U.S. General Services Administration

FPKI Management Authority Enabling Trust

Federal Public Key Infrastructure (FPKI) Overview

Version 2.3
September 9, 2020

Table of Contents

Revision History

The following table provides the release dates and revisions of this document.

Date	Version Number	Description	Author/Editor
09/21/2015	1.0	Initial version	FPKIMA
03/15/2020	2.0	Major revision	FPKIMA
08/24/2020	2.1	Minor updates	FPKIMA
08/28/2020	2.2	Minor updates	FPKIMA
09/09/2020	2.3	Minor updates	FPKIMA

1 Introduction

The E-Government Act of 2002 led to the creation of the Federal Public Key Infrastructure (FPKI), directing the General Services Administration (GSA) to establish and operate the Federal Bridge Certification Authority (FBCA). From this pilot program, the FPKI has grown into a diverse Public Key Infrastructure (PKI) ecosystem consisting of hundreds of certification authorities (CAs) for federal and state government agencies, as well as foreign and U.S. commercial PKIs.

The purpose of this document is to aid organizations considering the FPKI, as well as existing relying parties, to take advantage of the FPKI for their logical and physical identity, credential, and access management (ICAM) requirements by providing a technical overview of the FPKI Trust Infrastructure and its PKI operations.

2 Federal Public Key Infrastructure Overview

The following sections describe how the FPKI is used, who runs the FPKI, the FPKI Trust Infrastructure, and the FPKI ecosystem.

2.1 FPKI Value

The FPKI was created to benefit the government and is used to meet federal requirements around ICAM for both federal and citizen access to federal information systems. Part of using the FPKI requires executive support to invest in the FPKI Trust Infrastructure as well as software and hardware at the department/agency (D/A) level.

PKI is an infrastructure that enables and supports the use of public key cryptography to implement scalable, strong, and secure services such as authentication, authorization, non-repudiation, confidentially, and integrity. Applications utilize PKI as an enabling and supportive security infrastructure.

The FPKI offers many benefits. The following are a couple of its key objectives:

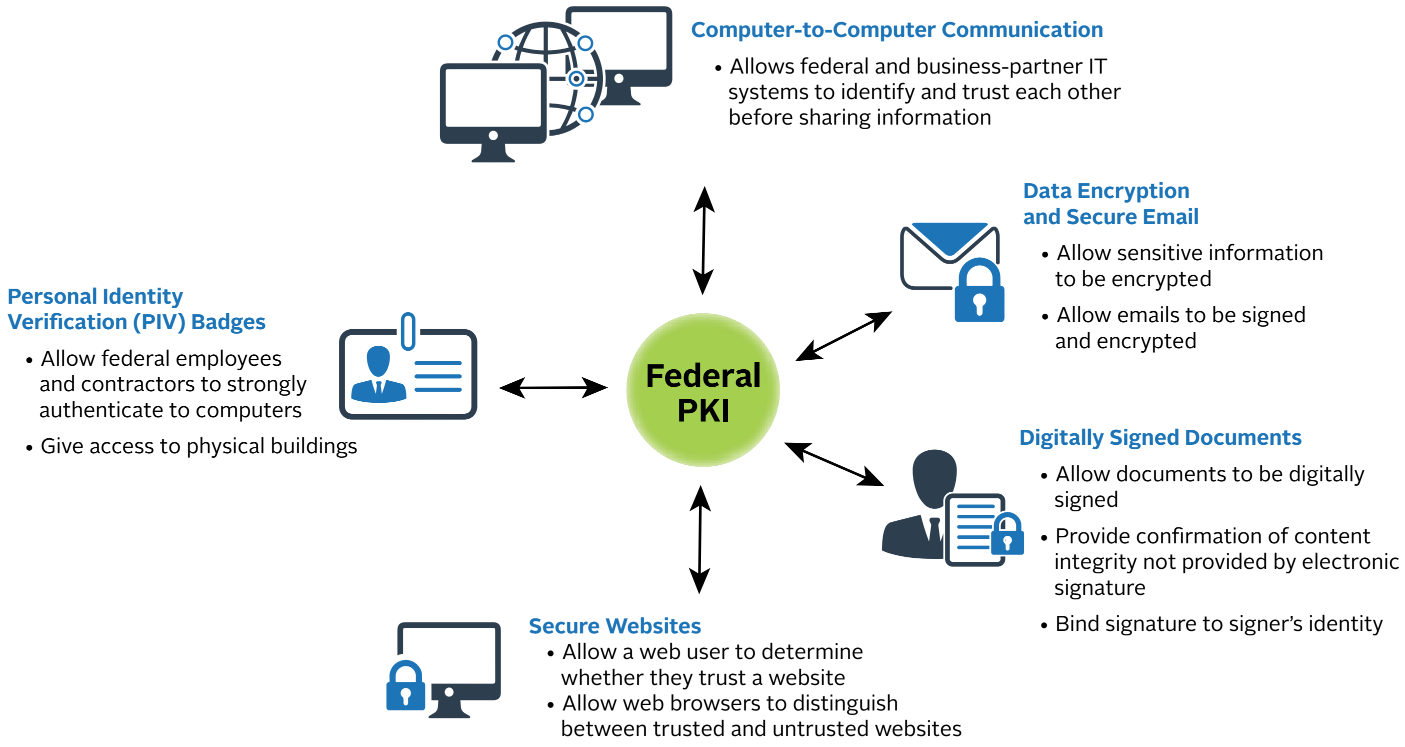
- **Increased security** reduces identity theft, weak credential (username, password) data breaches, and trust violations. PKI closes security gaps for user identification, authentication, sensitive-data encryption, and data integrity.
- **Compliance** with laws, regulations, and standards, as well as the resolution of security issues identified in GAO reports. Using the FPKI means nearly complete compliance with several executive orders, initiatives, and laws – and it can be used in contracts to ensure vendor compliance. The FPKI compliance team verifies and audits participating CAs, ensuring secure operation.

Because it meets government Federal Identity, Credentialing, and Access Management (FICAM) requirements, the FPKI can be used by federal agencies when writing contract vehicles for identity and authentication services.

- **Improved interoperability** with federal agencies and participating commercial CAs to trust PKI certificates. The FPKI is a federated trust fabric that reduces the need to issue multiple credentials.
- **Elimination of redundancy** through both PKI consolidation processes/workflows and provisioning governmentwide services. The FPKI reduces the need for multiple trust agreements and duplication of associated trust agreement tasks.

2.2 How PKI is Used in the Federal Government Today

The FPKI is critical to millions of daily tasks performed within the federal government. The figure below provides some examples.



Computer-to-Computer Communication

- Allows federal and business-partner IT systems to identify and trust each other before sharing information

Data Encryption and Secure Email

- Allow sensitive information to be encrypted
- Allow emails to be signed and encrypted

Personal Identity Verification (PIV) Badges

- Allow federal employees and contractors to strongly authenticate to computers
- Give access to physical buildings

Federal PKI

Digitally Signed Documents

- Allow documents to be digitally signed
- Provide confirmation of content integrity not provided by electronic signature
- Bind signature to signer's identity

Secure Websites

- Allow a web user to determine whether they trust a website
- Allow web browsers to distinguish between trusted and untrusted websites

Figure 1. Tasks Enabled by the FPKI

2.3 The FPKI Management Authority

The FPKI Management Authority (FPKIMA) operates Federal Common Policy and Federal Bridge CAs that enable trust in PKI credentials issued across the government and commercial partners. Managed by GSA, the FPKIMA is governed under the FPKI Policy Authority (FPKIPA) and provides the following core capabilities:

- **PKI Trust Framework** – governmentwide, interoperable PKI trust fabric for supporting the FICAM program
- **Trusted Infrastructure** – secure, high availability, 24/7 operations, and compliant with the federal government and industry
- **Efficiency** – reduces the need for individual agency PKI compliance programs to review and approve external credentials
- **Federal Shared Service** – increases federal return on investment by adding new federalwide PKI capabilities
- **Federal Alignment** – E-Government Act of 2020, HSPD-12, OMB memos (e.g., A-123, A-130), and NIST publications

2.4 The FPKI Trust Infrastructure and Participating CAs

The FPKI consists of the FPKI Trust Infrastructure and approximately 130 CAs who are root, intermediate, or issuing CAs. The figure below shows the FPKI ecosystem at a high level.

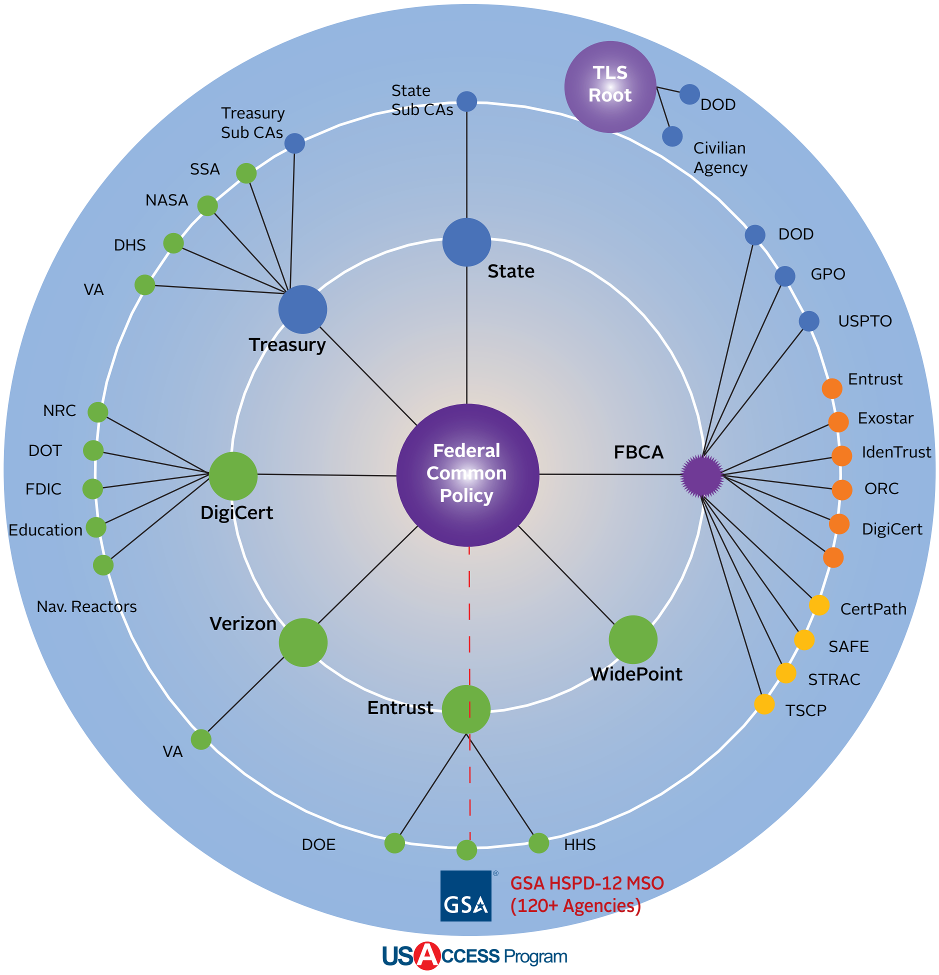


Figure 2. FPKI Trust Infrastructure and Participating CAs

The FPKI Trust Infrastructure consists of three leading CAs operated by the FPKIMA. Any CA in the FPKI can be referred to as an "FPKI CA," but only those operated by the FPKIMA are FPKI Trust Infrastructure CAs. The FPKI Trust Infrastructure CAs include:

- The **Federal Common Policy CA (FCPCA)** is the trust anchor[1] for the federal government. Through the Shared Service Provider (SSP) program, authorized CAs under the FCPCA issue certificates for exclusive use by the federal government for federal employees, contractors, and federal devices to include the PKI certificates on the PIV card. It was designed so any certificate issued by an FPKI CA can validate to a single point.
- The **FBCA** enables interoperability between different federal PKIs and between federal and external PKIs. The FBCA provides a means to map participating PKI certificate policies, so they validate to the FCPCA trust anchor.

[1] A trust anchor will be explained in more detail later in the guide.

- Planned: A joint effort between the Department of Defense (DOD) and GSA, the standalone **Transport Layer Security (TLS) Root CA** is a new government trust anchor for government-issued, publicly trusted, server authentication certificates to be used on public-facing government websites and applications. It is designed to comply with DHS BOD 18-01 and OMB M-15-13.

An FPKI-participating CA is either an industry, other government (e.g., state, local, or foreign), or federal agency CA. Examples of participating CAs:

- **Commercial CAs** are private-sector/industry PKI-participating CAs cross-certified with the FBCA that have shown a need to either do business with or provide PKI services to the federal government. These CAs are often referred to as non-federal issuers (NFIs).
- **Other Bridge CAs** are bridge CAs that connect member PKIs and are designed to enable interoperability between different PKIs operating under their Certificate Policy (CP)[2], not intended to be used as a trust anchor.
- **Other Government CAs** are CAs that support state, local, or foreign governments whose subscribers need to be authenticated to do business with U.S. federal agencies.
- **Federal Agency Legacy PKIs** are federal agency-operated internal PKIs cross-certified[3] with one or more FPKI Trust Infrastructure CA.
- **SSP CAs** are CAs subordinate to the FCPCA and under contract with one or more federal agencies to issue certificates exclusively to federal employees, contract support, and federal devices. The SSP may be a commercial vendor or a federal agency and is required to have an Authority to Operate (ATO), among other security requirements, to issue government certificates.

Note: For a dynamic version of the previous figure that includes all CAs, please visit fpki.idmanagement.gov/tools/fpkigraph.

3 Testing

The Community Interoperability Testing Environment (CITE) mirrors the FPKI production environment, allowing the FPKI community's test environments to be cross-certified with a test instantiation of the FPKI Trust Infrastructure. The FPKIMA uses CITE to conduct interoperability testing with FPKI applicant organizations as part of the cross-certification process. The FPKIMA coordinates with applicant organizations to provide interoperability testing, identify and resolve potential issues, and create and deliver reports of test results. The FPKI affiliates have the option of retaining their integration and participation with CITE. This allows cooperation to resolve technical issues across Affiliate PKIs and ensures proper functionality of their proposed system changes before deployment. For more information, please visit the CITE Participation Guide site at https://fpki.idmanagement.gov/tools/citeguide.

4 For More Information About the FPKI

Websites:

- FPKIMA: www.idmanagement.gov/fpkima
- FPKI Guides: fpki.idmanagement.gov

Email:

- FPKI@gsa.gov

[2] A more thorough description will be provided later in this guide.

[3] Cross-certification will be explained later in this guide, but is a method to show comparable security between organizational PKI policies.

Appendix: List of Abbreviations

ATO	Authority to Operate
CA	Certification Authority
CP	Certificate Policy
FBCA	Federal Bridge Certificate Authority
FCPCA	Federal Common Policy Certification Authority
FICAM	Federal Identity, Credential, and Access Management
FPKI	Federal Public Key Infrastructure
FPKIMA	FPKI Management Authority
FPKIPA	FPKI Policy Authority
GSA	General Services Administration
ICAM	Identity, Credential, and Access Management
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
SSP	Shared Service Provider
TLS	Transport Layer Security

www.gsa.gov
November 2020
05-21-00255
View, download, and order publications via www.gsa.gov/cmls.