

# GT 4.2.0 Release Notes: GSI-OpenSSH

## Table of Contents

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

<titleabbrev>Release Notes</titleabbrev>

## 1. Component Overview

GSI-OpenSSH is a modified version of OpenSSH that adds support for X.509 *proxy certificate* authentication and delegation, providing a single sign-on remote login and file transfer service. GSI-OpenSSH can be used to login to remote systems and transfer files between systems without entering a password, relying instead on a valid *proxy credential* for authentication. GSI-OpenSSH forwards proxy credentials to the remote system on login, so commands requiring proxy credentials (including GSI-OpenSSH commands) can be used on the remote system without the need to manually create a new proxy credential on that system.

## 2. Feature summary

Features new in GT 4.2.0

- None.

Other Supported Features

- The **gsissh** command provides a secure remote login service with forwarding of X.509 *proxy credentials*.
- The **gsisftp** and **gsiscp** commands provide a secure file transfer service authenticated with X.509 proxy credentials, mimicking the **rcp/scp** and **ftp/sftp** commands.
- All standard OpenSSH features are supported, excluding Kerberos authentication. Kerberos authentication is *not* compatible with GSI-enabled OpenSSH.
- The GSI-OpenSSH server can replace the standard system SSH server in typical environments.
- If no username is given on the command-line, GSI-OpenSSH automatically determines the username that corresponds to the X.509 proxy *certificate subject* in the server's `grid-mapfile`.

Deprecated Features

- None

## 3. Summary of Changes in GSI-OpenSSH

The following changes have occurred for GSI-OpenSSH since the last stable release, 4.0.x:

- Updated GPT package from 4.2 to 4.3.
- Upgraded to OpenSSH 5.0p1 to address [Globus Security Advisory 2008-01](#)<sup>1</sup>.
- Upgraded to [HPN13v1](#)<sup>2</sup>.

## 4. Bug Fixes

None.

## 5. Known Problems

The following problems and limitations are known to exist for GSI-OpenSSH at the time of the 4.2.0 release:

### 5.1. Limitations

- No known limitations exist.

### 5.2. Outstanding bugs

No bugs are known to exist for GSI-OpenSSH.

## 6. Technology dependencies

GSI-enabled OpenSSH depends on the following GT components:

- Non-WS Authentication and Authorization

GSI-enabled OpenSSH depends on the following 3rd party software:

- [OpenSSH](#)<sup>3</sup>

## 7. Tested platforms

Tested Platforms for GSI-OpenSSH

- Mac OS X 10.3
- i686 GNU/Linux
- ia64 GNU/Linux

---

<sup>1</sup> [http://www.globus.org/mail\\_archive/security-announce/2008/04/msg00000.html](http://www.globus.org/mail_archive/security-announce/2008/04/msg00000.html)

<sup>2</sup> <http://www.psc.edu/networking/projects/hpn-ssh/>

<sup>3</sup> <http://www.openssh.org/>

## 8. Backward compatibility summary

Protocol changes since GT 4.0.x

- None.

API changes since GT 4.0.x

- None.

Exception changes since GT 4.0.x

- Not applicable

Schema changes since GT 4.0.x

- Not applicable

## 9. Associated Standards

Associated standards for GSI-OpenSSH:

- [RFC 2743](http://www.ietf.org/rfc/rfc2743.txt)<sup>4</sup> GSSAPI
- [RFC 2744](http://www.ietf.org/rfc/rfc2744.txt)<sup>5</sup> GSSAPI: C-bindings
- [RFC 4462](http://www.ietf.org/rfc/rfc4462.txt)<sup>6</sup> GSSAPI Authentication and Key Exchange for the SSH Protocol

## 10. For More Information

See [GSI-OpenSSH](#) more information about this component.

## Glossary

### C

certificate subject

An identifier for the certificate owner, e.g. `"/DC=org/DC=doegrids/OU=People/CN=John Doe 123456"`. The subject is part of the information the CA binds to a public key when creating a certificate.

### P

proxy certificate

A short lived certificate issued using a EEC. A proxy certificate typically has the same effective subject as the EEC that issued it and can thus be used in its place. GSI uses proxy certificates for single sign on and delegation of rights to other entities.

<sup>4</sup> <http://www.ietf.org/rfc/rfc2743.txt>

<sup>5</sup> <http://www.ietf.org/rfc/rfc2744.txt>

<sup>6</sup> <http://www.ietf.org/rfc/rfc4462.txt>

For more information about types of proxy certificates and their compatibility in different versions of GT, see <http://dev.globus.org/wiki/Security/ProxyCertTypes>.

proxy credentials

The combination of a proxy certificate and its corresponding private key. GSI typically stores proxy credentials in `/tmp/x509up_u<uid>`, where `<uid>` is the user id of the proxy owner.

DRAFT