

# EGEE-II

## SHORT LIVED CREDENTIAL SERVICE USER GUIDE

---

Document identifier: EGEE-II-JRA1-TEC-788604-SLCS-  
USERGUIDE-v1-0.doc

Date: **24/10/2006**

Activity: **JRA1: Middleware**

Document status: **DRAFT**

Document link: <https://edms.cern.ch/document/788604/1>

---

Abstract: This document describes how the user can obtain a short lived credential from the Short Lived Credential Service (SLCS).

Copyright notice:

Copyright © Members of the EGEE-II Collaboration, 2006.

See [www.eu-egee.org](http://www.eu-egee.org) for details on the copyright holders.

EGEE-II ("Enabling Grids for E-science-II") is a project co-funded by the European Commission as an Integrated Infrastructure Initiative within the 6th Framework Programme. EGEE-II began in April 2006 and will run for 2 years.

For more information on EGEE-II, its partners and contributors please see [www.eu-egee.org](http://www.eu-egee.org)

You are permitted to copy and distribute, for non-profit purposes, verbatim copies of this document containing this copyright notice. This includes the right to copy this document in whole or in part, but without modification, into other documents if you attach the following reference to the copied elements: "Copyright © Members of the EGEE-II Collaboration 2006. See [www.eu-egee.org](http://www.eu-egee.org) for details".

Using this document in a way and/or for purposes not foreseen in the paragraph above, requires the prior written permission of the copyright holders.

The information contained in this document represents the views of the copyright holders as of the date such views are published.

THE INFORMATION CONTAINED IN THIS DOCUMENT IS PROVIDED BY THE COPYRIGHT HOLDERS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE MEMBERS OF THE EGEE-II COLLABORATION, INCLUDING THE COPYRIGHT HOLDERS, OR THE EUROPEAN COMMISSION BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THE INFORMATION CONTAINED IN THIS DOCUMENT, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trademarks: EGEE and gLite are registered trademarks held by CERN on behalf of the EGEE collaboration. All rights reserved"

**Document Log**

Issue	Date	Comment	Author/Partner
1.0	24/10/2006	Version 1	V.Tschopp/C.Witzig SWITCH

**Document Change Record**

Issue	Item	Reason for Change

## TABLE OF CONTENTS

<b>1. INTRODUCTION</b> .....	<b>4</b>
1.1. PURPOSE .....	4
1.2. APPLICATION AREA .....	4
1.3. REFERENCES.....	4
1.4. TERMINOLOGY .....	4
<b>2. INTRODUCTION</b> .....	<b>6</b>
<b>3. COMMAND LINE USAGE</b> .....	<b>7</b>
<b>4. STANDALONE INSTALLATION</b> .....	<b>8</b>
<b>5. FAQ</b> .....	<b>11</b>
5.1. HOW CAN I TEST THE ACCESS TO THE SLCS SERVICE? .....	11
5.2. WHICH IDENTITY PROVIDER DO I HAVE? .....	12
5.3. WHERE IS THE LOGFILE?.....	12
5.4. HOW CAN I CONTROL THE LOGGING INFORMATION?.....	12
5.5. WHICH CONFIGURATION FILES ARE THERE? .....	12
5.6. I INSTALLED THE SLCS CLIENT. HOW DO I MAKE MY SLCS CERTIFICATE KNOWN TO THE GRID SERVICES?....	12
5.7. WHERE DO I FIND MORE INFORMATION?.....	12

## TABLE OF TABLES

<b>Table 1: Table of references</b> .....	<b>4</b>
---	----------

## 1. INTRODUCTION

### 1.1. PURPOSE

This document describes how the user can obtain a short lived credential from the Short Lived Credential Service (SLCS).

### 1.2. APPLICATION AREA

The document contains information about the usage of the short lived credential service for general grid users who have an account with a Shibboleth Identity Provider.

### 1.3. REFERENCES

**Table 1: Table of references**

R 1	Shibboleth Interoperability through Short lived Credential Service <a href="https://edms.cern.ch/document/770102/1">https://edms.cern.ch/document/770102/1</a>
-----	---

### 1.4. TERMINOLOGY

This subsection provides the definitions of terms, acronyms, and abbreviations required to properly interpret this document. A complete project glossary is provided in the EGEE glossary <http://egee-jra2.web.cern.ch/EGEE-JRA2/Glossary/Glossary.html>.

#### Glossary

AAI	Authentication and Authorization Infrastructure
CA	Certificate Authority: An internal entity or trusted third party that issues, signs, revokes and manages digital certificates.
Certificate	Information issued by a trusted party. Used to identify an individual or system.
CP/CPS	Certificate Policy / Certification Practice Statement: see CP and CPS
CP	Certificate Policy: Rules that a request must comply with for the RA to approve the request or a CA to issue a certificate
CPS	Certification Practice Statement: Document that regulates rights and responsibilities of all the parties involved (RA, CA, End Entity, Relying Party) within a PKI infrastructure.
Identity Provider	Authority responsible for generating and asserting authentication, authorization and identity information about their users in a security domain
PMA	Policy Management Authority: Body responsible for defining the functioning of a PKI infrastructure by means of a CP/CPS
PKI	Public Key Infrastructure: Processes and technologies used to issue and manage digital certificates for the use of third parties to authenticate systems (individual users, services, hosts).
RA	Registration Authority: An entity, which asserts the identity of a certificate requester to the issuing Certificate Authority.

Service Provider	A collection of resources in the terminology of Shibboleth. Normally a Service Provider only contains only one resource.
Shibboleth	Federated identity management solution from Internet2/MACE (Middleware Architecture Committee for Education). It is the name of the architecture as well as the name of the opensource implementation.
Short lived X.509 certificate	An X.509 certificate with a life time of less than 1 mio seconds (approx. 11 days)
SLCS	Short lived credential service: A service returning a short lived X.509 certificate to a requester after successful authentication
SWITCHaai	Shibboleth Federation operated within the Swiss education and research sector. See <a href="http://www.switch.ch/aai">http://www.switch.ch/aai</a> for details.
UI	User Interface: host from where the user interacts with the grid software in the gLite middleware environment.
X.509	ITU-T standard for public key infrastructure. It defines among other things standard formats for certificates. See <a href="http://www.ietf.org/rfc/rfc2459.txt">http://www.ietf.org/rfc/rfc2459.txt</a> for details.
X.509 certificate	Certificate compliant with the format as specified in the X.509 standard.

## 2. INTRODUCTION

The SLCS (short lived<sup>1</sup> credential service) is a service that issues short lived X.509 credentials based upon successful authentication at a Shibboleth Identity Provider. The service is described in detail in [R1].

This service presents from the user's point of view (Figure 1) an X.509 certificate factory that issues him/her a certificate with which he/she can access grid resources. The user executes a shell command on a host (typically the gLite UI) and receives the certificate (`usercert.pem`) and its associated private key (`userkey.pem`) in the store directory `$HOME/.globus`. He/she can use this certificate until it expires, 11 days after it has been issued.

The prerequisite for using this service is

- to have an account with a Shibboleth federation
- to be given access to the SLCS service by an RA

Contact the system administrator of your Shibboleth Identity Provider for help using the SLCS service.

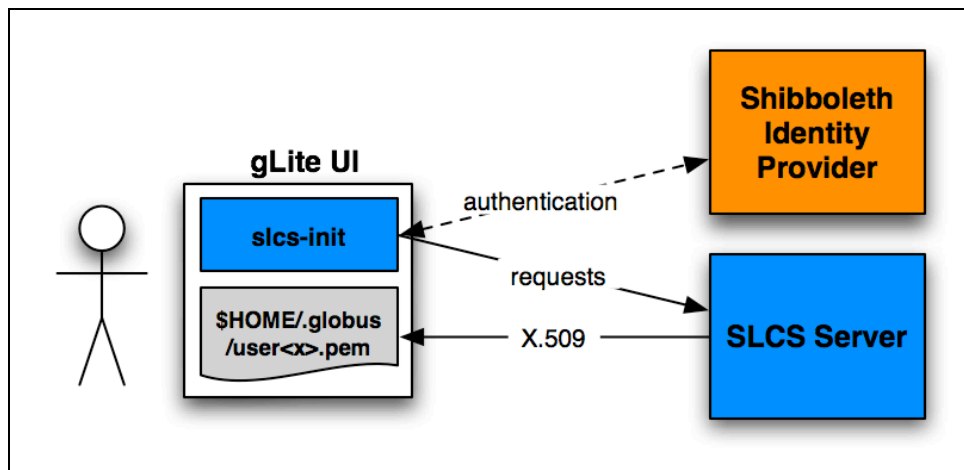


Figure 1: User's view of the SLCS service

<sup>1</sup> Short lived X.509 credentials have a lifetime of less than 1 mio seconds (approx. 11 days).

### 3. COMMAND LINE USAGE

The command line usage is:

```
slcs-init --idp <providerId> [options]
```

where <providerId> is the Shibboleth Identity Provider of the user, which must be known by the user.

The command `slcs-info` will list the configured Identity Providers with their respective providerId.

The `slcs-init` command supports the following arguments:

Command Argument	Explanation	Default Value
<code>--conf &lt;filename&gt;</code>	SLCS client XML configuration file	<code>/opt/glite/etc/glite-slcs-ui/slcs-init.xml</code>
<code>--storedir &lt;directory&gt;</code>	Overwrite the default cert/key files store directory	<code>\$HOME/.globus</code>
<code>--prefix &lt;prefix&gt;</code>	Optional filename prefix for the cert/key files	
<code>--idp &lt;providerId&gt;</code>	ProviderId of the Identity Provider as defined in the SLCS client XML configuration file	
<code>--user &lt;username&gt;</code>	Shibboleth user account	Current user
<code>--password &lt;passwd&gt;</code>	User's password for the Shibboleth user account	
<code>--keysize &lt;size&gt;</code>	Size of the private key (512, 1024, 2048)	1024
<code>--keypass &lt;passwd&gt;</code>	Private key passphrase	Same as Shibboleth password
<code>--help</code>	Display the help	
<code>--verbose</code>	Enables verbose output	

## 4. STANDALONE INSTALLATION

**This section is relevant only for users who want to install the SLCS client on their own.**

There are two ways to install the SLCS command line client (as described in [R1]):

1. Installation as part of the gLite UI
2. Standalone installation on the users desktop (independent of the gLite UI)

Whereas the first method is recommended for gLite deployment, the second may be useful for users who do not use the gLite middleware or just want to install their own software. This section describes how to install the SLCS client independent of gLite installation procedures.

### Prerequisites:

- Linux, Solaris or Mac OSX.
- Java version 1.4.2 or higher

### Installation Instructions:

1. Obtain the latest version of the file `glite-slcs-ui-<version>-<date>.tar.gz` from the SWITCH PKI website <http://www.switch.ch/pki/grid/test> <sup>2</sup>
2. Become root, e.g. by executing `su` or `sudo bash`
3. Untar the file into the `<install-dir>`:
  - a. If gLite UI is installed on the host:

```
cd /opt/glite/  
tar -zxf glite-slcs-ui-<version>-<date>.tar.gz
```

- b. If gLite UI is not installed on the host:

```
cd /usr/local (or any directory of your choice)  
tar -zxf glite-slcs-ui-<version>-<date>.tar.gz
```

4. Make sure your Identity Provider is listed in the file `<install-dir>/etc/glite-slcs-ui/slcs-init.xml`:

---

<sup>2</sup> Note that this URL will change once the SLCS service will become operational after it has been accredited by the EUGRIDPM (approx. January 2007)

```
<IdentityProvider id="switch.ch">
  <name>SWITCH</name>
  <url>https://aai-logon.switch.ch/shibboleth-idp/SSO</url>
  <authentication type="CAS">
    <url>https://aai-logon.switch.ch/cas/login</url>
    <form name="login_form">
      <username>username</username>
      <password>password</password>
    </form>
  </authentication>
</IdentityProvider>
```

Otherwise, add your Shibboleth Identity Provider definition in the section `<IdentityProviders>`, if it is not already listed there.

5. If you have added your own Shibboleth Identity Provider in the file `slcs-init.xml`, and it is using a non standard SSL certificate, then most likely you also have to add the Identity Provider's CA certificate in the truststore `<install-dir>/etc/glite-slcs-ui/truststore.switchaai.jks`, e.g. by using the command:

```
keytool -import -trustedcacerts -storepass switchaai
        -keystore truststore.switchaai.jks <your_CA_certificate>
```

6. If needed, edit the `<install-dir>/etc/glite-slcs-ui/log4j.properties` file and update the absolute location of the log file. E.g. `<install-dir>/log/slcs-init.log`
7. Update your `PATH` to include the directory `<install-dir>/bin` in it.
8. Exit the root shell.
9. First, test the web access to the SLCS by entering the SLCS Service URL as given by the command `slcs-info`. You should get an output like this:

```
tschopp@venus:~$ slcs-info
SLCS Service URL: https://hestia.switch.ch/SLCS/login
Identity Provider: SWITCH [switch.ch]
Identity Provider: Virtual Home Organization [vho-switchaai.ch]
...
```

Open a browser with the SLCS Service URL. Choose your Identity Provider and log in. If the web access does not work, you must check your Shibboleth account information (see also FAQ #1 in section 5).

10. As user execute the command `slcs-init -v --idp <yourIdpProvider>`. You should get an output like this:

```
tschopp@venus:~$ slcs-init -v --idp switch.ch
Config: slcs-init.xml
IdentityProvider: switch.ch
Username: tschopp
Shibboleth Password:
Key Password:
Shibboleth login...
SLCS login request...
Generate private key (1024 bits)...
Generate certificate request...
SLCS certificate request...
Store private key [/home/tschopp/.globus/userkey.pem]...
Store SLCS certificate [/home/tschopp/.globus/usercert.pem]...
Done.
```

11. You can inspect the certificate obtained using the command:

```
openssl x509 -text -noout -in ~/.globus/usercert.pem
```

## 5. FAQ

1. How can I test the access to the SLCS service?
2. Which Identity Provider do I have?
3. Where is the log file?
4. How can I change the logging information?
5. Which configuration files are there?
6. I installed the SLCS client on my host. How do I add the certificates into the /etc/grid-security directory?
7. Where do I find more information?

### 5.1. HOW CAN I TEST THE ACCESS TO THE SLCS SERVICE?

Open a browser to the SLCS Service URL. It can be found with the command `slcs-info` or in the configuration file `<install-dir>/glite-slcs-ui/slcs-init.xml`, the tag `<url>` value in the element `<ServiceProvider>`.

You should get a successful XML login response as shown in Figure 2 after a successful authentication at your Shibboleth Identity Provider:

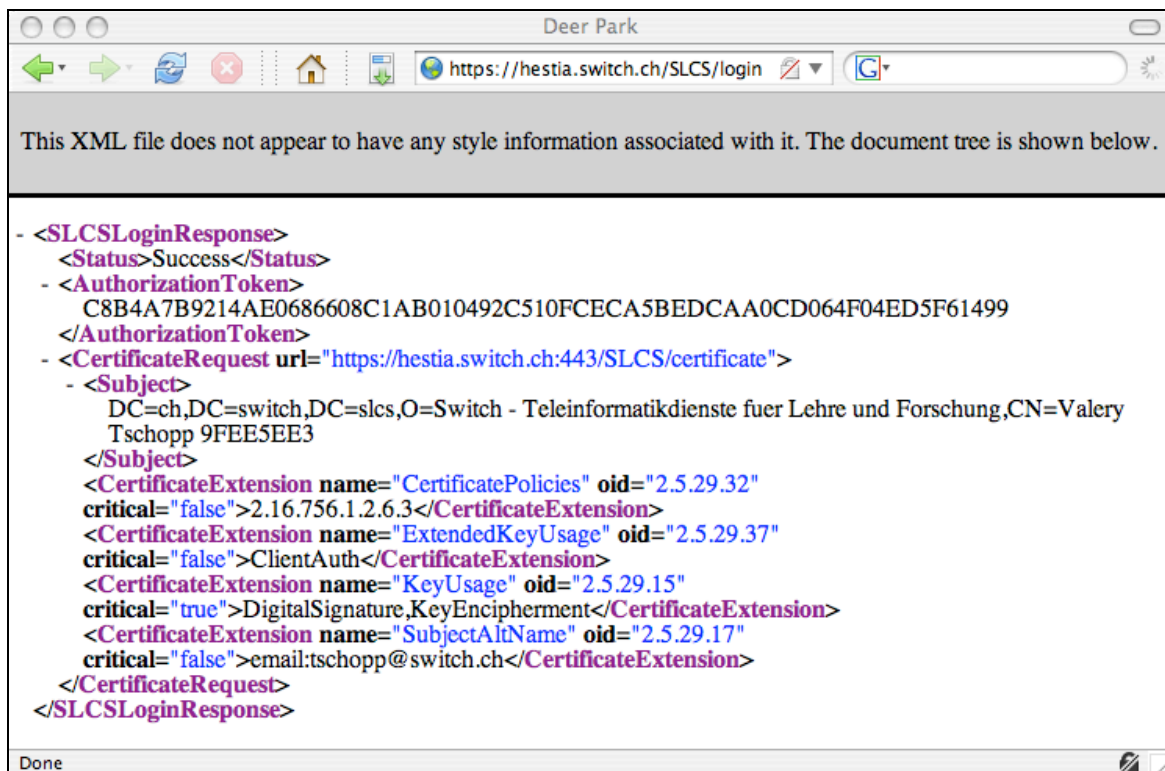


Figure 2: Webpage of the SLCS service after successful authentication at the Shibboleth Identity Provider

## 5.2. WHICH IDENTITY PROVIDER DO I HAVE?

That you have to find out on your own! You can run the command `slcs-info` and see if your Identity Provider is listed or look in the SLCS configuration file `<install-dir>/etc/glite-slcs-ui/slcs-init.xml` file, in the section `<IdentityProviders>` for the host, where you normally log on using your Shibboleth credentials.

## 5.3. WHERE IS THE LOGFILE?

The default location is `/opt/glite/log/slcs-init.log`.

## 5.4. HOW CAN I CONTROL THE LOGGING INFORMATION?

The command `slcs-init` uses `log4j` internally. Edit the file `<install-dir>/etc/glite-slcs-ui/log4j.properties` according to your taste.

## 5.5. WHICH CONFIGURATION FILES ARE THERE?

The main configuration file is `<install-dir>/etc/glite-slcs-ui/slcs-init.xml`. There is also the `log4j.properties` file as well as the truststore file in the directory `<install-dir>/etc/glite-slcs-ui/`

## 5.6. I INSTALLED THE SLCS CLIENT. HOW DO I MAKE MY SLCS CERTIFICATE KNOWN TO THE GRID SERVICES?

If the SLCS server is accredited by IGTF, then it will be update automatically if you use the `igtf` certificate distribution.

Otherwise you have to obtain the necessary files from the operator of the SLCS service. For SWITCH this is currently the directory <http://www.switch.ch/grid/test><sup>3</sup>

## 5.7. WHERE DO I FIND MORE INFORMATION?

More information can be found in the

- Description of the SLCS service in the EGEE MJRA1.4 document [R1]
- The SLCS Administrator guide
- The SWITCH PKI website <http://www.switch.ch/pki><sup>4</sup>
- The SWITCH AAI website <http://www.switch.ch/aa>

---

<sup>3</sup> Note that this website will change once the SLCS service has been accredited.

<sup>4</sup> This website will be available after the EUGRIDPMA accreditation.