Common Certificate Policy Change Proposal Number: <2012-01

To: Federal PKI Policy Authority (FPKIPA)
From: PKI Certificate Policy Working Group (CPWG)
Subject: Proposed modifications to the Common Certificate Policy
Date: May 3, 2012

Title: Time Stamp Authority Requirement with Code Signing Certificates
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 - 1.17 December 9, 2011

Change Advocate's Contact Information:

Organization requesting change: FPKIMA

Change summary: Require Organizations receiving a code signing certificate to have access to a Time Stamp Authority

Background:

The Common Policy CA root certificate is distributed as a trust anchor in the Microsoft Root Certificate Program. With the distribution of a root certificate, Microsoft sets properties stating the usages enabled for the root certificate. Microsoft changed their requirements to state organizations whose root CA are enabled for the code signing EKU (1.3.6.1.5.5.7.3.3) are required to run a Time Stamp Authority (TSA) in conjunction with their code signing service. As a best practice, code signing subscribers should time stamp the digital signatures when signing code.

Surveying federal agencies found a small number of agencies do use code signing certificates to sign code. The majority of the agencies who currently sign code said they already have access to a TSA and add a timestamp when signing code. Therefore, to meet the Microsoft requirement and retain the current setting of the code signing EKU with the Common Policy root certificate in the Microsoft Root Certificate Program, the requirement for a TSA is passed to the organization receiving a certificate used for code signing.

Currently, the way Microsoft described their validation process, code signed without a timestamp will not automatically fail validation. Therefore, although there is a requirement for a TSA, there is no current requirement to use it. This will allow transition time for agencies that do not yet require time stamping.

Implementation of this change proposal will preserve the code signing property associated with the Common Policy Root certificate in the Microsoft trust store. It is important that the full functionality of the Federal Common Policy Trust Anchor is available in the Microsoft product line. This ensures Federally signed code works transparently for end users.

Specific Changes:

Insertions are underlined, deletions are in ~~strikethrough~~:

4.1.1.4 Code Signing Certificates

A code signing certificate has an Extended Key Usage (EKU) containing a value of id-kp-codeSigning OBJECT IDENTIFIER ::= { id-kp 3 }(1.3.6.1.5.5.7.3.3) - See [CCP-PROF] for appropriate EKU bit settings.

An application for a code signing certificate shall be submitted by an authorized representative of the organization. The representative shall assert that the organization has access to a Time Stamp Authority (TSA) prior to issuance of the code signing certificate.

Estimated Cost:

Organizations that do not already have access to a TSA and receive code signing certificates will incur a cost to establish or outsource a TSA.

Implementation Date:

This policy change will be incorporated into the Common Policy Framework Certificate Policy immediately upon approval by the FPKIPA .

Prerequisites for Adoption:

Organizations that do not already have access to a TSA and receive code signing certificates will need to establish or outsource a TSA

Plan to Meet Prerequisites:

Organizations that do not already have access to a TSA and receive code signing certificates will need to develop and plan to establish or outsource a TSA

Approval and Coordination Dates:

Date presented to CPWG:	May 3, 2012
Date presented to FPKIPA:	June 12, 2012
Date of approval by FPKIPA:	June 12, 2012