Secure Addressing Profile 1.0

Status of This Document

This document provides a recommendation to the Grid community on how to bind WS-SecurityPolicy policy documents within WS-Addressing endpoint references, and how such endpoint references can be made to be tamper-evident. This profile describes precisely the requirements placed on the structure and handling of such endpoint references to ensure interoperability. Distribution is unlimited.

ABSTRACT

The *WS-Addressing 1.0 – Core* [WS-Addressing] specification is often used to address Web Service resources using endpoint reference (EPR) data structures. The WS-Addressing definition of the EPR describes the encapsulation of the network protocol and endpoint information for a given resource, but does not specifically indicate how the EPR can also be used to convey the secure-communication mechanisms (and ancillary security tokens) required by that resource. Such security requirements can be described using *WS-Security Policy 1.2* policy documents. This profile document normatively refines the *WS-Addressing 1.0 – Core* specification in order to facilitate the inclusion of such *WS-SecurityPolicy* assertions within WS-Addressing endpoint references.

It is often the case that WS-Addressing EPRs may be stored and exchanged by any number of intermediaries (such as directory services) before being consumed for actual communication. With this in mind, a particular interaction scenario may require guarantees of trust regarding the identity of the minter and the integrity of the EPR. This document also normatively describes how XML-Signature is used provide such guarantees.

CONTENTS

1 INTRODUCTION

This document defines the *Secure Addressing Profile 1.0* (hereafter, "the Profile"), a set of conformance statements that facilitate the discovery of interoperability requirements of Web service resources. The term *resource* is used within the context of this document to connote any logical message-processing entity.

Normative profiles are useful tools for understanding and defining the interactions amongst existing Web services specifications in order to achieve interoperability. They are particularly important within the context of secure communication: common treatment of Web services security and addressing specifications (e.g., SSL/TLS [TLS 1.0], WS-Security [WS-S] and related token profiles, XML-Encryption [XML-Enc], XML-Signature [XML-DigSig], WS-Addressing [WS-A Core], etc.) is crucial for real-world interoperability.

More specifically, this profile refines the *WS-Addressing 1.0 – Core* specification in order to provide a means for advertising and discovering secure communication requirements using WS-Addressing endpoint references (EPRs). The EPR data structure is a useful construct because it provides an "invocation context": the necessary information required by a client to establish meaningful communication with a resource exposed by a Web service endpoint. The EPR is an important data-structure that is incorporated into many Web service interfaces, particularly those adopted into and developed by the OGF. In many cases, these service interfaces follow a "factory" design pattern in which one Web service endpoint is used to dynamically create and service many stateful resources, such as job activities or logical data files.

Unfortunately the core EPR definition is not sufficient to describe a complete invocation context for a Web service resource that has been configured to require particular secure communication requirements (i.e., authentication, integrity, and confidentiality). As specified by WS-Addressing, the EPR does not provide a normative approach for advertising any resource-specific secure communication requirements, actions, or the security tokens that would be needed by a client. This Profile remedies this deficiency by describing the mechanism by which WS-SecurityPolicy security policies should be included within an EPR to describe such communication requirements of the referenced resource.

The *WS-SecurityPolicy 1.2* [WS-SecurityPolicy] specification defines a base set of assertions that describe how Web services messages are to be secured. It is an extension of the *Web Services Policy 1.5 – Framework* [WS-Policy], which is a flexible grammar for expressing capabilities, requirements, and general characteristics of Web services-based entities. WS-SecurityPolicy provides a flexible, extensible approach for defining token requirements, cryptographic algorithms, and mechanisms (both at the transport and message levels).

The *Web Services Policy 1.5 - Attachment* [WS-PolicyAttachment] specification defines mechanisms for associating policies with subjects for which they apply. Specifically, it profiles the use of these mechanisms for associating WS-Policy with WSDL and UDDI descriptions. This Profile extends the WS-PolicyAttachment by describing how to specify WS-SecurityPolicy policy alternatives within the extensible metadata section of a WS-Addressing endpoint reference. The policy subjects of such security policies within an EPR are WS-Addressing actions upon the referenced endpoint. These policy alternatives describe the security mechanisms expected by the referenced endpoint for the specified actions as well as provide any security tokens required by those mechanisms.

In addition to the WS-Addressing extensions designed to advertise secure communication requirements, this document also profiles the XML digital signature of the EPR document to ensure trust of the minter and to deter tampering.

By itself, this document is not sufficient to guarantee the interoperability of all compliant Web service clients and resources. Rather, the Profile adopts the view that specific secure communication requirements may vary between communities of resource providers and consumers. The intent is for applications and communities to self-select such requirements that

are appropriate and then leverage this Profile to achieve interoperability between its participants (and/or cleanly discover where interoperability is not possible).

The remainder of this profile is organized as follows. Section 2, "Document Conventions," describes notational conventions utilized by the Profile. Section 3, "Profile Conformance," explains what it means to be conformant to the Profile. Section 4 defines additional terminology. Section 5 describes the mechanism by which policy documents are conveyed within endpoint references. Section 6 profiles the digital signature of an endpoint reference. Note that there is no relationship between the section numbers in this document and those in the referenced profiles and specifications. Section 7 presents an example EPR conveying the security requirements of an Web service resource.

2 DOCUMENT CONVENTIONS

This Profile is a *Recommended Profile as Proposed Recommendation,* as defined in the OGSA Profile Definition [OGSA Profile Definition]. Additional document conventions of the Profile are defined normatively in *WS-I Basic Profile 1.1* [WS-I BP], and are briefly summarized below.

2.1 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 RFC-2119 [RFC2119].

Normative statements of requirements in the Profile (i.e., those impacting conformance, as outlined in Section 3, “Conformance Requirements") are presented in the following manner:

Rnnnn Statement text here.

where "*nnnn*" is replaced by a number that is unique among the requirements in the Profile, thereby forming a unique requirement identifier.

Extensibility points in underlying specifications are presented in a similar manner:

Ennnn Extensibility Point Name - Description

where "*nnnn*" is replaced by a number that is unique among the extensibility points in the Profile.

This specification uses a number of namespace prefixes throughout; their associated URIs are listed in the table below:

Table 1 Namespaces used by Secure Addressing Profile 1.0

Prefix	Namespace	Specification(s)
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd	[WS-S]
ds	http://www.w3.org/2000/09/xmldsig#	[XML-DigSig]
wsu	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-utility-1.0.xsd	[WS-S]
wsa	http://www.w3.org/2005/08/addressing	[WS-Addressing]
wsp	http://schemas.xmlsoap.org/ws/2004/09/policy	[WS-Policy], [WS-PolicyAttachment]
sp	http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702	[WS-SecurityPolicy]

wsdl	http://schemas.xmlsoap.org/wsdl	[WSDL]
secaddr	http://www.ogf.org/ogsa/2007/05/secure-addressing	This document

2.2 Security Considerations

In addition to interoperability requirements (which are made in *Rnnnn* statements and intended to improve interoperability), the Profile makes a number of security considerations intended to improve security. These Security Considerations are presented as follows:

Cnnnn Statement text here.

where "*nnnn*" is replaced by a number that is unique among the security considerations in the Profile, thereby forming a unique security consideration identifier. Each security consideration contains a *SHOULD* or a *MAY* to highlight exactly what is being considered; however, these considerations are informational only and are non-normative.

2.3 Profile Identification and Versioning

This document is identified by a name (in this case, *Secure Addressing*) and a version number (here, 1.0). Together, they identify a particular profile instance. Version numbers are composed of a major and minor portion, in the form "major.minor". Version numbers indicate profile instance precedence: higher version numbers indicate a more recent instance that supersedes earlier instances.

3 PROFILE CONFORMANCE

Conformance to the Profile is defined by adherence to the set of requirements defined for a specific target, within the scope of the Profile. This section explains these terms and describes how conformance is defined and used.

3.1 Conformance Requirements

Requirements state the criteria for conformance to the Profile. They typically refer to an existing specification and embody refinements, amplifications, interpretations and clarifications to it in order to improve interoperability. All requirements in the Profile are considered normative, and those in the specifications it references that are in-scope (see Section 3.3, “Conformance Scope") should likewise be considered normative.

Each requirement is individually identified (e.g., R9999) for convenience.

For example;

R9999 Any *WIDGET* SHOULD be round in shape.

This requirement is identified by "R9999", applies to the target WIDGET (see below), and places a conditional requirement upon widgets; i.e., although this requirement must be met to maintain conformance in most cases, there are some situations where there may be valid reasons for it not being met (which are explained in the requirement itself, or in its accompanying text).

3.2 Conformance Targets

Conformance targets identify what artifacts (e.g., SOAP messages, XML elements, etc.) or parties (e.g., SOAP processors, end users, etc.) that the requirements stated within this Profile apply to.

This allows for the definition of conformance in different contexts, to assure unambiguous interpretation of the applicability of requirements, and to allow conformance testing of the specific artifacts and parties defined below (e.g., *POLICY, POLICY_ALTERNATIVE*).

The Profile discusses elements defined within the *WS-SecurityPolicy 1.2* [WS-SecurityPolicy] profile. The following conformance targets are inherited from those in the WS-SecurityPolicy:

- *POLICY* - A collection of *POLICY_ALTERNATIVEs*. A <wsp:Policy> element is used in conjunction with its child <wsp:ExactlyOne> element to indicate a policy expression as a union of mutually-exclusive *POLICY_ALTERNATIVEs*. If there is only one logical *POLICY_ALTERNATIVE*, the compact policy form can be used in which the requisite *POLICY_ASSERTIONs* are placed as direct children of the <wsp:Policy> element and the <wsp:ExactlyOne> and <wsp:All> elements are omitted.
- *POLICY_ALTERNATIVE* - A child element of <wsp:ExactlyOne> that is to be treated as a logical alternative to its sibling elements. A *POLICY_ALTERNATIVE* may be manifested as a single *POLICY_ASSERTION* (the compact policy form) or as a <wsp:All> element specifying a cohesive group of *POLICY_ASSERTIONs*.
- *POLICY_ASSERTION* - An individual requirement, capability, other property, or a behavior. (E.g., the <sp:SignedParts> element is an assertion indicating which portions of a document are to be signed.)
- *ENDPOINT_POLICY_SUBJECT* – A *POLICY_SUBJECT* indicating the association of a *POLICY* with an entire Web service endpoint (i.e., a service describable by a <wsdl:binding> or a <wsdl:port>). A Profile-compliant *ENDPOINT_POLICY_SUBJECT* is manifested as a <wsp:URI> of the form "urn:wsaaction:*".
- *OPERATION_POLICY_SUBJECT* – A *POLICY_SUBJECT* indicating the association of a *POLICY* with a particular Web service operation (i.e., a message exchange describable by a <wsdl:operation>). Profile-compliant *OPERATION_POLICY_SUBJECT* is manifested as a <wsp:URI> of the form "urn:wsaaction:<wsa-action>" where <wsa-action> is a valid WS-Addressing action for the referenced endpoint.

The Profile is an extension of the *Web Services Policy 1.5 - Attachment* [WS-PolicyAttachment] specification. The following conformance targets are inherited from those in the WS-PolicyAttachment:

- *POLICY_SUBJECT* – An entity (e.g., an endpoint, message, resource, operation, action, etc.) with which a *POLICY* can be associated.
- *POLICY_SCOPE* – A collection of *POLICY_SUBJECT*s to which a *POLICY* may apply.
- *POLICY_ATTACHMENT* – A mechanism for associating *POLICY* with one or more *POLICY_SCOPE*s. *POLICY_ATTACHMENTS* are represented in XML as <wsp:PolicyAttachment> elements.

This Profile defines the following conformance targets:

- *ENDPOINT_REFERENCE* – A <wsa:EndpointReference> endpoint reference element as defined by the WS Addressing 1.0 [WS-Addressing] specification.
- *SECURE_EPR* – an *ENDPOINT_REFERENCE* conformant to this Profile.
- *EPR_SIGNATURE* – an (optional) <ds:Signature> XML-Signature signature element that is a child element of the <wsa:EndpointReference> element and represents a signature over the EPR's <wsa:Address>, <wsa:ReferenceParameters>, and <wsa:Metadata> child elements. For further requirements, see Section 6: Digital Signing.

- *SECURITY_POLICY_ATTACHMENT* – A *POLICY_ATTACHMENT* child of the *SECURE_EPR* <wsa:Metadata> element whose *POLICY_SUBJECT*s are valid WS-Addressing actions.

3.3 Conformance Scope

The scope of the Profile delineates the technologies that it addresses; in other words, the Profile only attempts to improve interoperability within its own scope. Generally, the Profile's scope is bounded by the specifications referenced by it (Section 9).

Referenced specifications often provide extension mechanisms and unspecified or open-ended configuration parameters. The Profile defines such extensibility points within referenced specifications, possibly refining them in the process. The extensibility points exposed by the Profile are enumerated in Appendix A. These extensibility points (e.g., mechanisms or parameters) are outside the scope of the Profile, and their use or non-use is not relevant to conformance.

3.4 Claiming Conformance

Claims of conformance to the Profile are the same as normatively described in *WS-I Basic Profile 1.1* [WS-I BP 1.1]. The conformance claim URI for this Profile is:

http://www.ogf.org/ogsa/2007/05/secure-addressing

4 MISCELLANEOUS TERMINOLOGY

This section defines terminology used within non-normative text of the Profile. These definitions are not considered conformance targets because they do not appear in any conformance requirements.

- *Initiator* - The role sending the initial message in a message exchange.
- *Resource* – The logical message recipient, identifiable with an *ENDPOINT_REFERENCE*. A resource may have different cryptographic identity than the transport-level or message-level service(s) within which it resides. For example, multiple stateful resources may be exposed via the same Web service, and multiple Web services may be exposed via a Web server handling HTTP requests on a specific port.

5 POLICY ATTACHMENT

The Profile incorporates by reference Section 2, "Endpoint References" of the *Web Services Addressing 1.0 - Core* [WS-A Core] specification. (Other sections of the WS-A Core pertain to message addressing properties, the requirements of which are not inherited by the Profile as they are considered out of scope of the Profile.)

The Profile defines the following extensibility points from WS-Addressing:

- E0301 – WS-Addressing Extensibility – WS-Addressing allows extensibility elements for the <wsa:EndpointReference> element.
- E0302 – WS-Addressing Metadata Extensibility – WS-Addressing allows extensibility elements for metadata as children of the <wsa:Metadata> element.
- E0303 – WS-Addressing Reference Parameters Extensibility – WS Addressing allows extensibility elements for Reference Parameters as children of the <wsa:ReferenceParameters> element

This section of the Profile also incorporates by reference the *Web Services Policy 1.5 - Attachment* [WS-PolicyAttachment] specification. The Profile defines the following extensibility points from WS-PolicyAttachment:

- E0304 – WS-PolicyAttachment "AppliesTo" Extensibility – WS-PolicyAttachment requires that the `<wsp:AppliesTo>` element be extended in order to define a domain expression for identifying policy scope.

5.1 Policy Attachment Profile

This section describes how to attach WS-SecurityPolicy *POLICIES* within the extensible metadata section of a WS-Addressing endpoint reference using *SECURITY_POLICY_ATTACHMENTs*. The Profile uses IRIs to specify the *POLICY_SUBJECTs* for which a given *POLICY* is bound. *POLICIES* can be attached to *ENDPOINT_POLICY_SUBJECTs* as well as *OPERATION_POLICY_SUBJECTs*. The IRIs for *OPERATION_POLICY_SUBJECTs* incorporate the WS-Addressing action for that operation. In this manner, different *POLICIES* can be specified for different actions upon the endpoint.

- R0350 – All *SECURITY_POLICY_ATTACHMENTs* MUST be children of the `<wsa:Metadata>` element.
- R0351 – In order to indicate *POLICY_SCOPE*, all *SECURITY_POLICY_ATTACHMENTs* MUST include an `<wsp:AppliesTo>` element conformant to *WS-PolicyAttachment Section 3.4.1: URI Domain Expression*. Such `<wsp:AppliesTo>` elements MUST contain one or more `<wsp:URI>` children (i.e., an *ENDPOINT_POLICY_SUBJECT* and/or *OPERATION_POLICY_SUBJECTs*) that indicate the *POLICY_SUBJECT*s for which the subsequent *POLICY* is applicable.
- R0352 – A *SECURE_EPR* MUST NOT contain more than one *ENDPOINT_POLICY_SUBJECT*. The semantics of the *ENDPOINT_POLICY_SUBJECT* MAY be overridden by policy attached to specific *OPERATION_POLICY_SUBJECTs* using the methodology outlined in WS-SecurityPolicy for calculating effective policy.
- C0300 – *SECURE_EPR*s SHOULD reference common *POLICIES* using the `<wsp:PolicyReference>` instead of the redefining policies using the `<wsp:Policy>` element for efficiency.

6 DIGITAL SIGNATURE

In many scenarios it will be necessary to validate the integrity and trustworthiness of an EPR before using the information it contains for communication. (For example, consider the use-case in which an initiator obtains a *SECURE_EPR* for a particular resource from a third party such as a directory service.) This section of the Profile is intended to:

- Allow an initiator to establish that a *SECURE_EPR* was minted by a trusted source.
- Allow an initiator to detect tampering of a *SECURE_EPR* after minting.

This Profile facilitates such trust and integrity properties by requiring and profiling the XML digital signing of the *SECURE_EPR* document.

- R0353 – A *SECURE_EPR* document MUST incorporate digital signing as per this section of the Profile.

The requirements for XML-Signature are incorporated by reference from *Section 8, "XML-Signature"* section of the *WS-I Basic Security Profile Version 1.0* [WS-I BSP] and referenced specifications.

This section of the Profile leverages extensibility point E0301 to define the *EPR_SIGNATURE* signature element.

- R0354 – The *EPR_SIGNATURE* element MUST be a child element of the `<wsa:EndpointReference>` element.
- R0355 – The *EPR_SIGNATURE* MUST contain `<ds:Reference>` elements that appropriately reference the EPR's `<wsa:Address>`, `<wsa:ReferenceParameters>`, and `<wsa:Metadata>` child elements. (As per the WS-I BSP, `<ds:Manifest>` elements MUST NOT be used to group these data objects.)
- R0356 – The *EPR_SIGNATURE*'s `<ds:KeyInfo>` element MUST contain a `<wsse:SecurityTokenReference>` element containing either a `<wsse:Embedded>` or a `<wsse:Reference>` element indicating a `<wsse:BinarySecurityToken>` of type "X509PKIPathv1" or "X509v3" as defined in the *Web Services Security: X.509 Token Profile* [WS-S: X509 TP].

In order to trust such signatures, implementations should ensure that the signing tokens are valid and chain to a properly configured set of trust roots. The process by which an implementation ensures the integrity and trustworthiness of an embedded security token is outside the scope of the Profile.

- C0301 – The X.509 token referenced by the *EPR_SIGNATURE* element SHOULD be validated and determined to chain to a properly configured set of trust roots.

7 EXAMPLE *SECURE_EPR*

The following shows an example *SECURE_EPR* conformant to the Profile. This example provides two *POLICY_ALTERNATIVE*s for secure communication with a particular resource: (a) username-token authentication of the client over server-authenticated TLS, and (b) mutually authenticated X.509 message-level communication in which message exchange is integrity-protected. The EPR is also signed to facilitate trust verification.

It should be noted that several of the components of the policies shown in this example are profiled in the *Secure Communication Profile 1.0* [OGSA SCP], and are shown here for illustrative purposes only.

```
(01) <wsa:EndpointReference>
(02)
(03)   <wsa:Address wsu:Id='TheAddress'>
(04)     http://www.example.org/some/path
(05)   </wsa:Address>
(06)
(07)   <wsa:ReferenceParameters wsu:Id='TheRefParams'>
(08)      ...
(09)   </wsa:ReferenceParameters>
(10)
(11)   <wsa:Metadata wsu:Id='TheMetadata'>
(12)
(13)     <!-- This policy attachment applies to all actions on this endpoint -->
(14)     <wsp:PolicyAttachment>
(15)       <wsp:AppliesTo>
(16)         <wsp:URI>urn:wsaaction:*</wsp:URI>
(17)       </wsp:AppliesTo>
(18)
(19)       <!-- Collection of policy alternatives -->
(20)       <wsp:Policy>
(21)         <wsp:ExactlyOne>
(22)
(23)           <!-- Alternative 1: Server-authenticated TLS + Username-token -->
(24)           <wsp:All>
```

```
(25)            <wsp:PolicyReference>
(26)              http://www.ogf.org/ogsa/2007/05/secure-communication#ServerTLS
(27)            </wsp:PolicyReference>
(28)            <wsp:PolicyReference>
(29)              http://www.ogf.org/ogsa/2007/05/secure-communication#UsernameToken
(30)            </wsp:PolicyReference>
(31)          </wsp:All>
(32)
(33)          <!-- Alternative 2: X.509 message-level authentication -->
(34)          <wsp:All>
(35)            <wsp:PolicyReference>
(36)              http://www.ogf.org/ogsa/2007/05/secure-communication#MutualX509
(37)            </wsp:PolicyReference>
(38)          </wsp:All>
(39)
(40)        </wsp:ExactlyOne>
(41)      </wsp:Policy>
(42)    </wsp:PolicyAttachment>
(43)
(44)    ...
(45)
(46)  </wsa:Metadata>
(47)
(48)  <!-- Digital Signature of the EPR document -->
(49)  <ds:Signature xmlns:ds='http://www.w3.org/2000/09/xmldsig#'>
(50)    <ds:SignedInfo>
(51)      <ds:CanonicalizationMethod Algorithm='http://.../xml-exc-c14n#'/>
(52)      <ds:SignatureMethod Algorithm='http://.../xmldsig#rsa-sha1'/>
(53)      <ds:Reference URI='#TheAddress'>
(54)        <ds:Transforms>
(55)          <ds:Transform Algorithm='http://.../xml-exc-c14n#'/>
(56)        </ds:Transforms>
(57)        <ds:DigestMethod Algorithm='http://.../xmldsig#sha1'/>
(58)        <ds:DigestValue>+VTJraRYFT3pl7Z4uAWhmr5+bf4=</ds:DigestValue>
(59)      </ds:Reference>
(60)      <ds:Reference URI='#TheRefParams'>
(61)        <ds:Transforms>
(62)          <ds:Transform Algorithm='http://.../xml-exc-c14n#'/>
(63)        </ds:Transforms>
(64)        <ds:DigestMethod Algorithm='http://.../xmldsig#sha1'/>
(65)        <ds:DigestValue>+VTJraRYFT3pl7Z4uAWhmr5+bf4=</ds:DigestValue>
(66)      </ds:Reference>
(67)      <ds:Reference URI='#TheMetadata'>
(68)        <ds:Transforms>
(69)          <ds:Transform Algorithm='http://.../xml-exc-c14n#'/>
(70)        </ds:Transforms>
(71)        <ds:DigestMethod Algorithm='http://.../xmldsig#sha1'/>
(72)        <ds:DigestValue>+VTJraRYFT3pl7Z4uAWhmr5+bf4=</ds:DigestValue>
(73)      </ds:Reference>
(74)    </ds:SignedInfo>
(75)    <ds:SignatureValue>+diIuEyDpV7qxVoUOkb5rj61+Zs=</ds:SignatureValue>
(76)    <ds:KeyInfo>
(77)      <wsse:SecurityTokenReference>
(78)        <wsse:Embedded>
(79)          <wsse:BinarySecurityToken wsu:Id='SomeCert'
(80)              ValueType="http://...-wss-x509-token-profile-1.0#X509v3"
(81)              EncodingType="http://...-message-security-1.0#Base64Binary">
(82)        GJW5xM3aHnLxOpGVIpzSg4V486hHFe7sHET/uxxVBovT7JV1A2RnWSWkXm9jAEdsm/...
(83)          </wsse:BinarySecurityToken>
(84)        </wsse:Embedded>
(85)      </wsse:SecurityTokenReference>
(86)    </ds:KeyInfo>
(87)  </ds:Signature>
(88)
(89) </wsa:EndpointReference>
```

- Lines 01-83: An example *ENDPOINT_REFERENCE.*
- Lines 14-42: An example of a *POLICY ATTACHMENT* element is shown.

- Lines 15-17: The <wsp:AppliesTo> element indicates that the subsequent policies are within scope for all supported WS-Addressing actions.
- Lines 20-41: An enclosing *POLICY* containing a set of two mutually-exclusive *POLICY_ALTERNATIVEs*.
- Lines 24-31: A *POLICY ALTERNATIVE* indicating username-token authentication of the client over server-authenticated TLS. The <wsp:TransportBinding> policy referenced is defined in Section 7.2 of the *Secure Communication Profile 1.0* [OGSA SCP]. The referenced <wsp:SupportingToken> policy indicating username-token is defined in Section 7.4 of the OGSA SCP.
- Lines 34-38: A *POLICY ALTERNATIVE* indicating mutually authenticated X.509 message-level communication in which both the request and response messages within the message exchange are integrity-protected through XML digital signature. The particular "MutualX509" binding assertion policy is defined in Section 5.2.1 of the *OGSA Security Policy Profile*.
- Lines 49-87: The XML digital signature indicating the minter of the EPR and providing protection against tampering
- Lines 53-59: Signature reference indicating that the signature covers the <wsa:Address> data object.
- Lines 60-66: Signature reference indicating that the signature covers the <wsa:ReferenceProperties> data object.
- Lines 67-73: Signature reference indicating that the signature covers the <wsa:Metadata> data object.
- Lines 76-86: <ds:KeyInfo> element indicating the X.509 identity of the EPR minter, which includes the public key necessary for signature verification.

8 CONTRIBUTORS

8.1 Author Information

Duane Merrill
Computer Science Department
University of Virginia
Charlottesville, VA 22903
Email: dgm4d@cs.virginia.edu

8.2 Acknowledgements

We are grateful to colleagues for discussions on the topics covered in this document, in particular (in alphabetical order, with apologies to anybody we've missed) Blair Dillaway, Andrew Grimshaw, John Karpovich, Hiro Kishimoto, Mark Morgan, Andreas Savva, and David Snelling.

9 INTELLECTUAL PROPERTY STATEMENT

available; neither does it represent that it has made any effort to identify any such rights. Copies of claims of rights made available for publication and any assurances of licenses to be made available, or the result of an attempt made to obtain a general license or permission for the use of such proprietary rights by implementers or users of this specification can be obtained from the OGF Secretariat.

The OGF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this recommendation. Please address the information to the OGF Executive Director.

10 DISCLAIMER

This document and the information contained herein is provided on an "As Is" basis and the OGF disclaims all warranties, express or implied, including but not limited to any warranty that the use of the information herein will not infringe any rights or any implied warranties of merchantability or fitness for a particular purpose.

11 FULL COPYRIGHT NOTICE

12 REFERENCES

12.1 Normative References

- [RFC2119] S. Bradner (ed.): Key words for use in RFCs to Indicate Requirement Levels, The Internet Engineering Task Force Best Current Practice, March 1997. http://www.ietf.org/rfc/rfc2119
- [HTTP-TLS] E. Rescorla (ed.): HTTP Over TLS, Internet Engineering Task Force, May 2000. http://www.ietf.org/rfc/rfc2818
- [TLS 1.0] T. Dierks, C. Allen (ed.): The TLS Protocol Version 1.0, Internet Engineering Task Force, January 1999. http://www.ietf.org/rfc/rfc2246
- [WS-Addressing] M. Gudgin and Marc Hadley (ed.), Web Services Addressing 1.0 - Core, W3C Candidate Recommendation 9 May 2006, http://www.w3.org/TR/2006/REC-ws-addr-core-20060509

- [WS-I BP 1.1] K. Ballinger, D. Ehnebuske, C. Ferris, M. Gudgin, C.K. Liu, M. Nottingham, and P. Yendluri (ed.): Basic Profile Version 1.1, Web Services Interoperability Organization Final Material, 24 August 2004. http://www.ws-i.org/Profiles/BasicProfile-1.1.html
- [WS-I BSP 1.0] A. Barbir, M. Gudgin, M. McIntosh, and K.S. Morrison (ed.): Basic Security Profile Version 1.0, Web Services Interoperability Organization, Working Group Draft, 17 August 2006. http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2006-08-17.html
- [X.509] Information Technology - Open Systems Interconnection - The Directory: Authentication Framework, 08/05. http://www.itu.int/rec/T-REC-X.509-200508-I
- [WS-Policy] A. Vedamuthu, D. Orchard, F. Hirsch, M. Hondo, P. Yendluri, T. Boubez, Ü. Yalçinalp (ed.): Web Services Policy 1.5 – Framework. W3C Candidate Recommendation, 05 June 2007. http://www.w3.org/TR/2007/CR-ws-policy-20070605
- [WS-SecurityPolicy] A. Nadalin, M. Goodner, A. Barbir, H. Granqvist (ed.): WS-SecurityPolicy 1.2. Oasis Standard, 01 July 2007. http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf
- [WS-PolicyAttachment] A. Vedamuthu, D. Orchard, F. Hirsch, M. Hondo, P. Yendluri, T. Boubez, Ü. Yalçinalp (ed.): Web Services Policy 1.5 – Attachment. W3C Candidate Recommendation 05 June 2007. http://www.w3.org/TR/2007/CR-ws-policy-attach-20070605
- [WS-S X509 TP] P. Hallam-Baker, C. Kaler, R. Monzillo, A. Nadalin (ed) Web Service Security X.509 Certificate Token Profile, OASIS Standard, 200401, March 2004. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf

12.2 Non-Normative References

- [WS-S] A. Nadalin, C. Kaler, P. Hallam-Baker and R. Monzillo (ed.): Web Services Security: SOAP Message Security 1.0 (WS-Security 2004), OASIS Standard, 200401, March 2004. http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf
- [XML-DigSig] D. Eastlake, J. Reagle, D. Solo (ed.): XML-Signature Syntax and Processing, W3C Recommendation, Feb 12, 2002. http://www.w3.org/TR/xmldsig-core/
- [XML-Enc] D. Eastlake, J. Reagle (ed.): XML Encryption Syntax and Processing, W3C Recommendation, Dec 10, 2002. http://www.w3.org/TR/xmlenc-core/
- [OGSA Profile Definition] T. Maguire. and D. Snelling: OGSA Profile Definition Version 1.0. Open Grid Forum, Lemont, Illinois, U.S.A., GFD-I.059, January 2006. http://www.ogf.org/gf/docs/?final
- [OGSA SCP] D. Merrill: Secure Communication Profile 1.0. Global Grid Forum OGSA-WG, Draft, 01 May 2007
- [WSDL] E. Christensen, F. Curbera, G. Meredith, S. Weerawarana: Web Services Description Language (WSDL) 1.1. W3C Note, March 15, 2001. http://www.w3.org/TR/wsdl

APPENDIX A. EXTENSIBILITY POINTS

This section identifies extensibility points for the Profile. Except for the use of E0301, E0302, and E0304 as profiled in this document, these mechanisms are out of the scope of the Profile. As such, their use may affect interoperability, and may require private agreement between the parties to a Web service.

In *WS-Addressing 1.0 – Core* [WS-Addressing]:

- E0301 – WS-Addressing Extensibility – WS-Addressing allows extensibility elements for the `<wsa:EndpointReference>` element.
- E0302 – WS-Addressing Metadata Extensibility – WS-Addressing allows extensibility elements for metadata as children of the `<wsa:Metadata>` element.
- E0303 – WS-Addressing Reference Parameters Extensibility – WS Addressing allows extensibility elements for Reference Parameters as children of the `<wsa:ReferenceParameters>` element

In *WS-PolicyAttachment 1.5* [WS-PolicyAttachment]:

- E0304 – WS-PolicyAttachment “AppliesTo” Extensibility – WS-PolicyAttachment requires that the `<wsp:AppliesTo>` element be extended in order to define a domain expression for identifying policy scope.

APPENDIX B. REFERENCED SPECIFICATION STATUS AND ADOPTION LEVEL CLASSIFICATION

The classification of this Profile's referenced specifications at the time of writing is shown below:

Table 2 Status of specifications referenced by Secure Addressing Profile 1.0

OGSA Referenced Specifications: Secure Addressing Profile 1.0														
December 17, 2007	Status							Adoption						
Specification/Profile Name	De Facto	Institutional	Evolving Institutional	Draft Institutional	Consortium	Evolving Consortium	Draft	Ubiquitous	Adopted	Community	Interoperable	Implemented	Unimplemented	**Note**
Specifications														
None														
WS-Addressing 1.0		X									<	X		IBM, Apache implementing
WS-Policy 1.5 - Framework			X								X			W3C Proposed Recommendation
WS-Policy 1.5 - Attachment			X								X			W3C Proposed Recommendation
WS-Security Policy 1.2		X									X			OASIS Standard
WS-Security X.509 Token Profile 1.1		X									X			OASIS Standard
Profiles														
None														
WS-I Basic Profile 1.1		X												Final Material
WS-I Basic Security Profile 1.0		X												Final Material

Legend:

X	Specification or profile is currently at this status or adoption level
<	Specification or profile is approaching this status or adoption level
	Status or adoption level is not applicable