GWD-R (draft-gwdrp-ogsa-basic-security-profile-v2-draft-003)
Category: Recommendation
Open Grid Services Architecture Working Group

David Snelling, Fujitsu

6 December 2007

OGSA® Basic Security Profile 2.0 (draft 003)

Status of This Document

This document provides a recommendation to the Grid community on securing OGSA services. Existing security profiles are combined to define a basic level of security for OGSA based services. Distribution is unlimited.

Trademarks

OGSA is a registered trademark and service mark of the Open Grid Forum.

Obsoletes

This document obsoletes OGSA Basic Security Profile 1.0 – Core **[GFD.86]** and OGSA Security Profile 1.0 – Secure Channel **[GFD.99]**.

Abstract

An OGSA basic profile is a profile in the style of WS-Interoperability (WS-I) that defines recommended usage of infrastructure-level standards for Grid scenarios. OGSA services are expected to use one such profile for each infrastructure capability needed. This document defines such a basic profile for security by bringing together two general, non-OGSA specific, profiles on secure addressing and secure communication.

This profile can be composed with other basic profiles. In particular this profile satisfies the security requirements of the WSRF Basic Profile 1.0 and can be composed with it.

The OGSA Basic Security Profile 2.0 described in this document is an *OGSA Recommended Profile as Proposed Recommendation,* as defined in the OGSA Profile Definition **[GFD.59]**.

ogsa-wg@ggf.org

Contents

1 Introduction

This document defines the OGSA Basic Security Profile 2.0 (hereafter, "the Profile").

An OGSA basic profile is a profile in the style of WS-Interoperability (WS-I) that defines recommended usage of infrastructure-level standards for Grid scenarios **[GFD.*glossary*]**. OGSA services are expected to use one such profile for each infrastructure capability needed.

This Profile defines a basic level of security for OGSA based services by referencing two general (i.e., not OGSA-specific) profiles. Conformance to this Profile is sufficient to meet the requirements for a secure OGSA service, but is not necessary. OGSA allows the definition of more than one basic profile for the same infrastructure capability, so there may be other OGSA profiles that meet the requirements for basic security.

The Profile can be used in combination with other OGSA basic profiles. In particular the OGSA WSRF Basic Profile 1.0 **[GFD.72]** requires composition with a basic security profile that exposes the generic basic security claim http://www.ggf.org/ogsa/2006/01/bsp. Therefore this Profile in addition to its own specific conformance claim also exposes this generic claim to satisfy the requirements of the WSRF Basic Profile 1.0.

The OGSA Basic Security Profile 2.0 described in this document is an *OGSA Recommended Profile as Proposed Recommendation,* as defined in the OGSA Profile Definition **[GFD.59]**.

1.1 Relationships to Other Profiles

The Profile links two other profiles to define an OGSA Basic Security Profile. Specifically the Profile requires implementations to conform to the two following profiles:

- Secure Addressing Profile 1.0 **[GFD.*secadd*]**
- Secure Communication Profile 1.0 **[GFD.*seccom*]**

The Profile fulfills the requirements of the OGSA WSRF Basic Profile 1.0 **[GFD.72]**, Section 8, and can be used in combination with it. The Profile can also be used with other OGSA Basic Profiles.

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 [**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; 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

Prefix	Namespace
wsa	http://www.w3.org/2005/08/addressing
wsp	http://schemas.xmlsoap.org/ws/2004/09/policy

1.3 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,” and its version number is “2.0.”

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 DESCRIPTION.

- **DESCRIPTION** – descriptions of types, messages, interfaces and their concrete protocol and data format bindings, and the network access points associated with Web services (e.g., WSDL descriptions) (from WS-I Basic Profile 1.1).

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.ogf.org/ogsa/2007/11/bsp.

Additionally, this Profile is an OGSA Basic Security Profile as defined in the *OGSA WSRF Basic Profile 1.0* **[GFD.72]**, Section 8. As such, it also exposes the following generic conformance claim URI as required by the OGSA WSRF Basic Profile:

http://www.ggf.org/ogsa/2006/01/bsp

3 Security Specifications

This section of the Profile incorporates the following two profiles by reference and defines extensibility points within them, including extensibility points used by the profiles in their definition.

1. Secure Addressing Profile 1.0 **[GFD.*secadd*]**

   Extensibility points:

   - No extensibility points are defined by this profile.

   The profile makes use of the following extensibility points from *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.

   The profile makes use of the following extensibility points from *WS-PolicyAttachment 1.5* **[WS-PolicyAttachment]**:

   - E0303 – 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.

2. Secure Communication Profile 1.0 **[GFD.*seccom*]**

   Extensibility points:

   - E0304 – Additional transport-level binding assertions may be profiled in accordance to the requirements in Secure Communication Profile 1.0, Section 5.1: Security Mechanism Specifics.
   - E0305 – Additional message-level *PROFILED_MECHANISMs* may be profiled in accordance to the requirements in Secure Communication Profile 1.0, Section 5.

   The profile makes use of the following extensibility points from *WS-I Basic Security Profile 1.0* **[WS-I BSP 1.0]**:

   - E0306 – TLS Ciphersuites – TLS allows for the use of arbitrary encryption algorithms. This Profile restricts the set of allowable ciphersuites to those listed

in the *WS-SecurityPolicy 1.2* Section 6.1. (As per the WS-I BSP, only TLS Protocol Version 1.0 is incorporated into this profile.)

- E0307 – SSL Ciphersuites – SSL allows for the use of arbitrary encryption algorithms. This Profile restricts the set of allowable ciphersuites to those listed in the *WS-SecurityPolicy 1.2* Section 6.1. (As per the WS-I BSP, only SSL Protocol Version 3.0 is incorporated into this profile. SSL 2.0 MUST NOT be used.)

The profile makes use of the following extensibility points from In *WS-SecurityPolicy 1.2* **[WS-SecurityPolicy]**:

- E0308 – WS-SecurityPolicy Token Assertion Extensibility – WS-SecurityPolicy allows the extensibility of *TOKEN_ASSERTIONs*.

3.1 Secure Addressing 1.0

The Profile requires conformance to Secure Addressing Profile 1.0 **[GFD.*secadd*]**..

R0311 *A DESCRIPTION MUST have attached to the wsdl:portType a wsi:claim with the URI "http://www.ogf.org/ogsa/2007/05/secure-addressing" and MUST conform to the requirements set out in **[GFD.secadd]**.*

3.2 Secure Communication 1.0

The Profile requires conformance to the Secure Communication Profile 1.0 **[GFD.*seccom*]**.

R0312 *A DESCRIPTION MUST have attached to the wsdl:portType a wsi:claim with the URI "http://www.ogf.org/ogsa/2007/05/sp-secure-communication" and MUST conform to the requirements set out in **[GFD.seccom]**.*

4 Author Information

David Snelling
Fujitsu Laboratories of Europe
Hayes Park, Hayes
Middlesex, UK, UB4 8FE
Email: <David.Snelling@UK.Fujitsu.com>

4.1 Contributors

We gratefully acknowledge the contributions made to this specification by Hiro Kishimoto, Duane Merrill, Andreas Savva, TBD.....

4.2 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) Blair Dillaway, TBD....

5 Intellectual Property Statement

6 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.

7 Full Copyright Notice

8 References

8.1 Normative References

- **[GFD.72]** I. Foster, T. Maguire and D. Snelling: OGSA WSRF Basic Profile Version 1.0, Global Grid Forum, Lemont, Illinois, U.S.A., GFD.72, 4 September 2006. http://www.ogf.org/gf/documents/GFD.72.pdf
- **[GFD.*secadd*]** D. Merrill: Secure Addressing Profile 1.0. Open Grid Forum, Lemont, Illinois, U.S.A., DAY MONTH YEAR, GFD.XX, http://www.ogf.org/gf/documents/GFD.XX.pdf
- **[GFD.*seccom*]** D. Merrill: Secure Communication Profile 1.0. Open Grid Forum, Lemont, Illinois, U.S.A., DAY MONTH YEAR, GFD.XY, http://www.ogf.org/gf/documents/GFD.XY.pdf
- **[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]** M. Gudgin and Marc Hadley (eds.), Web Services Addressing 1.0 - Core, W3C 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
- **[WS-PolicyAttachment]** A. Vedamuthu, D. Orchard, F. Hirsch, M. Hondo, P. Yendluri, T. Boubez, Ü. Yalçinalp (eds.): Web Services Policy 1.5 – Attachment. W3C Candidate Recommendation 05 June 2007. http://www.w3.org/TR/2007/CR-ws-policy-attach-20070605

- **[WS-SecurityPolicy]** A. Nadalin, M. Goodner, A. Barbir, H. Granqvist (ed.): WS-SecurityPolicy 1.2. Oasis Standard, 1 July 2007. http://docs.oasis-open.org/ws-sx/ws-securitypolicy/200702/ws-securitypolicy-1.2-spec-os.pdf

8.2 Non-Normative References

- **[GFD.59]** T. Maguire and D. Snelling: OGSA Profile Definition Version 1.0, Global Grid Forum, Lemont, Illinois, U.S.A., GFD.59, 10 January 2006. http://www.ogf.org/documents/GFD.59.pdf
- **[GFD.86]** T. Mori and F. Siebenlist: OGSA® Basic Security Profile 1.0 – Core, Global Grid Forum, Lemont, Illinois, U.S.A. GFD.86, 12 January 2007. http://www.ogf.org/documents/GFD.86.pdf
- **[GFD.99]** T. Mori and F. Siebenlist: OGSA® Security Profile 1.0 – Secure Channel, Global Grid Forum, Lemont, Illinois, U.S.A. GFD.99, 22 February 2007. http://www.ogf.org/documents/GFD.99.pdf
- **[GFD.*glossary*]** J. Treadwell: Open Grid Services Architecture Glossary, Version 1.6, Open Grid Forum, Lemont, Illinois, U.S.A. GFD.XZ, DD MM YY. http://www.ogf.org/documents/GFD.XZ.pdf

Appendix A. Referenced Specifications

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

- Secure Addressing Profile 1.0 **[GFD.*secadd*]**
- Secure Communication Profile 1.0 **[GFD.*seccom*]**

Appendix B. Extensibility Points

This section identifies extensibility points for the Profile. Except for the use of E0301, E0302, E0303, E0306, E0307, and E0308 as profiled in the referenced specifications, 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 Secure Addressing Profile 1.0 **[GFD.*secadd*]**

The profile makes use of the following extensibility points from *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.

The profile makes use of the following extensibility points from *WS-PolicyAttachment 1.5* **[WS-PolicyAttachment]**:

- E0303 – 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.

In Secure Communication Profile 1.0 **[GFD.*seccom*]**

Extensibility points:

- E0304 – Additional transport-level binding assertions may be profiled in accordance to the requirements in Secure Communication Profile 1.0, Section 5.1: Security Mechanism Specifics.
- E0305 – Additional message-level *PROFILED_MECHANISMs* may be profiled in accordance to the requirements in Secure Communication Profile 1.0, Section 5.

The profile makes use of the following extensibility points from *WS-I Basic Security Profile 1.0* **[WS-I BSP 1.0]**:

- E0306 – TLS Ciphersuites – TLS allows for the use of arbitrary encryption algorithms. This Profile restricts the set of allowable ciphersuites to those listed in the *WS-SecurityPolicy 1.2* Section 6.1. (As per the WS-I BSP, only TLS Protocol Version 1.0 is incorporated into this profile.)
- E0307 – SSL Ciphersuites – SSL allows for the use of arbitrary encryption algorithms. This Profile restricts the set of allowable ciphersuites to those listed in the *WS-SecurityPolicy 1.2* Section 6.1. (As per the WS-I BSP, only SSL Protocol Version 3.0 is incorporated into this profile. SSL 2.0 MUST NOT be used.)

The profile makes use of the following extensibility points from In *WS-SecurityPolicy 1.2* **[WS-SecurityPolicy]**:

- E0308 – WS-SecurityPolicy Token Assertion Extensibility – WS-SecurityPolicy allows the extensibility of *TOKEN_ASSERTIONs*.

Appendix C. Referenced Specification Status and Adoption Level Classification

The classification of this Profile's referenced specifications at the time of writing is shown in Table 2.

Table 2 Status of specifications referenced by OGSA Basic Security Profile 2.0

OGSA Referenced Specifications: OGSA Basic Security Profile 2.0														
December 6, 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														
Profiles														
OGSA WSRF Basic Profile 1.0		X						--	--	--	--	--	--	
Secure Addressing Profile 1.0			<	X				--	--	--	--	--	--	
Secure Communication Profile 1.0			<	X				--	--	--	--	--	--	
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												