Alternative Means for Bronze and Silver Requirement to Discontinue SHA-1 Encryption for SAML Assertions

Audience for this Document: Identity Provider Operators that have been certified by the InCommon Assurance Program or are wishing to apply for certification by January 15, 2015.

Alternative Means Statement: Identity Provider (IdP) Operators may continue to use SHA-1 to sign assertions through January 15, 2015 without compromise to their InCommon Assurance certification. IdP Operators that send assertions to a FICAM-compliant US Government Agency service provider that requests an InCommon Assurance Profile after December 31, 2013 must sign those assertions using any SHA-2 algorithm.

1. **Requirements of the IAP that the alternative means is proposed to address**

   This alternative means addresses the criteria in the InCommon Identity Assurance Profiles version 1.2, section 4.2.7.3 Cryptographic Security that stipulates, "Cryptographic operations are required between an IdP and any SP. Cryptographic operations shall use Approved Algorithms."

   In SP800-131A, published in January 2011, NIST updated its recommendations for approved cryptographic algorithms and key lengths for use in the US Federal government, including the FICAM program that certifies InCommon's status as an approved Trust Framework Provider. In particular, NIST calls for discontinuing use of the SHA-1 digest function or hash algorithm in digital signatures effective January 1, 2014 and recommends using any of the digest functions known collectively as SHA-2 for use in digital signatures.

2. **Reasons for proposing the alternative**

   The predominant Identity Provider technology in use in the InCommon Federation is Shibboleth 2.X. A Shibboleth IdP must use a single signing algorithm for all assertions that it sends. Hence, to support a SHA-2 signature, a Shibboleth IdP must send SHA-2 signed assertions to *all* Service Providers (SP) with which it interoperates. Interactions with any non-compliant SP will fail until the SP is upgraded. Investigation into the SPs published in the InCommon metadata indicate that there are a few participant organizations with SPs that do not support SHA-256 (a SHA-2 algorithm). These InCommon SPs are expected to remediate their issues by June 30, 2014.

   Additionally, since many Identity Provider Operators (IdPOs) within InCommon rely on SPs outside of InCommon for critical services, each IdPO must validate SHA-2 readiness of such SPs before it can enable a SHA-2 signing algorithm in its Shibboleth IdP. IdPOs that wish to maintain their InCommon Assurance certification will thus have additional time in which to validate any non-InCommon SPs they rely on and ensure that any SPs that do not support a SHA-2 signing algorithm remediate their issues.

   If InCommon had enforced this change January 1, 2014, it would have effectively forced IdPOs with an InCommon Assurance certification to make a choice between continuing their certification or continuing their reliance on critical SPs that do not support SHA-2 by that date.

3. **Mitigation of risks potentially exposed by the alternative means**

   The risks include those that exist today when using a SHA-1 algorithm: possible compromise of the SAML assertion. No additional operation risks are incurred.

4. **Management assertion of the alternative means**

   SAML assertions sent after December 31, 2013 to US Government services requesting an InCommon Assurance Profile will be signed using a SHA-2 algorithm. SAML assertions sent after January, 15 2015 to any InCommon SP requesting an InCommon Assurance Profile will be signed using a SHA-2 algorithm.

5. **Why and how the alternative means is comparable or superior to the cited IAP requirement**

   The ability meets or exceeds the effect of the requirements in section 4.2.7.3 of the InCommon IAP version 1.2 because the risk to participants in the InCommon Federation of implementing this upgrade in a very short time frame and possibly rendering inoperable some of their critical operations is higher than continuing to allow the current SHA-1 algorithm for another six months.