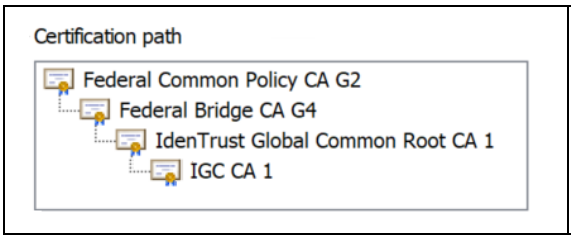
Change to Federal Common Policy CA Root Certificate

The following information pertains to the April 2021 rollover/resign of the **Federal Common Policy CA** root certificate and replacement with a new **Federal Common Policy CA G2** root certificate. To avoid any possible issues related to validation of IdenTrust ECA and IGC certificates, immediate action should be taken to update your certificate store(s) and applications with the new Federal root certificate using the following instructions.

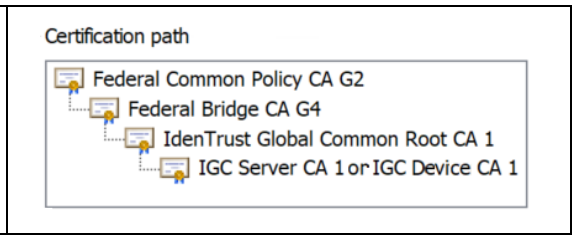
Overview of Changes

The Federal Common Policy CA/CA G4 certificates issue the Federal Bridge CA certificates under which IdenTrust operates the IdenTrust DoD ECA (ECA) and IdenTrust Global Common (IGC) policies. In order for ECA and IGC certificates issued under the Federal Bridge policy to chain and validate properly, the new Federal Common Policy CA G2 certificate must be added to your browser store and any other location where the current Federal Common Policy CA certificate is used. Once the new Federal Common Policy CA G2 all subordinate certificates will also be updated and end entity certificates will be validated properly. The following illustrates the updated root chains for IdenTrust policies once the new root certificate is installed:

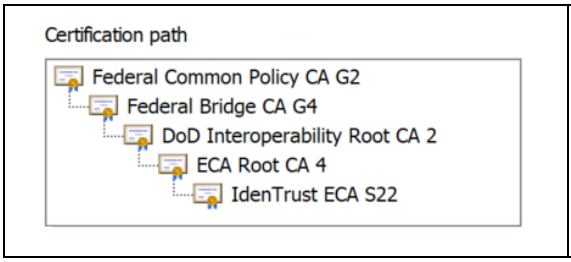
For IGC Human Certificates



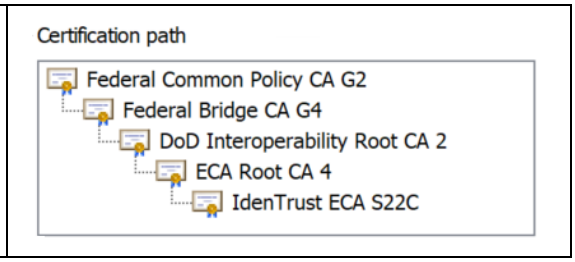
For IGC Device Certificates



For ECA Human Certificates



For ECA Server Certificates



Update Instructions

To ensure that certificates validate properly, you should install the new Federal Common Policy CA G2 certificate, which is available for download at https://www.identrust.com/support/downloads. The download will allow you to install the new certificate in your browser store.

Additionally, if you are a relying party, you should also take the following steps to ensure that the original root CA certificate is replaced with the new root CA certificate.

1. Evaluate your systems to determine where you use IGC or ECA certificates.
2. Locate anywhere in those systems where the Federal Common Policy CA (aka old root certificate) is used as a trust anchor or where there is any other reliance on the root certificate.

3. If you have not already done so, obtain the new Federal Bridge Policy CA G2 certificate from the IdenTrust website at https://www.identrust.com/support/downloads.
4. Once you have the new root, deploy it is so that both the old root and new root are available in your system.
5. We also suggest that you also deploy the Federal Bridge CA G4 certificate as an intermediate CA certificate in your systems. This certificate is also available on the IdenTrust website at the link provided in Step 3.
6. Completing these deployments will allow your current certificates to chain to the new Root.
7. Test your system processes.

Removal of Federal Common Policy CA Root Certificate

The Federal PKI indicates that April 20, 2021 is the target date to remove the old root CA certificate. To confirm that your systems will operate without the old root in place, you may wish to execute a test run prior to that date to remove the old root from your systems. An early test run will allow you to identify any issues, reinstall the old root and make any adjustments to your system(s) prior to the original root certificate removal date.

Additional Information

You can also visit the Federal PKI website at https://fpki.idmanagement.gov/common/ if you would like further background regarding this change.

NOTE: The FPKI realizes that each relying party implementation may be different. To help address this, the FPKI has created a set of instructions for common environments which is viewable at:

(https://fpki.idmanagement.gov/common/distribute-os/).

The FPKI has also created a repository for interested parties to share their implementation approach.