GFD-R-P.099
Category: Recommendation
Open Grid Services Architecture Working Group

T. Mori, NEC
F. Siebenlist, ANL

January 22, 2007

# OGSA™ Security Profile 1.0 - Secure Channel

Status of This Memo

This memo provides a recommendation to the Grid community on how to secure interactions with OGSA services. This profile describes precisely the requirements placed on the security mechanisms for communications of such services to ensure interoperability. Distribution is unlimited.

Copyright Notice

Trademarks

## 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. The WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**] defines a collection of normative profiles that provide guidance on issues of interoperability for secure communication of basic Web services based on such specifications.

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 Security Profile 1.0 - Secure Channel, a profile that 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**] together with OGSA Basic Security Profile 1.0 – Core [**OGSA Basic Security Profile - Core**].

The OGSA Security Profile 1.0 - Secure Channel described in this document is an *OGSA Recommended Profile as Proposed Recommendation* as defined in the OGSA Profile Definition [**OGSA Profile Definition**]. The OGSA Security Profile 1.0 - Secure Channel describes uses of widely accepted specifications that have been found to enable interoperability. The specifications considered in this profile are specifically those concerned with security of Web services: WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**] and its associated specifications. The requirements stated in this profile are concerned with security mechanisms for communications to ensure mutual authentication, integrity and confidentiality; the profile prescribes the use of these mechanisms to ensure secure communication of OGSA services in an inherently unsafe environment such as the Internet.

Contents

# 1 Introduction

This document defines the OGSA Security Profile 1.0 – Secure Channel (hereafter, "the Profile"). "Secure Channel" means a secure transport layer protocol with mutual authentication, integrity and confidentiality attributes. The Profile defines a Web services security profile along with clarifications, refinements, interpretations and amplifications of the underlying specifications that promote interoperability among implementations of those specifications in the context of OGSA services.

OGSA services are not required to use this Profile. OGSA services that require a secure transport should use this Profile in combination with an OGSA Basic Security Profile, for example, the "OGSA Basic Security Profile 1.0 – Core". Section 1.2 discusses in detail the relationship of the Profile with other profiles.

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 profiles and their extensibility points, followed by subsections that address individual parts of the component profiles. Note that there is no relationship between the section numbers in this document and those in the referenced profiles.

## 1.1 Profile Overview

The Profile is intended for use when securing interactions between 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 for communication defined in the WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**]. The Profile defines a set of conformance statements in order to ensure interoperability when using transport layer security for secure interactions between these services based on those profiles. A service implementation that is conformant with the Profile and with the OGSA WSRF Basic Profile 1.0 may be said to be an "implementation of the OGSA Security Profile 1.0 - Secure Channel" as well as an "implementation of the OGSA WSRF Basic Profile 1.0."

The primary issues addressed in the Profile are as follows:

- *Mutual Authentication.* The Profile mandates the use of a secure transport layer protocol to ensure mutual authentication of both ends of a Web service communication.
- *Integrity.* The Profile mandates the use of a secure transport layer protocol to ensure data integrity while communicating with Web services.
- *Confidentiality.* The Profile mandates the use of a secure transport layer protocol to ensure confidentiality of a Web service communication.

This is not a complete list; see the sections that follow for details.

Although the WS-I Basic Security Profile defines a security mechanism based on Web Services Security: SOAP Message Security 1.0 [**WS-Security**] (Message Level Security), the Profile does not specify anything about its use. This topic is out of scope of the Profile, but is expected to be addressed by other security profiles.

## 1.2 Relationships to Other Profiles

This Profile extends the WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**], in particular section 4, "Transport Layer Security." All requirements specified in WS-I BSP 1.0 pertain to this Profile.

The Profile addresses mutual authentication, integrity and confidentiality of communications of OGSA services, which are profiled by one of the OGSA Basic Profiles, such as the OGSA WSRF Basic Profile 1.0 [**OGSA WSRF Basic Profile**]. Another security issue which is considered to be common to all OGSA services, key information binding to an endpoint reference, is addressed in OGSA Basic Security Profile 1.0 – Core [**OGSA Basic Security Profile - Core**]. Thus the Profile is intended to be used in conjunction with the OGSA Basic Security Profile 1.0 – Core [**OGSA Basic Security Profile - Core**].

### 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 Security Profile 1.0 – Secure Channel**

| **Prefix** | **Namespace** |
|---|---|
| wsdl | http://schemas.xmlsoap.org/wsdl |

This Profile uses a number of special terms to refer to referenced specifications:

- **Basic-Security-Profile** – WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**]
- **HTTP-TLS** – HTTP Over TLS [**HTTP-TLS**]
- **TLS-Protocol** – The TLS Protocol Version 1.0 [**TLS 1.0**]

### 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 Security Profile – Secure Channel” 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

Since the Profile is an extension of the WS-I Basic Security Profile 1.0 it may place further restrictions on conformance targets defined in WS-I Basic Security Profile 1.0.

The following conformance targets are used in the Profile:

- **INSTANCE** – software that implements a wsdl:port (from WS-I Basic Profile 1.1, without “bindingTemplate” from the namespace urn:uddi-org:api_v2)

- **CONSUMER** – software that invokes an INSTANCE (from WS-I Basic Profile 1.1)
- **SENDER** – software that generates a particular message according to the protocol(s) associated with that message (from WS-I Basic Profile 1.1)
- **RECEIVER** – software that consumes a message according to the protocol(s) associated with that message (e.g., SOAP processors) (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/2006/01/sp–sc.

## 3 Security Profile

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

- WS-I Basic Security Profile Version 1.0 [**WS-I BSP 1.0**] extensibility points:
    - E0009 **– TLS Ciphersuites –** TLS allows for the use of arbitrary encryption algorithms. Note that while section 4.2 of **Basic-Security-Profile** mandates, recommends, and discourages support for certain ciphersuites, **Basic-Security-Profile** does not prohibit use of any specific ciphersuite. While section 3.3, 3.4 and 3.5 of the Profile prohibits certain ciphersuites, the Profile does not prohibit use of any specific ciphersuite other than those.
    - E0010 **– TLS Extensions –** TLS allows for extensions during the handshake phase.
    - E0011 **– SSL Ciphersuites –** SSL allows for the use of arbitrary encryption algorithms. Note that while section 4.2 of **Basic-Security-Profile** mandates, recommends, and discourages support for certain ciphersuites, **Basic-Security-Profile** does not prohibit use of any specific ciphersuite. While section 3.3, 3.4 and 3.5 of the Profile prohibits certain ciphersuites, the Profile does not prohibit use of any specific ciphersuite other than those.
    - E0002 **– Security Tokens –** Security tokens may be specified in additional security token profiles.
    - E0012 – **Certificate Authority** – The choice of the Certificate Authority is a private agreement between parties.
    - E0013 – **Certificate Extensions** – X.509 allows for arbitrary certificate extensions.

### 3.1 Secure Communication

The Profile defines a set of conformance statements for the use of TLS (Transport Layer Security) as a mean of securing communication. The objective of the use of this security mechanism is to secure interactions between services, and this Profile places the following constraints on its use.

#### *3.1.1 Using Transport Layer Security as a mean of Secure Communication*

All messages are subject to interference and corruption during transmission. To mitigate the risks of intentional or accidental modification to, or disclosure of, message data, the Profile defines the following constraints with regard to transmitting messages.

R0301 *An INSTANCE MUST support Transport Layer Security as profiled in section 3.2 of this Profile.*

R0302 *A CONSUMER MUST support Transport Layer Security as profiled in section 3.2 of this Profile.*

## 3.2 Transport Layer Security

The Profile defines a profile for the use of Transport Layer Security as an underlying protocol for message transmission. The Profile places the following constraints on its use.

### *3.2.1 SSL and TLS*

When using the Transport Layer Security as an underlying protocol for message transmission, the Profile places the following constraints on its use.

R0303 *When establishing an HTTP connection with Transport Layer Security a SENDER MUST use **HTTP-TLS** as profiled by **Basic-Security-Profile** section 4 and section 10.*

R0304 *When establishing an HTTP connection with Transport Layer Security a RECEIVER MUST use **HTTP-TLS** as profiled by **Basic-Security-Profile** section 4 and section 10.*

R0305 *When establishing a non-HTTP connection with Transport Layer Security a SENDER MUST use the SSL or **TLS-Protocol** and be compliant with **Basic-Security-Profile** section 4 and section 10.*

R0306 *When establishing a non-HTTP connection with Transport Layer Security a RECEIVER MUST use the SSL or **TLS-Protocol** and be compliant with **Basic-Security-Profile** section 4 and section 10*

### *3.2.2 Recommended Ciphersuites*

**Basic-Security-Profile** defines the mandatory and recommended ciphersuites to be supported by Web Services. The Profile defines the following constraints on the use of the ciphersuites.

R0307 *A TLS-capable INSTANCE and CONSUMER which support TLS_RSA_WITH_AES_128_CBC_SHA SHOULD use TLS_RSA_WITH_AES_128_CBC_SHA in establishing a secure communication.*

R0308 *A SSL-capable INSTANCE and CONSUMER which support SSL_RSA_WITH_AES_128_CBC_SHA SHOULD use SSL_RSA_WITH_AES_128_CBC_SHA in establishing a secure communication.*

R0309 *A TLS-capable INSTANCE and CONSUMER which support TLS_RSA_WITH_3DES_EDE_CBC_SHA but does not support AES algorithm SHOULD use TLS_RSA_WITH_3DES_EDE_CBC_SHA in establishing a secure communication.*

R0310 *A SSL-capable INSTANCE and CONSUMER which support SSL_RSA_WITH_3DES_EDE_CBC_SHA but does not support AES algorithm SHOULD use SSL_RSA_WITH_3DES_EDE_CBC_SHA in establishing a secure communication.*

## 3.3 Authentication

In order to provide both authorization and auditing of both parties in an interaction, this Profile requires mutually authenticated Web services communication.

### *3.3.1 Authentication*

The Profile prohibits anonymous communication and requires mutual authentication. This profile places the following constraints on authentication.

> R0317 *When establishing a secure communication, a CONSUMER MUST authenticate itself as part of the SSL or **TLS-Protocol**.*

> R0318 *When establishing a secure communication, an INSTANCE MUST authenticate itself as part of the SSL or **TLS-Protocol**.*

Ciphersuites listed in Table 2 in Appendix C do not provide mutual authentication. Therefore, the Profile prohibits their use.

## 3.4 Confidentiality

In order to provide confidentiality between both parties in an interaction, this Profile requires encrypted Web service communication.

### 3.4.1 Confidentiality

The Profile mandates the use a ciphersuite with a secure cipher algorithm. The Profile places the following constraints on confidentiality.

> R0319 *When establishing a secure communication, a SENDER and a RECEIVER MUST NOT use a ciphersuite with a cipher algorithm known to be insecure.*

> R0320 *When establishing a secure communication, a SENDER or a RECEIVER MUST NOT use a ciphersuite that uses a key with its length less than 64 bits.*

Ciphersuites listed in Table 3 in Appendix C meet the criteria of R0319 and R0320 at the time of publication of the Profile. On the other hand, the ciphersuites listed in Table 4 in Appendix C are known to be insecure and the Profile prohibits their use. Note that the tables shown in Appendix C are non-normative and their status are applicable at the time of publication of the Profile.

## 3.5 Message Integrity

In order to provide message integrity in an interaction, this Profile requires secure hash algorithm to be used.

### 3.5.1 Message Integrity

The Profile mandates the use a ciphersuite with secure hash algorithm. The Profile places the following constraints on confidentiality.

> R0321 *When establishing a secure communication, a SENDER and a RECEIVER MUST NOT use a ciphersuite with a hash algorithm known to be insecure.*

Ciphersuites listed in Table 3 in Appendix C meet the criteria of R0321 at the time of publication of the Profile. On the other hand the ciphersuites listed in Table 5 in Appendix C are known to be insecure and the Profile prohibits their use. Note that the tables shown in Appendix C are non-normative and their status are applicable at the time of publication of the Profile.

# 4 Contributors

## 4.1 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>

## 4.2 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.

## 4.3 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 and Alan Sill.

# 5 Intellectual Property Statement

The OGF 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 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.

# 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

- **[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-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

### 8.2 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, 1 September 2005. http://www.ggf.org/documents/GFD.72.pdf
- **[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
- **[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 - Core]** T. Mori and F. Siebenlist: OGSA Basic Security Profile 1.0 – Core, Open Grid Forum, Lemont, Illinois, U.S.A, GFD.86, November 2006. http://www.ggf.org/gf/docs/?final

## Appendix A. Referenced Specifications

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

- Basic Profile 1.1 [**WS-I BP 1.1**]
- Basic Security Profile Version 1.0 [**WS-I BSP 1.0**]
- HTTP Over TLS [**HTTP-TLS**]
- The TLS Protocol Version 1.0 [**TLS 1.0**]

## 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 WS-I Basic Security Profile 1.0 [**WS-I BSP 1.0**]:

- E0009 **– TLS Ciphersuites –** TLS allows for the use of arbitrary encryption algorithms. Note that while section 4.2 of the Basic Security Profile 1.0 mandates, recommends, and discourages support for certain ciphersuites, the Basic Security Profile 1.0 does not prohibit use of any specific ciphersuite. While section 3.3, 3.4 and 3.5 of the Profile prohibits certain ciphersuites, the Profile does not prohibit use of any specific ciphersuite other than those.

- E0010 **– TLS Extensions –** TLS allows for extensions during the handshake phase.

- E0011 **– SSL Ciphersuites –** SSL allows for the use of arbitrary encryption algorithms. Note that while section 4.2 of the Basic Security Profile 1.0 mandates, recommends, and discourages support for certain ciphersuites, the Basic Security Profile 1.0 does not prohibit use of any specific ciphersuite. While section 3.3, 3.4 and 3.5 of the Profile prohibits certain ciphersuites, the Profile does not prohibit use of any specific ciphersuite other than those.

- E0002 **– Security Tokens –** Security tokens may be specified in additional security token profiles.

- E0012 **– Certificate Authority –** The choice of the Certificate Authority is a private agreement between parties.

- E0013 **– Certificate Extensions –** X.509 allows for arbitrary certificate extensions

## Appendix C. Ciphersuites

(1) Anonymous Ciphersuites

The following table lists ciphersuites that do no provide authentication. The Profile prohibits their use.

**Table 2 Ciphersuites that do not provide authentication**

- TLS_DH_anon_EXPORT_WITH_RC4_40_MD5
- TLS_DH_anon_WITH_RC4_128_MD5
- TLS_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- TLS_DH_anon_WITH_DES_CBC_SHA
- TLS_DH_anon_WITH_3DES_EDE_CBC_SHA
- SSL_DH_anon_EXPORT_WITH_RC4_40_MD5
- SSL_DH_anon_WITH_RC4_128_MD5
- SSL_DH_anon_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_anon_WITH_DES_CBC_SHA
- SSL_DH_anon_WITH_3DES_EDE_CBC_SHA

(2) Allowed Ciphersuites

The following tables lists ciphersuites that are allowed by the Profile.

**Table 3 Allowed ciphersuites**

- TLS_DHE_DSS_WITH_AES_256_CBC_SHA
- TLS_DHE_RSA_WITH_AES_256_CBC_SHA
- TLS_RSA_WITH_AES_256_CBC_SHA
- TLS_DH_DSS_WITH_AES_256_CBC_SHA
- TLS_DH_RSA_WITH_AES_256_CBC_SHA
- TLS_DHE_DSS_WITH_AES_128_CBC_SHA
- TLS_DHE_RSA_WITH_AES_128_CBC_SHA
- TLS_RSA_WITH_AES_128_CBC_SHA
- TLS_DH_DSS_WITH_AES_128_CBC_SHA
- TLS_DH_RSA_WITH_AES_128_CBC_SHA
- TLS_DHE_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_DH_DSS_WITH_3DES_EDE_CBC_SHA
- TLS_DH_RSA_WITH_3DES_EDE_CBC_SHA
- TLS_RSA_WITH_RC4_128_SHA
- SSL_DHE_DSS_WITH_3DES_EDE_CBC_SHA

- SSL_DHE_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_DH_DSS_WITH_3DES_EDE_CBC_SHA
- SSL_DH_RSA_WITH_3DES_EDE_CBC_SHA
- SSL_RSA_WITH_RC4_128_SHA

(3) Ciphersuites with Insecure Encryption Algorithm

The following table lists ciphersuites that are known to use insecure encryption algorithms. The Profile prohibits their use.

**Table 4 Ciphersuites with Insecure Encryption Algorithm**

- TLS_RSA_WITH_NULL_MD5
- TLS_RSA_WITH_NULL_SHA
- TLS_RSA_EXPORT_WITH_RC4_40_MD5
- TLS_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- TLS_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_RSA_WITH_DES_CBC_SHA
- TLS_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
- TLS_DH_DSS_WITH_DES_CBC_SHA
- TLS_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DH_RSA_WITH_DES_CBC_SHA
- TLS_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_DSS_WITH_DES_CBC_SHA
- TLS_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA
- TLS_DHE_RSA_WITH_DES_CBC_SHA
- SSL_RSA_WITH_NULL_MD5
- SSL_RSA_WITH_NULL_SHA
- SSL_RSA_EXPORT_WITH_RC4_40_MD5
- SSL_RSA_EXPORT_WITH_RC2_CBC_40_MD5
- SSL_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_RSA_WITH_DES_CBC_SHA
- SSL_DH_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_DSS_WITH_DES_CBC_SHA
- SSL_DH_RSA_EXPORT_WITH_DES40_CBC_SHA
- SSL_DH_RSA_WITH_DES_CBC_SHA
- SSL_DHE_DSS_EXPORT_WITH_DES40_CBC_SHA
- SSL_DHE_DSS_WITH_DES_CBC_SHA
- SSL_DHE_RSA_EXPORT_WITH_DES40_CBC_SHA

- `SSL_DHE_RSA_WITH_DES_CBC_SHA`
- `SSL_FORTEZZA_DMS_WITH_NULL_SHA`

(4) Ciphersuites with Insecure Hash Algorithm

The following table lists ciphersuites that are known to use insecure hash algorithms. The Profile prohibits their use.

**Table 5 Ciphersuites with Insecure Hash Algorithm**

- `TLS_RSA_WITH_RC4_128_MD5`
- `SSL_RSA_WITH_RC4_128_MD5`

## 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 6.

**Table 6 Status of specifications referenced by OGSA Security Profile 1.0 – Secure Channel**

| **OGSA Referenced Specifications: OGSA Security Profile 1.0 - Secure Channel** | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| December 5, 2006 | **Status** | | | | | | | **Adoption** | | | | | | |
| **Specification/Profile Name** | De Facto | Institutional | Evolving Institutional | Draft Institutional | Consortium | Evolving Consortium | Draft | Ubiquitous | Adopted | Community | Interoperable | Implemented | Unimplemented | **Note** |
| **Specifications** | | | | | | | | | | | | | | |
| RFC2246: The TLS Protocol Version 1 | X | | | | | | | X | | | | | | |
| RFC2818: HTTP Over TLS | X | | | | | | | X | | | | | | |
| | | | | | | | | | | | | | | |
| **Profiles** | | | | | | | | | | | | | | |
| WS-I Basic Profile 1.1 | | X | | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | Final Material |
| WS-I Basic Security Profile 1.0 | | < | X | | | | | ▨ | ▨ | ▨ | ▨ | ▨ | ▨ | Working Group Draft |
| | | | | | | | | | | | | | | |

| | | |
|---|---|---|
| **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 |

**Goto:** Index EditMaster CopyMaster