

GT4 Java WS A&A Release Notes

Table of Contents

1. Component Overview	1
2. Feature Summary	1
3. Summary of Changes in Java WS A&A	3
4. Bug Fixes	4
5. Known Problems	5
6. Technology dependencies	6
7. Tested platforms	6
8. Backward compatibility summary	7
9. Associated Standards	7
10. For More Information	8

<titleabbrev>Release Notes</titleabbrev>

1. Component Overview

The Web Services portion of GT 4.2.0 uses SOAP over HTTP for communicating messages. WS Authentication & Authorization in Java (Java WS A&A) implements the WS-Security standard and the WS-SecureConversation specification to provide message protection for SOAP messages. Features include:

- authentication of the sender
- encryption of the message
- integrity protection of the message
- replay attack protection

Java WS A&A provides a secure channel by using HTTP over SSL/TLS (HTTPS) for transporting the messages. This security mechanism supports all of the security features provided by SSL/TLS with the addition of support for X.509 *Proxy Certificates*. The Authorization Framework component of Java WS A&A provides the infrastructure to process attributes and protect resource access based on access policy. It allows for authorization policy to be configured and enforced at various levels of granularity (container, service or resource). It also provides client-side authorization to allow clients to authorize the services they access. The framework is pluggable and can be configured to use custom mechanisms for attribute collection and policy evaluation. It also provides multiple authorization module implementations; for example, support for gridmap-based authorization, a callout module that uses the SAML protocol to query an external service for an authorization decision and such.

2. Feature Summary

2.1. Authentication/message protection features

Features new in GT 4.2.0

None.

Other Supported Features

- Compliance with published IBM/Microsoft WS-Trust and WS-SecureConversation specifications
- Compliance with the Web Services Security 1.0 standard
- HTTPS support
- Message encryption, integrity protection and replay attack prevention
- Establishment of a session key for light-weight message protection

Deprecated Features

- None.

2.2. Authorization features

Features new in GT 4.2.0:

- *Enhanced server-side attributed-based authorization framework:* The server-side authorization framework has been reworked to support attribute based authorization with delegation of rights. The framework allows for configuring a chain of Policy Information Points(PIPs) and Policy Decision Points(PDPs) and a combining algorithm that processes the individual decisions returned by the PDPs. Some of the key changes from the previous versions are:
 - Java Server side authorization framework has been moved to an independent module. Refer to Changes Summary for details.
 - Authorization framework uses a set of attributes to identify entities
 - The authorization engine uses Java Security provider framework to allow different combining algorithms to be plugged in.
 - A default implementation of permit override combining algorithm, which looks for a permit decision chain, to allow for fine grained delegation of rights.

Refer [Chapter 5, Architecture and design overview](#) for detailed information on the architecture.

- *Host or Self Authoriation:* Support for a pluggable PDP that does host authorization, and if that fails, tries self authorization.
- The security descriptor framework, used to configure security properties for the security framework has been enhanced. Detailed information about the framework is provided [Java WS A&A Security Descriptor Framework](#).

Other Supported Features

- Authorization based on `grid-mapfile` and other access control lists.
- Ability to implement custom authorization modules.
- A SAML callout authorization module enables outsourcing of authorization decisions to an authorization service (e.g. PERMIS).

Deprecated Features

- None

3. Summary of Changes in Java WS A&A

3.1. Summary of Changes in message/transport-level security

The following changes have occurred for Message/Transport-level Security since GT 4.0.x :

- Added support for signing policy enforcement. Disabling the enforcement is provided directly by the CoG JGlobus library, [Section 2, “Signing Policy Location”](#).
- The security descriptor framework, used to configure security properties for the security framework has been enhanced. Detailed information about the framework is provided at [Chapter 1, Security Descriptors Introduction](#).
- Java WS Authentication code honors environment variables to pick up credential to use as described [here](#)¹.
- Java WS Authentication code allows configuration of trust certificate in non-default location as described [here](#)².

3.2. Summary of Changes in WS Authorization Framework

The server side authorization framework has been reworked to support attribute-based authorization. The APIs and framework have been enhanced to deal with a representation where each entity is identified by a bag of attributes.

Also the default engine used for combining the individual Policy Decision Point(PDP) decision has been changed from a deny-override algorithm to a permit override scheme that looks for a chain of delegation of rights from the resource owner to the requestor.

Refer [Chapter 5, Architecture and design overview](#) for detailed information on the architecture.

Important

The WS authorization interfaces have been frozen as of the GT 4.1.2 release.

Note

All the PDPs that were distributed with the previous version have been ported to new framework and are supported.

3.2.1. Java WS Authorization Code reorganization *[post 4.1.3 only]*

The Java WS server side authorization code has been moved to a separate module called `authorization`. The work was tracked as part of [Bug 5559](#)³ and while this does not change any interface on the server side, it separates the code from the Java WS Core module.

A migration guide, that outlines the changes needed for services that build on Java WS Core is provided [here](#)⁴.

¹ http://bugzilla.mcs.anl.gov/globus/show_bug.cgi?id=4146

² http://bugzilla.mcs.anl.gov/globus/show_bug.cgi?id=3843

³ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5559

⁴ http://dev.globus.org/wiki/Java_WS_Core/Independent_Java_Authz_Module

4. Bug Fixes

- [Bug 2535](#):⁵ <proxy-file> causes container to fail
- [Bug 2651](#):⁶ /dev/random vs. /dev/urandom
- [Bug 2743](#):⁷ grid-mapfile location should be in global security descriptor
- [Bug 2207](#):⁸ Missing security error 'timestampNotOk'
- [Bug 2651](#):⁹ /dev/random vs. /dev/urandom
- [Bug 2743](#):¹⁰ grid-mapfile location should be in global security descriptor
- [Bug 2899](#):¹¹ relative path does not work for credentials in Security Descriptor
- [Bug 2900](#):¹² Job submission does not work using relative path in global_security_descriptor.xml and absolute path in sudoers.
- [Bug 2955](#):¹³ Job submission fails when container is started from non GLOBUS_LOCATION
- [Bug 2969](#):¹⁴ Too relaxed rules on DN comparisons (all versions of GT)
- [Bug 3849](#):¹⁵ Container descriptor is shared across containers in one JVM
- [Bug 3689](#):¹⁶ Possible royalty / patent issue with BouncyCastle jar IDEA Algorithm
- [Bug 3891](#):¹⁷ Public credentials of client in peer subject
- [Bug 3965](#):¹⁸ Credential refresh problems
- [Bug 4021](#):¹⁹ globus-start-container -containerDesc not working
- [Bug 4136](#):²⁰ At least one of the headers used in dispatch was not secured error
- [Bug 4146](#):²¹ setting default container security via environment
- [Bug 4507](#):²² Problem with corrupted CRL

⁵ http://bugzilla.globus.org/globus/show_bug.cgi?id=2535

⁶ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2651

⁷ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2743

⁸ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2207

⁹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2651

¹⁰ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2743

¹¹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2899

¹² http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2900

¹³ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2955

¹⁴ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2955

¹⁵ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3849

¹⁶ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3689

¹⁷ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3891

¹⁸ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3965

¹⁹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4021

²⁰ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4136

²¹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4146

²² http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4146

- [Bug 4535](#)²³ Client security descriptor does not allow for GSI Transport configuration
- [Bug 4584](#)²⁴ security descriptor uses operation field name instead of QName
- [Bug 4837](#)²⁵ Username/password not working.
- [Bug 4846](#)²⁶ Authorization framework should preserve the order of attributes
- [Bug 4893](#)²⁷ Improve ParameterPIP test
- [Bug 5076](#)²⁸ Authorization interface declares serializable, but impls are not
- [Bug 5544](#)²⁹ Interceptor initializes twice
- [Bug 5608](#)³⁰ More details in security logging please
- [Bug 5756](#)³¹ allow developer to bypass secure msg consistency check
- [Bug 5757](#)³² allow developer to bypass sending cert chain in secure message

5. Known Problems

The following problems and limitations are known to exist for Java WS A&A at the time of the 4.2.0 release:

5.1. Limitations

- No known limitations exist.

5.2. Outstanding bugs

- [Bug 2362](#)³³ location of user proxy for java inconsistencies
- [Bug 2445](#)³⁴ Holder problem
- [Bug 2907](#)³⁵ Secure Conversation (Encryption) does not provide any message level security for the SOAP headers
- [Bug 3027](#)³⁶ Kerberos based authentication option for GT4
- [Bug 3171](#)³⁷ add RFC 2253 principal name to JAAS subject
- [Bug 3449](#)³⁸ ERROR container.GSIServiceThread

²³ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4535

²⁴ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4584

²⁵ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4837

²⁶ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4846

²⁷ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4893

²⁸ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5076

²⁹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5544

³⁰ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5608

³¹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5756

³² http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5757

³³ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2362

³⁴ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2445

³⁵ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2907

³⁶ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3027

³⁷ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3171

³⁸ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3449

- [Bug 3603](#).³⁹ Remote exceptions thrown contain server specific information
- [Bug 3928](#).⁴⁰ IPv6 addresses in reverse lookups - fix or faq?
- [Bug 3941](#).⁴¹ Expired credentials detected - candidate for sec error msg improvements
- [Bug 4222](#).⁴² Allow for credential refresh in subscriptions
- [Bug 4403](#).⁴³ Secure calls for secure context establishment
- [Bug 4442](#).⁴⁴ Security descriptor refresh
- [Bug 5008](#).⁴⁵ voms-proxy-init creates non-critical KeyUsage extension which causes Java GSI to raise exception
- [Bug 5026](#).⁴⁶ Signarure validation failure on GRAM/RFT interaction on some cases

6. Technology dependencies

Java WS A&A depends on the following GT components:

- Java WS Core.

Authentication and message-protection depends on the following 3rd party software:

- Apache WSFX Security Libraries
- PureTLS Libraries
- BouncyCastle JCE provider
- Cryptix Libraries
- Apache XML Security Libraries

The authorization framework depends on the following 3rd party software:

- OpenSAML

7. Tested platforms

Java WS A&A should work on any platform that supports J2SE 1.3.1 or higher.

Tested Platforms for Java WS A&A:

- Linux (Red Hat 7.3)
- Windows 2000

³⁹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3603

⁴⁰ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3928

⁴¹ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=3941

⁴² http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4222

⁴³ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4403

⁴⁴ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4442

⁴⁵ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5008

⁴⁶ http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5026

- Solaris 9

8. Backward compatibility summary

8.1. Authentication compatibility

Since GT 4.0.x release, some incompatible changes have been made:

- Security Descriptors: The security descriptor schema has changed since GT 4.0.x and the descriptors from GT 4.0.x cannot be used as is.
- Secure Conversation port type: The WS Addressing version in Java WS Core has been updated and the secure conversation port type has changed to reflect this. Therefore, GT 4.0.x secure conversation clients are incompatible with GT 4.2.x servers and vice versa.

8.2. Authorization compatibility

The authorization framework has been reworked as described in [Change Summary](#). The configuration and authorization interfaces have since changed and a [Migration Guide](#) is provided.

9. Associated Standards

Associated standards for Java WS A&A:

- [WS-Security](#)⁴⁷
- [WS-Security: X.509 Certificate Tokens](#)⁴⁸
- [WS-Security: Username Tokens](#)⁴⁹
- [WS-Trust](#)⁵⁰
- [WS-Secure Conversation](#)⁵¹
- [WS-I Basic Security Profile](#)⁵²
- [RFC 3820](#)⁵³ Proxy Certificates
- [RFC 2818](#)⁵⁴ HTTP over TLS
- [RFC 2246](#)⁵⁵ TLS
- [JAAS](#)⁵⁶

⁴⁷ <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-soap-message-security-1.0.pdf>

⁴⁸ <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-x509-token-profile-1.0.pdf>

⁴⁹ <http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-username-token-profile-1.0.pdf>

⁵⁰ <ftp://www6.software.ibm.com/software/developer/library/ws-trust052004.pdf>

⁵¹ <ftp://www6.software.ibm.com/software/developer/library/ws-secureconversation052004.pdf>

⁵² <http://www.ws-i.org/Profiles/BasicSecurityProfile-1.0.html>

⁵³ <http://www.faqs.org/rfcs/rfc3820.html>

⁵⁴ <http://www.faqs.org/rfcs/rfc2818.html>

⁵⁵ <http://www.faqs.org/rfcs/rfc2246.html>

⁵⁶ <http://java.sun.com/products/jaas/>

Associates standards for the authorization framework:

- [Simple Assertion Markup Language](#)⁵⁷
- [SAML Schema Protocol](#)⁵⁸

10. For More Information

See [Java WS A&A](#) for more information about this component.

DRAFT

⁵⁷ http://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security

⁵⁸ <http://www.oasis-open.org/committees/download.php/3407/oasis-sstc-saml-schema-protocol-1.1.xsd>