

Search Words from illustration:

Bridge
External
Shared Service Provider (PIV)
FPKI Trust Infrastructure
Federal PKI
SHA-1 Providers
Subordinate or oneway
Two way cross certified
State
SHA1 FRCA
FBCA
ORC
Entrust
Verizon
Symantec
Treasury
CertiPath Bridge
DoD IRootCA 1
CertiPath Bridge - G2
DoD IRoot CA 2
DEA
DigiCert NFI
Entrust NR
Exostar NR
GPO
IdentTrust ACES
IndeTrust ACES
IdentTrust ACES
ORC AC ES
ORC NFI
SAFE Bridge CA
State of Illinois
Symantec NFI (4 CAs)
USPTO
Verizon NFI

[Edit this page](#)

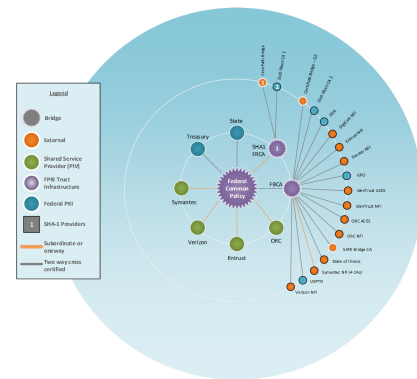
Certification Authorities

A **certification authority** is a system that issues digital certificates. These digital certificates are based on *cryptography* and follow the X.509 standards defined for information security.

The Federal PKI (FPKI) is a network of hundreds of certification authorities (CAs) that are either *root*, *intermediate*, or *issuing* CAs.

Any CA in the FPKI may be referred to as a *Federal PKI CA*. The three highest level CAs in the FPKI hierarchy are the **FPKI Trust Infrastructure CAs**, which are operated and managed by the Federal PKI Management Authority (FPKIMA) Program Office:

- [Federal Common Policy Certification Authority](#)
- [Federal Bridge Certification Authority](#)
- [SHA-1 Federal Root Certification Authority G2](#)



The FCPCA serves as the *root* and *trust anchor* for the *intermediate* and *issuing* CAs operated by:

- Federal Government Executive Branch Agencies
- State, Local, Tribal, Territorial, and International Governments
- Commercial Partners

Public trust for websites

A new effort is in the planning stages to establish another Federal Government root and issuing CAs dedicated to Public Trust Transport Layer Security (TLS) device certificates. Follow or contribute to the

development of the Federal Government's new certificate policy for this Public Trust effort at <https://github.com/uspki/policies>

Federal Common Policy Certification Authority

The *Federal Common Policy CA* may be referred to as the *FCPCA*, or as *COMMON* in documents. As the FPKI root and trust anchor for the Federal Government, the FCPCA supports government person trust and enterprise devices, including [Personal Identity Verification \(PIV\) credentials](#). The FCPCA's design enables any certificate issued by any FPKI CA to validate its certificate path to a single root CA.

Many commercial vendors include the FCPCA root certificate in their commercial-off-the-shelf (COTS) products' [Trust Stores](#). This enables Federal Government systems to trust person and enterprise device certificates issued by FPKI CAs. It is possible to add the FCPCA root certificate to trust stores for *government managed* devices and servers, if it's not available by default.



The FCPCA root certificate is included in the trust stores for some platforms such as Microsoft, Apple, and Adobe. Other platforms, such as Mozilla, do not include the FCPCA by default.

Federal Bridge Certification Authority

The FBCA is the *Federal Bridge CA 2016*.



The FBCA is a PKI Bridge or link between the FCPCA and other CAs that comprise the FPKI network and that may operate under comparable but *different* certificate policies.


The FBCA provides a means to map these certificate policies and CAs and allow certificates to validate to the FCPCA root certificate.

The CAs with certificates signed by the Federal Bridge CA 2016 are *cross certified*. These CAs have established a trust relationship with the FPKI and are audited annually for conformance to the certificate policies. This cross-certification process has extended the reach of the FPKI well beyond the boundaries of the Federal Government.

SHA-1 Federal Root Certification Authority

The SHA-1 Federal Root CA G2 (SHA1 FRCA) was created and is maintained to facilitate backwards interoperability for government legacy systems unable to transition to SHA-256.

The deprecated SHA-1 hash algorithm has been deemed not secure enough for today’s federal systems. Federal agencies should no longer generate, use, or accept certificates with the SHA-1 hash.

 Certificates using the SHA 1 signature hash algorithm under current policy are limited to legacy systems and are being completely phased out.

All Federal PKI Certification Authorities

A CA that is part of the FPKI is called a *participating certification authority*. Hundreds of participating CAs form the FPKI network.


For historical records, we might *label* or identify CA systems using a category that shows *when* the system was established and for what types of *communities* it is or was used.



We realize all the acronyms and labels may be confusing and welcome your input to help us improve, add information over time, and simplify where needed.

Certification Authority Category	Description
PKI Shared Service Provider (SSP) Certification Authorities	An SSP CA is <i>subordinate</i> to the FCPCA. Any certificate that an SSP CA creates, signs, and issues to people or devices is in the FCPCA <i>trust chain</i> . An SSP must adhere to strict federal IT security standards and requirements. The SSPs are granted a FISMA Authority To Operate (ATO), undergo continuous monitoring, and are contracted by the Federal Government to issue certificates to federal employees and contractors, as well as devices that are deployed in federal agency networks.

Certification Authority Category	Description
Private Sector Certification Authorities	A Private Sector CA that is cross-certified has shown a valid need to conduct business or provide PKI services to the Federal Government
Access Certificates for Electronic Services (ACES) Certification Authorities	The ACES CAs issue certificates to authorized U.S. business representatives who need to digitally sign documents or access certain web based systems. ACES was established in the late 1990s and is the predecessor for the development of today’s Federal PKI. See note below on ACES CA and credential deprecation.
Other Government Certification Authorities	These CAs are managed and operated by State, Local, Tribal, Territorial, or International Governments
Bridge Certification Authorities	Bridge CAs connect member PKIs and are designed to enable interoperability between different PKIs operating under their own certificate policies. A Bridge CA is not a <i>root</i> .
Federal Agency Legacy	Prior to 2004, some agencies had already deployed and invested in their own PKI and CAs. Some of these agencies opted out of migrating to the SSP Program and continued to manage their existing infrastructures. These Federal Agencies Legacy operate one or more CAs that are cross-certified with a Federal PKI Trust Infrastructure CA

 ACES credentials are deprecated for Private Sector Certification Authorities or Bridge Certification Authorities. For more information, see the GSA ACES Sunset FAQ Sheet at https://www.idmanagement.gov/wp-content/uploads/sites/1171/uploads/gsa_aces_sunset_guide.pdf or email the GSA ACES Program at GSA-ACES@GSA.gov

The GSA logo consists of the letters "GSA" in white, bold, sans-serif font, centered within a dark blue square.The CIO.gov logo features the text "CIO.gov" in a dark blue, sans-serif font. The letter "O" is stylized with a white power symbol (a circle with a vertical line) inside it.

Feedback? Create an issue on the [code repository](#) or email us at fpki@gsa.gov.

Have an idea? Read our [contribution guidelines](#).

As a work of the United States government, this project is in the public domain. Copyright is also waived internationally via a CC0 1.0 waiver.

[Read More.](#)

[Privacy Policy](#)

Certification Authorities

A certification authority is a system that issues digital certificates. These digital certificates are based on cryptography and follow the X.509 standards defined for information security.

The Federal PKI (FPKI) is a network of hundreds of certification authorities (CAs) that are either root, intermediate, or issuing CAs.

Any CA in the FPKI may be referred to as a Federal PKI CA. The three highest level CAs in the FPKI hierarchy are the FPKI Trust Infrastructure CAs, which are operated and managed by the Federal PKI Management Authority (FPKIMA) Program Office:

FPKI Trust Infrastructure

- Federal Common Policy Certification Authority
- Federal Bridge Certification Authority
- SHA-1 Federal Root Certification Authority G2

The FCPCA serves as the root and trust anchor for the intermediate and issuing CAs operated by [circular sidebar graphic of this text description]

- Federal Government Executive Branch Agencies
- State, Local, Tribal, Territorial, and International Governments
- Commercial Partners

Source, Accessed Nov. 17, 2018 9:26am EST

Federal Public Key Infrastructure Guides, Certification Authorities

<https://fpki.idmanagement.gov/ca/#federal-common-policy-certification-authority>