SAML Metadata Signing Policy and Aggregation Practice Statement Draft Framework

Presented at REFEDS, 5th December 2008

Rodney McDuff, The University of Queensland
r.mcduff@uq.edu.au
Viviani Paz, AAF Project Manager,
Security Assurance Manager, AusCERT
viviani@auscert.org.au

THE UNIVERSITY OF QUEENSLAND
AUSTRALIA

AusCERT

Parallels between PKI and SAML

• The root CA is the trust root of a PKI	• The metadata signing certificate/key is the trust root of a SAML federation
• A CA typically has one CPS and multiple CPs	• A metadata aggregator typically has one process (or practice) to gather a set of EntityDescriptors but may publish multiple signed metadata subsets. • Targeted to different audiences and purposes

However there is no SAML equivalent to CPS and CP

Perhaps it is time to define them?

CPS and CP in PKI

- CPS and CP(s) are all about:
  - **Who**, **What**, **Why** and **How**.
- Certification Practice Statement

  "Statement of the practices which a certification authority employs in issuing certificates".
  - **How** is a certificate created?
  - **Who** creates a certificate?
- Certificate Policy

  "Named set of rules that indicates the applicability of a certificate to a particular community and/or class of application".
  - **Why** was the certificate created?
  - **What** should the certificate be used for?

RFC 3647

- Internet X.509 Public Key Infrastructure Certificate Policy and Certification Practices Framework
  - Defines a standard template to assist authors of CPS and CP.
  - Provides a comprehensive “set of provisions” that need to be covered.
    - Collaboratively determined by the PKI community through the IETF.
    - Over 200 topics defined over 9 primary components.

```
• Introduction
• Publication and Repository
• Identification and Authentication
• Certificate Life-Cycle Operational Requirements
• Facilities, Management, and Operational Controls
• Technical Security Controls
• Certificate, CRL, and OCSP Profile
• Compliance audit
• Other Business and Legal Matters
```

Who are Consumers of CP and CPS?

- Relying Party
  - Gets better understanding how a CA operates.
  - Gets better understanding of the risks involved.
  - Gets better sense of trustworthiness of CA.
- Auditors
  - Third party verification that CPS and CP are true reflections of CA's practices and policies.
  - All RPs in auditor's scope benefit from manifested trustworthiness of the CA.
- Interfederating Parties
  - Can more easily gauge whether 2 PKIs are compatible for cross-certification and at what points.

SMAPS and SMSP in SAML (Proposed)

- SMAPS and SMSP(s) are all about:
  - **Who**, **What**, **Why** and **How**.
- SAML Metadata Aggregation Practice Statement

  "Statement of the practices which a metadata aggregator employs in publishing SAML Metadata".
  - **How** is the metadata aggregation created?
  - **Who** creates the metadata aggregation?
- SAML Metadata Signing Policy

  "Named set of rules that indicates the applicability of a aggregation of SAML metadata to a particular community and/or class of application".
  - **Why** was the metadata aggregation created?
  - **What** should the metadata aggregation be used for?

Who are Consumers of SMAPS and SMSP?

- Relying Party: IdP and SP
  - Gets better understanding how a core component of a federation operates.
  - Gets better understanding of the risks involved in using published metadata.
  - Gets better sense of trustworthiness of a federation.
- Auditors
  - Third party verification that SMAPS and SMSP are true reflections of federation's aggregation practices and policies.
  - All RPs in auditor's scope benefit from the manifested trustworthiness of the federation.
- Interfederating Parties
  - Can more easily gauge whether 2 federation are compatible for interfederation and at what points.

Scope of Audits

- "Trust, **but** verify", Ronald Reagan (1911-2004)
  - 3rd party audit manifests trustworthiness but only over the scope of the auditor.
- In PKI an audit can be at a global scope:
  - Webtrust Audit. Covers most commodity trust lists requirements. Expensive!
- Or a lesser scope:
  - IGTF. Scoped only over Grid EE, hosts and services.
  - IGTF members audit each other. Cheaper?
- Same with SAML.
  - Governments, Corporations may require global scope.
  - Can R&E use a lesser scope in the spirit of the IGTF model?
  - Perhaps REFEDS is in an ideal position to help? (as suggested by Vic)

Example (sub) Set of Provisions

- **Identification and Authentication.**
  - of SAML End Points.
  - of person/organisation submitting EntityDescriptors and Extensions.
- **Metadata Life-Cycle Operational Requirements.**
  - Enrolment and processing of submitted EntityDescriptors.
  - Modifying EntityDescriptors, re-keying KeyInfos, Extensions.
  - Revoking EntityDescriptors and Extensions.
- **Facilities, Management, and Operational Controls**
  - Physical Security, Procedural and Personnel Controls.
- **Technical Security Controls.**
  - Signing certificate/key generation and protection.

Set of Provisions may need to encompass dynamic metadata!

Next Steps?

If there is sufficient interest:

- Create a SAML equivalent of RFC 3647?
  - "SAML Metadata Signing Policy and Aggregation Practice Statement Framework."
  - What process should be used? Where should it be developed? IETF? OASIS?
  - Gather SAML communities list of topics that need addressing.
- Create a SAML Metadata Aggregation Best Practices Guide?
  - Not all SPs are the same!
- If R&E federations choose to audit each other
  - SAML Auditor's Framework