement Section 5.5 – Records Archival and Section 5.5.2 - Retention Period for Archive, the WidePoint PIV SSP maintains collected information for 10 years and 6 months in accordance with retention requirements specified for medium levels of assurance. The WidePoint PIV SSP does not currently issue high level of assurance. In the event that the WidePoint PIV SSP is approved to issue high level of assurance credentials, the retention period would extend to 20 years in accordance with FPCPF Section 5.5. No records retention schedule has been approved by the National Archives and Records Administration for the WidePoint PIV SSP.

2.0 Openness and Transparency

2.1: Will individuals be given notice before the collection, maintenance, use or dissemination and/or sharing of personal information about them? Yes

2.1 Explain: If not, please explain.
The FPCPF Certificate Policy Section 9.4 Privacy of Personal Information and subsections along with the WidePoint PIV SSP CPS Section 9.4 Privacy of Personal Information and subsections provide public notice of what data is collected, what data is treated as private and what data is deemed not private, and how that data is to be protected. Additional notices are determined by the federal department/agency that is sponsoring the individual for a PIV Card.

3.0 Data Minimization

3.1: Why is the collection and use of the PII necessary to the project or system?
In accordance with Federal Information Processing Standard 201-2 Personal Identity Verification (PIV) of Federal Employees and Contractors, hereafter referred to as “FIPS 201-2”, the WidePoint PIV SSP does collect information that is personably identifiable in order to issue a PIV credential to a Federal Employee or a Contractor. Types of PII data is detailed in Section 2 of FIPS 201-2, in particular Section 2.4 – Biometric Data Collection for PIV Card, and Section 2.6 – Chain of Trust which describes the data captured to tie an individual to the biometric data captured as described in Section 2.4.

3.2: Will the system, application, or project create or aggregate new data about the individual?
Yes

3.2 Explained: If so, how will this data be maintained and used?
The WidePoint PIV SSP collects PII information as defined in Section 3.3 of this document and ties that information to digital certificates that are issued to PIV credentials so that PIV Credential holders may assert their identity electronically. Only Name, email address and affiliation are tied to the certificate (not SSN).

3.3 What protections exist to protect the consolidated data and prevent unauthorized access?
The WidePoint PIV SSP systems that collect PII data and issue digital certificates in accordance with the FPCPF are certified by the General Services Administration (GSA) up to FISMA-Moderate. The latest FISMA-Moderate ATO can be found in APPENDIX B of this document.

In order to protect data and prevent unauthorized access, roles are defined within the WidePoint PIV SSP CPS in Section 5.2.1 – Trusted Roles. There are 4 trusted roles:

Administrator – The WidePoint PIV SSP refers to the Administrator role as the WidePoint Certificate Authority Administrator. This role is responsible for installation, configuration and operation of the WidePoint PIV SSP

Certificate Authorities and Certificate Status Authorities.
Officer – The WidePoint PIV SSP refers to the Officer role as the WidePoint Registration Authority. This role is responsible for issuing and revoking certificates/credentials. The role may have further sub classification in terms of the issuance of PIV credentials (i.e., Registrar and Issuer).
Auditor - The Corporate Security Auditor is responsible for backing up and archiving all audit data and reviewing the audit logs recorded by WidePoint PIV SSP Certificate Authorities, Card Management Systems, Registration Authority Workstations, and Certificate Status Servers.
Operator - The WidePoint PIV SSP refers to the Operator as the WidePoint System Administrator. This role is primarily responsible for administration of WidePoint PIV SSP Certificate Authorities, Card Management Systems, Registration Authority Workstations, and Certificate Status Servers host computers and operating systems to include initial configuration, account management, network configuration and system backup and recovery among other things.

Privacy data is protected at several levels. With respect to the application and the machine running those applications, two party control is implemented. WidePoint Certificate Authority Administrators are responsible for the application that hosts the PII data – i.e. WidePoint PIV SSP Certificate Authorities, Card Management Systems, Registration Authority Workstations, and Certificate Status Servers. WidePoint System Administrators are responsible for the machine that hosts these applications. The applications and machines are physically hosted within the WidePoint Secure Network Operations Center (SNOC) in a cage that requires one WidePoint Certificate Authority Administrator and one WidePoint System Administrator in order to access the cage hosting the systems. Additionally, WidePoint System Administrators have root access privileges to the systems but do not have the ability to operate the applications. WidePoint System Administrators must grant WidePoint Certificate Authority Administrators root privileges in order for the WidePoint Certificate Authority Administrators to administer the applications of CMS, CA or CSS. All work is done under two party control.

With respect to the process of issuing PIV credentials to individual subscribers, the WidePoint Registrar role is responsible for gathering user information and vetting that information before passing that information onto the Issuer role who is responsible for the issuance of the PIV credential to the user. Issuance of a PIV credential requires both a WidePoint Registrar and WidePoint Issuer to complete. No person may act as both a WidePoint Registrar and WidePoint Issuer for the issuance of a particular PIV credential. WidePoint Registrar and WidePoint Issuers must authenticate under a secure session using their individual PIV credential to the WidePoint PIV SSP Card Management System (WidePoint PIV SSP CPS) in order perform their duties with respect to PIV credential issuance. User privacy data is restricted to authenticated access by either the WidePoint Registrar or WidePoint Issuer.

3.4 Will the system monitor the public, GSA employees, or contractors?
None

3.4 Explain: Please elaborate as needed.
No. Performance monitoring is at the operating system level. Since this is not a system that does continuous monitoring of the credentials that it issues or performs periodic re-vetting of individuals who already have credentials..

3.5 What kinds of report(s) can be produced on individuals?
Monthly reports of active PIV Credentials that show user name, email address, issuance date and expiration date, employee or contractor status are generated and submitted to customer departments/agencies. Reports are encrypted and provided to the departments/agencies through a secure portal that requires access by a designated Point of Contact within the department/agency. Only the designated Point of Contact can download the report.

3.6 Will the data included in any report(s) be de-identified?
No

3.6 Explain: If so, what process(es) will be used to aggregate or de-identify the data?

3.6 Why Not: Why will the data not be de-identified?

The WidePoint PIV SSP is a credentialing system which creates digital identities for federal employees and their contractors. Any report from the WidePoint PIV SSP will by necessity need to have identifying information. Reports which are created by the WidePoint PIV SSP are reports which identify the users who have digital identities created by the WidePoint PIV SSP.

4.0 Limits on Using and Sharing Information

4.1: Is the information in the system, application, or project limited to only the information that is needed to carry out the purpose of the collection?
Yes

4.2: Will GSA share any of the information with other individuals, federal and/or state agencies, or private-sector organizations?
None

4.2How: If so, how will GSA share the information?
PII information collected by the WidePoint PIV SSP is not shared with other individuals, Federal and/or state agencies, except those departments/agencies who are subscribers to the WidePoint PIV SSP for issuance of PIV credentials to their federal employees or contractors. Individuals may view their own PII data and, as stipulated in section 4.1.1 Who can submit a Key Recovery Application of the FPKI Key Recovery Policy (see here - https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/fpki-krp-v1.0-10-6- 2017.pdf), authorized third-party requestors (e.g. law enforcement personnel) with a court order from a competent court.

4.3: Is the information collected:
Directly from the Individual

4.3Other Source: What is the other source(s)?
Biometric PII information including fingerprints, eye and hair color, and height - is collected directly from the user during an in-person enrollment process as described in FIPS 201-2, FPCPF, and the WidePoint PIV SSP CPS. PII information of non-biometric data may be directly uploaded by the department/agency for which the individual is a federal employee or contractor.

4.4: Will the system, application, or project interact with other systems, applications, or projects, either within or outside of GSA?
No

4.4WhoHow: If so, who and how?
No. The WidePoint PIV SSP does not share data with any other systems. The WidePoint PIV SSP has no interconnection agreements. Data may only be shared as previously stipulated and in accordance with the governing documents: FIPS 201-2, FPCPF Certificate Policy, the FPKI Key Recovery Policy and the WidePoint PIV SSP CPS.

4.4Formal Agreement: Is a formal agreement(s) in place?
No

4.4NoAgreement: Why is there not a formal agreement in place?
The WidePoint PIV SSP does not share data with any other systems. The WidePoint PIV SSP has no interconnection agreements. Data may only be shared as previously stipulated and in accordance with the governing documents: FIPS 201-2, FPCPF Certificate Policy, the FPKI Key Recovery Policy and the WidePoint PIV SSP CPS.

5.0 Data Quality and Integrity

5.1: How will the information collected, maintained, used, or disseminated be verified for accuracy and completeness?
PII data collected is verified against physical documentation that is used to establish the identity of the PIV credential recipient. The biometric capture devices use algorithms to determine if the capture is a good capture and repeatable in the case of fingerprint capture.

6.0 Security

6.1a: Who or what will have access to the data in the system, application, or project?
Employees of the the WidePoint PIV SSP who have access to PII contained within the WidePoint PIV SSP are in trusted roles assigned by the WidePoint Chief Security Officer and who have undergone role-based training as outlined in the WidePoint System Security Plan, Awareness and Training Control AT-3 Role-Based Security Training. AT-3 Role-Based Training applies to WidePoint Certificate Authority Administrators who are responsible for the WidePoint PIV SSP applications, WidePoint System Administrators who are responsible for the WidePoint PIV SSP systems and operating systems, WidePoint Issuers who approve the issuance of the PIV Credential, and WidePoint Registrars who perform the vetting of the individual to receive the PIV Credential. These role assignments include review of all governing policy, practice and procedure documents.

6.1b: What is the authorization process to gain access?
Role Based users may have access to PII Data contained within the system as previously detailed in Section 3.5 of this document. For WidePoint Certificate Authority Administrators and WidePoint System Administrators that govern the operating system and the application respectively, risk is mitigated by having two-party control on all systems that contain PII data (i.e. one (1) WidePoint Certificate Authority Administrator and one (1) WidePoint System Administrator must authenticate to the system before any action can be accomplished). The WidePoint systems that collect PII data and issue digital certificates in accordance with the FPCPF are certified by the General Services Administration (GSA) up to FISMA-Moderate.

6.2: Has a System Security Plan (SSP) been completed for the Information System(s) supporting the project?
Yes

6.2a: Enter the actual or expected ATO date from the associated authorization package.
3/31/2022

6.3: How will the system or application be secured from a physical, technical, and managerial perspective?
The WidePoint systems that collect PII data and issue digital certificates in accordance with the FPCPF are certified by the General Services Administration (GSA) up to FISMA-Moderate. The latest FISMA-Moderate ATO can be found in APPENDIX B of this document. Physical and technological controls are defined in the WidePoint PIV SSP CPS Section 5 Facility, Management, and Operational Controls and Section 6 Technical Security Controls. These are further defined in the WidePoint System Security Plan through Control Family Physical and Environmental Protection all controls, Control Family System and Services Acquisition Control, in particular SA-4: Acquisition Process, Control Family Personnel Security all controls, Control Family Media Protection all controls, Control Family Maintenance all controls.

6.4: Are there mechanisms in place to identify and respond to suspected or confirmed security incidents and breaches of PII?
Yes

6.4What: What are they?
The WidePoint PIV SSP is certified at FISMA-Moderate and is audited by a third party auditor. Systems are configured to provide audit logging capabilities in compliance with the WidePoint System Security Plan Audit and Accountability Control AU-2 Type of events and collected to a Splunk system that is used to analyze operating system level logging. Systems are evaluated by Nessus and OWASP scans and internal POA&Ms in accordance with Security Assessment and Authorization Control CA-5- Plan of Action and Milestones are conducted to address any findings. Penetration tests are performed in accordance with Security Assessment and Authorization Control CA-8 Penetration Testing. Additionally, WidePoint conducts annual exercises for incident responses and is detailed in the WidePoint PIV SSP Incident Response Plan. WidePoint has also developed and conducts exercises in incident response separate from contingency planning.

7.0 Individual Participation

7.1: What opportunities do individuals have to consent or decline to provide information?

In order for federal employees and contractors to obtain PIV credentials consistent with FIPS 201-2, Federal Employees and Contractors must present PII data as specified in Section 3.2 of this document. Federal employees and contractors who decline to provide information are not eligible to receive a PIV from the WidePoint PIV SSP. Additionally, PIV Card applicants are employees or contractors of federal departments or agencies, and are governed by the policies of their respective department or agency. PIV card applicants are advised by the WidePoint PIV SSP system of the Conditions of Use for their PIV card. These conditions are spelled out below:
the PIV card is your identification for the Agency. The PIV card is the property of the department or agency, is issued by the department or agency to the cardholder only, and is non-transferable.
use of the PIV card may be revoked at the department or agency's request or by the WidePoint PIV SSP's sole discretion for violation of the department or agency's and or WidePoint PIV SSP's policies and procedures. Employees and contractors must relinquish the card upon separation from the department or agency. The department or agency must revoke the card and properly destroy.
the PIV card must be presented upon request at the time of use to obtain access or to establish official Agency status. The PIV Card is to be used only by the person to whom it is issued. Only the cardholder can present the PIV Card for access and other privileges. The PIV Card will be confiscated, certificates revoked, and card destroyed if presented by someone other than the Cardholder.
the department agency rules and regulations govern the use of the PIV card.

7.1Opt: Can they opt-in or opt-out?
No

7.1Explain: If there are no opportunities to consent, decline, opt in, or opt out, please explain.
The WidePoint PKI system issues PIV credentials, to remain compliant with HSPD-12 opting out of providing required information to obtain a PIV card is not permissible.

7.2: What are the procedures that allow individuals to access their information?
This is governed by the policies of the WidePoint PIV SSP department/agency customers. Additionally, the WidePoint PIV SSP Digital Identity Acceptance Statement under Identification and Authentication Control IA-1: Identification and Authentication Policy and Procedures defines the respective Assurance Levels of the WidePoint PIV SSP. The Identity Assurance Level for the WidePoint PIV SSP is IAL3 as the PIV Credential issuance process requires physical presence for identity proofing. The Authentication Assurance Level for the WidePoint PIV SSP is AAL2 as the PIV Credential issued through this process is a multi-factor authentication vehicle for the PIV Credential holder. The PIV Credential provides three (3) levels of authentication: Have: individual has PIV credential/certificates on that credential that uniquely identify the holder of that credential. Know: Certificates and biometric data that are stored in the secure container of the PIV credential are protected by a strong PIN. Are: Biometrics (fingerprints, photo) are stored in the secure container of the PIV credential and protected by a strong PIN. The Federation Assurance Level for the WidePoint PIV SSP is Not Applicable. The WidePoint PIV SSP requires in person vetting of individuals and does not have any Federation process to receive information about that individual during the vetting process. The WidePoint PIV SSP requires I-9 documentation from the individual prior to allowing PIV Credential issuance. The WidePoint PIV SSP does not federate any individual PII data post issuance. PII Data is maintained solely by the WidePoint PIV SSP as a means to prove that sufficient identifying information was gathered to allow for the creation of a PIV Credential to that individual.

7.3: Can individuals amend information about themselves?
Yes

7.3How: How do individuals amend information about themselves?
Individuals may amend data about themselves as stipulated in Section 2.9.2 – PIV Card Post Issuance Update Requirements of FIPS 201-3, Section 4.8 – Certificate Modification of the FPCPF CP, and Section 4.8 – Certificate Modification of the WidePoint PIV SSP CPS. They are not able to update their data without the help of an approved Issuer that has role-based access to the system. A WidePoint PIV SSP approved Issuer must act in accordance with the provisions stipulated in the listed governing documents. Amendment of information about the Subscriber may result in the issuance of a new WidePoint PIV SSP PIV credential as the underlying PII information that was collected to establish the Subscriber's identity at the time of the previous issuance has changed and the new PII data about the Subscriber shall be asserted in the new WidePoint PIV SSP PIV credential issued to the Subscriber.

8.0 Awareness and Training

8.1: Describe what privacy training is provided to users, either generally or specifically relevant to the system, application, or project.

The WidePoint PIV SSP conducts privacy and security training in accordance with the WidePoint System Security Plan, Awareness and Training Control AT-2 – Security Awareness Training which is mandatory for all employees. Employees who have access to PII contained within the WidePoint PIV SSP are in trusted roles assigned by WidePoint with executive authorization and who have undergone role-based training as outlined in the WidePoint System Security Plan, Awareness and Training Control AT-3 – Role-Based Security Training. AT-3 Role-Based Training applies to CAAs, SAs, Issuers, and Registrars. These role assignments include review of all governing policy and practice documents as previously defined.

9.0 Accountability and Auditing

9.1: How does the system owner ensure that the information is used only according to the stated practices in this PIA?

The WidePoint SSP is audited and accredited by an independent third party in accordance with the FPKIPA Certificate Policy and the WidePoint SSP Certification Practice Statement. The audits are performed on an annual basis and submitted to the FPKIPA. WidePoint has an internal Corporate Security Auditor that reviews audit log data gathered as referenced in section 6.5 of this document, and in accordance with the certificate policy which states that logs are reviewed at a minimum every 2 months. Reports are posted to an internal share and management is notified of the report and any issues that may arise from that report.