Federal PKI Graph

**Last Update:** November 12, 2018
The FPKI Graph displays the relationships between the Certification Authorities in the Federal PKI (FPKI) ecosystem. It graphically depicts how each Certification Authority links to another, through cross certificates, subordinate certificates, or Bridge CAs.

The Federal Common Policy Certificate Authority (CA) ("COMMON") is shown at the center of the Graph, and the rings of dots represent the outbound CAs.

- Click on any dot in the Graph to see a CA's inbound and outbound CA certificates.
- *Inbound* means the CA certificate is signed by the *Inbound CA*.
- *Outbound* means the CA has signed the *Outbound CA* certificate.
- The *Search* function is on the upper right-hand corner.
- The *Zoom* scroll bar is in the upper left-hand corner.

You cannot download the certificates from the Graph. To download the certificates, you need to retrieve the certificates from the Authority Information Access (AIA) or Subject Information Access (SIA) URIs. (See below for
more information on AIAs and SIAs.)

**How the FPKI Graph Works**

The Graph uses information published in each CA certificate’s AIA and SIA extensions. This is public information: all CAs in the FPKI are required to publish and maintain their AIA certificate bundles.

All CA and End Entity certificates that have a certificate path (trust chain) to COMMON will have an AIA extension in their public certificates. An AIA extension contains a URI where you can find the certificate(s) used to sign that CA or End Entity certificate.

Most CA certificates will also have an SIA extension with a URI to the CA certificates that have been issued by that CA. For example, you can find the SIA for COMMON at http://http.fpki.gov/fcpca/caCertsIssuedByfcpca.p7c.

- To use this SIA, retrieve the file (.p7c) using the link above and open it.
- You will find a dozen or more certificates that are issued by COMMON (Root) to other intermediate or issuing CAs.
- The SIA URIs from each of these certificates can then be retrieved to find the next set of signed certificates.

**Acknowledgment**

The FPKI Graph was built by using the same tools and code as the [Berkley ICSI SSL Notary](http://berkeleyicisslnotary.org).
Feedback? Create an issue on the [code repository](https://github.com/iotc/fpki-graph) or email us at [fpki@gsa.gov](mailto:fpki@gsa.gov).

Have an idea? Read our [contribution guidelines](https://github.com/iotc/fpki-graph/blob/master/CONTRIBUTING.md).

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](https://github.com/iotc/fpki-graph)

[Privacy Policy](https://github.com/iotc/fpki-graph/blob/master/LICENSE)