T. Mori, NEC
F. Siebenlist, ANL

Thursday, February 9, 2006

OGSA™ Basic Security Profile 1.0 – Core

Status of This Memo

This memo provides a recommendation to the Grid community on common security requirement for securing OGSA services. The intention of this profile is to describe precisely the requirements placed on key information binding to Endpoint Reference of such services to ensure interoperability. Distribution is unlimited.

Abstract

The growing number of Web services specifications makes it important to understand and define the interaction and use of these specifications to ensure interoperability. In the wider technical domain of distributed system management and grid computing, the OGSA WSRF Basic Profile 1.0 [**OGSA WSRF Basic Profile**] provides the first normative profile, addressing issues regarding the addressing, modeling and management of WS-Resources, but it does not address the details of the security aspects of interoperability issues.

Therefore, in order to ensure the secure and interoperable interaction of Web services in the context of distributed resource management and grid computing, we define here the OGSA Basic Security Profile 1.0 – Core, a profile which is intended to be used along with one of the OGSA Basic Profiles, such as the OGSA WSRF Basic Profile 1.0 [**OGSA WSRF Basic Profile**].

The OGSA Basic Security Profile 1.0 – Core described in this document is an *OGSA Recommended Profile as Proposed Recommendation,* as defined in the OGSA Profile Definition [**OGSA Profile Definition**]. The OGSA Basic Security Profile 1.0 – Core describes uses of widely accepted specifications that have been found to enable interoperability. The specification considered in this profile is the basic Web services specification which is used to enable addressing of resources: WS-Addressing 1.0 [**WS-Addressing**]. The requirements stated in the profile are concerned with binding of key information to an endpoint reference; the profile defines a core security profile which is considered to be common to all OGSA services to ensure security in an inherently unsafe environment such as the Internet.

Contents

1 Introduction

This document defines the OGSA Basic Security Profile 1.0 – Core (hereafter, "the Profile"). The word “core” is used here because the Profile addresses a security issue that is considered to be common to all OGSA services, especially binding of key information to Endpoint References. The Profile defines a Web services profile in order to ensure the security of Web services in the context of OGSA.

Section 1 introduces the Profile, and explains its relationships to other profiles.

Section 2, "Profile Conformance," explains what it means to be conformant to the Profile.

Section 3 addresses a component of the Profile, and consists of two parts: an overview detailing the component specification and its extensibility points, followed by a subsection that addresses individual parts of the component specification. Note that there is no relationship between the section numbers in this document and those in the referenced specification.

1.1 Profile Overview

The Profile is intended for use when communicating key information of services that are concerned with distributed resource management, grid computing, or other purposes that involve the modeling and management of stateful entities as profiled by one of the OGSA Basic Profiles, such as the OGSA WSRF Basic Profile 1.0 [**OGSA WSRF Basic Profile**].

These services can benefit from the use of security mechanisms defined in the WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**]. The services can also benefit from the use of syntax and semantics defined in WS-Addressing [**WS-Addressing**] to address resources. A service implementation that is conformant with the Profile and with the OGSA WSRF Basic Profile 1.0 [**OGSA WSRF Basic Profile**] may be said to be an “implementation of the OGSA Basic Security Profile 1.0 – Core” as well as an “implementation of the OGSA WSRF Basic Profile 1.0.”

The issue addressed in the profile is:

- *Key Information Binding to Endpoint Reference.* The Profile mandates the use of the Key Information Binding to Endpoint Reference defined in Appendix C of the Profile when associating key information with Web services.

Although the WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**] defines security mechanisms for Web services communication, that profile does not address the issue of how to bind key information to the address of a Web service. By conforming to the Profile, key information for secure communication can be specified by an endpoint reference, and thus an appropriate key for secure communication with the peer service can be selected.

1.2 Relationships to Other Profiles

The Profile addresses key information binding to endpoint reference which can be used to establish a secure communication with a Web service addressed by that endpoint reference.

This Profile, the OGSA Basic Security Profile 1.0 - Core, may be combined and used with other OGSA Security Profiles. For example, it may be combined with the OGSA Basic Security Profile – 1.0 [**OGSA Basic Security Profile – Secure Channel**] when transport level security is required.

This Profile is expected to be used with an OGSA Basic Profile, for example the OGSA WSRF Basic Profile 1.0 [**OGSA WSRF Basic Profile**].

1.3 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 [**RFC2119**].

Normative statements of requirements in the Profile are presented in the manner detailed in the WS-I Basic Profile 1.1 Conformance Requirements section.

Both requirement statements and extensibility statements can be considered namespace-qualified.

This specification uses a number of namespace prefixes throughout; their associated URIs are listed below. Note that the choice of any namespace prefix is arbitrary and not semantically significant.

Table 1 Namespaces used by OGSA Basic Security Profile 1.0 – Core

Prefix	Namespace
wsa	http://www.w3.org/2005/03/addressing
bsp-core	http://schemas.ggf.org/ogsa/2006/01/bsp-core

This Profile uses of the following special terms to refer to referenced specifications:

- **WS-Addressing** – Web Services Addressing 1.0 – Core [**WS-Addressing**]

1.4 Profile Identification and Versioning

Profile identification and versioning uses the style described in WS-I Basic Profile 1.1 and abides by the normative descriptions contained therein. The name of this Profile is "OGSA Basic Security Profile – Core," and its version number is "1.0."

2 Profile Conformance

Conformance to the Profile is defined normatively in WS-I Basic Profile 1.1. This Profile abides by those definitions.

2.1 Conformance Targets

The Profile defines a conformance target called ENDPOINTREFERENCE.

- **ENDPOINTREFERENCE** – the serialization of the wsa:EndpointReference element and its content

2.2 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.ggf.org/ogsa/2006/01/bsp-core.

This Profile conforms to the OGSA Basic Security Profile defined in OGSA WSRF Basic Profile 1.0. Thus this Profile also exposes the following conformance claim URI for OGSA Basic Security Profile: http://www.ggf.org/ogsa/2006/01/bsp.

3 Key Information Binding to Endpoint Reference

This section of the Profile incorporates the following specification by reference, and defines extensibility points within it:

- Web Services Addressing 1.0 - Core [**WS-Addressing**] extensibility points:
  - 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.

3.1 Endpoint Reference

The following specification (or sections thereof) is referred to in this section of the Profile:

- Web Services Addressing, Section 2 [**WS-Addressing**]

WS-Addressing defines the endpoint reference structure for referencing services and WS-Resources. The Profile mandates the use of that structure, and places the following constraints on its use:

3.1.1 Key Information Binding to Endpoint Reference

Before establishing a secure communication, the key information of an instance needs to be communicated to the consumer. The referenced specifications do not state anything on how to communicate such information between an instance and a consumer. Therefore, the Profile defines key information binding to an endpoint reference by using the Metadata element in the EndpointReference element in Appendix C. It enables the consumer to retrieve the key information which is necessary for establishing a secure communication with the instance from the endpoint reference of it. The Profile places the following constraints on the use and the communication of key information.

R0301 *When providing key information as part of an ENDPOINTREFERENCE, the ENDPOINTREFERENCE MUST include that information as an ogsa-bsp:EndpointKeyInfo element as defined in Appendix C.*

Author Information

Takuya Mori
NEC Corporation
2-11-5 Shibaura
Minato, Tokyo 108-8557
Email: <moritaku@bx.jp.nec.com>

Frank Siebenlist
Math & Computer Science Division
Argonne National Laboratory
Argonne, IL 60439
Email: <franks@mcs.anl.gov>

Contributors

We gratefully acknowledge the contributions made to this specification by Abdeslem Djaoui, Ian Foster, Hiro Kishimoto, Sam Meder, Tom Maguire, Andreas Savva, David Snelling, Jem Treadwell, and Latha Srinivasan.

Acknowledgements

We are grateful to numerous colleagues for discussions on the topics covered in this document, in particular (in alphabetical order, with apologies to anybody we've missed) Michael Behrens, Dave Berry, Andrew Grimshaw, Marty Humphrey, Vivian Li, Mark McKeown, Mark Morgan, Steven Newhouse, Ravi Subramaniam, Steve Tuecke, Jay Unger, Pete Ziu.

Intellectual Property Statement

Full Copyright Notice

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
- **[WS-Addressing]** D. Box and F. Curbera (ed.): Web Services Addressing 1.0 – Core (WS-Addressing), W3C Last Call, 31 March 2005. http://www.w3.org/TR/2005/WD-ws-addr-core-20050331
- **[WS-Security]** 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
- **[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, 29 August 2005. http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0-2005-08-29.html
- **[XML-Signature]** M. Bartel, J. Boyer, B. Fox, B. LaMacchia, and E. Simon: XML-Signature Syntax and Processing. http://www.w3.org/TR/2002/REC-xmldsig-core-20020212/

Non-Normative References

- **[OGSA WSRF Basic Profile]** I. Foster, T. Maguire and D. Snelling: OGSA WSRF Basic Profile Version 1.0, Global Grid Forum OGSA-WG, GWD-R, 1 September 2005. http://forge.gridforum.org/projects/ogsa-wg/document/draft-ggf-ogsa-wsrf-basic-profile/en/36
- **[OGSA Profile Definition]** T. Maguire and D. Snelling: OGSA Profile Definition Version 1.0, Global Grid Forum OGSA-WG, 10 January 2006. http://www.ggf.org/documents/GFD.59.pdf
- **[OGSA Basic Security Profile – Secure Channel]** T. Mori and F. Siebenlist: OGSA Basic Security Profile 1.0 – Secure Channel, Global Grid Forum OGSA-WG, Draft, 31 January 2006. https://forge.gridforum.org/projects/ogsa-wg/document/draft-ggf-ogsa-basic-security-profile-secure-channel/en/16

Appendix A. Referenced Specifications

The following specification's requirements are incorporated into the Profile by reference, except where superseded by the Profile:

- WS-Addressing – Web Services Addressing 1.0 – Core [**WS-Addressing**]

Appendix C of this document refers to and depends on the following specifications:

- Web Services Security: SOAP Message Security 1.0 [**WS-Security**]
- XML-Signature Syntax and Processing [**XML-Signature**]

Appendix B. Extensibility Points

This section identifies extensibility points for the Profile's component specifications. These mechanisms are out of the scope of the Profile; their use may affect interoperability, and may require private agreement between the parties to a Web service.

In Web Services 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.

Appendix C. Key Information Binding to Endpoint Reference Normative Description

C.1 Introduction

This appendix defines key information communication of a peer endpoint by using a Metadata element in an EndpointReference element defined in the WS-Addressing specification.

C.2 Use cases

The followings are use cases that the Profiles specified in the appendix cover:

- When a client wants to send any encrypted message to a service, it will have to know the key associated with that service.
- When a client wants to make a policy decision regarding whether or not it wants a certain service to serve its request, it has to know the service's key-info.

C.3 Namespaces

This appendix uses the following namespaces:

Table 2 Namespaces used in definition of Key Information Binding

Prefix	Namespace
wsa	http://www.w3.org/2005/03/addressing
xsd	http://www.w3.org/2001/XMLSchema
xsi	http://www.w3.org/2001/XMLSchema-instance
ds	http://www.w3.org/2000/09/xmldsig#
wsse	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
bsp-core	http://schemas.ggf.org/ogsa/2006/01/bsp-core

This note also uses the following entity references to ease the description of the URIs:

Table 3 Entity references

Entity reference	Definition
&wsse;	http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd
&bsp-core;	http://schemas.ggf.org/ogsa/2006/01/bsp-core

C.4 Example

The following shows an example which the Profile is intended to define.

```
(01) <wsa:EndpointReference>
```

```
(02)   <wsa:Address>
(03)     http://www.example.org/some/path
(04)   </wsa:Address>
(05)   <wsa:Metadata>
(06)     <bsp-core:EndpointKeyInfo>
(07)       <wsse:SecurityTokenReference
                 wsse:Usage="&bsp-core;#signature">
(08)         <wsse:Reference URI="#token1"/>
(09)       </wsse:SecurityTokenReference>
(10)       <wsse:SecurityTokenReference
                 wsse:Usage="&bsp-core;#encryption">
(11)         <wsse:Embedded>
(12)           <wsse:BinarySecurityToken
                     ValueType="&wsse;X509PKIpathv1">
(13)                 MIIC.....
(14)           </wsse:BinarySecurityToken>
(15)         </wsse:Embedded>
(16)       </wsse:SecurityTokenReference>
(17)     </bsp-core:EndpointKeyInfo>
(18)   </wsa:Metadata>
(19) </wsa:EndpointReference>
```

(01)-(19) An example wsa:EndpointReference

(06)-(17) An example of bsp-core:EndpointKeyInfo element is shown. The actual key information contained in the bsp-core:EndpointKeyInfo element is bound to the endpoint specified by the enclosing wsa:EndpointReference.

(07)-(09) An example of actual key information is shown. The key is expressed by using wsse:SecurityTokenReference and the wsse:Usage attribute shows that the key should be used for signature. The key data is referenced by the same document reference, "#token1".

(10)-(16) Another example of key information is shown. The key is also expressed by using wsse:SecurityTokenReference, but the actual key data is embedded in the element as a wsse:BinarySecurityToken in wsse:Embedded. The usage of the key is specified as encryption by the wsse:Usage attribute.

C.5 Infoset

The following paragraphs provide the descriptions or definitions of the infosets referenced by or defined in this appendix.

- /wsa:EndpointReference/wsa:Metadata:

  WS-Addressing defines an optional wsa:Metadata element which is used to hold metadata that is relevant to the interaction with the endpoint.

- /wsa:EndpointReference/wsa:Metadata/osga-bsp:EndpointKeyInfo:

  The bsp-core:EndpointKeyInfo is defined as a ds:KeyInfoType which is defined in the XML-Signature specification to contain generic key information. In this Profile, the element is used to specify key information that should be used to interact with the endpoint.

- /wsa:EndpointReference/wsa:Metadata/ogsa-bsp:EndpointKeyInfo/wsse:SecurityTokenReference:

  Although the XML-Signature specification defines various types of elements which are intended to be used as child elements of the ds:KeyInfoType element and the specification also allows the ds:KeyInfoType element to have arbitrary types of elements in its content, this Profile mandates the use of wsse:SecurityTokenReference elements under the bsp-core:EndpointKeyInfo element.

- /wsa:EndpointReference/wsa:Metadata/ogsa-bsp:EndpointKeyInfo/wsse:SecurityTokenReference/@wsse:Usage:

  WS-Security defines this optional attribute which is used to type the usage of the wsse:SecurityTokenReference element.

This Profile defines the following values for the @wsse:Usage attribute to specify the usage of the key referenced by the wsse:SecurityTokenReference:

Table 4 Usage attribute values

Value	Usage
&bsp-core;#encryption	Encryption key needed to interact with the endpoint.
&bsp-core;#signature	Signature verification key needed to interact with the endpoint.

Absence of this attribute means that the key can be used for both encryption and signature verification.

Implementations which create the key-info data MUST NOT set an inconsistent value with the usage in the referenced key to this @wsse:Usage attribute. For example, if the KeyUsage certificate extension of an X.509 public key certificate is marked as CRITICAL and set to Signing, then an implementation MUST NOT set &bsp-core;#encryption to the @wsse:Usage attribute. (Thus, in this case, the certificate cannot be used as an encryption key.)

Implementations which detect an inconsistency between the value of @wsse:Usage attribute and the usage specified in the referenced key itself MUST report an error and MUST NOT use the key for the usage specified by the @wsse:Usage attribute.

C.6 Schema

This section contains the normative XML Schema definitions for bsp-core:EndpointKeyInfo element. The definitions in this section MUST be considered normative.

```
<?xml version="1.0" encoding="UTF-8"?>
<!--
The GGF takes no position regarding the validity or scope of any
intellectual property or other rights that might be claimed to
pertain to the implementation or use of the technology described in
this document or the extent to which any license under such rights
might or might not be 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 GGF Secretariat.

The GGF 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 GGF
Executive Director.

Copyright (C) Global Grid Forum (2005-2006). All Rights Reserved.

This document and translations of it may be copied and furnished to
others, and derivative works that comment on or otherwise explain it
or assist in its implementation may be prepared, copied, published
and distributed, in whole or in part, without restriction of any
kind, provided that the above copyright notice and this paragraph
are included on all such copies and derivative works. However, this
document itself may not be modified in any way, such as by removing
the copyright notice or references to the GGF or other
organizations, except as needed for the purpose of developing Grid
Recommendations in which case the procedures for copyrights defined
in the GGF Document process must be followed, or as required to
translate it into languages other than English.

The limited permissions granted above are perpetual and will not be
revoked by the GGF or its successors or assigns.
This document and the information contained herein is provided on an
"AS IS" basis and THE GLOBAL GRID FORUM 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."

-->
<xsd:schema
  xmlns="http://www.w3.org/2001/XMLSchema"
  xmlns:xsd="http://www.w3.org/2001/XMLSchema"
  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"
  xmlns:ds="http://www.w3.org/2000/09/xmldsig#"
  xmlns:wsa="http://www.w3.org/2005/03/addressing"
  xmlns:bsp-
core="http://www.ggf.org/namespaces/2005/08/OGSABasicSecurityProfile
-1.0.xsd"
  elementFormDefault="qualified"
  attributeFormDefault="unqualified"
  targetNamespace=
"http://www.ggf.org/namespaces/2005/08/OGSABasicSecurityProfile-
1.0.xsd" >

  <xsd:import
    namespace="http://www.w3.org/2000/09/xmldsig#"
    schemaLocation="http://www.w3.org/2000/09/xmldsig#" />

  <xsd:import
    namespace="http://www.w3.org/2005/03/addressing"
```

```
    schemaLocation="http://www.w3.org/2005/03/addressing/" />

  <xsd:element name="EndpointKeyInfo"
               type="ds:KeyInfoType" />

</xsd:schema>
```

C.7 Interoperability

To ensure interoperability, a wsse:SecurityTokenReference element MUST conform to the requirements defined in section 4.2 of the WS-I Basic Profile 1.0 document (SecurityTokenReferences).

To ensure interoperability, if the wsse:BinarySecurityToken refers to or embeds an X.509 certificate, the wsse:BinarySecurityToken MUST conform to the requirements defined in chapter 6 of WS-I Basic Profile 1.0 (X.509 Certificate Token Profile).

Appendix D. Referenced Specification Status and Adoption Level Classification

The classification of this Profile's referenced specifications at the time of writing is shown in Table 5.

Table 5 Status of specifications referenced by OGSA Basic Security Profile 1.0 - Core

OGSA Referenced Specifications: OGSA Basic Security Profile 1.0 - Core														
September 1, 2005	Status							Adoption						
Specification/Profile Name	De Facto	Institutional	Evolving Institutional	Draft Institutional	Consortium	Evolving Consortium	Draft	Ubiquitous	Adopted	Community	Interoperable	Implemented	Unimplemented	Note
Specifications														
WS-Addressing 1.0		<	X									<	X	IBM, Apache implementing
WS-Security 1.0		X									X			
XML-Signature		X									X			
Profiles														
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												