Internet Engineering Task Force (IETF)
Request for Comments: 6711
Category: Informational
ISSN: 2070-1721

L. Johansson
NORDUNet

August 2012

# An IANA Registry for Level of Assurance (LoA) Profiles

## 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 Security Assertion Markup Language (SAML) 2.0 and OpenID Connect.

## Status of This Memo

This document is not an Internet Standards Track specification; it is published for informational purposes.

This document is a product of the Internet Engineering Task Force (IETF). It represents the consensus of the IETF community. It has received public review and has been approved for publication by the Internet Engineering Steering Group (IESG). Not all documents approved by the IESG are a candidate for any level of Internet Standard; see Section 2 of RFC 5741.

Information about the current status of this document, any errata, and how to provide feedback on it may be obtained at http://www.rfc-editor.org/info/rfc6711.

Table of Contents



## 1. Introduction

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

[SAML] provides 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".

Another definition of an "assurance level" is given in RFC 4949 [RFC4949], which also identifies the roots of such profiles in the NIST special publication series, in particular SP 800-63 [SP63]. Level of Assurance Profiles are used in various protocols, including the Security Assertion Markup Language (SAML) version 2.0 and OpenID Connect.

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. While the quote above references SAML, the notion of a level of assurance has gained widespread acceptance and should be treated as a protocol-independent concept. The newly created IANA registry attempts to reflect this.

Although the registry will contain URIs that reference SAML Authentication Context Profiles, other protocols may use such URIs to identify level of assurance definitions without relying on or transmitting their SAML XML definitions. Use of the registry by protocols other than SAML is encouraged.

For instance, OpenID Connect defines the standard claim 'acr' as a identifier that may reference a SAML Authentication Context Class even though OpenID Connect is not itself based on XML or SAML.

Protocol designers who want to reference the registry should be aware that registered LoAs may depend on assumptions that do not carry over to all protocols and that such assumptions may vary among the protocols for which the LoAs were originally registered.

## 2. Name of Registry

The name of the registry shall be "Level of Assurance (LoA) Profile", in plural "Level of Assurance (LoA) Profiles".

## 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 [SAML]. The registry key (the URI) is the unique identifier for the Context Class.

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

Informational URL: A URL containing auxiliary information. This URL must minimally reference contact information for the administrative authority of the level of assurance definition and must use either the http or https scheme.

Note that it is possible for a single SAML Authentication Context Class to contain definitions of multiple URIs. In that case, a separate registration is to be used for each URI. Both the name and the URI are to uniquely and unambiguously 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 is defined by the following ABNF (as defined in RFC 5234 [RFC5234]):

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

The elements defined by the following ABNF productions represent a set of reserved values for the name element and are not to be registered:

```
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. Email address of requester: jrandom@example.com

3. Organization of requester: Example Trust Frameworks LLP

4. Requested registration:

URI http://foo.example.com/assurance/loa-1

Name foo-loa-1

Informational URL https://foo.example.com/assurance/

SAML 2.0 Authentication Context Class Definition

```
<?xml version="1.0" encoding="UTF-8"?>
<xs:schema
    targetNamespace="http://foo.example.com/assurance/loa-1"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    xmlns="http://foo.example.com/assurance/loa-1"
    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/loa-1
                    Defines Level 1 of the Foo Assurance Framework
            </xs:documentation>
        </xs:annotation>
        <xs:complexType name="GoverningAgreementRefType">
          <xs:complexContent>
            <xs:restriction base="GoverningAgreementRefType">
              <xs:attribute name="governingAgreementRef"
                type="xs:anyURI"
                fixed="https://foo.example.com/assurance/"
                use="required"/>
              </xs:restriction>
          </xs:complexContent>
        </xs:complexType>
    </xs:redefine>
  </xs:schema>
```

### 3.2. Note on the Example

The example is borrowed (slightly modified) from [SAML]. The example should not be registered.

## 4. Registration Policy

The registry is to be operated under the "Expert Review" policy from RFC 5226 [RFC5226], employing a pool of experts. IANA will be kindly asked to do rough, randomized load-balancing among the experts and also to perform an initial review of each submission to ensure that the name and URI are unique within the registry. The review criteria are outlined below.

For 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 that they can be identified as belonging to the same set of registrations. For instance, fruitLoA1, fruitLoA2, and fruitLoA3 are preferred over apple, pear, and banana when these names refer to a single set of policies defining three LoAs.

### 4.1. Reviewer Expectations

The expectation of the IANA LoA Registry is that it will contain registrations of bona fide Level of Assurance Profiles while not presenting a very high bar for entry.

Expert reviewers are expected to verify that:

- the registration is consistent and that the provided XML fulfills the requirements of [SAML].
- the name element is clearly associated with the registered LoA Profile and is not a reserved value.
- the URI and name elements are not already registered.
- the Informational URL can be expected to be stable and permanent.

Note that multiple registrations may share a common Informational URL.

The reviewers should exclude registrations where the name does not unambiguously identify the LoA definition or where the name is a simple variation on one of the reserved names.

Expert reviewers are expected to allow registrations made in good faith that fulfill these requirements.

## 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 (e.g., SAML 2.0 or OpenID Connect) management tools.

Note that consumers of the registry, being implementations of [SAML], are expected to allow configuration of LoA URIs at system deployment time. If multiple sources of LoA URIs are permitted in addition to the registry (e.g., manual input), then it is important to avoid collisions with URIs found in the registry.

The presence of an entry in the registry does not imply any semantics or quality beyond that which results from the review done by the expert reviewer 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

The registry is not a federation or trust framework. Consumers of the registry are strongly advised to review the information about an LoA before relying on it.

## 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 document were socialized in the Kantara Federation Interoperability WG and in other parts of the identity community.

## 9. References

### 9.1. Normative References

[RFC5234] Crocker, D. and P. Overell, "Augmented BNF for Syntax Specifications: ABNF", STD 68, RFC 5234, January 2008.

[SAML] Morgan, RL., Madsen, PM., and S. Cantor, "SAML V2.0 Identity Assurance Profiles, Version 1.0", November 2010, <http://docs.oasis-open.org/security/saml/Post2.0/sstc-saml-assurance-profile.html>.

### 9.2. 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