

GT4 Delegation Service User's Guide

DRAFT

GT4 Delegation Service User's Guide

Introduction

The Delegation Service can be used when a user wants to delegate rights to a service that is hosted in the same container as the Delegation Service. The Delegation Service accepts a credential from the user and provides access to that credential to any authorized service that runs in the same container. Upon delegation to the service, an endpoint reference to the delegated credential is returned to the client, which can then be furnished to other services as a handle to the credential.

Moreover, the endpoint reference returned on delegation can be used by the client to refresh the credential stored with the delegation service. When the client performs a refresh, the service sends notifications to any service that has registered interest in that particular credential.

General clients that can be used for the Delegation Service:

- The generic client `wsrf-destroy` can be used to remove the delegated credential.
- The `wsrf-query` can be used to query the termination time of the delegation resource, which is the lifetime of the credential. The resource property to query is `{http://docs.oasis-open.org/wsrf/2004/06/wsrf-WS-ResourceLifetime-1.2-draft-01.xsd}TerminationTime`.



Note

If the service being contacted is using GSI *Secure Transport*, then the container credentials configured for the service will be used, even if service/resource-level credentials are configured. Hence, authorization needs to be done based on the DN of the container credentials.

Table of Contents

I. Command-line tools	?
globus-credential-delegate	6
globus-credential-refresh	7
globus-delegation-client	9
wsrf-destroy	12
wsrf-query	14
1. Troubleshooting	1
1. Error Messages	2
2. CoG Configuration and troubleshooting	4
Glossary	5

DRAFT

List of Tables

1. globus-credential-delegate options	6
2. globus-credential-refresh options	8
3. Common options	10
4. Application-specific options	10
5. Common options	13
6. Common options	15
1.1. WS A&A Delegation Service Error Messages	3

DRAFT

Command-line tools

Note the **wsrp-destroy** and **wsrp-query** commands are common Java WS Core commands.

DRAFT

Name

globus-credential-delegate -- Delegation client

globus-credential-delegate

Tool description

Used to contact a Delegation Factory Service and store a delegated credential. A delegated credential is created and stored in a delegated credential WS-Resource, and the Endpoint Reference(EPR) of the credential is written out to a file for further use.

Command syntax

```
globus-credential-delegate [options] <eprFilename>
```

Table 1. globus-credential-delegate options

-a, --anonymous	Enables anonymous authentication. Only supported with transport security or the GSI Secure Conversation authentication mechanism.
-c, --serverCertificate <file>	Specifies the server's <i>certificate</i> file used for encryption. Only needed for the GSI Secure Message authentication mechanism.
-debug	Runs the client with debug message traces and error stack traces.
-f, --descriptor <file>	Specifies a client security descriptor. Overrides all other security settings.
-g, --delegation <mode>	Enables delegation. mode can be either ' limited ' or ' full '. Only supported with the GSI Secure Conversation authentication mechanism.
-help	Prints the usage message for the client.
-l, --contextLifetime <value>	Sets the lifetime of the client security context. value is in milliseconds. Only supported with the GSI Secure Conversation authentication mechanism.
-x, --proxyFilename <value>	Sets the proxy file to use as the client credential.
-m, --securityMech <type>	Specifies the authentication mechanism. type can be ' msg ' for GSI Secure Message, or ' conv ' for GSI Secure Conversation.
-p, --protection <type>	Specifies the protection level. type can be ' sig ' for signature or ' enc ' for encryption.
-s, --service <url>	Specifies the Delegation Factory Service URL.
-x, --proxyFilename <value>	Sets the proxy file to use as client credential.
-y, --lifetme <value>	Lifetime of delegated credential in seconds. Default is 43200 (which is 12 hours).
-z, --authorization <type>	Specifies authorization type. type can be ' self ', ' host ', ' none ', or a string specifying the expected identity of the remote party.
<eprFilename>	Filename to write the EPR of delegated credential to.

Name

globus-credential-refresh -- Delegation refresh client

globus-credential-refresh

Tool description

Used to refresh delegated credentials pointed to by the specified EPR. A new credential is generated and the one previously created by the Delegation Service is overwritten.

Command syntax

globus-credential-refresh [options]

DRAFT

Table 2. globus-credential-refresh options

-a, --anonymous	Enables anonymous authentication. Only supported with transport security or the GSI Secure Conversation authentication mechanism.
-c, --serverCertificate <file>	Specifies the server's <i>certificate</i> file used for encryption. Only needed for the GSI Secure Message authentication mechanism.
-debug	Runs the client with debug message traces and error stack traces
-e, --eprFile <file>	Specifies an <i>XML</i> file that contains the <i>WS-Addressing</i> endpoint reference. The EPR would be of the delegation resource that is to be refreshed.
-f, --descriptor <file>	Specifies a client security descriptor. Overrides all other security settings.
-g, --delegation <mode>	Enables delegation. mode can be either 'limited' or 'full' . Only supported with the GSI Secure Conversation authentication mechanism.
-help	Prints the usage message for the client.
-k, --key <name value>	Specifies the resource key. The name is the QName of the resource key in the string form: {namespaceURI}localPart , where localPart is the simple value of the key. For complex keys, use the --eprFile option. For Delegation resource, the name will be as specified in the <i>delegationResourceKey</i> element and will replace <i>delegationResourceKey</i> with the actual key: -k " {http://www.globus.org/08/2004/delegationService}DelegationKey delegationResourceKey"
-l, --contextLifetime <value>	Sets the lifetime of the client security context. value is in milliseconds. Only supported with the GSI Secure Conversation authentication mechanism.
-m, --securityMech <type>	Specifies the authentication mechanism. type can be 'msg' for GSI Secure Message, or 'conv' for GSI Secure Conversation.
-p, --protection <type>	Specifies the protection level. type can be 'sig' for signature or 'enc' for encryption.
-s, --service <url>	Specifies the Delegation Factory Service URL.
-x, --proxyFileName <value>	Sets the proxy file to use as the client credential.
-y, --lifetime <value>	Lifetime of delegated credential in seconds. Defaults to 43200 (which is 12 hours).
-z, --authorization <type>	Specifies authorization type. type can be 'self' , 'host' , 'none' , or a string specifying the expected identity of the remote party.

Name

globus-delegation-client -- C Delegation client

```
globus-delegation-client [OPTION...] {SERVICE-SPECIFIER} {{EPR-FILENAME} | {-refresh}}
```

Description

Create or refresh delegated credentials in a service container. If the `-refresh` option is specified on the command-line, then the credential associated with an existing `DelegationService` resource is updated with a new credential. Otherwise, the `SERVICE-SPECIFIER` is interpreted as a `DelegationFactoryService` and a new `DelegationService` resource is created.

Command syntax

```
globus-delegation-client [OPTION...] {SERVICE-SPECIFIER} {{EPR-FILENAME} | {-refresh}}
```

`SERVICE-SPECIFIER`: [-s URI [-k KEY VALUE] | -e FILENAME]

`EPR-FILENAME`: Name of file to store EPR of new delegated credential.

Table 3. Common options

-a --anonymous	Use anonymous authentication. Requires either -m 'conv' or transport (https) security.
-d, --debug	Enables debug mode. In debug mode, all SOAP messages will be displayed to stderr and full WSRF Fault messages will be displayed.
-e --eprFile FILENAME	Load service EPR from FILENAME. This EPR is used to contact the WSRF service.
-h --help	Displays help information about the command.
-k --key KEYNAME VALUE	Set resource key in the service EPR to be named KEYNAME with VALUE as its value. This can be combined with -s to construct an EPR without having an xml file on hand. The KEYNAME is a QName string in the format {namespaceURI}localPart . while the VALUE is a literal string to place in the element. For example, the option -k '{http://www.globus.org}MyKey' 128 would be rendered as <MyKey xmlns="http://www.globus.org">128</MyKey>
-m, --securityMech TYPE	Set authentication mechanism. TYPE is one of msg for WS-SecureMessage or conv for WS-SecureConversation.
-p, --protection LEVEL	Set message protection level. LEVEL is one of sig for digital signature or enc for encryption. The default is 'sig'.
-s --service ENDPOINT	Set ENDPOINT the service URL to use. Will be composed with the -k parameter if present to add ReferenceProperties to the ENDPOINT
-t --timeout SECONDS	Set client timeout to SECONDS.
-u --usage	Print short usage message.
-V --version	Show version information and exit.
-v --certKeyFiles CERTIFICATE-FILENAME KEY-FILENAME	Use credentials located in CERTIFICATE-FILENAME and KEY-FILENAME . The key file must be unencrypted.
-x --proxyFilename FILENAME	Use proxy credentials located in FILENAME .
-z --authorization TYPE	Set authorization mode. TYPE can be self , host , none , or a string specifying the identity of the remote party. The default is self .
--versions	Show version information for all loaded modules and exit.

Table 4. Application-specific options

-g --delegation MODE	Set the delegation mode. MODE can be 'limited' or 'full'. The default is 'limited'
-r --refresh	Refresh a credential instead of creating a new delegated credential resource.

Examples

Create a new delegated credential resource and store the EPR of the resource in `~/ .globus/delegation.epr`:

```
% globus-delegation-client -z host -s https://gridhost.virtual.org:8443/wsrf/services/Dele
```

Refresh the previously delegated credential:

```
% globus-delegation-client -z host -e ~/delegation.epr -refresh
```

Destroy the delegated credential:

```
% globus-wsrf-destroy -z host -e ~/delegation.epr
```

DRAFT

Name

`wsrf-destroy --` Destroys a resource

`wsrf-destroy`

Tool description

Destroys a resource.

Command syntax

`wsrf-destroy [options]`

DRAFT

Table 5. Common options

-h, --help	Displays help information about the command.
-d, --debug	Enables debug mode. For example, full stack traces of errors will be displayed.
-e, --eprFile <file>	Specifies an <i>XML</i> file that contains the <i>WS-Addressing</i> endpoint reference.
-s, --service <url>	Specifies the service URL.
-k, --key <name value>	Specifies the resource key. The name is the QName of the resource key in the string form: {namespaceURI}localPart , while the value is the simple value of the key. For complex keys, use the --eprFile option. Example: <pre>-k "{http://www.globus.org}MyKey" 123</pre>
-f, --descriptor <file>	Specifies a client security descriptor. Overrides all other security settings.
-a, --anonymous	Enables anonymous authentication. Only supported with transport security or the GSI Secure Conversation authentication mechanism.
-g, --delegation <mode>	Enables delegation. mode can be either 'limited' or 'full' . Only supported with the GSI Secure Conversation authentication mechanism.
-l, --contextLifetime <value>	Sets the lifetime of the client security context. value is in milliseconds. Only supported with the GSI Secure Conversation authentication mechanism.
-m, --securityMech <type>	Specifies the authentication mechanism. type can be 'msg' for GSI Secure Message, or 'conv' for GSI Secure Conversation.
-c, --serverCertificate <file>	Specifies the server's <i>certificate</i> file used for encryption. Only needed for the GSI Secure Message authentication mechanism.
-p, --protection <type>	Specifies the protection level. type can be 'sig' for signature or 'enc' for encryption.
-x, --proxyFilename <value>	Sets the proxy file to use as client credential.
-z, --authorization <type>	Specifies authorization type. type can be 'self' , 'host' , 'none' , or a string specifying the expected identity of the remote party.
-t, --timeout <timeout>	Specifies client timeout (in seconds). The client will wait maximum of the timeout value for a response from the server before returning an error. By default the timeout value is 10 minutes.

Example:

```
$ wsrfl-destroy -s http://localhost:8080/wsrfl/services/CounterService \ -k
  "{http://counter.com}CounterKey" 123
```

Name

`wsrf-query` -- Performs query on a resource property document

`wsrf-query`

Tool description

Queries the resource property document of a resource. By default, a simple XPath query is assumed that returns the entire resource property document.

Command syntax

```
wsrf-query [options] [query expression] [dialect]
```

DRAFT

Table 6. Common options

-h, --help	Displays help information about the command.
-d, --debug	Enables debug mode. For example, full stack traces of errors will be displayed.
-e, --eprFile <file>	Specifies an <i>XML</i> file that contains the <i>WS-Addressing</i> endpoint reference.
-s, --service <url>	Specifies the service URL.
-k, --key <name value>	Specifies the resource key. The name is the QName of the resource key in the string form: {namespaceURI}localPart , while the value is the simple value of the key. For complex keys, use the --eprFile option. Example: <pre>-k "{http://www.globus.org}MyKey" 123</pre>
-f, --descriptor <file>	Specifies a client security descriptor. Overrides all other security settings.
-a, --anonymous	Enables anonymous authentication. Only supported with transport security or the GSI Secure Conversation authentication mechanism.
-g, --delegation <mode>	Enables delegation. mode can be either 'limited' or 'full' . Only supported with the GSI Secure Conversation authentication mechanism.
-l, --contextLifetime <value>	Sets the lifetime of the client security context. value is in milliseconds. Only supported with the GSI Secure Conversation authentication mechanism.
-m, --securityMech <type>	Specifies the authentication mechanism. type can be 'msg' for GSI Secure Message, or 'conv' for GSI Secure Conversation.
-c, --serverCertificate <file>	Specifies the server's <i>certificate</i> file used for encryption. Only needed for the GSI Secure Message authentication mechanism.
-p, --protection <type>	Specifies the protection level. type can be 'sig' for signature or 'enc' for encryption.
-x, --proxyFilename <value>	Sets the proxy file to use as client credential.
-z, --authorization <type>	Specifies authorization type. type can be 'self' , 'host' , 'none' , or a string specifying the expected identity of the remote party.
-t, --timeout <timeout>	Specifies client timeout (in seconds). The client will wait maximum of the timeout value for a response from the server before returning an error. By default the timeout value is 10 minutes.

Examples:

```
$ wsrif-query -s https://127.0.0.1:8443/wsrif/services/DefaultIndexService \
  "count(//*[local-name()='Entry'])"
```

```
$ wsrif-query -s https://127.0.0.1:8443/wsrif/services/DefaultIndexService \
  "number(//*[local-name()='GLUECE']/glue:ComputingElement/glue:State/@glue:FreeCPUs)=0"
```

```
$ wsrif-query -s http://localhost:8080/wsrif/services/ContainerRegistryService \
  "/*/*/*/*[local-name()='Address']"
```

Chapter 1. Troubleshooting




For a list of common errors in GT, see [Error Codes](#).

DRAFT

1. Error Messages

DRAFT

Table 1.1. WS A&A Delegation Service Error Messages

Error Code	Definition	Possible Solutions
<p>AuthorizationException: "test DN" is not authorized to use operation: {http://www.globus.org/08/2004/delegationService}requestSecurityToken</p>	<p>This exception can occur when a client whose DN is not in the <i>grid map file</i> configured for the delegation factory service attempts to delegate (using <u>globus-credential-delegate</u>) a credential to the factory service.</p> <p> Note</p> <p>The <i>test DN</i> specified in the error message is just a placeholder and will contain the DN of the user attempting to access the credential.</p>	<p>Ensure that the client is authorized to access delegation service. This requires the client DN to be added in the gridmap file.</p>
<p>AuthorizationException: "test DN" is not authorized to use operation: {http://www.globus.org/08/2004/delegationService}refresh</p>	<p>This exception can occur when a client attempts to refresh a credential it did not delegate (using <u>globus-credential-refresh</u>).</p> <p> Note</p> <p>The <i>test DN</i> specified in the error message is just a placeholder and will contain the DN of the user attempting to access the credential.</p>	<p>This is a delegation service policy and only client who delegates can refresh the credential.</p>
<p><i>test user DN</i> is not authorized to access this resource</p>	<p>Similar to above error but experienced by developers using the API - Only the user who created the delegated credential is allowed to access it. There are two sets of API functions for getting the credential and registering listeners: one in which the caller's DN is picked up from the current thread and the other in which a JAAS subject (containing the caller's DN) is explicitly passed as a function parameter. If the caller's DN (picked up from thread or specified explicitly) does not match the DN of the user who created the credential, this error is thrown.</p> <p> Note</p> <p>The <i>test DN</i> specified in the error message is just a placeholder and will contain the DN of the user attempting to access the credential.</p>	<p>Ensure that the DN explicitly specified or the client DN associated with the thread matches the creator's DN.</p>
<p>Unable to retrieve caller DN, cannot register</p>	<p>Developers come across this error when attempting to register a listener with a delegated credential resource without a JAAS subject. There are two ways of registering: either the JAAS subject can be explicitly passed using the API or the JAAS subject can be picked up from the current message context (the subject representing the client). If the latter mechanism for registering is used and there is no client credential associated with the thread that is calling the register function, then this exception is thrown.</p>	<p>Make sure to use the API call that explicitly passes the subject.</p>

2. CoG Configuration and troubleshooting

Also, for security related troubleshooting the [CoG FAQ](#)¹ might prove useful (especially sections on configuring credentials, CAs and so on.)

DRAFT

¹ <http://www.globus.org/cog/distribution/1.2/FAQ.TXT>

Glossary

C

certificate A public key plus 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.

G

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 `/etc/grid-security/grid-mapfile`. For more information see the Gridmap section [here](#).

T

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

W

Web Services Addressing (WSA) The WS-Addressing specification defines transport-neutral mechanisms to address web services and messages. Specifically, it defines XML elements to identify web service endpoints and to secure end-to-end endpoint identification in messages. See the [W3C WS Addressing Working Group](#)¹⁴ for details.

X

XML Extensible Markup Language (XML) is standard, flexible, and extensible data format used for web services. See the [W3C XML site](#)²⁰ for details.

¹⁴ <http://www.w3.org/2002/ws/addr/>

²⁰ <http://www.w3.org/XML/>