Network Working Group
Internet-Draft
Intended status: Informational
Expires: August 21, 2012

L. Johansson
NORDUNet

February 18, 2012

An IANA registry for Level of Assurance (LoA) Profiles
draft-johansson-loa-registry-04

Abstract

This document establishes an IANA registry for Level of Assurance (LoA) 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.

Status of this Memo

Copyright Notice

Table of Contents

1. Introduction

This document establishes an IANA registry for Level of Assurance Profiles. One definition of a 'level of assurance' is given in RFC4949 [RFC4949] which also identifies the roots of such profiles in the NIST special publication series, in particular SP 800-63 [SP63]. 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.

1.1. 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 [RFC2119].

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. In addition the requester is expected to provide basic contact information and the name of the organization on behalf of which the LoA definition is registered.

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
```

The reason for excluding these productions is a desire to avoid a race to register overly generic LoA profiles under names like "AL1" or "LOA2".

3.1. Example Registration

1. Name of requester: J. Random User

2. E-mail address of requester: jrandom@example.com

3. Organization of requester: Random Trust Frameworks LLP

4. Requested registration:

URI http://foo.example.com/assurance/loa1

Name foo-loa-1

SAML 2.0 Context Class Definition

```
 <?xml version="1.0" encoding="UTF-8"?>
 <xs:schema
     targetNamespace="http://foo.example.com/assurance/loa1"
     xmlns:xs="http://www.w3.org/2001/XMLSchema"
     xmlns="http://foo.example.com/assurance/loa1"
     finalDefault="extension"
     blockDefault="substitution"
     version="2.0">
   <xs:redefine
      schemaLocation="saml-schema-authn-context-loa-profile.xsd">
       <xs:annotation>
           <xs:documentation>
               Class identifier:
                   http://foo.example.com/assurance/loa1
                   Defines Level 1 of FAF
           </xs:documentation>
       </xs:annotation>
       <xs:complexType name="GoverningAgreementRefType">
         <xs:complexContent>
           <xs:restriction base="GoverningAgreementRefType">
             <xs:attribute name="governingAgreementRef"
               type="xs:anyURI"
               fixed="http://foo.example.com/foo_assurance.pdf#section1"
               use="required"/>
             </xs:restriction>
         </xs:complexContent>
       </xs:complexType>
   </xs:redefine>
 </xs:schema>
```

3.2. Note on the Example

The example is borrowed from sstc.saml-assurance-profile [OASIS.sstc.saml-assurance-profile]

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.

Registrations that reference multiple LoAs in a consistent set of policies - for instance when a trust framework defines multiple levels of assurance - the registered LoA Name and URIs SHOULD be consistently named so as to be easily identified as belonging to the same set of registrations. For instance fruitLoA1,fruitLoA2 and fruitLoA3 is preferred over apple,pear and banana when these Names refer to a single set of policies defining 3 LoAs.

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].

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

RL 'Bob' 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')

9.4. since -03

- comments from PROTO writeup, AD and document shepherd
- remove initial list of reviewers - it will be decided by IESG
- example registration

10. References

10.1. 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.

10.2. Informative References

[RFC4949] Shirey, R., "Internet Security Glossary, Version 2", RFC 4949, August 2007.

[RFC5226] Narten, T. and H. Alvestrand, "Guidelines for Writing an IANA Considerations Section in RFCs", BCP 26, RFC 5226, May 2008.

[SP63] NIST, "Electronic Authentication Guideline, NIST Special Publication 800-63", June 2004.

Author's Address

Leif Johansson
NORDUNet
Tulegatan 11
Stockholm
Sweden

Email: leifj@nordu.net