Employee News
Enterprise Systems
Sponsors
Agency Tools
Military News

IM Wiki Home Page

NAVSUP Security Model Overview

Security API

Developer Handbook

Server to Server Communication

Code Examples ▾

Configuration ▾

Cook books ▾

NAVSUP Apps A-M ▾

NAVSUP Apps N-Z ▾

Policy ▾

Release Notes ▾

Standards ▾

Documents

Contact Us

12c Migration

Obtaining a New Application Client Certificate Using OpenSSL

Steps for Generating New Signed Application Certificates

Please use the naming conventions defined in the Server to Server Communication Standards section

Installing OpenSSL

Install Win64 OpenSSL v1.1.0h from http://slproweb.com/products/Win32OpenSSL.html

Set OPENSSL_CONF=C:\OpenSSL-Win64\bin\cnf\openssl.cnf

A copy of Win64 OpenSSL is also available on the share drive at:

\\naeamechfs101v.nadsusea.nads.navy.mil\navsup04$\BSC\NAVSUP ENTERPRISE WEB\Identity Management\DevTools\openssl.zip

Create a new private key

```
C:\OpenSSL-Win64\bin\openssl.exe genrsa -out [appname]_test.key 2048
```

Generate a Certificate request

NOTE: For prod the CN would be `[appname].applications.navsup`. for test it will be `[appname].applicationstest.navsup`.

```
C:\OpenSSL-Win64\bin\openssl.exe req -new -key [appname]_test.key -out
[appname]_test.csr -subj "/CN=
[appname].applicationstest.navsup/OU=USN/OU=PKI/OU=DoD/O=U.S. Government/C=US"
```

Verify the request

```
C:\OpenSSL-Win64\bin\openssl.exe req -text -noout -verify -in [appname]_test.csr
```

Submiting a CA Signed Certificate Request

1) Navigate to the NPE Portal Website using Chrome or Firefox. https://npe-portal.csd.disa.mil/

2) Under the Certificate Management menu select Conduct Certificate Operations > Submit Certificate Application...

3) Copy the entire certificate request (including the BEGIN and END lines) into the text area provided on the certificate request form.

4) Certificate Profile should be TLS Server

5) Certificate CC/S/A should be USN

6) DNS Name should be <application name>.applications<environment>.navsup

7) Key Usage Selections should be: digitalSignature, keyEncipherment

8) Extended Key Usage Selection should be: id-kp-server/Auth, id-kp-client/Auth

9) Submit, and copy down the request ID number to be used for inquiring about status or communication with the LRA (Tony Arturet and Kevin McNamara for NAVSUP Business Systems Center).

10) Send an email to kevin.k.mcnamara@navy.mil;antonio.arturetmilla@navy.mil using the template defined in See the Server to Server Communication Application Client Certificate Request Template.

Processing the CA Signed Certificate Request

Once your certificate signing request has been processed you should have a signed public certificate available to you (see the Server to Server Communication page for an overview of the certificate signing process).

1) Check on request status by going to the NPE Portal Website and selecting Conduct Certificate Operations > View My Certificate Applications...

2) When issued, click on the Issued certificate and select Status

3) Select the Download button and select X509 Certificate

4) Save the file contents of that section of the response to a PEM file by either selecting All Files and saving as .pem or renaming the file from .cer to .pem (i.e. [appname]-ca.pem)

NOTE: Make sure to use the issued certificate which includes the chain of authority. For the purposes of these instructions we assume this certificate has been saved as “[appname]_test.pem”.

Exporting to a PKCS12 (p12) File

You will need to generate a p12 file from your keystore so youcan to import your certificate into your web browser for registration purposes.

```
C:\OpenSSL-Win64\bin\openssl.exe pkcs12 -export -inkey [appname]_test.key -in
[appname]_test.pem -out [appname]_test.p12
```

Please use the naming conventions defined in the Server to Server Communication Standards section. Examples of a application client certificate name and key store is: myapp_test.jks or myapp_prod.jks

Creating the Application Certificate Java Keystore

This is needed so it can be presented to the NAVSUP Security API and update the unix server keystore. you will need the keytool from java JDK .

A) Import the p12 cert file to create the java keystore used for Security API communications.

```
C:\java\jdk1.8.0_211\bin\keytool.exe -importkeystore -srckeystore
[appname]_test.p12 -srcstoretype PKCS12 -srcstorepass [password] -srcalias [appname]
-destkeystore [appname]_test.jks -deststoretype JKS -deststorepass [password] -
destalias [appname] -noprompt -v
```

NOTE: You will need to know the password protecting the p12. Note that the password of the private key stored inside the keystore is not affected. and you will need to set the same password for the destination java keystore

Have a sys admin update the application java keystore file [appname]_test.jks on the server. See the Server to Server Communication Updating Java Keystore on Server