Network Working Group	L. Johansson
Internet-Draft	NORDUNet
Intended status: Informational	April 14, 2011
Expires: October 16, 2011	

An IANA registry for SAML 2.0 Level of Assurance Context Classes
draft-johansson-loa-registry-01

Abstract

This document establishes an IANA registry for Level of Assurance Context Classes for SAML 2.0. The registry is intended to be used as an aid to discovering such LoA definitions.

Requirements Language

The key words "MUST", "MUST NOT", "REQUIRED", "SHALL", "SHALL NOT", "SHOULD", "SHOULD NOT", "RECOMMENDED", "MAY", and "OPTIONAL" in this document are to be interpreted as described in RFC 2119 *[RFC2119]*.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document establishes an IANA registry for Level of Assurance Context Profiles for SAML 2.0. Such objects are XML schema definitions that fulfil the requirements of sstc-saml-loa-authncontext-profile-draft-01 *[OASIS.sstc.saml-loa-authncontext-profile-draft-01]*. Quoting from this specification we find the following definition of the concept of level of assurance:

Many existing (and potential) SAML federation deployments have adopted a “levels of assurance” (or LOA) model for categorizing the wide variety of authentication methods into a small number of levels, typically based on some notion of the strength of the authentication. Federation members (service providers or “relying parties”) then decide which level of assurance is required to access specific protected resources, based on some assessment of “value” or “risk”.

Several so called trust frameworks and identity federations now exist, some of which define one or more LoAs. The purpose of this specification is to create an IANA registry where such LoA definitions can be discovered.

Although the registry will contain URIs that reference SAML Authentication Context Profiles other protocols MAY use such URIs to represent levels of assurance definitions without relying on their SAML XML definitions. Use of the registry by protocols other than SAML is encouraged.

2. Name of Registry

The name of the registry shall be "SAML 2.0 LoA Context Class", in plural "SAML LoA Context Classes". The term LoA is an abbreviation of Level of Assurance.

3. Registration Template

The following information MUST be provided with each registration:

URI: A URI referencing a SAML 2.0 LoA Context Class. This is the registry key.

Context Class: A valid XML schema definition for the SAML 2.0 LoA Context Class fulfilling the requirements of sstc-saml-loa-authncontext-profile-draft-01 *[OASIS.sstc.saml-loa-authncontext-profile-draft-01]*.

Informational URL: A URL containing auxilliary information. This URL MUST minimally reference contact information for the administrative authority of the level of assurance definition.

Note that it is not uncommon for a single XML Schema to contain definitions of multiple URIs. In that case the registration MUST be repeated for each URI. Since the registry key (the URI) is unique by design there is no need for namespace management for this registry.

4. Registration Policy

The registry is to be operated under the "Designated Expert Review" policy from RFC5226 *[RFC5226]* employing a pool of experts. IANA is kindly asked to do rough randomized load-balancing among the experts. The initial pool of expert and the review criteria are outlined below.

4.1. Reviewer Expectations

The of the IANA LoA Registry is that it contain bona fide SAML 2.0 LoA Context Class definitions while not presenting a very high bar for entry. Expert reviewers SHOULD NOT place undue value in any percieved or actual quality of the associated trust framework or federation and SHOULD only exclude such registrations that in the view of the experts do not represent bona fide attempts at defining an LoA.
The designated experts are also expected to verify that the registration is consistent and that the provided XML fulfills the requirements of sstc-saml-loa-authncontext-profile-draft-01 *[OASIS.sstc.saml-loa-authncontext-profile-draft-01]*.

4.2. Designated Experts Pool

TBD

5. Registry Semantics

The intended use for this registry is to serve as a basis for discovery of LoA definitions that might for instance be used by SAML management tools. Consumers of the registry MUST NOT treat it as a complete list of all existing LoA definitions and MUST provide a way for the user to provide additional LoA Context Class definitions by other means. It is not expected that all LoA definitions will be contained in this registry.
The presense of an entry in the registy MUST NOT be taken to imply any semantics beyond the review done by the expert reviewers as part of the registration process.

6. IANA Considerations

This document sets up a registry with IANA making the whole document a set of considerations for IANA.

7. Security Considerations

An implementor of MUST NOT treat the registry as a trust framework or federation and MUST NOT make any assumptions about the properties of any of the listed level of assurance URIs or their associated trust frameworks or federations based on their presense in the IANA registry.

8. Acknowledgements

Bob 'RL' Morgan, Scott Cantor, Lucy Lynch and John Bradley were involved in the initial discussions around this idea and contributed to the semantics of the registry.

9. Changes

Note to the RFC editor: This section should be removed before publication.

9.1. since -00

*Clarified the security considerations wrt the status of the IANA registry.

*Text in the introduction that explains that the registry can be used by other protocols than SAML and that this is encouraged.

10. References

[RFC2119]	Bradner, S., "Key words for use in RFCs to Indicate Requirement Levels", BCP 14, RFC 2119, March 1997.
[RFC5226]	

	Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.
[OASIS.sstc.saml-loa-authncontext-profile-draft-01]	Tiffany, E., Madsen, P. and S. Cantor, "Level of Assurance Authentication Context Profiles for SAML 2.0", July 2008.

Author's Address

Leif Johansson Johansson NORDUNet Tulegatan 11 Stockholm, Sweden
EMail: leifj@nordu.net