Application Note: Web Services Addressing Endpoint References and Identity

September 7, 2007

Authors

Jan Alexander, Microsoft

Giovanni Della-Libera, Microsoft
Martin Gudgin, Microsoft

Kirill Gavrylyuk, Microsoft

Tomasz Janczuk, Microsoft

Michael McIntosh, IBM

Anthony Nadalin, IBM

Bruce Rich, IBM

Doug Walter, Microsoft

Copyright Notice

Abstract

This note provides a mechanism to describe security-verifiable identity for endpoints by leveraging extensibility of the WS-Addressing specification. Specifically, this note introduces XML [XML 1.0, XML Namespaces] elements for identity that can be provided as part of WS-Addressing Endpoint Reference. This mechanism enables messaging systems to support multiple trust models across networks that include processing nodes such as endpoint managers, firewalls, and gateways in a transport-neutral manner.

Acknowledgments

None

Table of Contents

1. Introduction

1.2. Notational Conventions

1.3. XML Namespaces

1.4. Schema and WSDL Files

1.5. Terminology

2 Endpoint Reference [Identity] Property

2.1 Default Value

3 Identity Representation

3.1 DNS name

3.2 Service Principal Name

3.3 User Principal Name

3.4 KeyInfo

3.4.1. Example specifying an RSA Public Key

3.4.2. Example specifying an X509 Certificate

5 Security Considerations

6 References

1. Introduction

A Web service endpoint is a (referenceable) entity, processor, or resource where Web service messages can be targeted. WS-Addressing's Endpoint references convey the information needed to reference a Web service endpoint, and may be used in several different ways: endpoint references are suitable for conveying the information needed to access a Web service endpoint, but are also used to provide addresses for individual messages sent to and from Web services.

Web Services Addressing Identity extends WS-Addressing's *endpoint reference* by providing *identity* information about the endpoint that can be verified through a variety

of security means. These means include transport security technologies like https or the wealth of WS-Security specifications.

Here is an example:

```
<wsa:EndpointReference>
    <wsa:Address>http://wh1.fabrikam123.com/Purchasing</wsa:Address>
    <wsid:Identity>
      <wsid:DnsClaim>fabrikam123.com</wsid:DnsClaim>
    </wsid:Identity>
</wsa:EndpointReference>
```

1.2. Notational Conventions

The keywords "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.

Namespace URIs of the general form "some-URI" represents some application-dependent or context-dependent URI as defined in RFC3986.

1.3. XML Namespaces

The following namespaces are used in this document. The choice of any namespace prefix is arbitrary.

Prefix	Namespace
wsa	http://www.w3.org/2005/08/addressing
wsid	http://schemas.xmlsoap.org/ws/2006/02/addressingidentity
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
ds	http://www.w3.org/2000/09/xmldsig#

1.4. Schema and WSDL Files

The schemas can be located at:

```
http://schemas.xmlsoap.org/ws/2006/02/addressingidentity
```

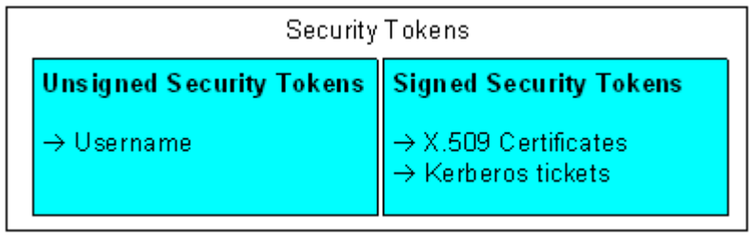
1.5. Terminology

The following definitions establish the terminology and usage in this document.

Trust Identity – A *trust identity* is a verifiable claim about a principal (e.g. name, identity, key, group, privilege, capability, etc).

Security Token – A *security token* represents a collection of claims.

Signed Security Token – A *signed security token* is a security token that is asserted and cryptographically endorsed by a specific authority (e.g. an X.509 certificate or a Kerberos ticket).



Proof-of-Possession – The *proof-of-possession* information is data that is used in a proof process to demonstrate the sender's knowledge of information that SHOULD only be known to the claiming sender of a security token.

Integrity – *Integrity* is the process by which it is guaranteed that information is not modified in transit.

Confidentiality – *Confidentiality* is the process by which data is protected such that only authorized actors or security token owners can view the data

Digest – A *digest* is a cryptographic checksum of an octet stream.

Signature - A *signature* is a cryptographic binding of a proof-of-possession and a digest. This covers both symmetric key-based and public key-based signatures. Consequently, non-repudiation is not always achieved.

2 Endpoint Reference [Identity] Property

This note adds [Identity] property to Endpoint Reference [WS-Addressing] and leverages extensibility of the `wsa:EndpointReferenceType` schema to include a `wsid: Identity` element as described below:

```
<wsa:EndpointReference>
  ...
  <wsid:Identity>...Claim...</wsid:Identity>
  ...
</wsa:EndpointReference>
```

The Identity element inside EndpointReference can hold any of the claims defined in section 3 or section 4 below.

2.1 Default Value

If an EndpointReference does not contain an Identity element, dns claim can be assumed by extracting the hostname from the Address URI.

If the URI does not have a hostname, it does not have an implicit identity value and can not be verified by the mechanisms defined in this document.

3 Identity Representation

3.1 DNS name

The DNS claim implies that the remote principal is trusted to speak for that DNS name. For instance the DNS claim could specify “fabrikam.com”. When challenged, the endpoint contacted must be able to prove its right to speak for “fabrikam.com”. The service could prove its right by proving ownership of a certificate containing a reference

to fabrikam.com and signed by a trusted Certificate Authority (eg. VeriSign). The following element of type xs:string can be used to represent DNS claim within wsid:Identity element.

```
<wsid:DnsClaim>fabrikam.com</wsid:DnsClaim>
```

3.2 Service Principal Name

The SPN claim implies that the remote principal is trusted to speak for that SPN, a mechanism common in intranet domains. Its format is <serviceClass>/<host>. For example, the SPN for a generic service running on "server1.fabrikam.com" would be "host/server1.fabrikam.com". The client could confidentially speak to the service and verify replies back from the service by obtaining a Kerberos ticket from the realm's domain controller. The following element of type xs:string can be used to represent SPN claim within wsid:Identity element.

```
<wsid:SpnClaim>host/hrweb</wsid:SpnClaim>
```

3.3 User Principal Name

The UPN claim implies that the remote principal is a particular user in a domain. Its format is: <user>@<domain>. For example, the UPN for a user "someone" at a domain "example.com" would be "someone@example.com". A service could prove its UPN by providing the password for the user associated with "someone@example.com". The following element of type xs:string can be used to represent UPN claim within wsid:Identity element.

```
<wsid:UpnClaim>someone@example.com</wsid:UpnClaim>
```

3.4 KeyInfo

This identity value is similar to the previous three but rather than describing an attribute of the target, this mechanism describes a reference (embedded or external) to keying material associated with the target. This allows confirmation of the target trust identity through encryption. These values can also be used to compare authenticated identities similar to the basic trust identity values by comparing the hash of the specified trust identity value with a hash of the authenticated identity of the service. The ds:KeyInfo element defined in [XML Signature] can be used

```
<ds:KeyInfo>...</ds:KeyInfo>
```

3.4.1. Example specifying an RSA Public Key

The PublicKey claim states the public key of the remote principal. A service could prove its ownership of the key by signing some data with the private key.

```
<wsid:Identity>
  <ds:KeyInfo>
```

```
    <ds:RSAKeyValue>
      <ds:Modulus>xA7SEU+e0yQH5...</ds:Modulus>
      <ds:Exponent>AQAB</ds:Exponent>
    </ds:RSAKeyValue>
  </ds:KeyInfo>
</wsid:Identity>
```

3.4.2. Example specifying an X509 Certificate

This example shows a certificate of the remote principal being used as the identity value.

```
<wsid:Identity>
  <ds:KeyInfo>
    <ds:X509Data>
      <ds:X509Certificate>MIICXTCCA...</ds:X509Certificate>
    </ds:X509Data>
  </ds:KeyInfo>
</wsid:Identity>
```

3.5 Security Token

A security token can be an identity value representing claims about the identity of an endpoint. E.g.

```
<wsid:Identity>
      <wsse:BinarySecurityToken ValueType="...#X509v3">
            <!--base64 encoded value of the X509 certificate-->
      </wsse:BinarySecurityToken>
</wsid:Identity>
```

3.6 Security Token Reference

Similarly to ds:KeyInfo, wsse:SecurityTokenReference element can be used within wsid:Identity element to reference a token representing collection of claims about the identity of an endpoint. E.g.

```
<wsid:Identity>
      <wsse:SecurityTokenReference>
           <wsse:KeyIdentifier ValueType="...#ThumbprintSHA1">
                <!-- thumbprint of the X509 certificate  -->
           </wsse:KeyIdentifier>
      </wsse:SecurityTokenReference>
</wsid:Identity>
```

5 Security Considerations

It is recommended that Endpoint Reference elements be signed to prevent tampering.

Endpoint Reference should not be accepted unless it is signed and have an associated security token to specify the signer has the right to "speak for" the endpoint. That is, the relying party should not use an endpoint reference unless the endpoint reference is signed and presented with sufficient credentials to pass the relying parties acceptance criteria.

It is recommended that an endpoint reference be encrypted when it contains claims and other sensitive information.

When included in a SOAP message, endpoint references are recommended to be protected using the mechanisms described in WS-Security [WS-Security]

6 References

[KEYWORDS]
S. Bradner, "Key words for use in RFCs to Indicate Requirement Levels," RFC 2119, Harvard University, March 1997

[URI]
T. Berners-Lee, R. Fielding, L. Masinter, "Uniform Resource Identifiers (URI): Generic Syntax", RFC 3986, MIT/LCS, Day Software, Adobe Systems, January 2005.

[WS-Addressing]
W3C Recommendation, "Web Service Addressing (WS-Addressing)", 9 May 2006.

[XML-Signature]
W3C Recommendation, "XML-Signature Syntax and Processing", 12 February 2002.

[WS-Security]
OASIS, " Web Services Security: SOAP Message Security", March 2004.