**FBCA Technical Working Group**


# Implementation Guidance for Relying Parties Using the Common Policy Root

February 2007

## 1.0 Background

While applications that use public key certificates may be designed to accept any valid certificates, many applications will have a requirement to only accept certificates that were issued in conformance with certain policy requirements. With some applications, this may be accomplished by configuring the application to only accept certificates that validate with respect to a certain set of policy object identifiers (OIDs). The specific set of policy OIDs that should be specified as acceptable for an application will depend not only the application's policy requirements but also on the trust anchor that is used for path validation. This document provides guidance for selecting the set of acceptable policy OIDs when the Common Policy Root CA is used as a trust anchor.

The guidance in this document is based on the set of certificate policies and policy mappings that are currently asserted in certificates issued by the Common Policy Root CA. At the time this document was written, the certificates issued by the Common Policy Root CA to the Federal Bridge CA (FBCA) do not reflect certificate policies that were defined within the past year (e.g., id-pki-common-high, id-fpki-certpcy-mediumHardware, id-fpki-certpcy-medium-CBP, and id-fpki-certpcy-mediumHW-CBP). When new cross-certificates are issued by the Common Policy Root CA to the FBCA to incorporate these new policy OIDs, this guidance will need to be updated.

## 2.0 Policy OIDs Asserted by the Common Policy Root CA

At the time that this document was written, the Common Policy Root CA asserted the following policy OIDs in the certificates that it issued:

- id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}
- id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}
- id-fpki-common-devices ::= {2 16 840 1 101 3 2 1 3 8}
- id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}
- id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}
- id-fpki-common-cardAuth ::= {2 16 840 1 101 3 2 1 3 17}
- id-fpki-certpcy-rudimentaryAssurance ::= { 2 16 840 1 101 3 2 1 3 1}
- id-fpki-certpcy-basicAssurance ::= {2 16 840 1 101 3 2 1 3 2}
- id-fpki-certpcy-highAssurance ::= {2 16 840 1 101 3 2 1 3 4}

The Common Policy Root CA does not assert id-fpki-certpcy-mediumAssurance, however, id-fpki-common-policy and id-fpki-common-devices both map to id-fpki-certpcy-mediumAssurance. So, if a relying party lists either id-fpki-common-policy or id-fpki-common-devices then any certificates issued under a policy that maps to id-fpki-certpcy-mediumAssurance will also be considered acceptable.

In configuring an application, relying parties must specify all policy OIDs from this list that are acceptable for the application. For example, a relying party that is willing to accept any certificates that were issued at the basic assurance level should specify the following OIDs: id-fpki-certpcy-basicAssurance, id-fpki-common-policy, id-fpki-common-hardware, id-fpki-common-devices, id-fpki-common-authentication, id-fpki-common-High, and id-fpki-certpcy-highAssurance.

When selecting acceptable policy identifiers based on assurance level, it should be noted that id-fpki-common-policy and id-fpki-common-devices map to id-fpki-certpcy-mediumAssurance, id-fpki-common-hardware maps to id-fpki-certpcy-mediumHardware, and id-fpki-common-High maps to id-fpki-certpcy-highAssurance. While the assurance level of id-fpki-common-authentication is comparable to that of id-fpki-certpcy-mediumHardware, id-fpki-common-authentication does not require certificates to include a non-empty subject name. The private keys corresponding to the public keys in certificates that assert id-common-cardAuth may be used without being activated by the subscriber, so id-common-cardAuth does not correspond to any other assurance level.

Once the relying party has determined the set of policy OIDs that should be considered acceptable for an application, that selection of acceptable policy OIDs must be configured into the relying party's Path Discovery and Validation (PD-Val)[1] product. Additionally, the PD-Val product should be configured with the Common Policy Root CA as the trust anchor. It is important to note that the application software should not accept or reject certificates based on the policy OIDs that are asserted in the end entity certificates' certificatePolicies extensions, but rather the set of acceptable policy OIDs should be provided to the PD-Val product, which will determine if a valid certification path exists that satisfies the specified policy requirements. The PD-Val product will take into account any policy mappings that are included in intermediate certificates.

## 2.1 Policy OIDs and e-Authentication Levels

Some applications may need to filter certificates based on e-Authentication level. The table below lists the policy OIDs that should be considered acceptable for applications that use the Common Policy Root CA as a trust anchor and that require a certain authentication level. There are no policies asserted by the Common Policy Root CA that satisfy e-Authentication level 2 that do not also satisfy e-Authentication level 3.

| E-Authentication Level | Acceptable certificate policy OIDs |
|---|---|
| 3 | id-fpki-common-policy ::= {2 16 840 1 101 3 2 1 3 6}<br>id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}<br>id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}<br>id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}<br>id-fpki-certpcy-basicAssurance ::= {2 16 840 1 101 3 2 1 3 2}<br>id-fpki-certpcy-highAssurance ::= {2 16 840 1 101 3 2 1 3 4} |
| 4 | id-fpki-common-hardware ::= {2 16 840 1 101 3 2 1 3 7}<br>id-fpki-common-authentication ::= {2 16 840 1 101 3 2 1 3 13}<br>id-fpki-common-High ::= {2 16 840 1 101 3 2 1 3 16}<br>id-fpki-certpcy-highAssurance ::= {2 16 840 1 101 3 2 1 3 4} |

[1] Relying Parties must choose their PD-Val products from the Federal PKI Policy Authority (PA)-approved Qualified Validation List (QVL) found at http://www.cio.gov/fbca/validation_solutions.htm.

Since e-Authentication levels only cover remote electronic authentication of human users, certificates issued under id-fpki-common-devices does not fall under any e-Authentication level. However, applications that accept certificates that satisfy e-Authentication level 3 and that also wish to accept certificates issued to devices should include id-fpki-common-devices in the set of acceptable policy OIDs.

While the e-Authentication levels are not directly relevant to applications that are not performing authentication, applications that use certificates to verify digital signature on documents or to perform key management may choose to use the above table as guidance in determining what policy OIDs should be considered acceptable. Since certificates that assert id-fpki-common-authentication should only be used when performing authentication, this OID may be excluded from the set of acceptable policy OIDs in applications that are using certificates to verify digital signatures on documents or to perform key management.