Security Assertion Markup Language (SAML) 2.0 Metadata Profile for Backend Attribute Exchange (BAE) v2.0

Final Version 1.0.0

January 23, 2012

Acknowledgments

The authors of this document, the Identity, Credential and Access Management (ICAM) Architecture Working Group (AWG), would like to acknowledge the work done by DHS Science & Technology Directorate and DOD DMDC West.

Table of Contents

1 SAML 2.0 Metadata Profile for BAE

BAE Brokers MUST use metadata to exchange information regarding identifiers, binding support, endpoints, certificates and keys, and so forth. The use of [SAMLMeta] and [SAMLMeta-Ext] which is RECOMMENDED is profiled in this section.

A producer of metadata that adheres to this profile may be an actual participant (e.g. A BAE Broker) in a SAML (or other) profile, or an aggregator of metadata describing many such participants (e.g. A centralized metadata service that describes multiple BAE Brokers. In either case, the content of the metadata itself is independent of its source and MUST stand alone as a description of the requirements for securely communicating with the entity (or entities) described therein, to the extent that the constructs of the SAML V2.0 metadata specification [SAMLMeta] can express these requirements.

Subject to any constraints of the exchange mechanisms in use, a conforming metadata instance may be rooted by either an `<EntityDescriptor>` or `<EntitiesDescriptor>` element, which correspond to metadata descriptions for a single BAE Broker, or an aggregated set of BAE Brokers.

1.1 Single BAE Broker Metadata

A BAE Broker that uses SAML V2.0 metadata MUST include an `<EntityDescriptor>` element that satisfies the following rules:

- The `entityID` attribute MUST be the unique identifier is assigned to the BAE Broker (i.e. the Locale Identifier LI) by the BAE Federation Operator.
    - The format of the unique identifier `(entityID)` assigned to each Requester and Responder in a BAE environment MUST be the following:

      `urn:idmanagement.gov:icam:bae:v2:[LI]`

      where [LI] = Locale Identifier as defined in the “Section 2 – SAML 2.0 Profile of Locale Identifier (LI) for BAE” in the “SAML 2.0 Identifier and Protocol Profiles for BAE v2.0” document.
- It MUST have a `validUntil` attribute that reflects the metadata’s validity period.
- It MUST include a `<AttributeAuthorityDescriptor>` element with a `protocolSupportEnumeration` attribute with the value “`urn:oasis:names:tc:SAML:2.0:protocol`"
- It MUST include a valid `<ds:Signature>` enveloped within the `<EntityDescriptor>` element.

- It is RECOMMENDED that <Organization> be present and include either OrganizationName or OrganizationDisplayName.
- It is RECOMMENDED that the <ContactPerson> be present and include either EmailAddress or TelephoneNumber at a minimum.

  The <AttributeAuthorityDescriptor> element MUST include:

  - A <KeyDescriptor> element with an attribute use with value "signing" that contains the certificate expressed using the <ds:KeyInfo> element and used to verify messages digitally signed by the BAE Broker. The value of the CN portion of the Subject DN of this certificate MUST be the (entityID) of the BAE Broker.
  - A <KeyDescriptor> element with an attribute use with value "encryption" that contains the certificate expressed using the <ds:KeyInfo> element and used to encrypt messages to this BAE Broker. The value of the CN portion of the Subject DN of this certificate MUST be the (entityID) of the BAE Broker.
  - The <X509Certificate> element MUST contain the certificate in base-64 encoded format without the "---BEGIN CERTIFICATE---" and "---END CERTIFICATE---" elements.
  - The same certificate MUST be used for both digital signature and encryption.
  - One or Two <AttributeService> elements:
    1. The SAML 2.0 endpoint of the BAE MUST be described using a Binding attribute with a value of "urn:oasis:names:tc:SAML:2.0:bindings:SOAP" and a Location attribute with a value that is the URL of the BAE Broker's External BAE Service SAML endpoint
    2. The SPML 2.0 endpoint of the BAE MUST be described using a Binding attribute with a value of "urn:idmanagement.gov:icam:bae:v2:SPML:bindings:SOAP" and a Location attribute with a value that is the URL of the BAE Broker's External BAE Service SPML endpoint
    3. The Location Attribute for both SAML and SPML MAY point to the same endpoint if the implementation supports both SAML and SPML operations via the same URL
  - One or more <NameIDFormat> elements with valid supported values. Current supported values include:
    - urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-format:fasc-n
    - urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName

        - `urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-format:uuid`
    - One or more `<AttributeProfile>` elements with valid supported values. Current supported values include:
        - `urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:attribute:nameid-cleartext`
        - `urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:attribute:nameid-encrypted`
- The `<AttributeAuthorityDescriptor>` MAY include one or more `<saml:Attribute>` elements.
    - All attributes defined by a Federtion Operator's Attribute Contract (i.e. list of minimum required attributes in a Federation) MUST be adverstised in this section.
    - The BAE Broker, if it supports attributes beyond the Federtion Operator required Attribute Contract, MAY advertise additional attributes in this section.
    - The semantics of the attributes themselves are out of scope of this profile.

1.2 Aggregated BAE Broker Metadata

An entity wishing to aggregate the metadata descriptions of multiple BAE Brokers must root the conforming metadata instance in an `<EntitiesDescriptor>` element and must follow the following rules:

- It MUST include a valid `<ds:Signature>` enveloped within the `<EntitiesDescriptor>` element.

1.3 SPML and SAML 2.0 Metadata for BAE

The BAE architecture supports both a real-time request response mechanism via SAML as well as a "batch" mode with SPML. The location of the SPML endpoint for a BAE compliant Attribute Service can be advertised in the Metadata as noted above in Section [1.1].

SPML 2.0 directly supports exposure of metadata via the `listTargets` operation. Please refer to the "SPML 2.0 Profile for BAE v2.0" for more information.

1.4 Examples

1.4.1 Single BAE Broker Metadata Example

```
<?xml version="1.0" encoding="UTF-8"?>
<EntityDescriptor
   xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="orga-bae-metadata-0001"
   entityID="urn:idmanagement.gov:icam:bae:v2:7000:0000">
   <AttributeAuthorityDescriptor
          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <KeyDescriptor use="signing">
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>
MIIDQDCCAiigAwIBAgIBAjANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUQxEDAOBgNVBAoTB0pIVS1BUEwxGDAWBgNVBAsUD0FQTF9HSUdf
VEVTVEJFRDEXMBUGA1UEAxQOR0lHX1RFU1RCRURfQ0EwHhcNMDkxMjA5MDE1OTE4
                        </ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </KeyDescriptor>
            <KeyDescriptor use="encryption">
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>
MIIDQDCCAiigAwIBAgIBAjANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUQxEDAOBgNVBAoTB0pIVS1BUEwxGDAWBgNVBAsUD0FQTF9HSUdf
VEVTVEJFRDEXMBUGA1UEAxQOR0lHX1RFU1RCRURfQ0EwHhcNMDkxMjA5MDE1OTE4
                        </ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </KeyDescriptor>
            <AttributeService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
                Location="https://orga.domain/ExternalBAEService/v2.0/PROD" />
          <AttributeService
              Binding="urn:idmanagement.gov:icam:bae:v2:SPML:bindings:SOAP"
              Location="https://orga.domain/ExternalBAEService/v2.0/PROD" />
            <NameIDFormat>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-
format:fasc-n</NameIDFormat>
            <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName</NameIDFormat>

<AttributeProfile>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:att
ribute:nameid-cleartext</AttributeProfile>

<AttributeProfile>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:att
ribute:nameid-encrypted</AttributeProfile>
            <saml:Attribute
               NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
               Name="urn:idmanagement.gov:icam:attribute:v1:givenName">
            </saml:Attribute>
            <saml:Attribute
               NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
               Name="urn:idmanagement.gov:icam:attribute:v1:sn">
            </saml:Attribute>
   </AttributeAuthorityDescriptor>
   <Organization>
          <OrganizationName xml:lang="en">OrgA</OrganizationName>
```

```
   </Organization>
   <ContactPerson>
          <GivenName>First</GivenName>
          <SurName>Last</SurName>
          <EmailAddress>first.last@orga.com</EmailAddress>
          <TelephoneNumber>111-222-3333</TelephoneNumber>
   </ContactPerson>
</EntityDescriptor>
```

1.4.2 Aggregated BAE Broker Metadata Example

```
<?xml version="1.0" encoding="UTF-8"?>
<EntitiesDescriptor
   xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="icam-bae-metadata-0001"
   validUntil="2009-07-17T22:26:50Z"
   Name="urn:idmanagement.gov:icam:bae:v2:metadata:v1">

   <ds:Signature>...</ds:Signature>

   <EntityDescriptor
   xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="orga-bae-metadata-0001"
   entityID="urn:idmanagement.gov:icam:bae:v2:7000:0000">
   <AttributeAuthorityDescriptor
          protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
            <KeyDescriptor use="signing">
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>
MIIDQDCCAiigAwIBAgIBAjANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUQxEDAOBgNVBAoTB0pIVS1BUEwxGDAWBgNVBAsUD0FQTF9HSUdf
VEVTVEJFRDEXMBUGA1UEAxQOR0lHX1RFU1RCRURfQ0EwHhcNMDkxMjA5MDE1OTE4
                        </ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </KeyDescriptor>
            <KeyDescriptor use="encryption">
                <ds:KeyInfo>
                    <ds:X509Data>
                        <ds:X509Certificate>
MIIDQDCCAiigAwIBAgIBAjANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUQxEDAOBgNVBAoTB0pIVS1BUEwxGDAWBgNVBAsUD0FQTF9HSUdf
VEVTVEJFRDEXMBUGA1UEAxQOR0lHX1RFU1RCRURfQ0EwHhcNMDkxMjA5MDE1OTE4
                        </ds:X509Certificate>
                    </ds:X509Data>
                </ds:KeyInfo>
            </KeyDescriptor>
            <AttributeService
                Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
                Location="https://orga.domain/ExternalBAEService/v2.0/PROD" />
          <AttributeService
              Binding="urn:idmanagement.gov:icam:bae:v2:SPML:bindings:SOAP"
              Location="https://orga.domain/ExternalBAEService/v2.0/PROD" />
            <NameIDFormat>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-
format:fasc-n</NameIDFormat>
```

```
          <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:X509SubjectName</NameIDFormat>

<AttributeProfile>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:att
ribute:nameid-cleartext</AttributeProfile>

<AttributeProfile>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:att
ribute:nameid-encrypted</AttributeProfile>
          <saml:Attribute
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
             Name="urn:idmanagement.gov:icam:attribute:v1:givenName">
          </saml:Attribute>
          <saml:Attribute
             NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
             Name="urn:idmanagement.gov:icam:attribute:v1:sn">
          </saml:Attribute>
   </AttributeAuthorityDescriptor>
   <Organization>
         <OrganizationName xml:lang="en">OrgA</OrganizationName>
   </Organization>
   <ContactPerson>
         <GivenName>First</GivenName>
         <SurName>Last</SurName>
         <EmailAddress>first.last@orga.com</EmailAddress>
         <TelephoneNumber>111-222-3333</TelephoneNumber>
   </ContactPerson>
   </EntityDescriptor>

    <EntityDescriptor
   xmlns="urn:oasis:names:tc:SAML:2.0:metadata"
   xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
   xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"
   ID="orgb-bae-metadata-0001"
   entityID="urn:idmanagement.gov:icam:bae:v2:2100:1700">
   <AttributeAuthorityDescriptor
         protocolSupportEnumeration="urn:oasis:names:tc:SAML:2.0:protocol">
          <KeyDescriptor use="signing">
              <ds:KeyInfo>
                  <ds:X509Data>
                      <ds:X509Certificate>
VEVTVEJFRDEXMBUGA1UEAxQOR0lHX1RFU1RCRURfQ0EwHhcNMDkxMjA5MDE1OTE4
MIIDQDCCAiigAwIBAgIBAjANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUQxEDAOBgNVBAoTB0pIVS1BUEwxGDAWBgNVBAsUD0FQTF9HSUdf
                      </ds:X509Certificate>
                  </ds:X509Data>
              </ds:KeyInfo>
          </KeyDescriptor>
          <KeyDescriptor use="encryption">
              <ds:KeyInfo>
                  <ds:X509Data>
                      <ds:X509Certificate>
VEVTVEJFRDEXMBUGA1UEAxQOR0lHX1RFU1RCRURfQ0EwHhcNMDkxMjA5MDE1OTE4
MIIDQDCCAiigAwIBAgIBAjANBgkqhkiG9w0BAQUFADBfMQswCQYDVQQGEwJVUzEL
MAkGA1UECBMCTUQxEDAOBgNVBAoTB0pIVS1BUEwxGDAWBgNVBAsUD0FQTF9HSUdf
                      </ds:X509Certificate>
                  </ds:X509Data>
              </ds:KeyInfo>
          </KeyDescriptor>
          <AttributeService
              Binding="urn:oasis:names:tc:SAML:2.0:bindings:SOAP"
              Location="https://orgb.domain/ExternalBAEService/v2.0/PROD" />
         <AttributeService
```

```
               Binding="urn:idmanagement.gov:icam:bae:v2:SPML:bindings:SOAP"
               Location="https://orgb.domain/ExternalBAEService/v2.0/PROD" />
            <NameIDFormat>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:nameid-
format:uuid</NameIDFormat>
            <NameIDFormat>urn:oasis:names:tc:SAML:1.1:nameid-
format:emailAddress</NameIDFormat>

<AttributeProfile>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:att
ribute:nameid-cleartext</AttributeProfile>

<AttributeProfile>urn:idmanagement.gov:icam:bae:v2:SAML:2.0:profiles:query:att
ribute:nameid-encrypted</AttributeProfile>
            <saml:Attribute
               NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
               Name="urn:idmanagement.gov:icam:attribute:v1:givenName">
            </saml:Attribute>
            <saml:Attribute
               NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"
               Name="urn:idmanagement.gov:icam:attribute:v1:sn">
            </saml:Attribute>
   </AttributeAuthorityDescriptor>
   <Organization>
          <OrganizationName xml:lang="en">OrgB</OrganizationName>
   </Organization>
   <ContactPerson>
          <GivenName>First</GivenName>
          <SurName>Last</SurName>
          <EmailAddress>first.last@orgb.com</EmailAddress>
          <TelephoneNumber>123-222-3333</TelephoneNumber>
   </ContactPerson>
   </EntityDescriptor>

</EntitiesDescriptor>
```

2 Security and Privacy Considerations

The motivation for this deployment profile is to specify a secure means of representing the metadata that is needed by a BAE Broker to bootstrap its entry into a BAE Attribute Federation as well as to advertise its capabilities to the Federation.

2.1 Metadata Security

As noted in [SAMLMIOP]:

> “Metadata becomes a critical tool for the revocation of compromised sites and keys, and all of the standard practices in the use of tools like CRLs become relevant to the consumption of metadata. The specification has the mechanisms to address these issues, but they have to be used. Specifically, metadata obtained via an insecure transport should be both signed, and should expire; so that consumers are forced to refresh it often enough to limit the damage from compromised information. Either the validUntil or cacheDuration attribute may be appropriate to mitigate this threat, depending on the exchange mechanism.
>
> In addition, distributing signed metadata without an expiration over an untrusted channel (e.g., posting it on a public web site) creates an exposure. An attacker can corrupt the channel and substitute an old metadata file containing a compromised key and proceed to use that key together with other attacks to impersonate a site. Repeatedly expiring (using a validUntil attribute) and reissuing the metadata limits the window of exposure, just as a CRL does. Note that the cacheDuration attribute does not prevent this attack"

3 Implementation Guidance

3.1 BAE Metadata Distribution

The BAE environment is dependent on the usage of metadata for bootstrapping both the initial setup of the environment as well as advertising capabilities that are associated with a BAE Broker. The mechanism that is used to distribute the metadata could be as simple as out of band distribution of the metadata file to a repository based scheme.

The actual mechanics of the metadata distribution are out of scope of this profile and will be defined for FICAM as part of the BAE Governance document (Communities outside FICAM may choose to implement their own mechanisms for metadata distribution).