Phase 1 Implementation Plan

Phase 1 Implementation Plan

This document is a plan to implement the Phase 1 Recommendations of the Metadata Distribution WG. For more detailed information, see the Phase 1 Implementation Plan FAQ.

Executive Summary

A timeline for the Phase 1 Implementation Plan is given below:

1. On December 18, 2013, InCommon Operations will deploy three new metadata aggregates at the following **permanent** HTTP locations:
    - http://md.incommon.org/InCommon/InCommon-metadata.xml (production metadata)
    - http://md.incommon.org/InCommon/InCommon-metadata-fallback.xml (fallback metadata)
    - http://md.incommon.org/InCommon/InCommon-metadata-preview.xml (preview metadata)
2. All new metadata aggregates will be signed using a new self-signed signing certificate set to expire on December 18, 2037.
    - https://ds.incommon.org/certs/inc-md-cert.pem
    - Although the signing certificate is new, the signing key is not.
3. All new metadata aggregates will be signed with the same key but the fallback metadata aggregate will use a different digest algorithm.
    - The *production metadata aggregate* will be signed using a SHA-2 digest algorithm (specifically, SHA-256).
    - Initially, the *fallback metadata aggregate* will be signed using the SHA-1 digest algorithm (which is what we use now).
    - Initially, the *preview metadata aggregate* will be identical to the *production metadata aggregate*.
4. **All deployments shall migrate to one of the new metadata aggregates ASAP but no later than March 29, 2014**.
    - The current metadata aggregate will be replaced with a redirect to the *fallback metadata aggregate* on March 29, 2014.
    - If your metadata process can verify an XML signature that uses the SHA-256 digest algorithm, migrate to either the *production metadata aggregate* or the *preview metadata aggregate*.
    - If your metadata process can **not** verify an XML signature that uses the SHA-256 digest algorithm, migrate to the *fallback metadata aggregate*.
5. **All deployments shall be able to verify an XML signature that uses a SHA-256 digest algorithm by June 30, 2014**.
    - On June 30, the *fallback metadata aggregate* will be synced with the *production metadata aggregate* (i.e., all aggregates will be signed using the SHA-256 digest algorithm).
    - After June 30, all metadata aggregates published by the InCommon Federation will be signed using the SHA-256 digest algorithm.

See the Actions section below for the current state of the Phase 1 Implementation Plan.

Policy

It is **strongly recommended** that InCommon SPs and IdPs **refresh and verify metadata** at least daily. The security implications of metadata refresh are discussed on the Metadata Consumption wiki page:

> *Regular metadata refresh protects users against spoofing and phishing, and is a necessary precaution in the event of key compromise. Failure to refresh metadata exposes you, your users, and other Federation participants to unnecessary risk.*

If you verify the digital signature on InCommon metadata (as recommended), the following implementation plan may affect your metadata refresh process. Even if you don't verify the signature (which is **not** recommended), note that the HTTP location of InCommon metadata is changing.

Drivers

1. The InCommon metadata signing certificate expires on May 2, 2014.
    - If we don't issue a new metadata signing certificate by May 2, 2014, an expired signing certificate will be bound to the XML signature in metadata.
2. The InCommon metadata signing certificate is signed by a legacy CA whose certificate expires on March 29, 2014.
    - If we don't issue a new metadata signing certificate by March 29, 2014, an expired CA certificate will be bound to the XML signature in metadata.
    - The CA certificate adds nothing to the security of metadata, so its presence (expired or not) only serves to confuse consumers.
3. The XML signature on InCommon metadata uses the deprecated (and soon-to-be disallowed) SHA-1 digest algorithm.
    - NIST deprecated the use of SHA-1 in conjunction with digital signatures on January 1, 2011.
    - NIST disallows the use of SHA-1 in conjunction with digital signatures after January 1, 2014.
    - See: NIST SP 800-57 Part 1, Revision 3 (July 2012), Tables 3 and 4
4. Multiple, heterogeneous services currently run on vhost `wayf.incommonfederation.org`, namely, Metadata Services and the Discovery Service. To provide better quality of service, these services need to be segregated onto their own vhosts (`md.incommon.org` and `ds.incommon.org`, resp.). This will allow us to fine-tune each service according to its requirements.
    - On March 29, 2014, all metadata resources on `wayf.incommonfederation.org` will be retired.
    - The InCommon Discovery Service will continue to be served from `wayf.incommonfederation.org` indefinitely.
    - Note: The InCommon Federated Error Handling Service is already running on `ds.incommon.org`.
5. Multiple metadata aggregates will allow us to deploy changes to InCommon metadata more quickly and safely. Metadata consumers will have options depending on the requirements of their deployment.

Actions

InCommon Operations will take the following actions:

1. Create a new self-signed signing certificate set to expire on December 18, 2037: [**DONE**]
    - https://ds.incommon.org/certs/inc-md-cert.pem
2. On December 18, 2013, deploy three new metadata aggregates: [**DONE**]
    a. A new *production metadata aggregate* that uses the new self-signed certificate **and** a SHA-2 digest algorithm (specifically, SHA-256):
        - http://md.incommon.org/InCommon/InCommon-metadata.xml
    b. A new *fallback metadata aggregate* that uses the new self-signed certificate **and** the SHA-1 digest algorithm (like we do now):
        - http://md.incommon.org/InCommon/InCommon-metadata-fallback.xml
    c. A new *preview metadata aggregate* that is aliased to the *production metadata aggregate*:
        - http://md.incommon.org/InCommon/InCommon-metadata-preview.xml
3. Advise all deployments to migrate to one of the new metadata aggregates ASAP but **no later than March 29, 2014**. [**DONE**]
4. Create discussion list metadata-support@incommon.org. [**DONE**]
5. Replace the current metadata aggregate with a redirect to the *fallback metadata aggregate* on March 29, 2014. [**DONE**]
6. Retire the following resources on March 29, 2014:
    - http://wayf.incommonfederation.org/InCommon/InCommon-metadata.xml [**DONE**]
    - http://wayf.incommonfederation.org/InCommon/InCommon-metadata-test.xml
    - https://wayf.incommonfederation.org/bridge/certs/inc-md-cert.pem
    - https://wayf.incommonfederation.org/bridge/certs/incommon.pem
    - https://wayf.incommonfederation.org/bridge/certs/ca.pem
    - http://incommoncrl1.incommonfederation.org/crl/eecrls.crl
    - http://incommoncrl2.incommonfederation.org/crl/eecrls.crl
7. Sync the *fallback metadata aggregate* with the *production metadata aggregate* on June 30, 2014. [**DONE**]
8. Remove the redirect to the *fallback metadata aggregate* on [**date TBD**].

If you have questions or problems regarding this transition, please post them to metadata-support@incommon.org.