

# **GT 4.0: Credential Management: SimpleCA**

---

## **GT 4.0: Credential Management: SimpleCA**

---

---

# Table of Contents

1. Key Concepts .....	1
1. Overview .....	1
2. Conceptual Details .....	1
3. Related Documents .....	4
2. Admin Guide .....	8
1. Introduction .....	8
2. Building and Installing .....	8
3. Configuring .....	13
4. Deploying .....	13
5. Testing .....	13
6. Security Considerations .....	14
7. Troubleshooting .....	14
3. Fact Sheet .....	15
1. Brief overview .....	15
2. Summary of features .....	15
3. Usability summary .....	15
4. Backward compatibility summary .....	15
5. Technology dependencies .....	15
6. Tested platforms .....	16
7. Associated standards .....	16
8. For More Information .....	16
4. 4.0.8 Release Notes .....	17
1. Introduction .....	17
2. Changes Summary .....	17
3. Bug Fixes .....	17
4. Known Problems .....	17
5. For More Information .....	17
5. 4.0.7 Release Notes .....	18
1. Introduction .....	18
2. Changes Summary .....	18
3. Bug Fixes .....	18
4. Known Problems .....	18
5. For More Information .....	18
6. 4.0.6 Release Notes .....	19
1. Introduction .....	19
2. Changes Summary .....	19
3. Bug Fixes .....	19
4. Known Problems .....	19
5. For More Information .....	19
7. 4.0.5 Release Notes .....	20
1. Introduction .....	20
2. Changes Summary .....	20
3. Bug Fixes .....	20
4. Known Problems .....	20
5. For More Information .....	20
8. 4.0.4 Release Notes .....	21
1. Introduction .....	21
2. Changes Summary .....	21
3. Bug Fixes .....	21
4. Known Problems .....	21
5. For More Information .....	21

9. 4.0.3 Release Notes .....	22
1. Introduction .....	22
2. Changes Summary .....	22
3. Bug Fixes .....	22
4. Known Problems .....	22
5. For More Information .....	22
10. 4.0.2 Release Notes .....	23
1. Introduction .....	23
2. Changes Summary .....	23
3. Bug Fixes .....	23
4. Known Problems .....	23
5. For More Information .....	23
11. 4.0.1 Release Notes .....	24
1. Introduction .....	24
2. Changes Summary .....	24
3. Bug Fixes .....	24
4. Known Problems .....	24
5. For More Information .....	24
12. 4.0.0 Release Notes .....	25
1. Component Overview .....	25
2. Feature Summary .....	25
3. Bug Fixes .....	25
4. Known Problems .....	25
5. Technology Dependencies .....	25
6. Tested Platforms .....	26
7. Backward Compatibility Summary .....	26
8. For More Information .....	26
GT 4.0 Security Glossary .....	27

---

## List of Tables

2.1. CA Name components .....	9
-------------------------------	---

---

# Chapter 1. GT 4.0 Security: Key Concepts

## 1. Overview

GSI uses public key cryptography (also known as asymmetric cryptography) as the basis for its functionality. Many of the terms and concepts used in this description of GSI come from its use of public key cryptography.

For a good overview of GSI contained in the Web Services-based components of GT4, see [Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective](#)<sup>1</sup>.

A reference for detailed information about public key cryptography is available in the book [Handbook of Applied Cryptography](#)<sup>2</sup>, by A. Menezes, P. van Oorschot, and S. Vanstone, CRC Press, 1996. [Chapter 8](#)<sup>3</sup> of this book deals exclusively with public key cryptography.

The primary motivations behind GSI are:

- The need for secure communication (authenticated and perhaps confidential) between elements of a computational Grid.
- The need to support security across organizational boundaries, thus prohibiting a centrally-managed security system.
- The need to support "single sign-on" for users of the Grid, including delegation of credentials for computations that involve multiple resources and/or sites.

## 2. Conceptual Details

### 2.1. Public Key Cryptography

The most important thing to know about public key cryptography is that, unlike earlier cryptographic systems, it relies not on a single key (a password or a secret "code"), but on two keys. These keys are numbers that are mathematically related in such a way that if either key is used to encrypt a message, the other key must be used to decrypt it. Also important is the fact that it is next to impossible (with our current knowledge of mathematics and available computing power) to obtain the second key from the first one and/or any messages encoded with the first key.

By making one of the keys available publicly (a public key) and keeping the other key private (a [private key](#)<sup>4</sup>), a person can prove that he or she holds the private key simply by encrypting a message. If the message can be decrypted using the public key, the person must have used the private key to encrypt the message.

*Important:* It is critical that private keys be kept private! Anyone who knows the private key can easily impersonate the owner.

### 2.2. Digital Signatures

Using public key cryptography, it is possible to digitally "sign" a piece of information. Signing information essentially means assuring a recipient of the information that the information hasn't been tampered with since it left your hands.

---

<sup>1</sup> GT4-GSI-Overview.pdf

<sup>2</sup> <http://www.cacr.math.uwaterloo.ca/hac/>

<sup>3</sup> <http://www.cacr.math.uwaterloo.ca/hac/about/chap8.pdf>

<sup>4</sup> #priv-key

To sign a piece of information, first compute a mathematical hash of the information. (A hash is a condensed version of the information. The algorithm used to compute this hash must be known to the recipient of the information, but it isn't a secret.) Using your private key, encrypt the hash, and attach it to the message. Make sure that the recipient has your public key.

To verify that your signed message is authentic, the recipient of the message will compute the hash of the message using the same hashing algorithm you used, and will then decrypt the encrypted hash that you attached to the message. If the newly-computed hash and the decrypted hash match, then it proves that you signed the message and that the message has not been changed since you signed it.

## 2.3. Certificates

A central concept in GSI authentication is the *certificate*. Every user and service on the Grid is identified via a certificate, which contains information vital to identifying and authenticating the user or service.

A GSI certificate includes four primary pieces of information:

- A subject name, which identifies the person or object that the certificate represents.
- The public key belonging to the subject.
- The identity of a Certificate Authority (CA) that has signed the certificate to certify that the public key and the identity both belong to the subject.
- The digital signature of the named CA.

Note that a third party (a CA) is used to certify the link between the public key and the subject in the certificate. In order to trust the certificate and its contents, the CA's certificate must be trusted. The link between the CA and its certificate must be established via some non-cryptographic means, or else the system is not trustworthy.

GSI certificates are encoded in the X.509 certificate format, a standard data format for certificates established by the Internet Engineering Task Force (IETF). These certificates can be shared with other public key-based software, including commercial web browsers from Microsoft and Netscape.

## 2.4. Mutual Authentication

If two parties have certificates, and if both parties trust the CAs that signed each other's certificates, then the two parties can prove to each other that they are who they say they are. This is known as *mutual authentication*. GSI uses the Secure Sockets Layer (SSL) for its mutual authentication protocol, which is described [below](#)<sup>5</sup>. (SSL is also known by a new, IETF standard name: Transport Layer Security, or TLS.)

Before mutual authentication can occur, the parties involved must first trust the CAs that signed each other's certificates. In practice, this means that they must have copies of the CAs' certificates--which contain the CAs' public keys--and that they must trust that these certificates really belong to the CAs.

To mutually authenticate, the first person (*A*) establishes a connection to the second person (*B*).

To start the authentication process, *A* gives *B* his certificate.

The certificate tells *B* who *A* is claiming to be (the identity), what *A*'s public key is, and what CA is being used to certify the certificate.

---

<sup>5</sup> #s-security-key-delegation

*B* will first make sure that the certificate is valid by checking the CA's digital signature to make sure that the CA actually signed the certificate and that the certificate hasn't been tampered with. (This is where *B* must trust the CA that signed *A*'s certificate.)

Once *B* has checked out *A*'s certificate, *B* must make sure that *A* really is the person identified in the certificate.

*B* generates a random message and sends it to *A*, asking *A* to encrypt it.

*A* encrypts the message using his private key, and sends it back to *B*.

*B* decrypts the message using *A*'s public key.

If this results in the original random message, then *B* knows that *A* is who he says he is.

Now that *B* trusts *A*'s identity, the same operation must happen in reverse.

*B* sends *A* her certificate, *A* validates the certificate and sends a challenge message to be encrypted.

*B* encrypts the message and sends it back to *A*, and *A* decrypts it and compares it with the original.

If it matches, then *A* knows that *B* is who she says she is.

At this point, *A* and *B* have established a connection to each other and are certain that they know each others' identities.

## 2.5. Confidential Communication

By default, GSI does not establish confidential (encrypted) communication between parties. Once mutual authentication is performed, GSI gets out of the way so that communication can occur without the overhead of constant encryption and decryption.

GSI can easily be used to establish a shared key for encryption if confidential communication is desired. Recently relaxed United States export laws now allow us to include encrypted communication as a standard optional feature of GSI.

A related security feature is communication integrity. Integrity means that an eavesdropper may be able to read communication between two parties but is not able to modify the communication in any way. GSI provides communication integrity by default. (It can be turned off if desired). Communication integrity introduces some overhead in communication, but not as large an overhead as encryption.

## 2.6. Securing Private Keys

The core GSI software provided by the Globus Toolkit expects the user's private key to be stored in a file in the local computer's storage. To prevent other users of the computer from stealing the private key, the file that contains the key is encrypted via a password (also known as a passphrase). To use GSI, the user must enter the passphrase required to decrypt the file containing their private key.

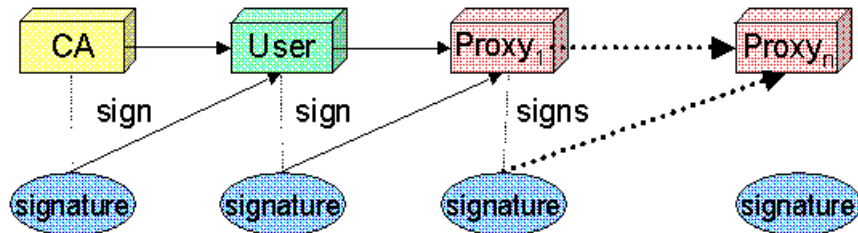
We have also prototyped the use of cryptographic smartcards in conjunction with GSI. This allows users to store their private key on a smartcard rather than in a file system, making it still more difficult for others to gain access to the key.

## 2.7. Delegation, Single Sign-On and Proxy Certificates

GSI provides a delegation capability: an extension of the standard SSL protocol which reduces the number of times the user must enter his passphrase. If a Grid computation requires that several Grid resources be used (each requiring

mutual authentication), or if there is a need to have agents (local or remote) requesting services on behalf of a user, the need to re-enter the user's passphrase can be avoided by creating a *proxy*.

A proxy consists of a new certificate and a private key. The key pair that is used for the proxy, i.e. the public key embedded in the certificate and the private key, may either be regenerated for each proxy or obtained by other means. The new certificate contains the owner's identity, modified slightly to indicate that it is a proxy. The new certificate is signed by the owner, rather than a CA. (See diagram below.) The certificate also includes a time notation after which the proxy should no longer be accepted by others. Proxies have limited lifetimes.



The proxy's private key must be kept secure, but because the proxy isn't valid for very long, it doesn't have to be kept quite as secure as the owner's private key. It is thus possible to store the proxy's private key in a local storage system without being encrypted, as long as the permissions on the file prevent anyone else from looking at them easily. Once a proxy is created and stored, the user can use the proxy certificate<sup>6</sup> and private key for mutual authentication without entering a password.

When proxies are used, the mutual authentication process differs slightly. The remote party receives not only the proxy's certificate (signed by the owner), but also the owner's certificate. During mutual authentication, the owner's public key (obtained from her certificate) is used to validate the signature on the proxy certificate. The CA's public key is then used to validate the signature on the owner's certificate. This establishes a chain of trust from the CA to the proxy through the owner.



### Note

GSI, and software based on it (notably the Globus Toolkit, GSI-SSH, and GridFTP), is currently the only software which supports the delegation extensions to TLS (a.k.a. SSL). The Globus Alliance has worked in the GGF and the IETF to standardize this extension in the form of Proxy Certificates (RFC 3820) [<http://www.ietf.org/rfc/rfc3820.txt>].

## 3. Related Documents

- [Globus Toolkit Version 4 Grid Security Infrastructure: A Standards Perspective](#)<sup>7</sup>
- [Handbook of Applied Cryptography](#)<sup>8</sup>

# GT 4.0 Security Glossary

## C

Certificate Authority ( CA )      An entity that issues certificates.

<sup>6</sup> #proxy-cert

<sup>7</sup> GT4-GSI-Overview.pdf

<sup>8</sup> <http://www.cacr.math.uwaterloo.ca/hac/>

CA Certificate	The CA's certificate. This certificate is used to verify signature on certificates issued by the CA. GSI typically stores a given CA certificate in <code>/etc/grid-security/certificates/&lt;hash&gt;.0</code> , where <code>&lt;hash&gt;</code> is the hash code of the CA identity.
CA Signing Policy	The CA signing policy is used to place constraints on the information you trust a given CA to bind to public keys. Specifically it constrains the identities a CA is trusted to assert in a certificate. In GSI the signing policy for a given CA can typically be found in <code>/etc/grid-security/certificates/&lt;hash&gt;.signing_policy</code> , where <code>&lt;hash&gt;</code> is the hash code of the CA identity. For more information see [add link].
certificate	A public key and information about the certificate owner bound together by the digital signature of a CA. In the case of a CA certificate the certificate is self signed, i.e. it was signed using its own private key.
Certificate Revocation List (CRL)	A list of revoked certificates generated by the CA that originally issued them. When using GSI this list is typically found in <code>/etc/grid-security/certificates/&lt;hash&gt;.r0</code> , where <code>&lt;hash&gt;</code> is the hash code of the CA identity.
certificate subject	A identifier for the certificate owner, e.g. <code>"/DC=org/DC=doegrids/OU=People/CN=John Doe 123456"</code> . The subject is part of the information the CA binds to a public key when creating a certificate.
credentials	The combination of a certificate and the matching private key.

## E

End Entity Certificate (EEC)	A certificate belonging to a non-CA entity, e.g. you, me or the computer on your desk.
------------------------------	--

## G

GAA Configuration File	A file that configures the Generic Authorization and Access control GAA libraries. When using GSI this file is typically found in <code>/etc/grid-security/gsi-gaa.conf</code> .
grid map file	A file containing entries mapping certificate subjects to local user names. This file can also serve as a access control list for GSI enabled services and is typically found in <code>/etc/grid-security/grid-mapfile</code> . For more information see the <a href="#">Gridmap file</a> <sup>9</sup> .
grid security directory	The directory containing GSI configuration files such as the GSI authorization callout configuration and GAA configuration files. Typically this directory is <code>/etc/grid-security</code> . For more information see <a href="#">Grid security directory</a> <sup>10</sup> .
GSI authorization callout configuration file	A file that configures authorization callouts to be used for mapping and authorization in GSI enabled services. When using GSI this file is typically found in <code>/etc/grid-security/gsi-authz.conf</code> .

---

<sup>9</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-gridmapfile](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-gridmapfile)

<sup>10</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-gridsecurity](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-gridsecurity)

## H

host certificate                    An EEC belonging to a host. When using GSI this certificate is typically stored in `/etc/grid-security/hostcert.pem`. For more information on possible host certificate locations see the [Credentials](#)<sup>11</sup>.

host credentials                 The combination of a host certificate and its corresponding private key..

## P

private key                        The private part of a key pair. Depending on the type of certificate the key corresponds to it may typically be found in `$HOME/.globus/userkey.pem` (for user certificates), `/etc/grid-security/hostkey.pem` (for host certificates) or `/etc/grid-security/<service>/<service>key.pem` (for service certificates). For more information on possible private key locations see the [Credentials](#)<sup>12</sup>

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 stead. GSI uses proxy certificates for single sign on and delegation of rights to other entities.

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.

public key                         The public part of a key pair used for cryptographic operations (e.g. signing, encrypting).

## S

service certificate                A EEC for a specific service (e.g. FTP or LDAP). When using GSI this certificate is typically stored in `/etc/grid-security/<service>/<service>cert.pem`. For more information on possible service certificate locations see the [Credentials](#)<sup>13</sup>.

service credentials               The combination of a service certificate and its corresponding private key.

## T

transport-level security         Uses transport-level security (TLS) mechanisms.

---

<sup>11</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)

<sup>12</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)

<sup>13</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)

trusted CAs directory      The directory containing the CA certificates and signing policy files of the CAs trusted by GSI. Typically this directory is `/etc/grid-security/certificates`. For more information see [Grid security directory](#)<sup>14</sup>.

## U

user certificate      A EEC belonging to a user. When using GSI this certificate is typically stored in `$HOME/.globus/usercert.pem`. For more information on possible user certificate locations see [Credentials](#)<sup>15</sup>.

user credentials      The combination of a user certificate and its corresponding private key.

---

<sup>14</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-gridsecurity](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-gridsecurity)

<sup>15</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)

---

# Chapter 2. GT 4.0 SimpleCA: Admin Guide

## 1. Introduction

This guide contains advanced configuration information for system administrators working with SimpleCA. It provides references to information on procedures typically performed by system administrators, including installation, configuring, deploying, and testing the installation.

### Important

This information is in addition to the basic Globus Toolkit prerequisite, overview, installation, security configuration instructions in the [GT 4.0 System Administrator's Guide](#)<sup>1</sup>. Read through this guide before continuing!

The following are instructions for how to use SimpleCA to set up certificates for a GT 4.0 installation.

## 2. Building and Installing

SimpleCA provides a wrapper around the OpenSSL CA functionality and is sufficient for simple Grid services. Alternatively, you can use OpenSSL's `CA.sh` command on its own. SimpleCA is suitable for testing or when a *certificate authority (CA)* is not available. You can find other CA options in [Obtaining host certificates](#)<sup>2</sup>.

### 2.1. Create users

Make sure you have the following users on your machine:

- Your *user* account, which will be used to run the client programs.
- A generic *globus* account, which will be used to perform administrative tasks such as starting and stopping the container, deploying services, etc. This user will also be in charge of managing the SimpleCA. To do this, make sure this account has read and write permissions in the `$GLOBUS_LOCATION` directory.

### 2.2. Run the setup script

A script was installed to set up a new SimpleCA. You only need to run this script *once* per Grid.

Run the setup script:

```
$GLOBUS_LOCATION/setup/globus/setup-simple-ca
```

#### 2.2.1. 2.1 Configure the subject name

This script prompts you for information about the CA you wish to create:

---

<sup>1</sup> [../admin/docbook/](#)

<sup>2</sup> <http://www.globus.org/toolkit/docs/4.0/admin/docbook/ch06.html#s-basic-host>

The unique subject name for this CA is:  
cn=Globus Simple CA, ou=simpleCA-mayed.mcs.anl.gov, ou=GlobusTest, o=Grid

Do you want to keep this as the CA subject (y/n) [y]:

where:

**Table 2.1. CA Name components**

cn	Represents "common name". It identifies this particular certificate as the <i>CA certificate</i> within the "GlobusTest/simpleCA-hostname" domain, which in this case is Globus Simple CA.
ou	Represents "organizational unit". It identifies this CA from other CAs created by SimpleCA by other people. The second "ou" is specific to your hostname (in this case GlobusTest).
o	Represents "organization". It identifies the Grid.

Press **y** to keep the default subject name (recommended).

### 2.2.2. Configure the CA's email

The next prompt looks like:

```
Enter the email of the CA (this is the email where certificate
requests will be sent to be signed by the CA):
```

Enter the email address where you intend to receive certificate requests. It should be your real email address that you check, not the address of the globus user.

### 2.2.3. Configure the expiration date

Then you'll see:

```
The CA certificate has an expiration date. Keep in mind that
once the CA certificate has expired, all the certificates
signed by that CA become invalid. A CA should regenerate
the CA certificate and start re-issuing ca-setup packages
before the actual CA certificate expires. This can be done
by re-running this setup script. Enter the number of DAYS
the CA certificate should last before it expires.
[default: 5 years (1825 days)]:
```

This is the number of days for which the CA certificate is valid. Once this time expires, the CA certificate will have to be recreated and all of its certificates regranted.

Accept the default (recommended).

### 2.2.4. Enter a passphrase

Next you'll see:

```
Generating a 1024 bit RSA private key
```

```
.....++++++
.....++++++
writing new private key to '/home/globus/.globus/simpleCA//private/cakey.p
Enter PEM pass phrase:
```

The passphrase of the CA certificate will be used only when signing certificates (with **grid-cert-sign**). It should be hard to guess, as its compromise may compromise all the certificates signed by the CA.

Enter your passphrase.

 **Important:**

Your passphrase must *not* contain any spaces.

## 2.2.5. Confirm generated certificate

Finally you'll see the following:

```
A self-signed certificate has been generated
for the Certificate Authority with the subject:

/O=Grid/OU=GlobusTest/OU=simpleCA-mayed.mcs.anl.gov/CN=Globus Simple CA

If this is invalid, rerun this script

setup/globus/setup-simple-ca

and enter the appropriate fields.

-----

The private key of the CA is stored in /home/globus/.globus/simpleCA//priv
The public CA certificate is stored in /home/globus/.globus/simpleCA//cace

The distribution package built for this CA is stored in

/home/globus/.globus/simpleCA//globus_simple_ca_68ea3306_setup-0.17.tar.gz
```

This information will be important for setting up other machines in your grid. The number `68ea3306` in the last line is known as your *CA hash*. It will be an 8 hexadecimal digit string.

Press any key to acknowledge this screen.

Your CA setup package finishes installing and ends the procedure with the following reminder:

```
*****

Note: To complete setup of the GSI software you need to run the
following script as root to configure your security configuration
directory:

/opt/gt4/setup/globus_simple_ca_68ea3306_setup/setup-gsi
```

For further information on using the `setup-gsi` script, use the `-help` option. The `-default` option sets this security configuration to be the default, and `-nonroot` can be used on systems where root access is not available.

```
*****  
  
setup-ssl-utils: Complete
```

We'll run the `setup-gsi` script in the next section. For now, just notice that it refers to your `$GLOBUS_LOCATION` and the `CA Hash` from the last message.

## 2.2.6. Complete setup of GSI

To finish the setup of GSI, we'll run the script noted in the previous step.

Run the following as root (or, if no root privileges are available, add the **-nonroot** option to the command line):

```
$GLOBUS_LOCATION/setup/globus_simple_ca_CA_Hash_setup/setup-gsi -default
```

The output should look like:

```
setup-gsi: Configuring GSI security  
Installing /etc/grid-security/certificates//grid-security.conf.CA_Hash...  
Running grid-security-config...  
Installing Globus CA certificate into trusted CA certificate directory...  
Installing Globus CA signing policy into trusted CA certificate directory.  
setup-gsi: Complete
```

## 2.3. Host certificates

You must request and sign a *host certificate* and then copy it into the appropriate directory for secure services. The certificate must be for a machine which has a consistent name in DNS; you should not run it on a computer using DHCP, where a different name could be assigned to your computer.

### 2.3.1. 3.1 Request a host certificate

As root, run:

```
grid-cert-request -host 'hostname'
```

This creates the following files:

- `/etc/grid-security/hostkey.pem`
- `/etc/grid-security/hostcert_request.pem`
- (an empty) `/etc/grid-security/hostcert.pem`

*Note:* If you are using your own CA, follow their instructions about creating a hostcert (one which has a commonName (CN) of your hostname), then place the cert and key in the `/etc/grid-security/` location. You may then proceed to [Section 2.4, "User certificates"](#).

## 2.3.2. Sign the host certificate

1. As globus, run:

```
grid-ca-sign -in hostcert_request.pem -out hostsigned.pem
```

2. A signed host certificate, named `hostsigned.pem`, is written to the current directory.
3. When prompted for a passphrase enter the one you specified in [Section 2.2.4, “Enter a passphrase”](#) (for the private key of the CA certificate).
4. As root move the signed host certificate to `/etc/grid-security/hostcert.pem`.

The certificate should be owned by root and be read-only for other users.

The key should be read-only by root.

## 2.4. User certificates

Users also must request *user certificates*, which you will sign using the *globus* user.

### 2.4.1. Request a user certificate

As your normal user account (*not globus*), run:

```
grid-cert-request
```

After you enter a passphrase, this creates

- `~$USER/.globus/usercert.pem` (empty)
- `~$USER/.globus/userkey.pem`
- `~$USER/.globus/usercert_request.pem`

Email the `usercert_request.pem` file to the SimpleCA maintainer.

### 2.4.2. Sign the user certificate

1. As the SimpleCA owner *globus*, run:

```
grid-ca-sign -in usercert_request.pem -out signed.pem
```

2. When prompted for a password enter the one you specified in [Section 2.2.4, “Enter a passphrase”](#) (for the private key of the CA certificate).
3. Now send the signed copy (`signed.pem`) back to the user who requested the certificate.
4. As your normal user account (*not globus*), copy the signed user certificate into `>~/ .globus/` and rename it as `usercert.pem`, thus replacing the empty file.

The certificate should be owned by the user and be read-only for other users.

The key should be read-only by the owner.

## 3. Configuring

[high-level characterization of the configuration options for the component here]

### 3.1. Configure SimpleCA for multiple machines

So far, you have a single machine configured with SimpleCA certificates. Recall that in [Section 2.2.5, “Confirm generated certificate”](#) a CA setup package was created in `.globus/simpleCA/globus_simple_ca_HASH_setup-0.17.tar.gz`. If you want to use your certificates on another machine, you must install that CA setup package on that machine.

To install it, copy that package to the second machine and run:

```
$GLOBUS_LOCATION/sbin/gpt-build globus_simple_ca_HASH_setup-0.17.tar.gz gcc32dbg
$GLOBUS_LOCATION/sbin/gpt-postinstall
```

Then you will have to perform **setup-gsi -default** from [Section 2.2.6, “Complete setup of GSI”](#).

If you are going to run services on the second host, it will need its own host certificate ([Section 2.3, “Host certificates”](#)) and grid-mapfile (as described in the basic configuration instructions in [Add Authorization](#)<sup>3</sup>).

You may re-use your *user certificates* on the new host. You will need to copy the requests to the host where the SimpleCA was first installed in order to sign them.

## 4. Deploying

[information about deploying the component into various containers/environments]

## 5. Testing

To verify that the SimpleCA certificate is installed in `/etc/grid-security/certificates` and that your certificate is in place with the correct permissions, run:

```
user$ grid-proxy-init -debug -verify
```

After entering your passphrase, successful output looks like:

```
[bacon@mayed schedulers]$ grid-proxy-init -debug -verify
```

```
User Cert File: /home/user/.globus/usercert.pem
```

```
User Key File: /home/user/.globus/userkey.pem
```

```
Trusted CA Cert Dir: /etc/grid-security/certificates
```

```
Output File: /tmp/x509up_u1817
```

```
Your identity: /O=Grid/OU=GlobusTest/OU=simpleCA-mayed.mcs.anl.gov/OU=mcs.anl.gov/
```

```
Enter GRID pass phrase for this identity:
```

```
Creating proxy .....
```

```
.....
```

<sup>3</sup> <http://www.globus.org/toolkit/docs/4.0/admin/docbook/ch06.html#s-basic-gridmap>

```
Done  
Proxy Verify OK  
Your proxy is valid until: Sat Mar 20 03:01:46 2004
```

## 6. Security Considerations

[describe security considerations relevant for this component]

## 7. Troubleshooting

[help for common problems sysadmins may experience]

---

# Chapter 3. GT 4.0 Component Fact Sheet: Credential Management - SimpleCA

## 1. Brief overview

SimpleCA is a package that provides a simplified certification authority for the purpose of issuing credentials to Globus Toolkit users and services.

## 2. Summary of features

Features new in GT 4.0

- None

Other Supported Features

- Easy creation of X.509 certificates for use with the Globus Toolkit
- Easy creation of GPT packages for the created SimpleCA

Deprecated Features

- None

## 3. Usability summary

This section does not apply for this component.

## 4. Backward compatibility summary

Protocol changes for SimpleCA since GT 3.2

- Not applicable

API changes since GT 3.2

- Not applicable

Exception changes since GT 3.2

- Not applicable

Schema changes since GT 3.2

- Not applicable

## 5. Technology dependencies

SimpleCA depends on the following GT components:

- Pre-WS Authentication and Authorization

SimpleCA depends on the following 3rd party software:

- OpenSSL

## 6. Tested platforms

No content is available at this time.

## 7. Associated standards

No content is available at this time.

## 8. For More Information

Click [here](#)<sup>1</sup> for more information about this component.

---

<sup>1</sup> index.html

---

# Chapter 4. GT 4.0.8 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.8. It includes a summary of changes since 4.0.7, bug fixes since 4.0.7 and any known problems that still exist at the time of the 4.0.8 release. This page is in addition to the top-level 4.0.8 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.8>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

Except for bug fixes, no changes have been made since 4.0.7.

## 3. Bug Fixes

No bugs have been fixed since the previous version.

## 4. Known Problems

- [Bug 5541](#):<sup>2</sup> grid-cert-request scripts should not require CA email

## 5. For More Information

Click [here](#)<sup>3</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=5541](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=5541)

<sup>3</sup> [index.html](#)

---

# Chapter 5. GT 4.0.7 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.7. It includes a summary of changes since 4.0.6, bug fixes since 4.0.6 and any known problems that still exist at the time of the 4.0.7 release. This page is in addition to the top-level 4.0.7 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.7>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

Except for a bug fix, no changes have been made since 4.0.6.

## 3. Bug Fixes

No bugs have been fixed since the previous version.

## 4. Known Problems

- [Bug 1712](#):<sup>2</sup>-default should not be required the first time

## 5. For More Information

Click [here](#)<sup>3</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=1712](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=1712)

<sup>3</sup> [index.html](#)

---

# Chapter 6. GT 4.0.6 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.6. It includes a summary of changes since 4.0.5, bug fixes since 4.0.5 and any known problems that still exist at the time of the 4.0.6 release. This page is in addition to the top-level 4.0.6 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.6>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

Except for a bug fix, no changes have been made since 4.0.5.

## 3. Bug Fixes

- [Bug 4529](#):<sup>2</sup> setup-simple-ca bug

## 4. Known Problems

- [Bug 1712](#):<sup>3</sup> -default should not be required the first time

## 5. For More Information

Click [here](#)<sup>4</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=4529](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=4529)

<sup>3</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=1712](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=1712)

<sup>4</sup> [index.html](#)

---

# Chapter 7. GT 4.0.5 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.5. It includes a summary of changes since 4.0.4, bug fixes since 4.0.4 and any known problems that still exist at the time of the 4.0.5 release. This page is in addition to the top-level 4.0.5 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.5>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

Except for a bug fix, no changes have been made since 4.0.4.

## 3. Bug Fixes

- [Bug 4819](#):<sup>2</sup> grid-cert-request -help returns error

## 4. Known Problems

There are no new known problems for SimpleCA at the time of the 4.0.5 release.

## 5. For More Information

Click [here](#)<sup>3</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [http://bugzilla.globus.org/globus/show\\_bug.cgi?id=4819](http://bugzilla.globus.org/globus/show_bug.cgi?id=4819)

<sup>3</sup> [index.html](#)

---

# Chapter 8. GT 4.0.4 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.4. It includes a summary of changes since 4.0.3, bug fixes since 4.0.3 and any known problems that still exist at the time of the 4.0.4 release. This page is in addition to the top-level 4.0.4 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.4>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

The only change for 4.0.4 was a minor bug fix.

## 3. Bug Fixes

- [Bug 4725](#):<sup>2</sup> Version number typo in setup-simple-ca and a minor error in Makefile.in

## 4. Known Problems

There are no new known problems for SimpleCA at the time of the 4.0.4 release.

## 5. For More Information

Click [here](#)<sup>3</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [http://bugzilla.globus.org/globus/show\\_bug.cgi?id=4725](http://bugzilla.globus.org/globus/show_bug.cgi?id=4725)

<sup>3</sup> [index.html](#)

---

# Chapter 9. GT 4.0.3 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.3. It includes a summary of changes since 4.0.2, bug fixes since 4.0.2 and any known problems that still exist at the time of the 4.0.3 release. This page is in addition to the top-level 4.0.3 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.3>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

No changes have been made for SimpleCA since 4.0.2.

## 3. Bug Fixes

No bug fixes have been made to SimpleCA since 4.0.2.

## 4. Known Problems

There are no new known problems for SimpleCA at the time of the 4.0.3 release.

## 5. For More Information

Click [here](#)<sup>2</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [index.html](#)

---

# Chapter 10. GT 4.0.2 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.2. It includes a summary of changes since 4.0.1, bug fixes since 4.0.1 and any known problems that still exist at the time of the 4.0.2 release. This page is in addition to the top-level 4.0.2 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.2>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

Other than bug fixes, no changes have been made for SimpleCA since 4.0.1.

## 3. Bug Fixes

The following bug fixes have been made to SimpleCA since 4.0.1:

- [Bug 3702](#):<sup>2</sup> SimpleCA build fails on HP-UX/IA-64 platform
- [Bug 3958](#):<sup>3</sup> bash-ism in SimpleCA
- [Bug 4164](#):<sup>4</sup> Simple CA installation fails on RH 4 on IBM zSeries.

## 4. Known Problems

There are no new known problems for SimpleCA.

## 5. For More Information

Click [here](#)<sup>5</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [http://bugzilla.globus.org/globus/show\\_bug.cgi?id=3702](http://bugzilla.globus.org/globus/show_bug.cgi?id=3702)

<sup>3</sup> [http://bugzilla.globus.org/globus/show\\_bug.cgi?id=3958](http://bugzilla.globus.org/globus/show_bug.cgi?id=3958)

<sup>4</sup> [http://bugzilla.globus.org/globus/show\\_bug.cgi?id=4164](http://bugzilla.globus.org/globus/show_bug.cgi?id=4164)

<sup>5</sup> [index.html](#)

---

# Chapter 11. GT 4.0.1 Incremental Release Notes: SimpleCA

## 1. Introduction

These release notes are for the incremental release 4.0.1. It includes a summary of changes since 4.0.0, bug fixes since 4.0.0 and any known problems that still exist at the time of the 4.0.1 release. This page is in addition to the top-level 4.0.1 release notes at <http://www.globus.org/toolkit/releasenotes/4.0.1>.

For release notes about 4.0 (including feature summary, technology dependencies, etc) go to the [SimpleCA 4.0 Release Notes](#)<sup>1</sup>.

## 2. Changes Summary

No changes have occurred for SimpleCA.

## 3. Bug Fixes

No bug fixes were made to SimpleCA.

## 4. Known Problems

There are no new known problems for SimpleCA.

## 5. For More Information

Click [here](#)<sup>2</sup> for more information about this component.

---

<sup>1</sup> [http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred\\_Mgmt\\_SimpleCA\\_Release\\_Notes.html](http://www.globus.org/toolkit/docs/4.0/security/simpleca/Cred_Mgmt_SimpleCA_Release_Notes.html)

<sup>2</sup> [index.html](#)

---

# Chapter 12. GT 4.0 Release Notes: SimpleCA

## 1. Component Overview

SimpleCA is a package that provides a simplified certification authority for the purpose of issuing credentials to Globus Toolkit users and services.

## 2. Feature Summary

Features new in GT 4.0

- None

Other Supported Features

- Easy creation of X.509 certificates for use with the Globus Toolkit
- Easy creation of GPT packages for the created SimpleCA

Deprecated Features

- None

## 3. Bug Fixes

- [Bug 1866](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=1866)<sup>1</sup>: setup-simple-ca fails on Solaris due to nonportable I/O r...
- [Bug 1878](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=1878)<sup>2</sup>: Allow -passin options to be used when creating a CA/signi...
- [Bug 2100](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2100)<sup>3</sup>: grid-ca-sign fails with message mandatory organizationNam...
- [Bug 2212](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2212)<sup>4</sup>: Security Risk when running grid-ca-sign; possibly others
- [Bug 2888](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2888)<sup>5</sup>: Problems with non-root SimpleCA install

## 4. Known Problems

No content is available at this time.

## 5. Technology Dependencies

SimpleCA depends on the following GT components:

---

<sup>1</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=1866](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=1866)

<sup>2</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=1878](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=1878)

<sup>3</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=2100](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2100)

<sup>4</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=2212](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2212)

<sup>5</sup> [http://bugzilla.globus.org/bugzilla/show\\_bug.cgi?id=2888](http://bugzilla.globus.org/bugzilla/show_bug.cgi?id=2888)

- Pre-WS Authentication and Authorization

SimpleCA depends on the following 3rd party software:

- OpenSSL

## 6. Tested Platforms

No content is available at this time.

## 7. Backward Compatibility Summary

Protocol changes for SimpleCA since GT 3.2

- Not applicable

API changes since GT 3.2

- Not applicable

Exception changes since GT 3.2

- Not applicable

Schema changes since GT 3.2

- Not applicable

## 8. For More Information

Click [here](#)<sup>6</sup> for more information about this component.

---

<sup>6</sup> index.html

---

# GT 4.0 Security Glossary

## C

Certificate Authority ( CA )	An entity that issues certificates.
CA Certificate	The CA's certificate. This certificate is used to verify signature on certificates issued by the CA. GSI typically stores a given CA certificate in <code>/etc/grid-security/certificates/&lt;hash&gt;.0</code> , where <code>&lt;hash&gt;</code> is the hash code of the CA identity.
CA Signing Policy	The CA signing policy is used to place constraints on the information you trust a given CA to bind to public keys. Specifically it constrains the identities a CA is trusted to assert in a certificate. In GSI the signing policy for a given CA can typically be found in <code>/etc/grid-security/certificates/&lt;hash&gt;.signing_policy</code> , where <code>&lt;hash&gt;</code> is the hash code of the CA identity. For more information see [add link].
certificate	A public key and information about the certificate owner bound together by the digital signature of a CA. In the case of a CA certificate the certificate is self signed, i.e. it was signed using its own private key.
Certificate Revocation List (CRL)	A list of revoked certificates generated by the CA that originally issued them. When using GSI this list is typically found in <code>/etc/grid-security/certificates/&lt;hash&gt;.r0</code> , where <code>&lt;hash&gt;</code> is the hash code of the CA identity.
certificate subject	A identifier for the certificate owner, e.g. <code>"/DC=org/DC=doegrids/OU=People/CN=John Doe 123456"</code> . The subject is part of the information the CA binds to a public key when creating a certificate.
credentials	The combination of a certificate and the matching private key.

## E

End Entity Certificate (EEC)	A certificate belonging to a non-CA entity, e.g. you, me or the computer on your desk.
------------------------------	--

## G

GAA Configuration File	A file that configures the Generic Authorization and Access control GAA libraries. When using GSI this file is typically found in <code>/etc/grid-security/gsi-gaa.conf</code> .
grid map file	A file containing entries mapping certificate subjects to local user names. This file can also serve as a access control list for GSI enabled services and is typically found in <code>/etc/grid-security/grid-mapfile</code> . For more information see the <a href="#">Gridmap file</a> <sup>7</sup> .

---

<sup>7</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-gridmapfile](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-gridmapfile)

grid security directory	The directory containing GSI configuration files such as the GSI authorization callout configuration and GAA configuration files. Typically this directory is <code>/etc/grid-security</code> . For more information see <a href="#">Grid security directory</a> <sup>8</sup> .
GSI authorization callout configuration file	A file that configures authorization callouts to be used for mapping and authorization in GSI enabled services. When using GSI this file is typically found in <code>/etc/grid-security/gsi-authz.conf</code> .

## H

host certificate	An EEC belonging to a host. When using GSI this certificate is typically stored in <code>/etc/grid-security/hostcert.pem</code> . For more information on possible host certificate locations see the <a href="#">Credentials</a> <sup>9</sup> .
host credentials	The combination of a host certificate and its corresponding private key..

## P

private key	The private part of a key pair. Depending on the type of certificate the key corresponds to it may typically be found in <code>\$HOME/.globus/userkey.pem</code> (for user certificates), <code>/etc/grid-security/hostkey.pem</code> (for host certificates) or <code>/etc/grid-security/&lt;service&gt;/&lt;service&gt;key.pem</code> (for service certificates). For more information on possible private key locations see the <a href="#">Credentials</a> <sup>10</sup>
proxy certificate	<p>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 stead. GSI uses proxy certificates for single sign on and delegation of rights to other entities.</p> <p>For more information about types of proxy certificates and their compatibility in different versions of GT, see <a href="http://dev.globus.org/wiki/Security/ProxyCertTypes">http://dev.globus.org/wiki/Security/ProxyCertTypes</a>.</p>
proxy credentials	The combination of a proxy certificate and its corresponding private key. GSI typically stores proxy credentials in <code>/tmp/x509up_u&lt;uid&gt;</code> , where <code>&lt;uid&gt;</code> is the user id of the proxy owner.
public key	The public part of a key pair used for cryptographic operations (e.g. signing, encrypting).

## S

service certificate	A EEC for a specific service (e.g. FTP or LDAP). When using GSI this certificate is typically stored in <code>/etc/grid-security/&lt;service&gt;/&lt;service&gt;cert.pem</code> . For more information on possible service certificate locations see the <a href="#">Credentials</a> <sup>11</sup> .
service credentials	The combination of a service certificate and its corresponding private key.

---

<sup>8</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-gridsecurity](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-gridsecurity)

<sup>9</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)

<sup>10</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)

<sup>11</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)

## T

transport-level security	Uses transport-level security (TLS) mechanisms.
trusted CAs directory	The directory containing the CA certificates and signing policy files of the CAs trusted by GSI. Typically this directory is <code>/etc/grid-security/certificates</code> . For more information see <a href="#">Grid security directory</a> <sup>12</sup> .

## U

user certificate	A BEC belonging to a user. When using GSI this certificate is typically stored in <code>\$HOME/.globus/usercert.pem</code> . For more information on possible user certificate locations see <a href="#">Credentials</a> <sup>13</sup> .
user credentials	The combination of a user certificate and its corresponding private key.

---

<sup>12</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-gridsecurity](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-gridsecurity)

<sup>13</sup> [http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre\\_WS\\_AA\\_Public\\_Interfaces.html#prewsaa-env-credentials](http://www.globus.org/toolkit/docs/4.0/security/prewsaa/Pre_WS_AA_Public_Interfaces.html#prewsaa-env-credentials)