

caNI++

caNI++ team

University Of Oslo

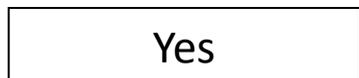
5th EMI AHM, Budapest

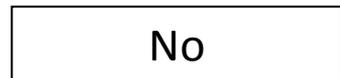
- Credential handling:
 - File-based credential handling based on OpenSSL
 - DB-based credential handling based on NSS
- Secure communication

Features of caNI++

	CSR generation	Extension (voms AC) inserting	Proxy/EEC signing
File-based (cert/key, CA certs, CRL are based on files) Implemented with OpenSSL lib	Yes	Yes	Yes/Yes
DB-based (cert/key, CA certs, CRL are based on nss db) Implemented with NSS lib	Yes	Yes	Yes/No


Has supported


Can support, not
yes supported

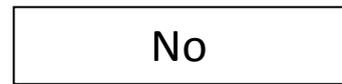

Cannot support

Features of caNI++

	Certificate verification (CRL)	Certificate verification (OCSP)	Certificate verification (OCSP stapling)	Secure communication
File-based	Yes	Yes	Yes	Yes
DB-based	Yes	Yes	No (not supported by nss lib)	Yes


Has supported

 Yes
Can support, not yet supported

 No
Cannot support

- OCSP stapling and OCSP
 - Easier the load of OCSP server
 - Alleviate the privacy concern for users
 - OCSP stapling is implemented in canl++ together with secure communication

- <http://svn.nordugrid.org/trac/workarea/browser/caNI%2B%2B/trunk>

Example

```
std::string repo_cert = cadir + "/certs" + "/cert.pem";  
std::string repo_key = cadir + "/certs" + "/key.pem";  
std::ofstream repo_cert_stream(repo_cert.c_str(), std::ofstream::trunc);
```

```
AuthN::Context ctx(AuthN::Context::EmptyContext);  
AuthN::Credentials eec(ctx);  
eec.GetCertificate(repo_cert_stream); repo_cert_stream.close();
```

```
AuthN::Context omsp_ctx(AuthN::Context::EmptyContext); omsp_ctx.SetCAPath(trusted_cadir);  
//Set the credential for validator, which will be  
//used to sign the OMSp request  
omsp_ctx.SetCredentials(repo_cert, repo_key);
```

```
AuthN::Validator omsp_validator(omsp_ctx);  
//Set the validation mode  
omsp_validator.SetMode(AuthN::Validator::ValidationOMSpIfPresent);  
//eec OMSp validation  
eec.SetValidator(omsp_validator);  
stat = eec.Validate();  
CPPUNIT_ASSERT_EQUAL(stat, AuthN::Status(0));
```

- Original Plan:
 - arcproxy (credential handling)
 - ARC delegation interface (credential handling)
 - ARC MCC TLS (secure communication), critical module of ARC
 - some other components that use credential handling of ARC (credential handling)

- Current Status:
 - caNI++ is only integrated with test release arcproxy
 - Other parts of integration will be postponed after EMI3 (Oct.31)

- Support credential source from Firefox's NSS internal PKCS#11 module
 - arcproxy –nssdb (-F)
 - By default, the location of nss db is parsed from
 - “`~/.mozilla/firefox/profiles.ini`”
 - “`~/.mozilla/seamonkey/profile.ini`”
 - “`~/.thunderbird/profile.ini`”

arcproxy (with nssdb)

```
dhcp114:credentials qiangweizhong$ ./arcproxy --nssdb
There are 2 nss base directories where the cert, key, and module databases live
Number 1 is: /Users/qiangweizhong/Library/Application Support/Firefox/Profiles/bphfwosy.my_profile
Number 2 is: /Users/qiangweizhong/Library/Thunderbird/Profiles/2iql8smt.default
Please choose the nss db you would use (1-2): 2
nss db to be accessed: /Users/qiangweizhong/Library/Thunderbird/Profiles/2iql8smt.default
Enter Password or Pin for "internal (software)":
There are 1 user certificates existing under nss database
Number 1 is with nickname: Imported Certificate (Weizhong Qiang)
    expiration time: 2013-05-02 16:18:27
Please choose the one you would use (1-1): Certificate to use is: Imported Certificate
Proxy generation succeeded
Your proxy is valid until: 2012-10-30 11:49:38
```

arcproxy (with nssdb and voms)



```
dhcp114:credentials qiangweizhong$ ./arcproxy --nssdb --voms testbed.univ.kiev.ua:all --vomses ./vomses
There are 2 nss base directories where the cert, key, and module databases live
Number 1 is: /Users/qiangweizhong/Library/Application Support/Firefox/Profiles/bphfwosy.my_profile
Number 2 is: /Users/qiangweizhong/Library/Thunderbird/Profiles/2iql8smt.default
Please choose the nss db you would use (1-2): 2
nss db to be accessed: /Users/qiangweizhong/Library/Thunderbird/Profiles/2iql8smt.default
Enter Password or Pin for "internal (software)":
There are 1 user certificates existing under nss database
Number 1 is with nickname: Imported Certificate (Weizhong Qiang)
    expiration time: 2013-05-02 16:18:27
Please choose the one you would use (1-1): Contacting VOMS server (named testbed.univ.kiev.ua): moldyngrid.org on port: 15112
Certificate to use is: Imported Certificate
Proxy generation succeeded
Your proxy is valid until: 2012-10-30 12:29:36
```

```
dhcp114:credentials qiangweizhong$ ./arcproxyalt -I -P /var/folders/gr/grXUpvDWEsiTN08Q0kXEVE+++TI/-Tmp-/x509up_u501
Subject: /O=Grid/O=NorduGrid/OU=fys.uio.no/CN=Weizhong Qiang/CN=1624804041
Issuer: /O=Grid/O=NorduGrid/OU=fys.uio.no/CN=Weizhong Qiang
Identity: /O=Grid/O=NorduGrid/OU=fys.uio.no/CN=Weizhong Qiang
Time left for proxy: 11 hours 59 minutes 55 seconds
Proxy path: /var/folders/gr/grXUpvDWEsiTN08Q0kXEVE+++TI/-Tmp-/x509up_u501
===== AC extension information for VO testbed.univ.kiev.ua =====
VO      : testbed.univ.kiev.ua
subject : /O=Grid/O=NorduGrid/OU=fys.uio.no/CN=Weizhong Qiang
issuer  : /DC=org/DC=ugrid/O=hosts/O=IMBG/CN=moldyngrid.org
uri     : moldyngrid.org:15112/testbed.univ.kiev.ua/weizhong:uniq_attr1=testattribute
uri     : moldyngrid.org:15112
attribute : /testbed.univ.kiev.ua
attribute : /testbed.univ.kiev.ua/weizhong
Time left for AC: 11 hours 59 minutes 54 seconds
```