SMAPS document

Contents
[hide]

Abstract

This document presents a framework to assist the writers of SAML Metadata Publishing Policies or SAML Metadata Aggregation Practice Statements for participants within SAML based infrastructures, such as federations, identity providers, service providers and other communities of interest that wish to rely on SAML Metadata. In particular, the framework provides a comprehensive list of topics that potentially (at the writer's discretion) need to be covered in a SAML Metadata Publishing Policy or Aggregation Practice Statement.

Back to SMAPS page

Introduction

Background

Purpose

Scope

Definitions

This document makes use of the following defined terms:

SAML Metadata Publishing Policy (SMPP) - A named set of rules that indicates the applicability of an particular aggregation of SAML metadata to a particular community and/or class of application with common security requirements.

SAML Metadata Aggregation Practice Statement (SMAPS) - A statement of the practices that a SAML Aggegrator employs in aggregating the SAML metadata of a defined set of SAML entities and managing this aggregate over the life-cycle of its components.

SAML Metadata Aggregation Practice Statement Summary - A subset of the provisions of a complete SMAPS that is made public by a SAML Aggegrator.

SAML Metadata Aggegrator (SMA) -

Set of provisions - A collection of practice and/or policy statements, spanning a range of standard topics, for use in expressing a SMPP or SMAPS employing the approach described in this framework.

Concepts

SAML Metadata Publishing Policy

SAML Metadata Publishing Policy Examples

SAML Metadata Aggregation Practice Statement

Relationship Between SAML Publishing Policy and SAML Metadata Aggregation Practice Statement

Sets of Provisions

A set of provisions is a collection of practice and/or policy statements, spanning a range of standard topics for use in expressing a SMPP or SMAPS employing the approach described in this framework by covering the topic appearing in Section 5 below. They are also described in detail in Section 4 below.

A SMPP can be expressed as a single set of provisions.

A SMAPS can be expressed as a single set of provisions with each component addressing the requirements of one or more SMPP policies, or, alternatively, as an organized collection of sets of provisions.

This framework outlines the contents of a set of provisions, in terms of nine primary components, as follows:

1. Introduction
2. Publication and Repository
3. Identification and Authentication
4. SAML Metadata Life-Cycle Operational Requirements
5. Facilities, Management, and Operational Controls
6. Technical Security Controls
7. SAML Metadata Profiles
8. Compliance audit
9. Other Business and Legal Matters

Contents of a Set of Provisions

Introduction

This component identifies and introduces the set of provisions, and indicates the types of entities and applications for which the document (either the SMPP or the SMAPS being written) is targeted.

Overview

Document Name and Identification

SAML Metadata Participants

This subcomponent describes the identity or types of entities that fill the roles of participants in the aggegration and publishing of SAML metadata, namely:

- SAML entity.
- Registrar of the SAML entity.
- SAML metadata aggregator.
- Relying parties.
- Other participants.

SAML Metadata Usage

Policy Administration

Definitions and Acronyms

Publication and Repository Responsibilities

This component contains any applicable provisions regarding:

- An identification of the entity or entities that operate the SAML Aggegrator;
- The responsibility of a SAML Aggegrator to publish information regarding its practices, certificates or keys used to digitally sign the metadata aggregates, and the current status of such certificates or keys, which may include the responsibilities of making the CP or CPS publicly available using various mechanisms and of identifying components, subcomponents, and elements of such documents that exist but are not made publicly available, for instance, security controls, clearance procedures, or trade secret information due to their sensitivity;
- When information including metadata aggregates must be published and the frequency of publication; and
- Access control on published information objects including metadata aggregates.

Identification and Authentication

This component describes the procedures to identify the SAML entity and its attributes, the organization(s) that controls the SAML entity and the individual (s) who are the registrars that submit the metadata of the SAML entity to SAML Metadata Aggegrator. In addition this component defines the procedures for authenticating these identities and the criteria for SAML Metadata Aggegrator to accept the metadata of the SAML entity. It also describes how individuals can prove their relationship with the SAML entity and the organization(s) that controls the SAML entity to the SAML Metadata Aggegrator so that these individuals can update or revoke the metadata of the SAML entity. This component also addresses naming practices, including the recognition of trademark rights in certain names.

SAML Metadata Life-Cycle Operational Requirements

This component is used to specify the requirements imposed upon the SAML metadata aggregator(s), publishers, subscribers and other participants with respect to the life-cycle of the metadata.

Facility, Management, and Operational Controls

This component describes non-technical security controls (that is, physical, procedural, and personnel controls) used by the SAML Aggrgator to securely perform the functions of metadata signing key generation, authentication of SAML entities, metadata publication, updating and revocation, auditing, and archiving.

Technical Security Controls

This component is used to define the security measures taken by the SAML aggregator to protect its cryptographic signing keys and activation data (e.g., PINs, passwords, or manually-held key shares). This component may also be used to impose constraints on metadata publishing, SAML entities, and other participants to protect their private keys, activation data for their private keys, and critical security parameters. Secure key management is critical to ensure that all secret and private keys and activation data are protected and used only by authorized personnel.

This component also describes other technical security controls used by the SAML metadata aggregator to perform securely the functions of signing key(s) generation, SAML entity registrar authentication, metadata revocation, auditing, and archiving. Technical controls include life-cycle security controls (including software development environment security, trusted software development methodology) and operational security controls.

This component can also be used to define other technical security controls on metadata publishing, SAML entity registrars, subscribers, and other participants.

SAML Metadata Profiles

This component is used to specify the format of an aggregation of SAML metadata. This includes information on profiles, versions, and extensions used.

Compliance Audit and Other Assessment

This component addresses the following:

- The list of topics covered by the assessment and/or the assessment methodology used to perform the assessment;
- Frequency of compliance audit or other assessment for each entity that must be assessed pursuant to a SMPP or SMAPS, or the circumstances that will trigger an assessment; possibilities include an annual audit, pre-operational assessment as a condition of allowing an entity to be operational, or investigation following a possible or actual compromise of security.
- The identity and/or qualifications of the personnel performing the audit or other assessment.
- The relationship between the assessor and the entity being assessed, including the degree of independence of the assessor.
- Actions taken as a result of deficiencies found during the assessment; examples include a temporary suspension of operations until deficiencies are corrected, revocation of published SAML metadata, changes in personnel, triggering special investigations or more frequent subsequent compliance assessments, and claims for damages against the assessed entity.
- Who is entitled to see results of an assessment (e.g., assessed entity, other participants, the general public), who provides them (e.g., the assessor or the assessed entity), and how they are communicated.

Other Business and Legal Matters

This component covers general business and legal matters.

Fees

Financial Responsibility

Confidentiality of Business Information

Privacy of Personal Information

Intellectual Property Rights

Representations and Warranties

Disclaimers of Warranties

Limitations of Liability

Indemnities

Term and Termination

Individual notices and communications with participants

Amendments

Dispute Resolution Procedures

Governing Law

Compliance with Applicable Law

Miscellaneous Provisions

Other Provisions

Security Considerations

Outline of a Set of Provisions

Acknowledgements

References

Notes

List of Acronyms