



**Common Policy CP Change Proposal Number: 2010-01**

**To:** Federal PKI Policy Authority  
**From:** Certificate Policy Working Group  
**Subject:** Proposed modifications to the Common Policy CP  
**Date:** September 15, 2010  
**Title:** CAs to assert policy OIDs in OCSP responder certificates for which the OCSP responder is authoritative

**Version and Date of Certificate Policy Requested to be changed:**

X.509 Certificate Policy for the U. S. Federal PKI Common Policy Framework Version 3647 – 1.11, August 16, 2010.

**Change Advocate's Contact Information:**

Name: Debbie Mitchell  
Organization: DoD

**Organization requesting change:** DoD

**Change summary:** Add requirement that OCSP responders assert certificate policy OIDs in OCSP responder certificates for which the OCSP responder is authoritative.

**Background:** The FCPF CP does not explicitly require that certificates issued to OCSP responders assert all the policy OIDs for which the responder provides responses. Since a responder acts as a surrogate to the CA, it should be issued a certificate that includes all the policies that the CA can assert. Client path validation fails in certain scenarios (particularly cross-certification) when the policies asserted by the responder don't match the policies asserted by the target certificate (which the responder is responding for).

**Specific Changes:** Specific changes are made to the following sections: 1.2 and 1.3.1.7

Insertions are underlined, deletions are in ~~striketrough~~ text:

**1.3.1.7 CERTIFICATE STATUS SERVERS**

PKIs may optionally include an authority that provides status information about certificates on behalf of a CA through on-line transactions. In particular, PKIs may include OCSP responders to provide on-line status information. Such an authority is termed a certificate status server (CSS). Where the CSS is identified in certificates as an authoritative source for revocation information, the operations of that authority are considered within the scope of this CP. A Certificate Status Server (CSS) shall assert all the policy OIDs for which it is authoritative.

Examples include OCSP servers that are identified in the authority information access (AIA) extension. OCSP servers that are locally trusted, as described in RFC 2560, are not covered by this policy.

**Estimated Cost:**

No additional cost to the Common Policy CA.

**Risk/Impact:**

Certificate validation using OCSP may fail in certain (particularly cross-certification) scenarios. Relying parties may be unable to validate some certificates. The certificate profile will need to be updated.

**Implementation Date:**

This change will be implemented within one year of approval by the FPKIPA and incorporation into the Common Policy CP.

**Prerequisites for Adoption:**

None

**Plan to Meet Prerequisites:**

None

**Approval and Coordination Dates:**

Date presented to CPWG: TBD

Date Presented to FPKIPA: TBD

Date of approval by FPKIPA: TBD