UCAIug ITCA Green Button Data Custodian Connect My Data Test Sheet  
Revised: 2/4/2016 12:16 PM

# Overview

This document contains the test data sheet and procedures for performing the Green Button Data Custodian Connect My Data certification tests for UCAIug.

## References

1. The Green Button Test Cases Spreadsheet: <http://files.gbitca.org/test-cases>
2. The latest version of this template: <http://files.gbitca.org/dc-cmd-test-data-sheet>
3. The policies and procedures for the UCAIug ITCA for Green Button: <http://files.gbitca.org/certification-policies-procedures>
4. Application for testing: <http://files.gbitca.org/dc-cmd-cert-form>

# Tests

## Instructions

### Configuring Test Harness for a New Test Applicant

Note: this document is extremely draft

#### Overview

The following steps describe how to configure the test harness for a Green Button Data Custodian Connect My Data certification applicant:

1. Obtain the following information from the applicant:
   1. OAuth 2.0 ***Client ID*** and ***secret***
   2. OAuth 2.0 ***registration\_access\_token*** value
   3. Applicant’s OAuth 2.0 Authorization Server Endpoint
   4. Applicant’s Resource Server Endpoint
2. Update the ***gbcmd\_target.conf*** file with the information provided by the applicant in step 1, and the Certification ID provided on the applicant’s certification application

2. Retrieve the TLS/SSL certificates from the applicant for their Authorization and Resource Servers

3. Store the retrieved certificates in the ***/etc/ssl/certs*** directory with hashes

4. Configure the stunnel proxy routing configuration file

### Sample gbcmd\_target.conf file

FileName="gbcmdcert\_target.conf"

// Certification Identifier from Applicant’s Certification Application

CertID="123456"

dataCustodianResourceEndpoint="https://localhost:8443/DataCustodian/espi/1\_1/resource"

authorizationServerTokenEndpoint="https://localhost:8443/DataCustodian/oauth/token"

// for retrieval of information for this third party, provide the IDs to use

// resourceUri:

// {dataCustodianResourceEndpoint}/ApplicationInformation/{applicationInformationId}

// authorizationUri:

// {dataCustodianResourceEndpoint}/Authorization/{authorizationId}

applicationInformationId="2"

authorizationId="4"

// OAuth 2.0 Test Applicant Assigned client id and secret

client\_id=""

client\_secret=""

// OAuth 2.0 registration\_access\_token

// either provide access token, or, id and secret

registration\_access\_token=""

registration\_access\_token\_client\_id="REGISTRATION\_surface\_tp"

registration\_access\_token\_secret="secret"

// client\_access\_token

// either provide access token, or, id and secret

client\_access\_token=""

client\_access\_token\_client\_id="surface\_tp\_admin"

client\_access\_token\_secret="secret"

scope="FB=4\_5\_15;IntervalDuration=3600;BlockDuration=monthly;HistoryLength=13"

certDataScopeFBs="FB=1\_4\_5\_15"

// if an offline authorization (FB\_XX) is used, provide the authorization id and access token

optionalOfflineAuthorizationID="5"

optionalOfflineAccess\_token="57673811-5a25-4412-89e1-e15043f9703f"

### Retrieve and Test Target Certificates

The certificates for the Authorization and Resource Server must be retrieved and installed on the test harness system.

For this step, run from the stunnelConfigDirectory directory and install certificates in the CApathDirectory. These paths are in the gbcmdcer.conf file.

#### Fetch Certificate and Install

host ($1) and port ($2) as arguments to retrieve certificate. Perform this once for each remote target server to be used.

cd {stunnelConfigDirectory}

sudo echo Q | openssl s\_client -showcerts -connect $1:$2 -CApath /etc/ssl/certs -cert openespi.pem -key openespi\_private\_key.pem | sed -ne '/-BEGIN CERTIFICATE-/,/-END CERTIFICATE-/p' > ~/Desktop/$1.pem

sudo cp ~/Desktop/$1.pem {CApathDirectory}/$1.pem

cd /etc/ssl/certs

sudo ln -s $1.pem `openssl x509 -hash -noout -in $1.pem`.0

#### Verify the Certificates are Accessible and Valid

From the stunnelConfigDirectory directory test each server - look for Verify return code:0 (ok):

echo Q | openssl s\_client -verify 10 -showcerts -CApath {CApathDirectory} -cert openespi.pem -key openespi\_private\_key.pem -connect $1:$2

Note: If there are any errors listed in the exchange (even if the verify is ok) you may need to check intermediate certificates in the chain from the "-showcerts" parameter. If so, you may need to acquire these certificates from DigiCert, Verisign or appropriate source and add them to the certs directory.

## Identification

Fill out the following table (*italics* fields come from the test application):

|  |  |
| --- | --- |
| *Date of Test:* |  |
| *Certificate Identifier:* |  |
| *Certification Lab:* |  |
| *Test Suite Version:* |  |
| *Company:* |  |
| *Product Name:* |  |
| *Product Version:* |  |
| *Function Blocks (FBs) to be Tested:* |  |
| *Company Representative (Testee):* |  |
| *Certification Engineer (Tester):* |  |
| *Starting Test URL:* |  |
| *Test Machine:* |  |
| *Test Browser:* |  |
| Date of Test: |  |
| *Product or system under test:* |  |
| *Company:* |  |
| *Function Blocks (FBs) to be Tested (minimum 1,2,4,5):* |  |
| *Test Lab:* |  |
| Company Representative (Testee): |  |
| Test Witness (Tester): |  |
| Starting Test URL: |  |
| Test Machine: |  |
| Test Browser: |  |

# Summary of Results

This section contains the results of the testing session. To review results use the following procedure.

## Results of testing

Procedure:

1. Type key sequence ^A (Control key + A) to select the entire document contents
2. Type the “F9” key to update results
3. Complete the following attestation to the results

|  |
| --- |
| <enter any comments or notes here including pasted images> |

\_\_ COMPLIANT \_\_ NONCOMPLIANT Tester Initials: \_\_\_\_ Testee Initials: \_\_\_\_

## Log of Results

This section contains an embedded object which contains a detailed log of experiment progress and results. To review results use the following procedure.

1. The following log of results can be reviewed by right-clicking on the object and selecting “Packager Shell Object/Activate Contents”
2. Review the results in opened in the notepad

