GFD-I.078
Individual submission

Von Welch, NCSA
February 24, 2006
Revised: May 30, 2006

Grid Security Infrastructure Message Specification

Abstract

This document provides a description of the mechanism used to secure messages exchanged by the Globus Toolkit pre-web services and the format of portion of those messages related to security. It captures the message formatting performed by the Grid Security Infrastructure (GSI) GSS-API libraries. It is applicable to developers wishing to interoperate with pre-web services GT services, including the GridFTP server.

Contents

1 Introduction

This document describes the order and content of the messages generated by the Globus Toolkit Grid Security Infrastructure (GSI) [GSI] as supplied in pre-web services Globus Toolkit libraries. This document does not attempt to define the full content of all these messages since their content is based on messages defined by the Secure Socket Layer version 3 (SSLv3); instead it defines only the differences and extensions that GSI makes to SSLv3. These messages are used for communications by pre-web services components of the Globus Toolkit, which at this time includes GridFTP and the pre-web services GRAM.

Depending on the application using GSI, the messages specified in this document may be carried directly over a TCP connection (and look very much like SSLv3), as with pre-web services GRAM, or they may be carried in higher-level protocols, such as GridFTP [GridFTP] ADAT packages [ADAT]. This document does not attempt to define full protocol specifications for all these scenarios, simply the flow and contents of the GSI messages carried in those protocols. Readers are directed to the referenced documents to see how GSI messages are used in those contexts.

Section 2 covers prerequisite reading for this document. Section 3 covers terminology used in this document. Section 4 contains the description of the contents of the GSI messages. Section 5 contains acknowledgements and Section 6 contains references.

2 Prerequisites

It is assumed that the reader is familiar with the following technologies:

- Public Key Infrastructure and X.509 Certificates [RFC 3280]: GSI bases its credentials on X.509 certificates.
- Secure Socket Layer version 3 (SSLv3) [SSL] protocol: GSI is built on SSLv3 and the GSI messages are described by reference to SSLv3 in a number of places in this document.
- Generic Security Services API (GSS-API) [GSS-API]. GSI is accessed via the GSS-API and understanding GSS-API will help a reader understand how GSI functions. Note however that the messages generated by GSI do not fully comply with the GSS-API specification in that they lack an identifying preamble.
- X.509 Proxy Certificates [RFC 3820, Proxies, GT4-Sec]: Proxy certificates are used as an extension to X.509 End Entity Certificates by GSI to support delegation and single sign-on.

3 Terminology

The following terms are used freely in this document. A more complete discussion of the different types of proxy certificates can be found in [GT4-Sec].

- *Client, Server*: The terms *client* and *server* are used throughout this document to describe the two parties exchanging GSI messages. The client is defined as the party which initiates the GSI message exchange. This is usually, but not always,

the party which initiates the underlying network connection over which the GSI messages are being exchanged. The server is defined as the party that receives the GSI message exchange. This is usually, but not always, the party which accepts the underlying network connection.

- *End Entity Certificate chain (EEC chain)*: A standard certificate chain for a user or server as defined by RFC 3280 [RFC3280].
- *GT2*: Globus Toolkit version 2.
- *GT3*: Globus Toolkit version 3.
- *GT4*: Globus Toolkit version 4.
- *GT2 Proxy Certificate Chain*: A X.509 certificate chain with one or more pre-RFC 3820 proxy certificates as described in [GT4-Sec]. These were predominately used in GT2 and are now deprecated.
- *GT4 Default Proxy Certificate Chain*: These proxies follow the format of RFC 3820 [Proxies], except they use a proprietary OID (1.3.6.1.4.1.3536.1.222) for the ProxyCertInfo extension. These are created by GT4 grid-proxy-init by default, but will be deprecated in a future version of the Globus Toolkit.
- *RFC 3820 Proxy Certificate Chain*: These proxies are fully compliant with RFC 3820 [Proxies] and can be created by the Globus Toolkit 'grid-proxy-init –rfc' command. They are expected to be the default in the future.
- *Proxy Certificate Chain:* When used without qualification, this term means any of the types of Proxy Certificate chain.
- *SSLv3:* Secure Socket Layer version 3 [SSL]
- *SSL Compatibility Mode:* Normally GSI extends the SSL protocol to allow for delegation and better performance. GSI can be run in SSL compatibility mode, which turns off these features and allows for GSI messages to be transmitted over a TCP connection to look identical to SSL over TCP. This mode is not used in general and is not covered in this document.

4 Specification of Messages

An exchange of GSI messages has three phases, which occur in the given order:

- Context establishment, where the two parties authenticate to each other and establish a context to protect further message exchange.
- Delegation, where the client may delegate credentials to the service for later use on their behalf; and
- Application-specific, in which application data is exchanged, optionally protected by the context established in the first phase. Further delegations may also take place during this phase

In the context of using the GSS-API, the authentication and delegation phases are accomplished by calls to the gss_init_sec_context() and gss_accept_sec_context() calls and application data protection is accomplished by the gss_wrap() call.

The following subsections describe each phase of messages in detail.

4.1 Context Establishment Messages

In this phase the client and server are authenticated to each other and security information is exchanged in order to provide message protection for further data exchanges. In terms of the wire protocol, the context establishment phase is nothing more than normal SSLv3 handshake messages being exchanged.

The following attributes apply to the exchange:

- Either client or server may use a standard EEC certificate chain or a Proxy Certificate chain for authentication.
- Client authentication is optional in terms of the protocol, though most GSI-based services require it.
- The client must send an SSL 3.0 client hello message and must not send an SSL 2.0 client hello message (see RFC 2246 Section E).
- GSI supports all the ciphers of the underlying SSL implementation it is built on. At the time of this writing that list is:
    - Encryption: DES, Triple-DES, IDEA, RC4, RC2
    - MAC: SHA1, MD5
    - The default cipher set is triple-DES with SHA1.
    - Encryption is optional, but integrity protection is required.

4.2 Delegation Messages

In this phase the client may, at the client discretion, delegate credentials to the server. These credentials can then be used by the server (or processes initiated by the server) on the client's behalf. GSI delegation consists of three messages:

1. A delegation flag from client to server indicating desire to delegate.
2. A PKCS10 certificate request [PKCS10] from server to client. This primarily serves to contain the public key of a newly generated key pair by the server.
3. A Proxy Certificate chain from client to server binding the public key provided by the server to an identity derived from the client identity.

While GSI does support delegation in either direction later during the exchange of application data (as described in Section 4.4), delegation during the delegation phase of the protocol may only occur from client to server.

Delegation messages are protected by the SSLv3 context established in the first phase of message exchanges. From the perspective of the SSLv3 protocol, they are treated as any other application data. This means they are, at a minimum, integrity protected and may also be encrypted, depending on the ciphers chosen during context establishment.

4.2.1 Delegation Flag

The first message is sent from client to server and indicates whether delegation will take place. This message consists of a single octet, which has the following legal values:

- "D" (ASCII code 68): Indicates that the client wishes to perform delegation.
- "0" (ASCII code 48): Indicates that the client does not wish to perform delegation.

No codes other than those above should be sent. Some early java implementations of GSI would send a "1" (ASCII code 49) instead of a "D"; it is believed that none of these implementations are still in use, but implementations desiring the greatest robustness should treat a "1" identically to a "D".

Behavior upon receiving other codes is undefined.

If the client does not wish to perform delegation, no further delegation messages are exchanged and further messages are application data as described in Section 4.3

If the client does wish to perform delegation, the rest of the messages described in section 4.2 are exchanged.

4.2.2 Certificate Request

In response to a client indicating that it wishes to perform delegation, the server should send a PKCS10 certificate request.

The following components of the certificate request are meaningful:

- *Public key:* This will be the public key placed in the returned Proxy Certificate.
- *Proxy Policy:* If a ProxyCertInfo extension, as defined in [Proxies], is present. The Proxy Policy and Policy Languages fields will be duplicated in the returned Proxy Certificate unless the client specifically overrides them.
- *Subject Name:* Some GT2 implementations treat the Subject Name in the certificate request as meaningful. To accommodate this a server expecting a client to delegate a GT2 Proxy Certificate (which should only happen if the client authenticated with a GT2 Proxy Certificate) should fill in the Subject Name in the certificate request with the subject name it expects to see in the delegated certificate (i.e. the client's subject name with a "CN=Proxy" component appended, see Section 4.5).

All other components of the certificate request are ignored by the client.

4.2.3 Delegated Certificate Chain

In response to the certificate request from the server, the client should respond by sending a Proxy Certificate chain. This chain should conform to the following:

- It must be a sequence of individual DER-encoded certificates (as opposed to a ASN.1 SEQUENCE).
- The new Proxy Certificate should be first, followed by other certificates, whose order is unimportant.

- The chain must include at least the new Proxy Certificate, but may include all certificates in the Proxy Certificate chain.
- If the client used a Proxy Certificate chain to authenticate, the type of new Proxy Certificate (i.e. GT2, GT4 Default, or RFC 3820 as described in Section 3) must match the type of Proxy Certiificate Chain used to authenticate.
- If the client did not use a Proxy Certificate chain to authenticate, the client is free to delegate using any type of Proxy Certificate chain, though GT2 Proxy Certificate Chains should be avoided. At some point RFC 3820 Proxy Certificates chains will become the preferred mechanism.

4.3 Application Data Protection

In this phase application-specific data is exchanged. It may be protected by GSI to provide integrity and confidentiality. Delegation can also occur during this phase as described in Section 4.4, but its framing will be completely application dependent.

There are three basic ways application data can be protected during this phase:

- *Using SSL-formated messages.* These application messages are simply the application data protected by SSLv3 using the context and ciphers derived during context establishment (Section 4.1). GSI does not add to or modify these messages as defined by SSL.
- *Using a separate signature.* In this mode the message format is completely application-specific, but GSI provides signature elements which provide integrity protection for these messages (via the GSS-API getmic() call). The signature element is composed of the sequence of an 8 octet sequence number, a 4 octet message length and then the normal digest (whose length depends on the digest mechanism selected during context establishment). How these signature elements are conveyed is application-specific. This was used in GT3 SOAP messages, but there is no current protocol that utilizes this.
- *Unprotected.* Messages may be completely unprotected by GSI and formatted in any manner the application desires.

It is possible, though not customary, to mix these various types of protection during an application session. How these changes in quality of protection are negotiated between the two parties is completely application dependent.

4.4 Delegation after Context Establishment

If an application wishes it may use the GGF-defined GSS-Extensions [GSS-Ext] to perform delegation at any time during application data exchange. This is typically only used in applications that do credential management (e.g. MyProxy [MyProxy]).

Note that in these cases it is up to the application to appropriately frame the delegation so that both sides are aware of the delegation.

Delegation in this context may occur in either direction (client to server or server to client) as framed by the application protocol.

The messages exchanged are identical to the messages exchanged in the delegation that happens immediately after context establishment (Section 4.2). Note that the delegation flag, as described in Section 4.2.1, contained in the first message must always be a "D" indicating the desire to delegate.

4.5 Supported Keys

GSI should, in theory, support any type and size of key supported by SSLv3 as part of either an end entity or proxy certificate chain. At this time the keys in general use are RSA keys (512, 1024, and 2048 bits).

4.6 Error Handling

During the context establishment phase, SSLv3 alert messages may be exchanged by either side to indicate that a local error has occurred. Upon receiving such an alert message, the recipient should discontinue the current attempt at context establishment.

In other phases of message exchange, GSI does not have a defined method for error handling.

5 Acknowledgements

Contributions to the GSI concepts and code and this document have been made by (in alphabetical order with apologies to anyone missed): Doug Engert, Ian Foster, Jarek Gawor, Carl Kesselman, Sam Lang, Sam Meder, Olle Mulmo, Laura Pearlman, Frank Siebenlist, Steve Tuecke, Von Welch.

We also thank Matt Crawford for comments made on an earlier version of this document.

Numerous parties contributed to the design of the IETF Proxy Certificate specification and are listed in that document [Proxies].

6 References

[ADAT] Horowitz, M. and Lunt S. FTP Security Extensions. Internet RFC 2228, 1997.

[GridFTP] W. Allcock (editor), GridFTP: Protocol Extensions to FTP for the Grid. GFD-20, April 2003. http://www.ggf.org/documents/GFD.20.pdf

[GSI] V. Welch, F. Siebenlist, I. Foster, J. Bresnahan, K. Czajkowski, J. Gawor, C. Kesselman, S. Meder, L. Pearlman, S. Tuecke. Security for Grid Services. *Twelfth International Symposium on High Performance Distributed Computing (HPDC-12)*, IEEE Press, to appear June 2003.

[GSS-API] Linn, J. Generic Security Service Application Program Interface, Version 2. *INTERNET RFC 2078*, 1997.

[GSS-Ext] Meder, S., Welch, V., Tucke, S., and Engert, D. GSS-API Extensions. GFD-E.024, June 2004. http://www.ggf.org/documents/GFD.24.pdf

[GT4-Sec] Globus Security Team, Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective. Version 4, September 12th, 2005. http://www.globus.org/toolkit/docs/4.0/security/GT4-GSI-Overview.pdf

[MyProxy] J. Basney, MyProxy Protocol. GFD-E.054 , November, 2005. http://www.gridforum.org/documents/GFD.54.pdf

[Proxies] Von Welch, Ian Foster, Carl Kesselman, Olle Mulmo, Laura Pearlman, Steven Tuecke, Jarek Gawor, Sam Meder, and Frank Siebenlist. X.509 Proxy Certificates for dynamic delegation. In Proceedings of the 3rd Annual PKI R&D Workshop, 2004. http://grid.ncsa.uiuc.edu/papers/pki04-welch-proxy-cert-final.pdf

[PKCS10] Kaliski, B., PKCS #10: Certification Request Syntax v1.5, RFC 2314, October 1997.

[RFC 3280] Houseley, R., Polk, W., Ford, W., and Solo, D. Internet X.509 Public Key Infrastructure Certificate and Certificate Revocation List (CRL) Profile, Internet RFC 3280, 2002.

[RFC 3820] Steven Tuecke, Von Welch, Doug Engert, Laura Perlman, and Mary Thompson. RFC3820: Internet X.509 Public Key Infrastructure (PKI) Proxy Certificate Profile. In RFC3820. Internet Engineering Task Force, 2004. http://www.ietf.org/rfc/rfc3820.txt

[SSL] Dierks, T. and Allen, C. The TLS Protocol Version 1.0, IETF, 1999. http://www.ietf.org/rfc/rfc2246.txt.

7 Security Considerations

This document contains the description of the implemented GSI message protocol. While this protocol has been successfully used for a number of years and undergone some scrutiny by the community, it has not received a full security protocol analysis and has not been critically reviewed by any OGF working group.

8 Author Information

Von Welch
vwelch@ncsa.uiuc.edu
1205 W. Clark
Urbana IL 61801
217-265-7139

9 Intellectual Property Statement

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 Full Copyright Notice