Metadata Distribution WG

Metadata Distribution Working Group of the InCommon Technical Advisory Committee (TAC)

Weekly Teleconferences

TIME
~~Thursdays, 12pm ET | 9am PT~~
This working group has completed its discussions and recommendations.

Mailing list

Archives: https://lists.incommon.org/sympa/arc/md-distro
List homepage: https://lists.incommon.org/sympa/info/md-distro
General information about InCommon mailing lists: https://lists.incommon.org/sympa/help/introduction

Mission/Goals

The mission of the Metadata Distribution Working Group is to develop a future-facing technical strategy for our metadata signing and distribution system.

We currently sign metadata using a signing key and certificate that is rooted in a traditional CA. The CA root certificate expires Mar 29 20:34:00 **2014** GMT. This working group will determine whether we simply renew, reissue, or come up with alternative approaches to signing the main InCommon public metadata aggregate.

The current method of metadata distribution relies on frequent local refreshes of a centrally maintained, monolithic metadata file containing all entities in the Federation. This distribution method will not scale if InCommon continues to grow at an exponential rate or for interfederation to succeed. Therefore, this working group is intended to help define, develop, and encourage the deployment of a new model of metadata distribution. Analogies have been made to the shift from /etc/hosts files to DNS, but the Internet Border Gateway Protocol (BGP) is thought by some to be closer to what is needed. In any case, substantial preparatory work has been developed (see this page summarizing TAC discussions regarding Metadata Distribution).

Deliverables for Phase 1: COMPLETED

Determine the fate of the metadata signing key.

1. Determine if the current metadata signing key and certificate needs to be replaced or renewed.
2. Determine if the key pair requires a traditional PKI.
3. Communicate to InCommon participants expectations and any required or recommended actions needed

Phase 1 completion date: End of August 2013

Deliverables for Phase 2: COMPLETED

Discuss, explore, and recommend alternative approaches to metadata distribution.

1. Elicit and capture requirements around metadata distribution
    a. short to mid-term requirements for metadata aggregation
    b. longer term requirements for per entity metadata
2. Devise a plan to transition the metadata signing algorithm to SHA-2
    a. this will be considered after SHA-2 testing of IdP endpoints is completed by TAC and Ops.
    b. the UK federation has blazed a welcome path for recommendation
3. Determine the desirability, feasibility, and impact of changing the InCommon metadata distribution point
    a. an outcome of the mid-term and long-term requirements discussion
4. Analyze and document alternative approaches to metadata distribution, and recommend one or more methods of metadata distribution for InCommon for the foreseeable future

Issues include:

- new endpoints for signed XML metadata distribution
- new signing key
- MDX support
- per-entity metadata
- per-organization metadata
- metadata aggregates based on self-asserted entity attributes
- support for both XML and JSON formats (both signed)

Phase 2 completion date: 16 January 2013

Membership

Membership in the working group is open to all interested parties. Members join the working group by joining the mailing list, phone calls, and otherwise participating actively in the work of the group. The chair of the working group is appointed by the InCommon TAC and is responsible for keeping the TAC informed regarding working group status. John Krienke is the current chair.

Minutes

- 2013-11-07
- 2013-10-31
- 2013-08-29
- 2013-08-15
- 2013-08-08
- 2013-07-25
- 2013-07-18
- 2013-07-11

References

InCommon *Federation* CA CPS -- PDF version online here. This CA is a long-standing self-signed CA, not to be confused with the InCommon Certificate service.

Terms

1. MD - metadata - SAML metadata for a given entity descriptor
2. MDA - metadata aggregate - a signed set of entity descriptor metadata
3. MDX - metadata query - a specification submitted to IETF, latest draft available here

Artifacts

- Phase 2 Recommendations
- Metadata Aggregates
- Sponsored Partner User Story
- Phase 1 Recommendations
    - Phase 1 Implementation Plan
    - Phase 1 Implementation Plan FAQ
- Metadata Query Protocol: A Consensus

Attachments

	File	Modified

No files shared here yet.