Global Federated Identity and Privilege Management (GFIPM) Metadata 1.0 Encoding Rules for Transport via SAML 2.0

By: Global Justice Information Sharing Initiative (Global) Security Working Group

February 15, 2008

BJA

This project was supported by Grant No. 2005-NC-BX-K164 awarded by the Bureau of Justice Assistance, in collaboration with the U.S. Department of Justice's Global Justice Information Sharing Initiative. The Bureau of Justice Assistance is a component of the Office of Justice Programs, which also includes the Bureau of Justice Statistics, the National Institute of Justice, the Office of Juvenile Justice and Delinquency Prevention, and the Office for Victims of Crime. Points of view or opinions in this document are those of the author and do not represent the official position or policies of the U.S. Department of Justice.

Table of Contents

1. Introduction

The purpose of the GFIPM metadata is to provide a common semantic model and structure, as well as a common syntax, for the purpose of passing information about federated users and systems between federation participants—identity providers (IDPs) and service providers (SPs).

The GFIPM Metadata Assertion Framework cleanly separates the metadata's definition and fundamental structure (specified formally via XML types and properties) from the methods and techniques used to encode the metadata in any particular transport protocol such as SAML 2.0. Figure 1 provides a visual diagram of this framework and clearly illustrates this separation. The lowest layer of the framework, called the SAML Assertion Layer, is the only layer that deals with transport of metadata. Please see the associated *Global Federated Identity and Privilege Management (GFIPM) Metadata 1.0 Overview* document for more detail about this framework.

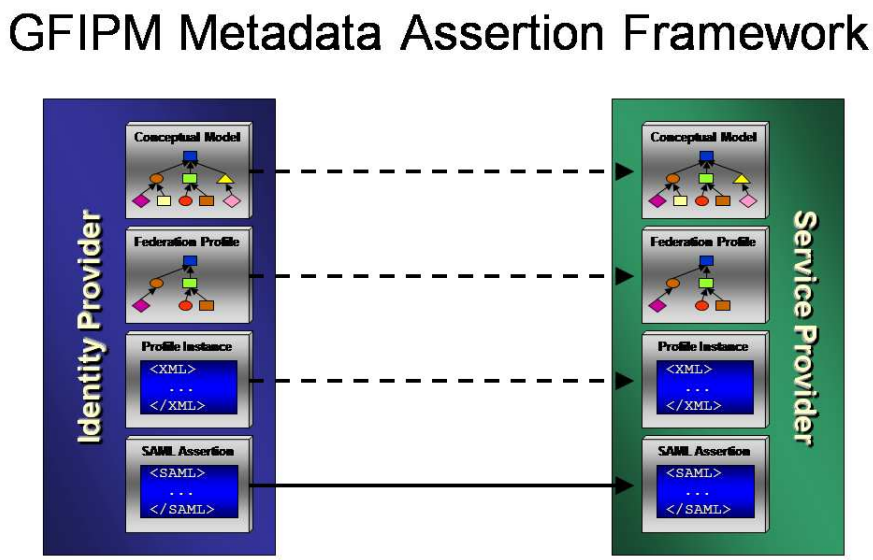

Figure 1: GFIPM Metadata Assertion Framework

For any given transport protocol, there are many potential ways to encode the GFIPM metadata for transport within it. Therefore, to enable any protocol used by IDPs and SPs to transport GFIPM metadata, it is necessary to define a set of encoding rules to facilitate interoperability among those IDPs and SPs. This document describes the encoding rules that must be used when encoding a GFIPM metadata assertion for transport within an SAML 2.0 environment.

Note that SAML 2.0 is only one of many possible transport mechanisms for GFIPM metadata. As the GFIPM metadata specification evolves and grows through use over time, additional encoding rules may be defined to address other metadata transport mechanisms as needed.

2. Encoding Rules

The following encoding rules must be obeyed when transporting a GFIPM metadata assertion via SAML from an identity provider (IDP) to a service provider (SP).

1. The IDP must send the GFIPM metadata assertion to the SP inside a SAML attribute statement.[1]

2. The SAML attribute statement must include an SAML attribute with the attribute name *GFIPMAssertion-1.0*. The name format of this attribute must be *urn:oasis:names:tc:SAML:2.0:attrname-format:basic*.

3. The value of the *GFIPMAssertion-1.0* attribute must be a base-64 encoded XML document that conforms to the GFIPM metadata schema as specified in the GFIPM metadata specification. This SAML attribute value must be of type *xs:string*.

3. Examples

Figures 2 and 3, respectively, illustrate a GFIPM assertion in its raw XML form and the corresponding SAML 2.0 assertion containing an attribute statement with the base-64 encoded GFIPM assertion in one of its attribute values. For additional examples of how GFIPM metadata should be encoded in SAML 2.0, please see the *SampleInstances\SAMLEncodings* directory in this metadata package.

[1] Within the SAML 2.0 standard, an attribute statement provides a flexible mechanism through which to specify an arbitrary number of attributes about a subject. An SAML attribute statement is typically tied to an SAML authentication statement via a common *Subject* identifier. The purpose of an authentication statement is to describe the details of an authentication event for a given subject. Through the combination of an authentication statement and an attribute statement, an SP can be sure that (1) the subject has authenticated with an IDP as stated in the authentication statement, and (2) the attributes associated with the subject are correct according to that IDP.

```
<?xml version="1.0" encoding="UTF-8"?>
<user:GFIPMUserAssertion
   xsi:schemaLocation="http://gfipm.net/assertion/user/1.0/...
schemas/conceptual/GFIPMUserAssertion.xsd"
   xmlns:ext="http://gfipm.net/assertion/extension/1.0"
   xmlns:user="http://gfipm.net/assertion/user/1.0"
   xmlns:j="http://niem.gov/niem/domains/jxdm/4.0"
   xmlns:nc="http://niem.gov/niem/niem-core/2.0"
   xmlns:n1="http://www.altova.com/samplexml/other-namespace"
   xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
   xmlns:ac="urn:oasis:names:tc:SAML:2.0:ac"
   xmlns:as="urn:oasis:names:tc:SAML:2.0:assertion">
  <user:UserIdentification>
  <user:User>
      <nc:PersonName>
        <nc:PersonGivenName>String</nc:PersonGivenName>
        <nc:PersonSurName>String</nc:PersonSurName>
      </nc:PersonName>
        <ext:FederationID>
          GFIPM:IDP:Organization:USER:LocalUsername
        </ext:FederationID>
    </user:User>
  </user:UserIdentification>
  <user:UserContactInformation>
    <ext:ContactInformation>
      <nc:ContactTelephoneNumber>
        <nc:FullTelephoneNumber>
          <nc:TelephoneNumberFullID>
            888-555-1234
          </nc:TelephoneNumberFullID>
        </nc:FullTelephoneNumber>
      </nc:ContactTelephoneNumber>
    </ext:ContactInformation>
  </user:UserContactInformation>
  <user:UserOrganizationalAffiliations>
    <user:UserEmploymentAssociation>
      <nc:Employer>
        <nc:EntityOrganization>
          <nc:OrganizationName>
            Justice / Law Enforcement Organization
          </nc:OrganizationName>
        </nc:EntityOrganization>
      </nc:Employer>
    </user:UserEmploymentAssociation>
  </user:UserOrganizationalAffiliations>
  <ext:ElectronicIdentification>
    <ext:ElectronicIdentity>
      <ext:IdentityProvider>
        <ext:IdentityProviderName>
          GFIPM:IDP:Organization
        </ext:IdentityProviderName>
      </ext:IdentityProvider>
    </ext:ElectronicIdentity>
  </ext:ElectronicIdentification>
</user:GFIPMUserAssertion>
```

Figure 2: GFIPM Assertion in Raw XML Form

```
<!-- Pure SAML 2.0 Assertion Envelope -->
<saml:Assertion ID="_c0594b43e28a2f94311d395d57d4ae5a"
  IssueInstant="2007-10-16T15:16:19.938Z" Version="2.0"
  xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion">
  <saml:Issuer
    Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">
    https://rhelidp.ref.gfipm.net/shibboleth
  </saml:Issuer>
  <saml:Subject>
    <saml:NameID
      Format="urn:oasis:names:tc:SAML:2.0:nameid-format:transient"
      NameQualifier="http://rhelidp.ref.gfipm.net/shib-idp/">
        _8ff677d9adccfa23242d46b10fd5a35a
    </saml:NameID>
    <saml:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData Address="130.207.204.222"
        InResponseTo="_30ee6ed689da8f1d13518a052d217be6"
        NotOnOrAfter="2007-10-16T15:21:19.938Z"
        Recipient="https://rhelsp.ref.gfipm.net/Shibboleth.sso/SAML2/POST" />
    </saml:SubjectConfirmation>
  </saml:Subject>
  <saml:Conditions NotBefore="2007-10-16T15:16:19.938Z"
    NotOnOrAfter="2007-10-16T15:21:19.938Z" />
  <saml:AuthnStatement AuthnInstant="2007-10-16T15:16:19.878Z"
    SessionNotOnOrAfter="2007-10-16T15:46:19.878Z">
    <saml:SubjectLocality Address="130.207.204.222"
      DNSName="130.207.204.222" />
    <saml:AuthnContext>
      <saml:AuthnContextDeclRef>
        urn:oasis:names:tc:SAML:2.0:ac:classes:unspecified
      </saml:AuthnContextDeclRef>
    </saml:AuthnContext>
  </saml:AuthnStatement>
  <saml:AttributeStatement>
    <saml:Attribute Name="GFIPMAssertion-1.0"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:unspecified">
      <saml:AttributeValue
        xmlns:xs="http://www.w3.org/2001/XMLSchema"
        xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
        xsi:type="xs:string">
PD94bWwgdmVyc2lvbj1cIjEuMFwiIGVuY29kaW5nPVwiVVRGLThcIj8+DQo8dXNlcjpHRklQTVVz
[Most of the base-64 encoded GFIPM metadata has been omitted for brevity.]
dHJvbmljSWRlbnRpZmljYXRpb24+DQo8L3VzZXI6R0ZJUE1Vc2VyQXNzZXJ0aW9uPg0K
      </saml:AttributeValue>
    </saml:Attribute>
  </saml:AttributeStatement>
</saml:Assertion>
```

Figure 3: SAML 2.0 Assertion With Base-64 Encoded GFIPM Metadata From Figure 2