Network Working Group
Internet-Draft
Intended status: Informational
Expires: July 1, 2012

L. Johansson
NORDUNet

December 29, 2011

An IANA registry for Level of Assurance Profiles
draft-johansson-loa-registry-03

Abstract

This document establishes an IANA registry for Level of Assurance Profiles. The registry is intended to be used as an aid to discovering such LoA definitions in protocols that use an LoA concept, including SAML 2.0 and OpenID Connect.

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

This Internet-Draft is submitted in full conformance with the provisions of BCP 78 and BCP 79.

Internet-Drafts are working documents of the Internet Engineering Task Force (IETF). Note that other groups may also distribute working documents as Internet-Drafts. The list of current Internet-Drafts is at http://datatracker.ietf.org/drafts/current/.

Internet-Drafts are draft documents valid for a maximum of six months and may be updated, replaced, or obsoleted by other documents at any time. It is inappropriate to use Internet-Drafts as reference material or to cite them other than as "work in progress."

This Internet-Draft will expire on July 1, 2012.

Table of Contents

1. Introduction

This document establishes an IANA registry for Level of Assurance Profiles. Such profiles are used in various protocols, including SAML 2.0 and OpenID Connect. For SAML 2.0 the registry entries reference XML schema definitions that fulfil the requirements of sstc.saml-assurance-profile [OASIS.sstc.saml-assurance-profile]. For OpenID Connect the registry consists a controlled vocabulary for the iso29115level claim type. Quoting from sstc.saml-assurance-profile [OASIS.sstc.saml-assurance-profile] 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 Level of Assurance (LoA). The purpose of this specification is to create an IANA registry where such LoA definitions can be discovered. While the quote above references SAML explicitly the notion of a "level of assurance" has gained wide-spread acceptance and should be treated as a protocol-independent concept. The proposed IANA registry attempts to reflects this.

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 or OpenID Connect 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 Level of Assurance Profile 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-assurance-profile [OASIS.sstc.saml-assurance-profile]. The registry key (the URI) is the unique identifier for the Context Class.

Name: A string uniquely identifying the LoA for use in protocols where URIs are not appropriate.

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. Both the name and the URI must uniquely identify the LoA. The name is meant to be used in protocols where URIs are not appropriate.

The name must fulfill the following ABNF:

```
label = ( ALPHA / DIGIT )
name = label 1*( label / '-' / '.' / '_' )
```

The following ABNF productions represent reserved values and names matching any of these productions MUST NOT be present in any registration:

```
reserved = loa / al / num
loa = ( 'l' / 'L' ) ( 'o' / 'O' ) ( 'a' / 'A') *DIGIT
al = ( 'a' / 'A') ( 'l' / 'L') *DIGIT
num = *DIGIT
```

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 and also do an initial review of each submission to ensure that the name is unique within the registry.The initial pool of expert and the review criteria are outlined below.

4.1. Reviewer Expectations

The expectation of the IANA LoA Registry is that it contain bona fide Level of Assurance Profiles 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-assurance-profile [OASIS.sstc.saml-assurance-profile].

4.2. Designated Experts Pool

The initial pool of experts is (in no particular order):

- 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 protocol-specific (eg SAML 2.0 or OpenID Connect) 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 Level of Assurance Profile references 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. The various versions of the draft was socialized in the Kantara Federation Interoperability WG and in other parts of the identity community.

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.

9.2. since -01

- Allow for registration of short identifiers.

9.3. since -02

- Make the text less explicitly dependent on SAML.
- Include OpenID Connect reference.
- Corrected the SSTC reference
- Reserve numeric-only LoA names (eg '1')

10. Normative References

[OASIS.sstc.saml-assurance-profile] Morgan, RL., Madsen, PM., and S. Cantor, "SAML V2.0 Identity Assurance Profiles Version 1.0", November 2010.

[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.

Author's Address

Leif Johansson
NORDUNet
Tulegatan 11
Stockholm
Sweden

Email: leifj@nordu.net