3D-SECURE-CONFIGURATION

OCB

|  |  |
| --- | --- |
| Prepared for : | OCB |
| Version of Document : | 1.0 |
| Status : | Draft |
| Release Date : | 18 OCT 2018 |
| Prepared by : | OpenWay Asia |
| Author : |  |
| Owner : | OpenWay Asia |

**Document Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Date | Description of Change | Change done by | Approved By |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

Copyright

© OpenWay InternationalLimited 2019. All rights reserved.

The Copyright of this complete document and every part it belongs to OpenWay International Limited. Proprietary material, brand or product names of other parties or trademarks remain with their respective owners. You may not, except with our express written permission, distribute or commercially exploit the content. Nor may you transmit it or store it in any other website or other form of electronic retrieval system. Any sample data used in examples below are completely fictitious unless otherwise noted.

Disclaimer

This document and the OpenWay International software it describes are furnished by OpenWay International Limited under a Software Licensing Agreement, Consultancy Agreement, Variation Request or Confidentiality Agreement, and may be used or copied only in accordance with the terms of such Agreement. Neither this document nor the OpenWay International software it describes may be used, sold, transferred, copied, translated, reproduced or transmitted in any form or by any means, electronic or mechanical, for any purpose, in whole or in part, other than in accordance with the terms of such Agreement, or otherwise without prior written consent of OpenWay International Limited.

This document describes a generic product or service and should be read in conjunction with other documents relevant to the configuration of any specific system. The licensee of OpenWay software or user of OpenWay International services is responsible for ensuring that the product or service described herein meets its own requirements. The information contained in this document is subject to change without notice and should not be taken as a commitment by OpenWay International Limited. OpenWay International Limited assumes no responsibility for any errors that may appear in this document.

Confidentiality

The information contained in this Document is the property of OpenWay International Ltd and contains CONFIDENTIAL information that is produced solely for the benefit of the receiving party named on the front page of this document. The recipient should keep this document and all its information confidential. On no account should this document, in whole or in part, be used, sold, transferred, copied, translated, reproduced or transmitted in any form or by any means, electronic or mechanical, or disclosed or disseminated to any third party, without the express written permission of OpenWay International Ltd.

[3D-SECURE-CONFIGURATION 1](#_Toc531609217)

[Document Version Control 1](#_Toc531609218)

[1 Introduction 6](#_Toc531609219)

[1.1 Disclaimer 6](#_Toc531609220)

[2 Architecture 7](#_Toc531609221)

[3 Install Application Server 8](#_Toc531609222)

[3.1 Create user way4 under group way4 8](#_Toc531609223)

[3.2 Edit parameters for /etc/sysctl.conf 8](#_Toc531609224)

[3.3 Edit parameters for /etc/security/limits.conf 8](#_Toc531609225)

[3.4 Checking the environment 9](#_Toc531609226)

[3.5 Install Application Server (ACS server and Egateway Server) 12](#_Toc531609227)

[4 Instal ACS, Demobank, Egateway 20](#_Toc531609228)

[4.1 Install ACS 20](#_Toc531609229)

[4.2 Install DEMOBANK 21](#_Toc531609230)

[4.3 Install EGATEWAY (Remember to change owner of bin directory) 22](#_Toc531609231)

[5 Install Eracom's libraries 25](#_Toc531609232)

[5.1 Copy the following two packages to the server 25](#_Toc531609233)

[5.2 Install Eracom's Libraries 25](#_Toc531609234)

[6 Configure DBM 27](#_Toc531609235)

[6.1 Configure Authentication Module 27](#_Toc531609236)

[6.1.1 Configure Authentication Domains 27](#_Toc531609237)

[6.1.2 Configure Authentication Type 28](#_Toc531609238)

[6.1.3 Configure event to generate OTP\_SMS and OTP\_EMAIL 31](#_Toc531609239)

[6.1.4 Generate CAVVK 1 and 2 34](#_Toc531609240)

[7 Configure EGATEWAY 36](#_Toc531609241)

[7.1 Edit log level of Egateway 36](#_Toc531609242)

[7.2 Configure netserv.ini 36](#_Toc531609243)

[7.3 Configure authserv.ini 37](#_Toc531609244)

[7.4 Configure acs\_gate.ini 39](#_Toc531609245)

[7.4.1 Link to Authentication Page 39](#_Toc531609246)

[7.4.2 Setup a non-hashed password for enrolment 39](#_Toc531609247)

[7.4.1 Uncomment CertStore 40](#_Toc531609248)

[7.4.2 Configure the rest parameters 40](#_Toc531609249)

[7.5 Configure hsm\_gate.ini 43](#_Toc531609250)

[7.5.1 Configure RSA key 44](#_Toc531609251)

[7.5.2 Configure DWK2 point to DWK1 44](#_Toc531609252)

[7.5.3 Configure currency 45](#_Toc531609253)

[8 Configure Transaction Switch 47](#_Toc531609254)

[9 Configure WAY4ACS 49](#_Toc531609255)

[9.1 Configure way4acs 49](#_Toc531609256)

[9.1.1 Copy Catalina folder 49](#_Toc531609257)

[9.1.2 Create way4acs folder in opt directory 49](#_Toc531609258)

[9.1.3 Add parameters to ACS configuration (opt/way4acs/work/way4acs/config.xml) 50](#_Toc531609259)

[9.1.4 Set LD\_LIBRARY\_PATH and full log: 52](#_Toc531609260)

[10 Configure WAY4 ACS Web 53](#_Toc531609261)

[10.1 Languages 53](#_Toc531609262)

[10.2 OTP Email 54](#_Toc531609263)

[10.3 OCB Logo 57](#_Toc531609264)

[11 Configure to support Eracom HSM connection 58](#_Toc531609265)

[11.1 Check the connection to Eracom Hsm 63](#_Toc531609266)

[12 Generate keys 65](#_Toc531609267)

[12.1 Generate 3DES Keys under Online HSM 65](#_Toc531609268)

[12.1.1 Creating components of a zone master key (ZMK) used to import working keys 65](#_Toc531609269)

[12.1.2 Form ZMK key from two components generated in the previous step (Form ZMK key from ZMK1, ZMK2) 66](#_Toc531609270)

[12.1.3 Generate working key (DWK) in HSM online (Thales) 66](#_Toc531609271)

[12.1.4 Add DWK1 working key created in the above step to the channel in Transaction Switch 67](#_Toc531609272)

[12.1.5 Import Zone Master Key (ZMK) to Eracom HSM 67](#_Toc531609273)

[12.1.6 Import working key (DWK1) to Eracom HSM 68](#_Toc531609274)

[12.1.7 Check the link in the 3D-Secure Gateway configuration file: 69](#_Toc531609275)

[12.2 Generate RSA keys to support SSL/TSL and digital signature of PaRes 72](#_Toc531609276)

[12.3 Check the key after import to the ERACOM's hsm 72](#_Toc531609277)

[13 Network configuration 73](#_Toc531609278)

[14 Configure Application Server 74](#_Toc531609279)

[14.1 Edit virtual host name and address 74](#_Toc531609280)

# Introduction

This document covers the business requirements for Instalments as defined by OCB during the discovery phase session which took place on September, 2018.

The technical solutions, Setup, and Configuration needed to be done in WAY4 to satisfy OCB’s Issuing requirements are defined as far as possible. These solutions are internal to WAY4 and are based on expertise and knowledge of OpenWay staff. The solutions will be updated and finalized during the system build phase by OpenWay. Any technical solution provided in this document can be updated or changed by OpenWay staff without any notification to OCB.

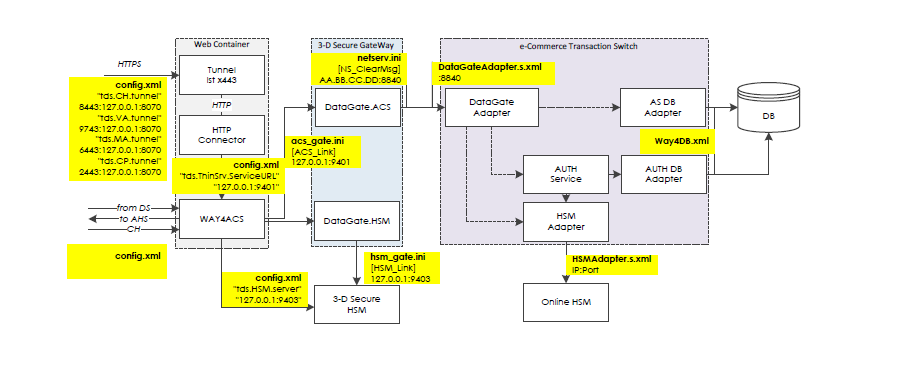
## Disclaimer

The purpose of this report is to present an accurate description of the requirements and work required to configure the system in line with these requirements. All development and configuration work to be undertaken on the project will be defined in accordance with the letter of agreement signed between the parties. The contractual documents will take precedence over this document.

# Architecture

WAY4 Ecommerce Issuing requires the following components:

* 3-D Secure, including:
  + 3-D Secure Gateway – gets authorization and financial requests from Internet merchants and service providers.
  + WAY4ACS – checks the cardholder according to requests coming in from external MPI (Merchant Plug-In) servers via the 3-D Secure protocol.
* Transaction Switch (e-Commerce Transaction Switch) – used in Transaction Switch solution
* WAY4 Cards



Network port numbers shown here are only used to illustrate a sample configuration

How to start 3Ds services

1. WAY4 Database
2. Transaction Switch
3. 3Ds E-gateway
4. WAY4 ACS
5. WAY4 ACS Web

# Install Application Server

## Create user way4 under group way4

|  |
| --- |
| [root@rhel3-mini distr]# groupadd way4  [root@rhel3-mini distr]# useradd way4 -g way4 |

## Edit parameters for /etc/sysctl.conf

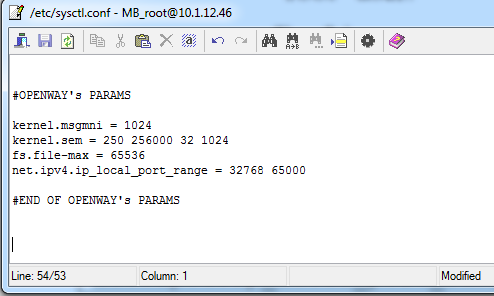
login under root user and edit the /etc/sysctl.conf

|  |
| --- |
| kernel.msgmni = 1024  kernel.sem = 250 256000 32 1024  fs.file-max = 65536  net.ipv4.ip\_local\_port\_range = 32768 65000 |

## Edit parameters for /etc/security/limits.conf

login under root user and edit the /etc/security/limits.conf

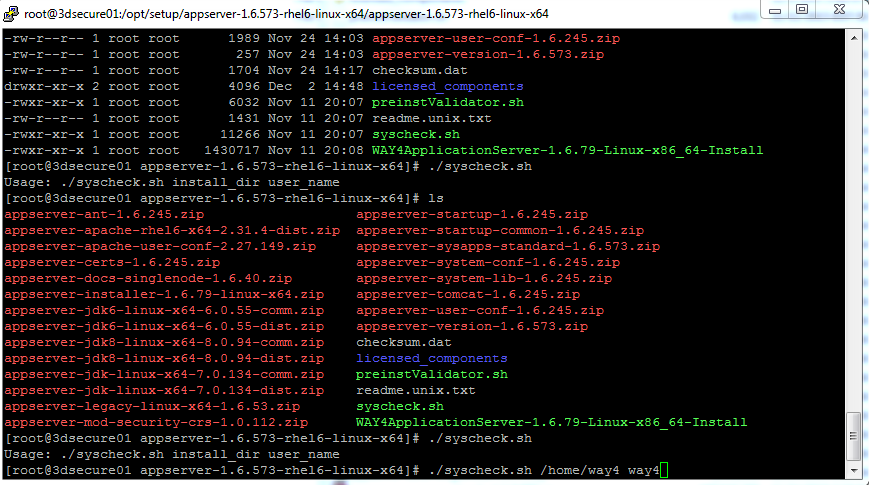
|  |
| --- |
| way4 soft nproc 32767  way4 hard nproc 32768  way4 soft nofile 65535  way4 hard nofile 65536 |



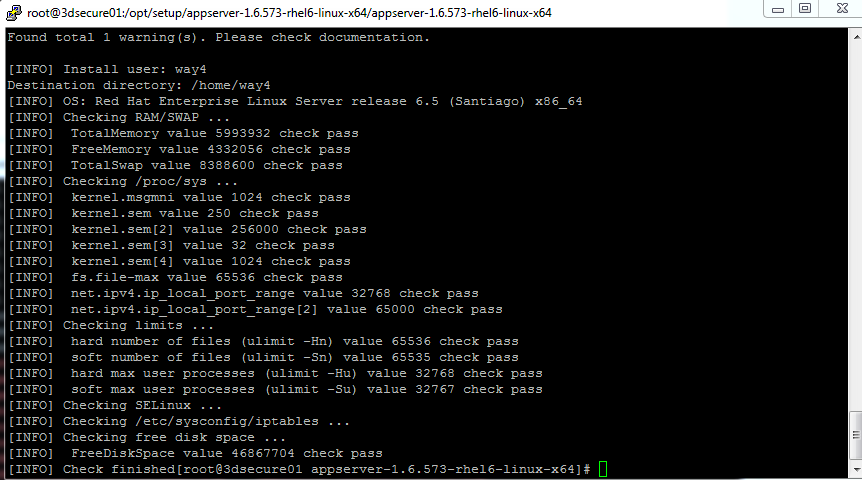
## Checking the environment

|  |
| --- |
| [root@3dsecure02 appserver]# ./syscheck.sh /home/way4 way4 |





[root@3dsecure02 appserver]# ./syscheck.sh /home/way4 way4



## Install Application Server (ACS server and Egateway Server)

Login as root, and go to the directory (it can be different depends on the version you will be delivered)

/opt/setup/appserver-1.6.573-rhel6-linux-x64/appserver-1.6.573-rhel6-linux-x64

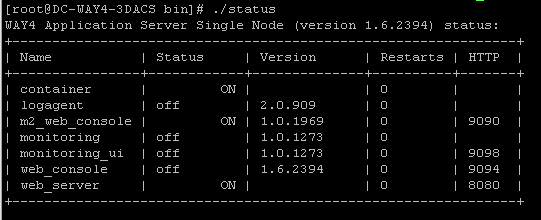


[root@3dsecure01 appserver-1.6.573-rhel6-linux-x64]# ./WAY4ApplicationServer-1.6.79-Linux-x86\_64-Install

During the installation process, you will be asked to key in password of the web console. You can use the following password or any value.

password = admin123

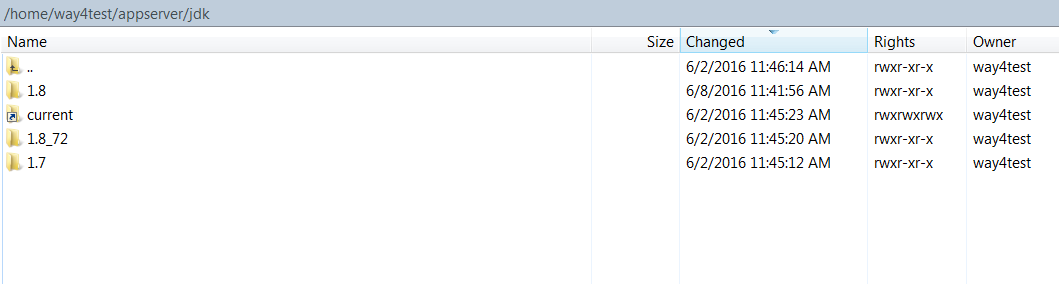
|  |
| --- |
| [root@DC-WAY4-3DACS appserver-1.6.2394-rhel7-linux-x64]# ./WAY4ApplicationServer-1.6.2394-Linux-x86\_64-Install  Distribution was checked for consistency - OK  This will install or upgrade standard configuration of Application Server with  version 1.6.2394 on your computer. Continue? [n/Y] Y  Enter OS user [way4]  Enter OS group [way4]  Where do you want to install WAY4ApplicationServer? [/home/way4]  Installing WAY4ApplicationServer...  Check passed  SilentMode = 0  WAY4 Application Server 1.6: system check.  [WARN] TotalSwap value 8257532 is less than 8388608  [WARN] kernel.sem[2] value 32000 is less than 256000  [WARN] kernel.sem[4] value 128 is less than 1024  [WARN] net.ipv4.ip\_local\_port\_range[2] value 60999 is less than 65000  [WARN] SELinux should be disabled. Set SELINUX=disabled in /etc/selinux/config and reboot server.  Found total 5 warning(s). Please check documentation.  child process exited abnormally. Continue? (y/N)  y  Debugging is turned on  Debug output is being saved to a debug log file  Debug log file is /home/way4/WAY4ApplicationServer-standard-setup-2018-12-01\_10-53-53.log  Type: New installation.  Installing appserver-ant-1.6.2394.zip ...  Installing appserver-apache-rhel7-x64-2.2-1.6.460-dist.zip ...  Installing appserver-apache-rhel7-x64-2.4-1.6.460-dist.zip ...  Installing appserver-apache-user-conf-1.6.460.zip ...  Installing appserver-certs-1.6.2394.zip ...  Installing appserver-docs-singlenode-1.6.2394.zip ...  Installing appserver-installer-1.6.2394-linux-x64.zip ...  Skipping: appserver-installer-1.6.2394-linux-x64.zip  Installing appserver-jdk-linux-x64-1.6.86-dist.zip ...  Installing appserver-legacy-linux-x64-1.6.2394.zip ...  Installing appserver-mod-security-crs-1.0.151.zip ...  Installing appserver-startup-1.6.2394.zip ...  Installing appserver-startup-common-1.6.2394.zip ...  Installing appserver-sysapps-standard-1.6.2394.zip ...  Installing appserver-system-conf-1.6.2394.zip ...  Installing appserver-system-lib-1.6.2394.zip ...  Installing appserver-tomcat-1.6.2394.zip ...  Installing appserver-user-conf-1.6.2394.zip ...  Installing appserver-version-1.6.2394.zip ...  Setting permissions ...  Applying executables ...  Registering ...  Invoking appsd/sys apps install...  Property file with AS installation path was created  Linking JDK ...  INIT\_FILE=/lib/systemd/system/WAY4ApplicationServer.service  Created symlink from /etc/systemd/system/default.target.wants/WAY4ApplicationServer.service to /usr/lib/systemd/system/WAY4ApplicationServer.service.  Appserver Service is installed.  Solution = standard  WAY4 Application Server Installer/Upgrader  Configuration update ...  Processing applications...  System Applications Install/Upgrade ...  Processing logagent with version 2.0.909 from file /home/way4/appserver/temp/sysapps/logagent-2.0.909.zip  Type: new installation  Installing logagent  Creinst output: [stdout] Application instance creator  Adding application 'logagent' ...  Application has been successfully added.  Processing m2\_web\_console with version 1.0.1969 from file /home/way4/appserver/temp/sysapps/m2\_web\_console-1.0.1969.war  Type: new installation  []  Building map of used ports com.openwaygroup.util.ant.appcontainer.FindPortsAdapter  Building map of used ports - finished. Checking busy ports com.openwaygroup.util.ant.appcontainer.FindPortsAdapter  Found free port: 9090  Installing m2\_web\_console on port 9090 ...  Creinst output: [stdout] Application instance creator  Adding application 'm2\_web\_console'...  Used ports (HTTP, Server, Redirect, AJP): 9090, 9091, 9092, 9093  You can change Web Application Parameters with security\_conf utility.  Application has been successfully added.  Processing web\_console with version 1.6.2394 from file /home/way4/appserver/temp/sysapps/web\_console-1.6.2394.war  Type: new installation  [/home/way4/appserver/applications/m2\_web\_console/conf/server.xml]  Building map of used ports com.openwaygroup.util.ant.appcontainer.FindPortsAdapter  Processing file /home/way4/appserver/applications/m2\_web\_console/conf/server.xml  Building map of used ports - finished. Checking busy ports com.openwaygroup.util.ant.appcontainer.FindPortsAdapter  Found free port: 9094  Installing web\_console on port 9094 ...  Creinst output: [stdout] Application instance creator  Adding application 'web\_console'...  Used ports (HTTP, Server, Redirect, AJP): 9094, 9095, 9096, 9097  You can change Web Application Parameters with security\_conf utility.  Application has been successfully added.  Processing monitoring\_ui with version 1.0.1273 from file /home/way4/appserver/temp/sysapps/monitoring\_ui-1.0.1273.war  Type: new installation  [/home/way4/appserver/applications/web\_console/conf/server.xml, /home/way4/appserver/applications/m2\_web\_console/conf/server.xml]  Building map of used ports com.openwaygroup.util.ant.appcontainer.FindPortsAdapter  Processing file /home/way4/appserver/applications/web\_console/conf/server.xml  Processing file /home/way4/appserver/applications/m2\_web\_console/conf/server.xml  Building map of used ports - finished. Checking busy ports com.openwaygroup.util.ant.appcontainer.FindPortsAdapter  Found free port: 9098  Installing monitoring\_ui on port 9098 ...  Creinst output: [stdout] Application instance creator  Adding application 'monitoring\_ui'...  Used ports (HTTP, Server, Redirect, AJP): 9098, 9099, 9100, 9101  You can change Web Application Parameters with security\_conf utility.  Application has been successfully added.  Processing monitoring with version 1.0.1273 from file /home/way4/appserver/temp/sysapps/monitoring-1.0.1273.zip  Type: new installation  Installing monitoring  Creinst output: [stdout] Application instance creator  Adding application 'monitoring' ...  Application has been successfully added.  WAY4 Application Server Installer/Upgrader finished  User: way4  Group: way4  Diag script executed. Exit code 0 Output Usage: /home/way4/appserver/bin/diag [type=OS|java\_app] [app\_name=application instance name]  by default type=OS  Executing diag script  Diag script executed successfully. Result saved in /home/way4/appserver/logs/diag-20181201-105431.301.log\* files.  Would you like to configure Apache Web Server? [n/Y] Y  Would you like to start Apache Web Server automatically? [n/Y] Y  Apache Web Server instruction, how to change HTTP and HTTPS ports to standard values described in docs/english/Administering\_WAY4\_Application\_Server.pdf  Would you like to configure logagent? [n/Y] Y  Input site\_name (for logagent) [bank1-prod]  Input server\_address (for logagent) [127.0.0.1]  Input port\_number (for logagent) [19096]  Logagent configuration was saved.  Would you like to configure Web Console? [n/Y] y  Do you want to use Modern Web Console (m2\_web\_console) [Y] instead of Classic  Web Console [n]? [n/Y] y  web\_console autostart is no.  m2\_web\_console autostart is yes.  Please enter a new password for user 'admin' (application 'm2\_web\_console') (7  characters minimum. Both numeric and alphabetic characters should be present):  Repeat password for user admin in Web Console:  Web Console application (m2\_web\_console) was configured on port 9090.  Would you like to launch WAY4ApplicationServer? [n/Y] y  Appserver Launch: ..  /home/way4/bin/appsd: Application Server has been started.  Appserver Launch RC: 0  Installation complete. |



Note: The appserver has the Java 8.0\_72 in it, and this version of Java has a bug related to PKCS11:  
<http://bugs.java.com/view_bug.do?bug_id=JDK-8149017>

So we need to downgrade java version for appserver in ACS Server. The following steps is needed to downgrade java version to Java 8.0\_51:

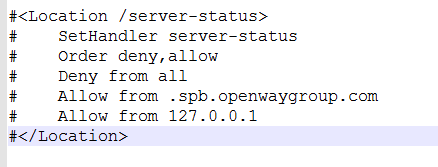
* Go to folder */home/way4/appserver/jdk*, rename folder 1.8 to 1.8\_72
* Copy java version 8.0\_51 to folder */home/way4/appserver/jdk*, rename to 1.8
* Make sure all files in *bin* and *jre/bin* folder have appropriate owner and rights
* Reboot server, check file container.log in folder */home/way4/appserver/logs*, make sure that java version is 1.8.0\_51





Disable server status:

Edit file /home/way4test/appserver/apache/conf/extra/httpd-info.conf



# Instal ACS, Demobank, Egateway

## Install ACS

Login under way4, and go to bin folder of the application server

/home/way4/appserver/bin

Key in the following command to install way4acs

Notes: In your production environment, you can change the name of the ACS application to the name you wish such as ocbacs. You just replace the app\_name= ocbacs. However, the port should be the unchanged.

./creinst app\_name=**way4acs** file=/opt/setup/way4acs/webapps/way4acs-1.0.149-675.war http\_port=**8060**

|  |
| --- |
| /home/way4/appserver/bin |
| [way4@DC-WAY4-3DACS ~]$ cd /home/way4/appserver/bin  [way4@DC-WAY4-3DACS bin]$ ./creinst app\_name=way4acs file=/opt/setup/way4acs/webapps/way4acs-1.0.149-675.war http\_port=8060  Application instance creator  Adding application 'way4acs'...  Used ports (HTTP, Server, Redirect, AJP): 8060, 8061, 8062, 8063  You can change Web Application Parameters with security\_conf utility.  Application has been successfully added. |
|  |



## Install DEMOBANK

Login under way4, and go to bin folder of the application server

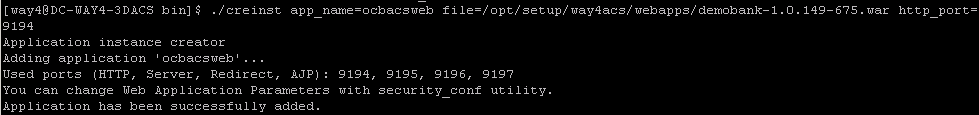
/home/way4/appserver/bin

Key in the following command to install way4acs

Notes: In your production environment, you can change the name of the Demobank application to the name you wish such as ocbacsweb. You just replace the app\_name= ocbacssweb. However, the port should be the unchanged.

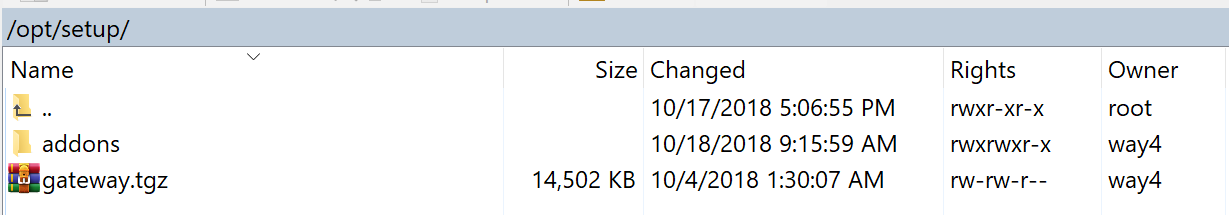
./creinst app\_name=ocbacsweb file=/opt/setup/way4acs/webapps/demobank-1.0.149-675.war http\_port=**9194**

|  |
| --- |
| [way4@DC-WAY4-3DACS bin]$ ./creinst app\_name=ocbacsweb file=/opt/setup/way4acs/webapps/demobank-1.0.149-675.war http\_port=9194  Application instance creator  Adding application 'ocbacsweb'...  Used ports (HTTP, Server, Redirect, AJP): 9194, 9195, 9196, 9197  You can change Web Application Parameters with security\_conf utility.  Application has been successfully added. |



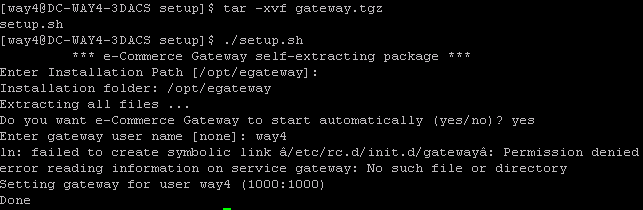
## Install EGATEWAY (Remember to change owner of bin directory)

Copy the installation package to the /opt/setup/



Go to the installation package and run the following command to extract the file

tar -xvf gateway.tgz

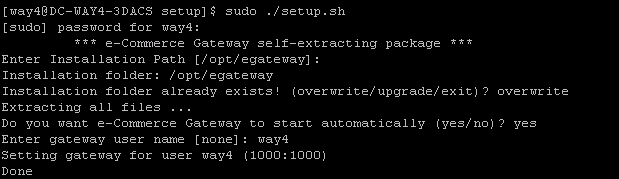


run tar to extract the file

|  |
| --- |
| Extract .tar file |
| [way4@DC-WAY4-3DACS setup]$ tar -xvf gateway.tgz  setup.sh  [way4@DC-WAY4-3DACS setup]$ ./setup.sh  \*\*\* e-Commerce Gateway self-extracting package \*\*\*  Enter Installation Path [/opt/egateway]:  Installation folder: /opt/egateway  Extracting all files ...  Do you want e-Commerce Gateway to start automatically (yes/no)? yes  Enter gateway user name [none]: way4  ln: failed to create symbolic link â/etc/rc.d/init.d/gatewayâ: Permission denied  error reading information on service gateway: No such file or directory  Setting gateway for user way4 (1000:1000)  Done |

Enter user name = way4 when you are prompted to key in user as the following picture

|  |
| --- |
| [way4@DC-WAY4-3DACS setup]$ sudo ./setup.sh  [sudo] password for way4:  \*\*\* e-Commerce Gateway self-extracting package \*\*\*  Enter Installation Path [/opt/egateway]:  Installation folder: /opt/egateway  Installation folder already exists! (overwrite/upgrade/exit)? overwrite  Extracting all files ...  Do you want e-Commerce Gateway to start automatically (yes/no)? yes  Enter gateway user name [none]: way4  Setting gateway for user way4 (1000:1000)  Done |



**Change the right of bin folder from root to way4**

go to the folder

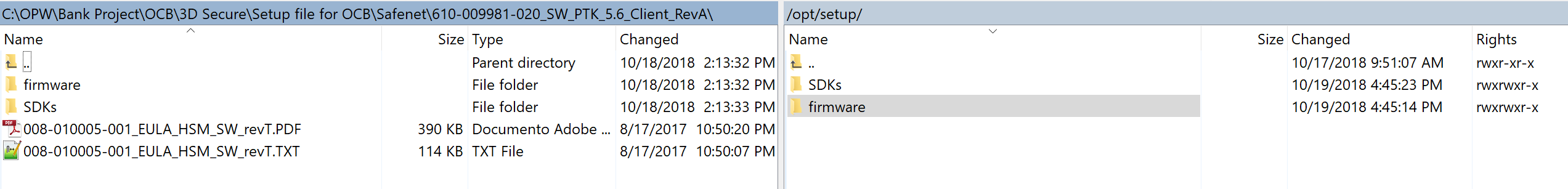
opt/egateway/

run the command sudo chown -R way4:way4 bin

# Install Eracom's libraries

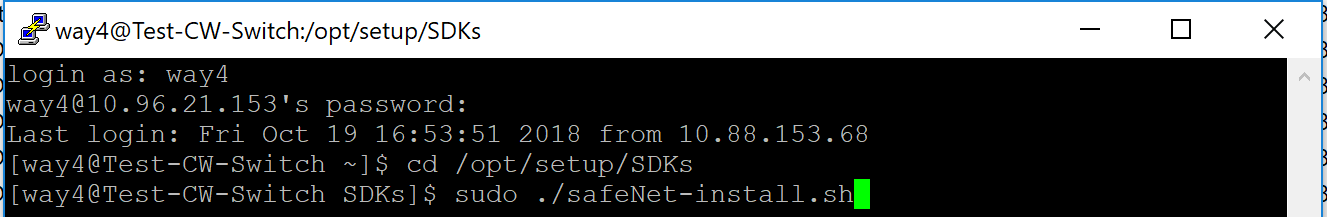
## Copy the following two packages to the server

* SDKs
* firmware

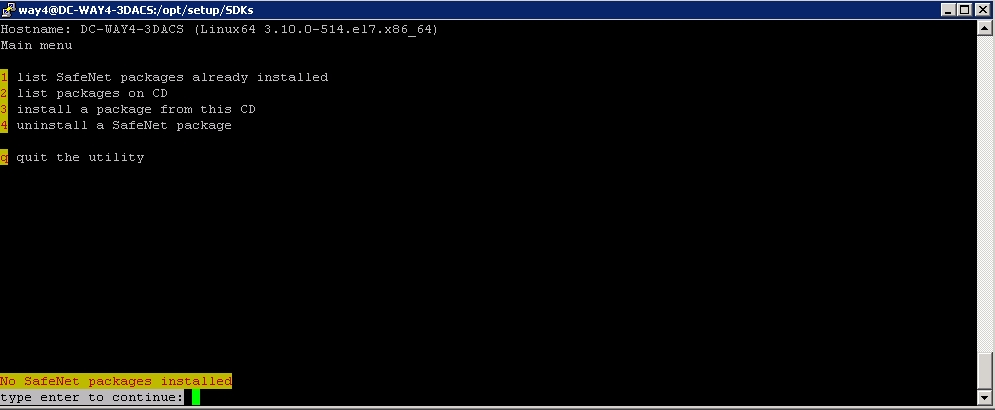


## Install Eracom's Libraries

CD /opt/setup/SDKs, run safeNet-install.sh

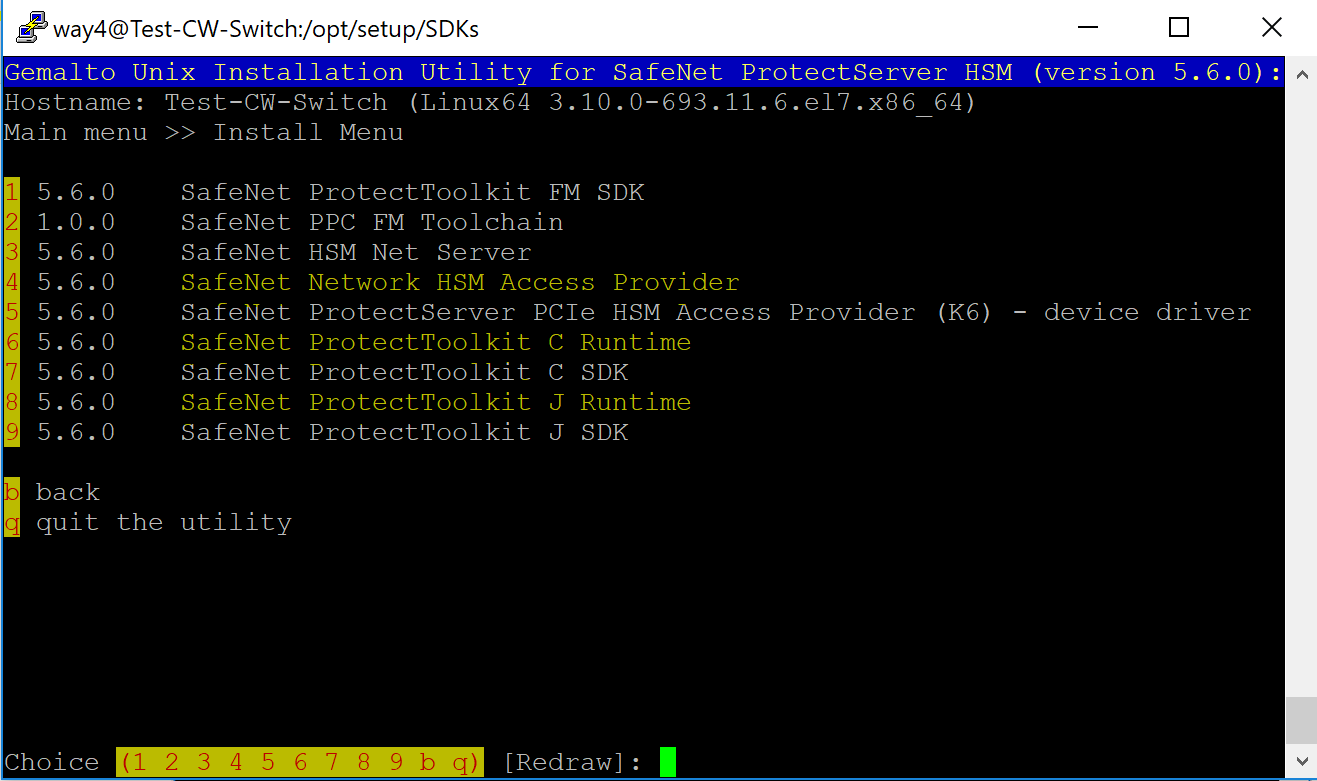


Choose 3 (install a package from thisCD)

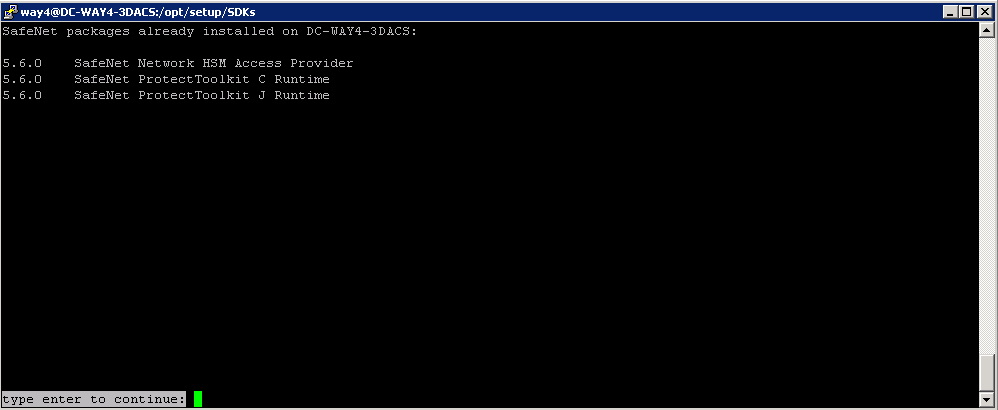


Choose following 3 packages: 4, 6, 8. Corresponding to SafeNet Network HSM Access Provider, SafeNet ProtectToolkit C Runtime, SafeNet ProtectToolkit J Runtime respectively

Enter each number per time to install



After install, you will get the following packages, check by choice 1 in install screen



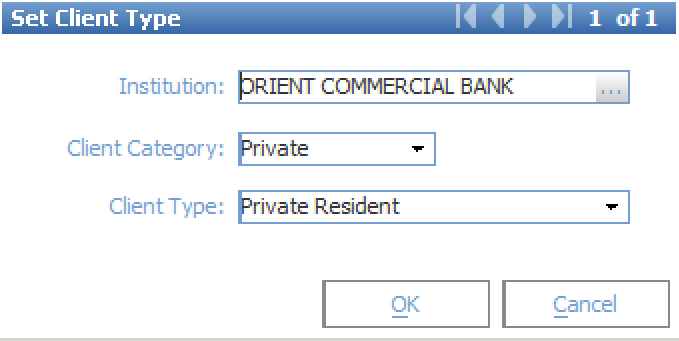
# Configure DBM

## Configure Authentication Module

### Configure Authentication Domains

Select Client type

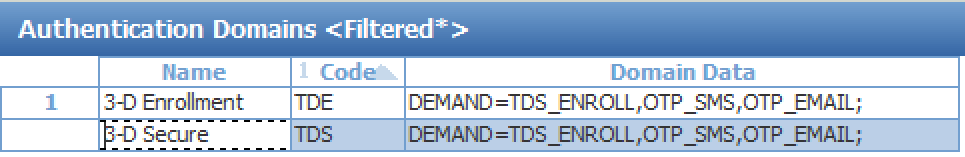
***Menu: OpenWay\Authentication Module\Set Client Type***



***Menu: OpenWay\Authentication Module\Authentication Domains***

Click [Ins] to insert a new row

Add the data as the following picture



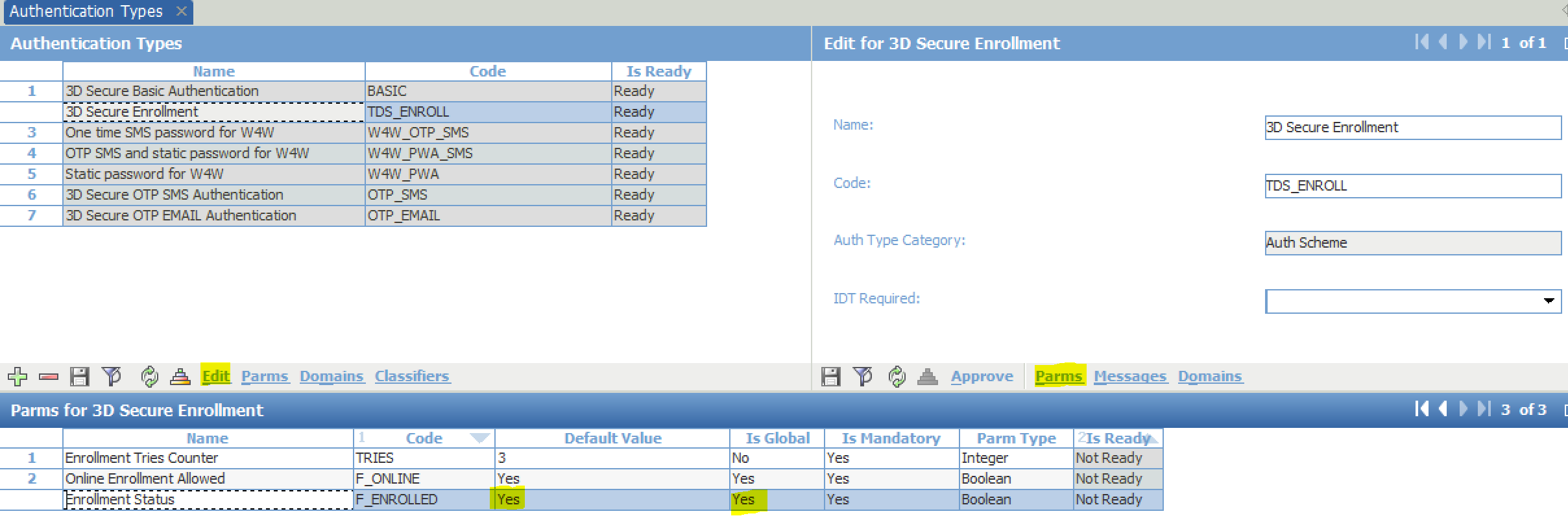
DEMAND=TDS\_ENROLL,OTP\_SMS,OTP\_EMAIL;

### Configure Authentication Type

***Menu :*** ***OpenWay\Authentication Module\Authentication Types***

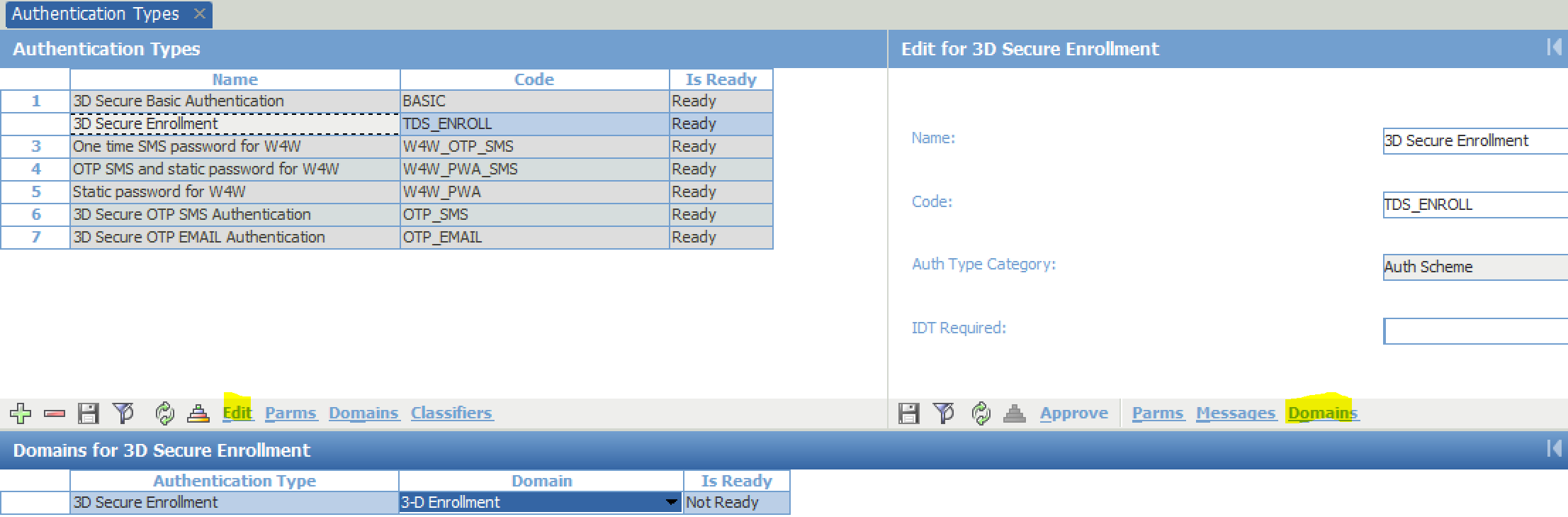
Edit existing 3D Secure Enrollment to auto enroll all cards

**Set value of field Enrollment Status to be “Yes” and field Is Global=”Yes”**



**ITD Require should be No**

**Set domain to 3-D Enrollment**



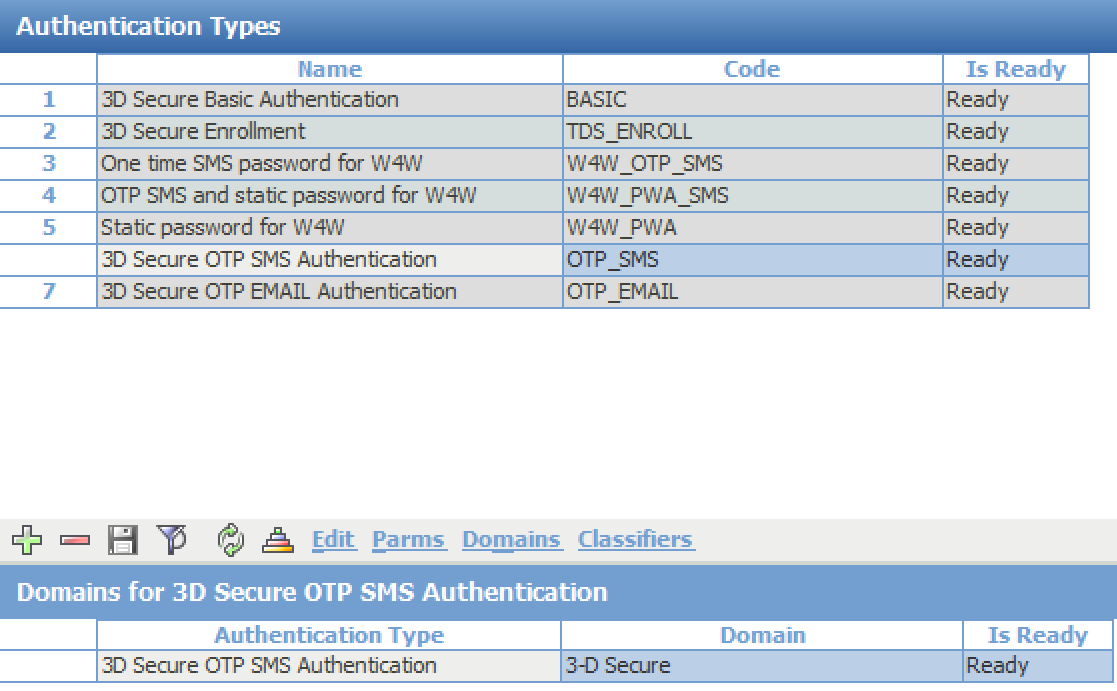
**Click [Approve] to finish**

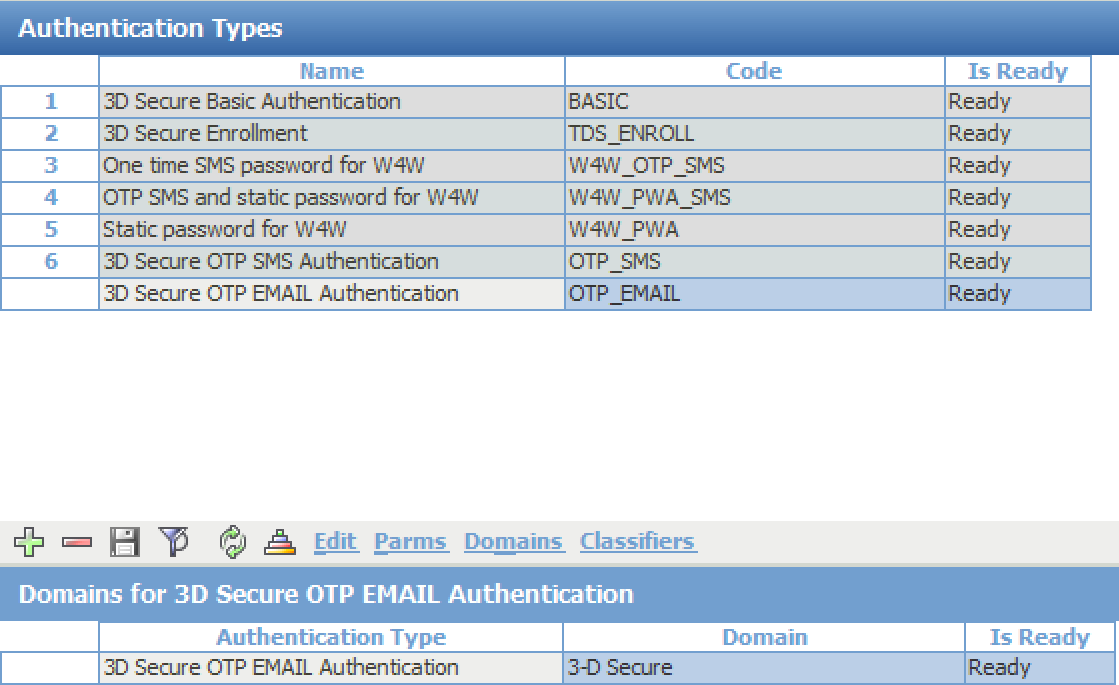
Add 2 Authentication Types as the following picture

* 3D Secure OTP SMS Authentication with Code: OTP\_SMS
* 3D Secure OTP EMAIL Authentication with Code: OTP\_EMAIL

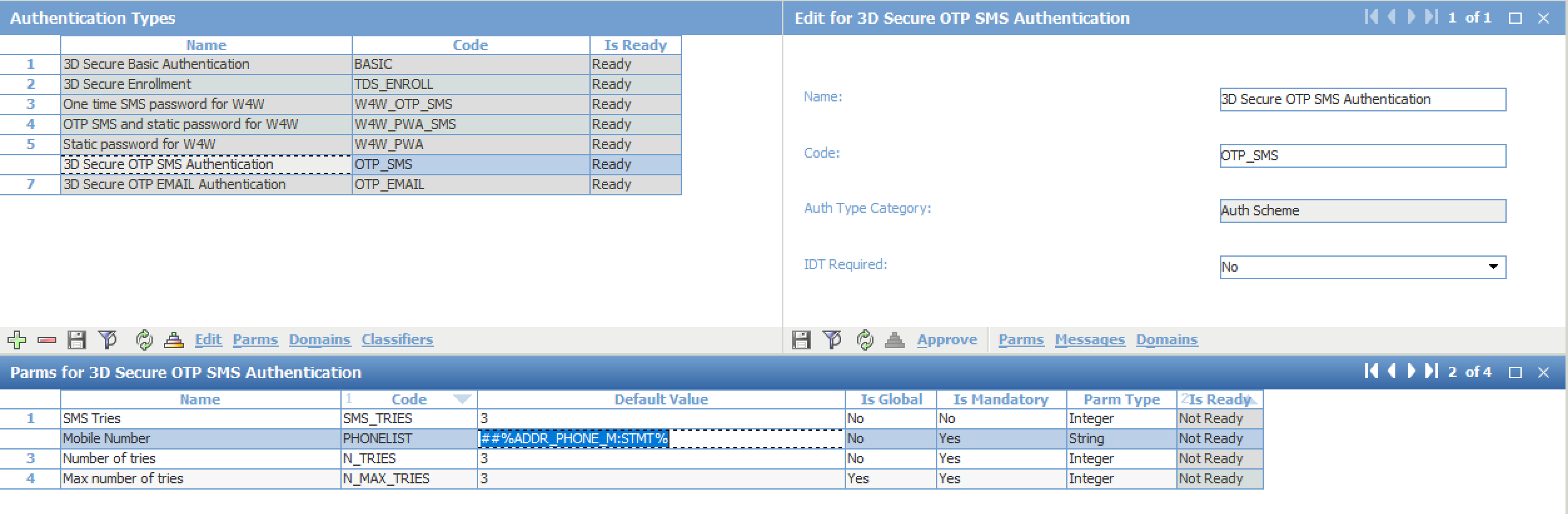
For each Authentication Type, add Domains

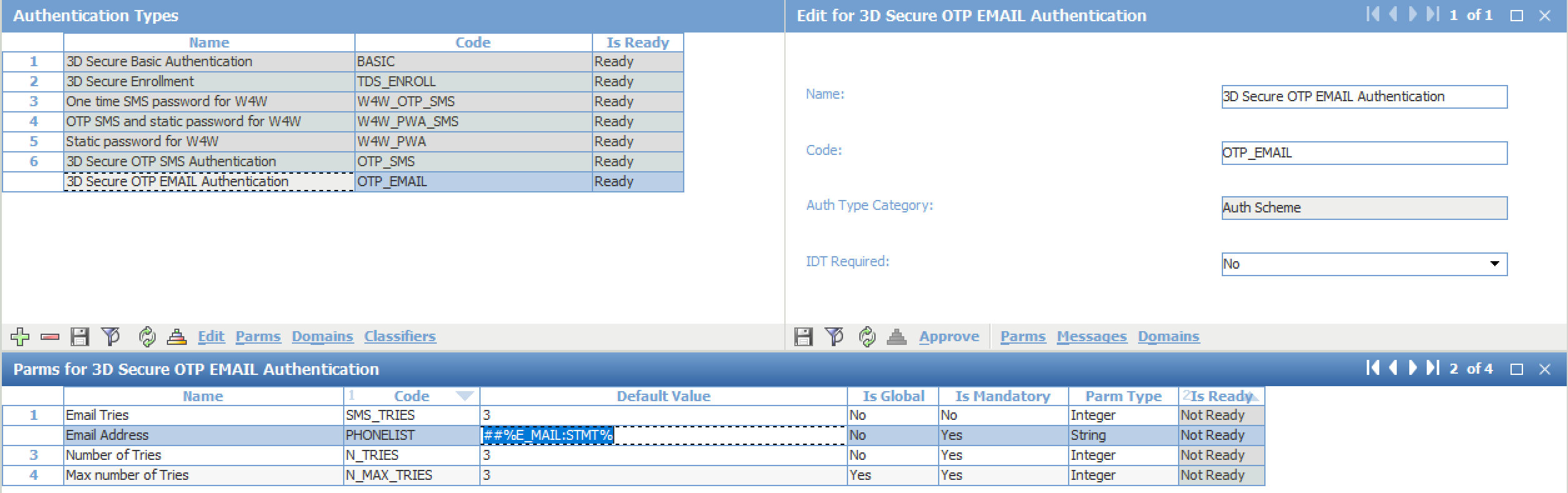
* 3-D Secure





For each Authentication Type, add Parms

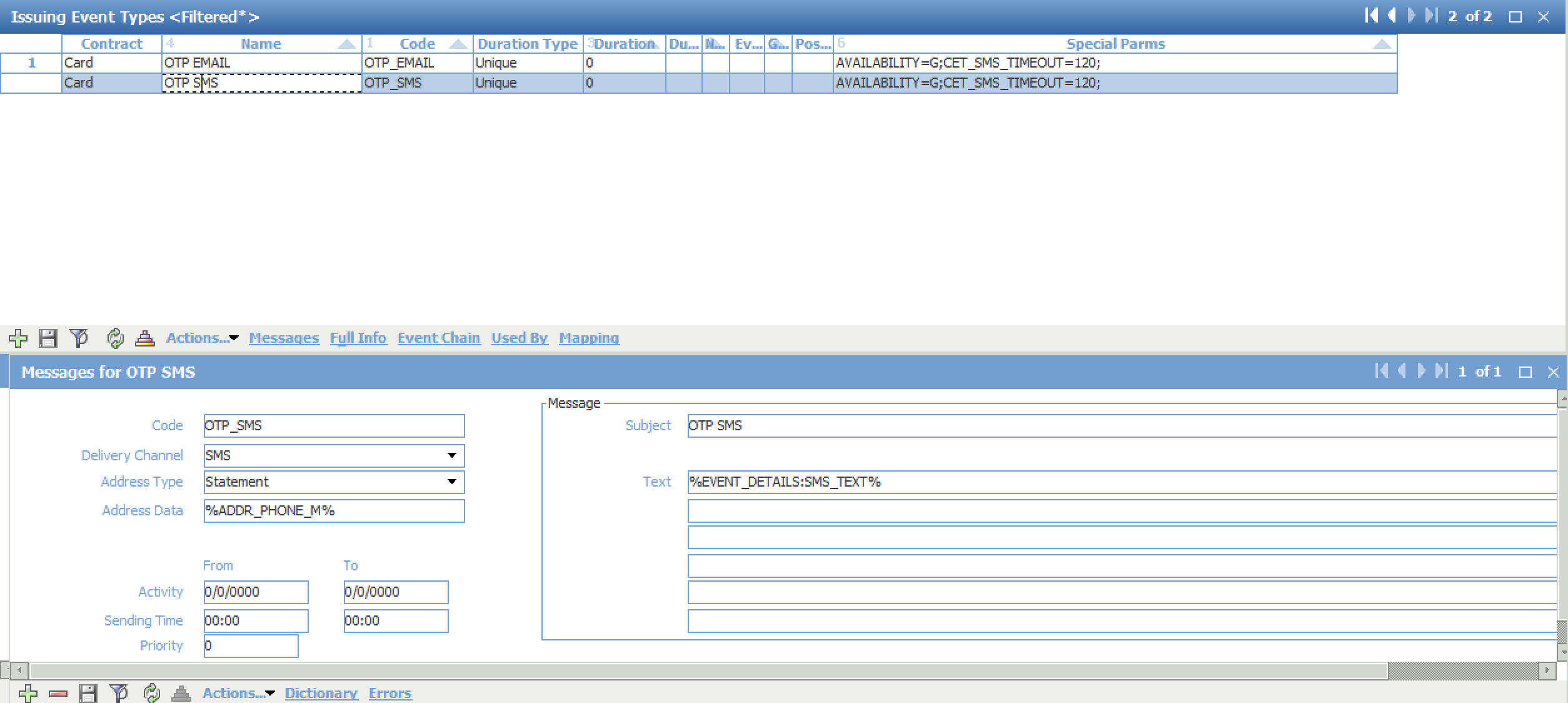




**Note: Email and Phone Number will be stored in Address of the client record which is linked to Card Contract with code STMT**

### Configure event to generate OTP\_SMS and OTP\_EMAIL

***Menu: ROOT\OpenWay\Full\Configuration Setup\Products\Issuing Private Products\Issuing Event Types***



Event Code: OTP\_SMS

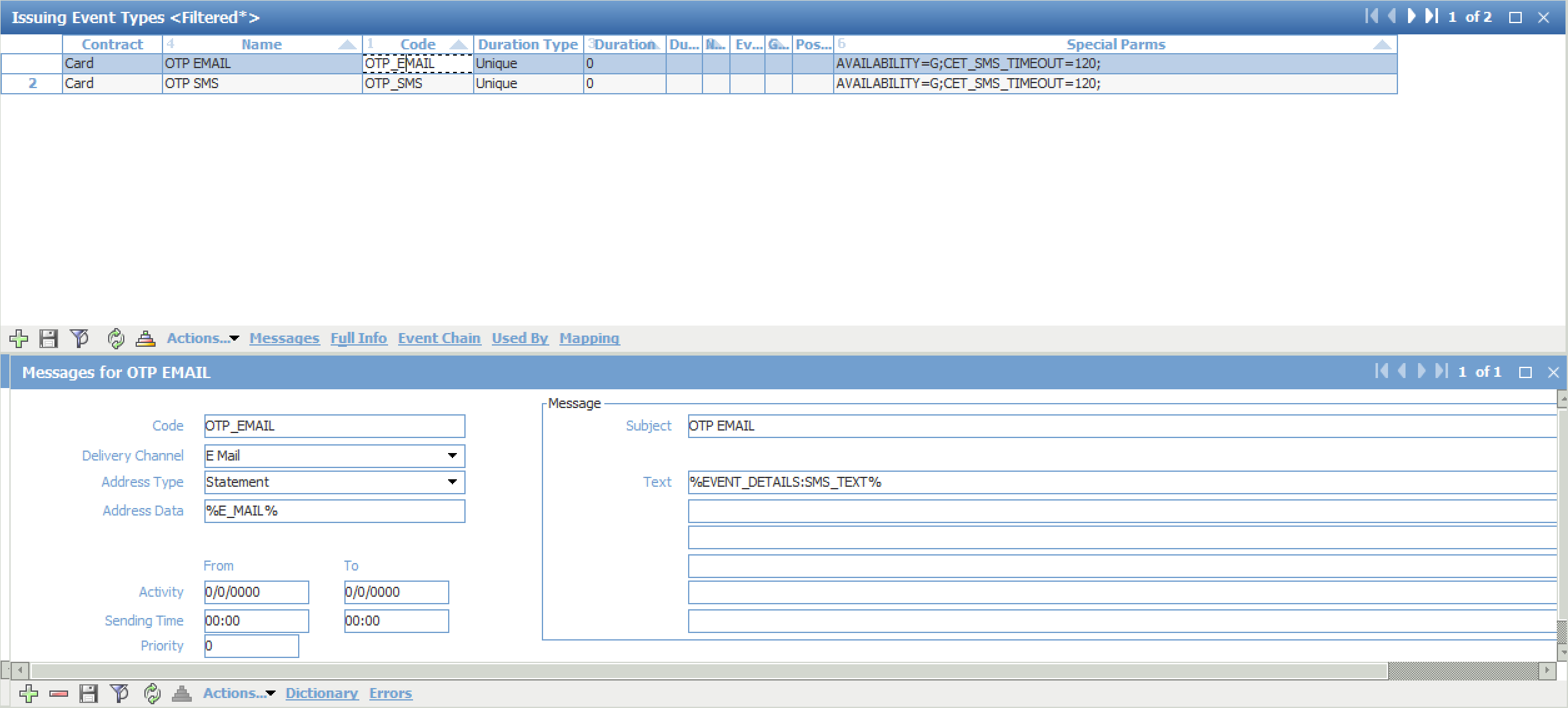
Delivery Channel: SMS

Address Type: Statement

Address Data: %ADDR\_PHONE\_M%

Text: %EVENT\_DETAILS:SMS\_TEXT%.

Special parm: AVAILABILITY=G;CET\_SMS\_TIMEOUT=120;



Event Code: OTP\_EMAIL

Delivery Channel: E Mail

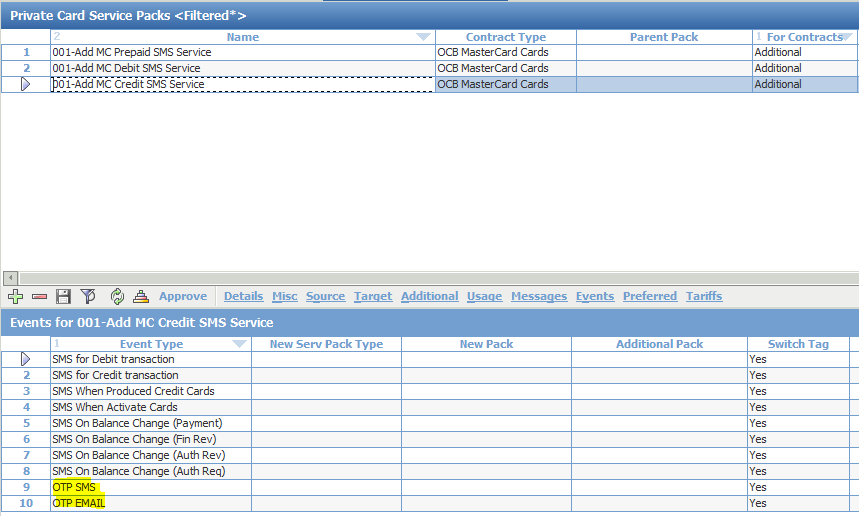
Address Type: Statement

Address Data: %E-MAIL%

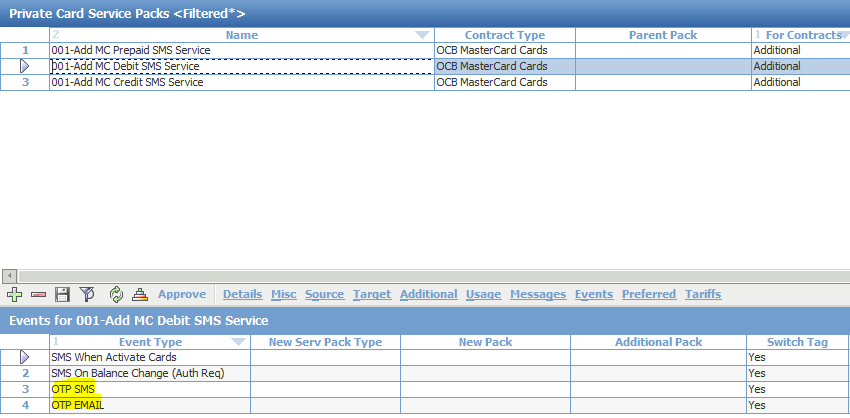
Text: %EVENT\_DETAILS:SMS\_TEXT%.

Special parm: AVAILABILITY=G;CET\_SMS\_TIMEOUT=120;

**Add event “OTP SMS” and “OTP EMAIL” to service packs (001-Add MC Credit SMS Service, 001-Add MC Prepaid SMS Service, 001-Add MC Debit SMS Service)**

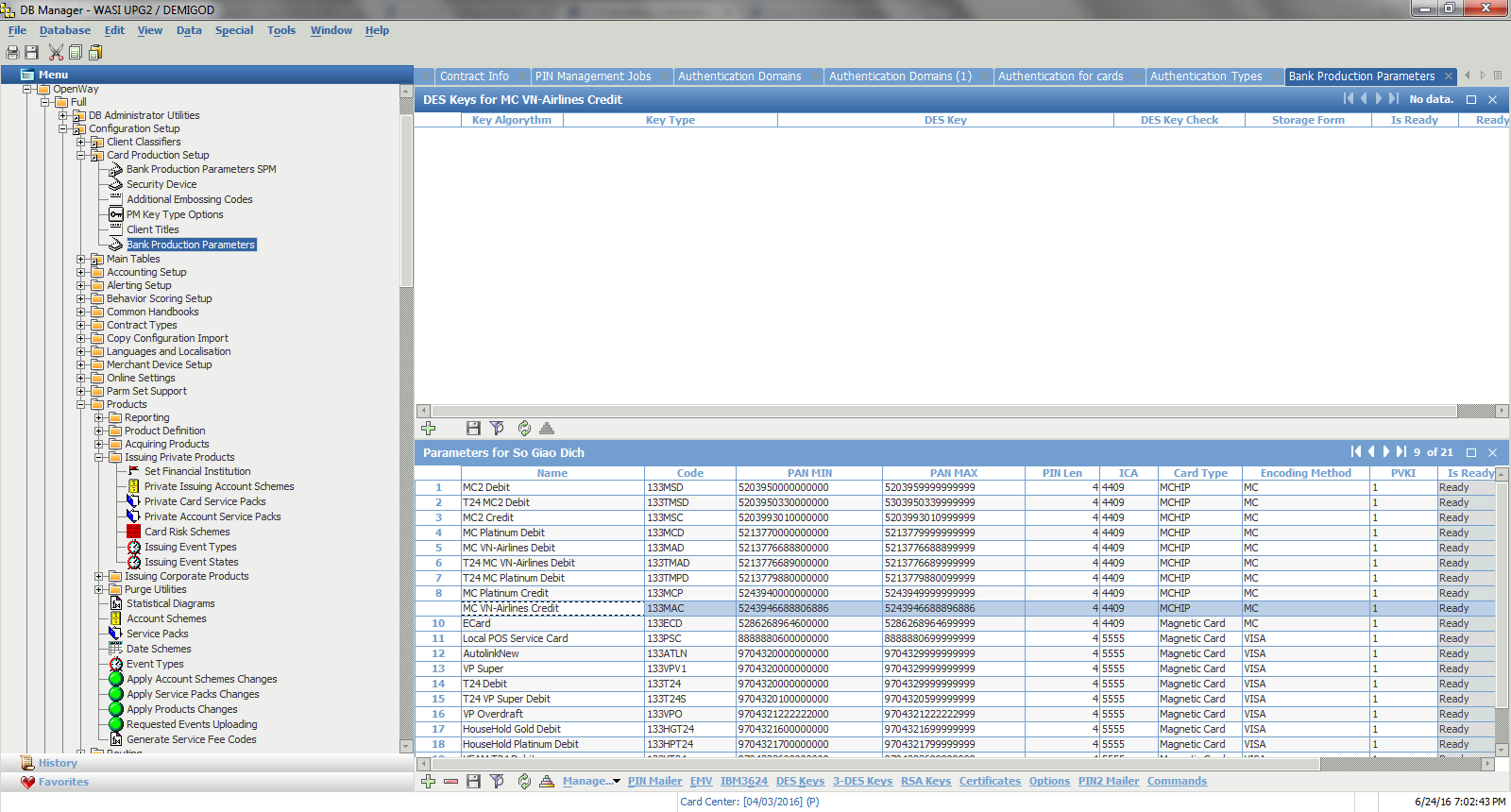




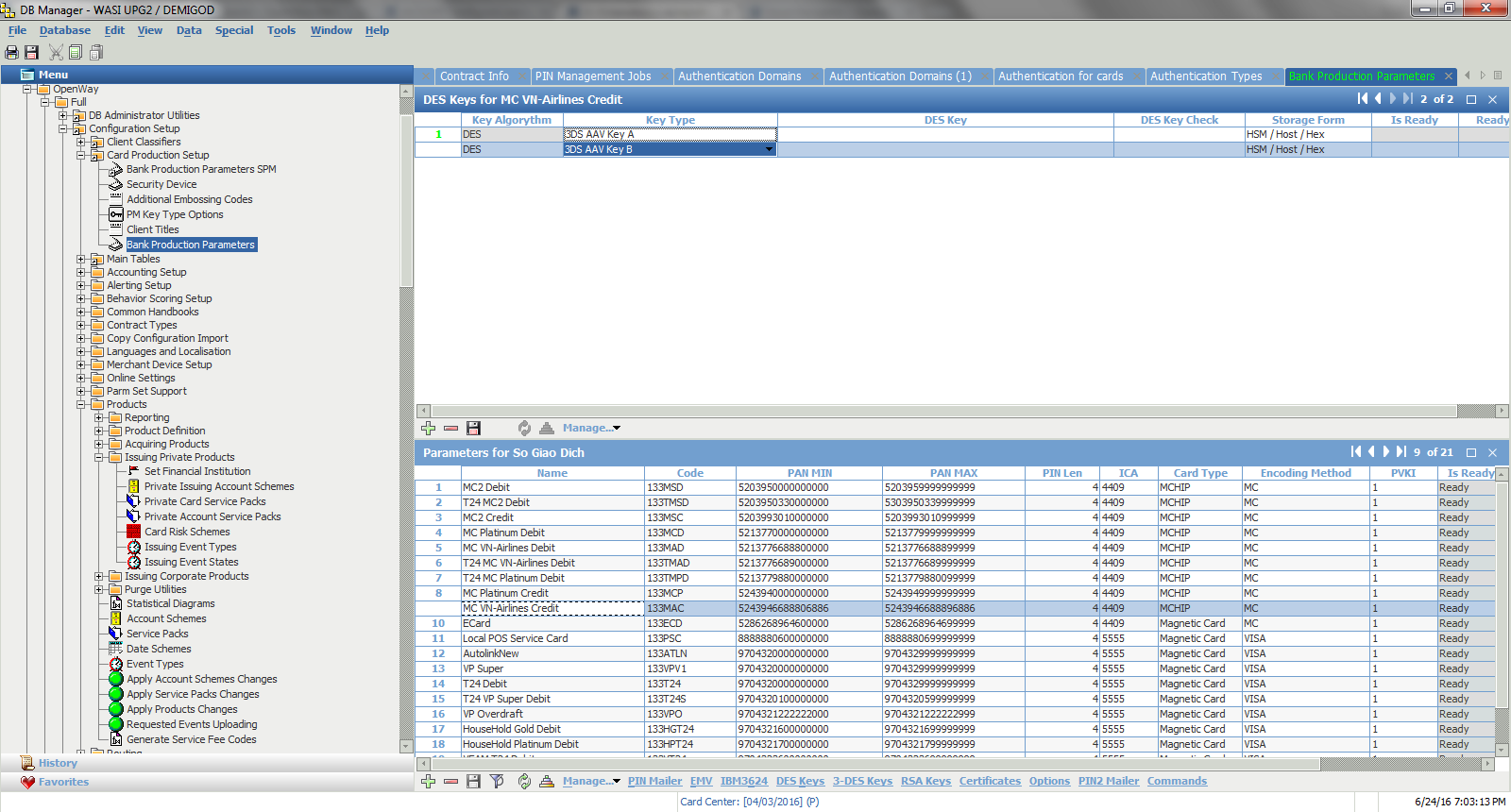


### Generate CAVVK 1 and 2

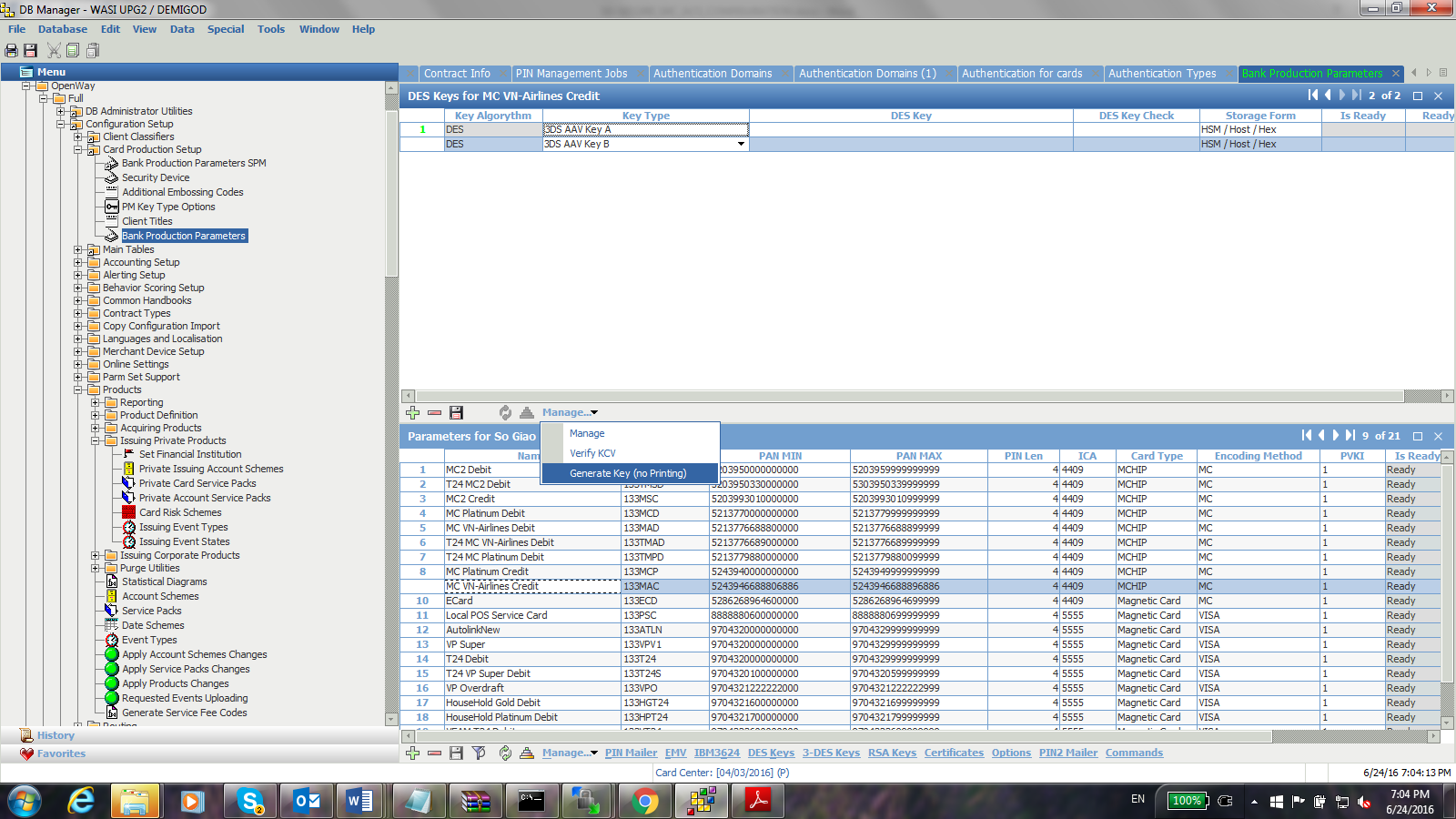
ROOT.OpenWay.Full.Configuration Setup.Card Production Setup.Bank Production Parameters

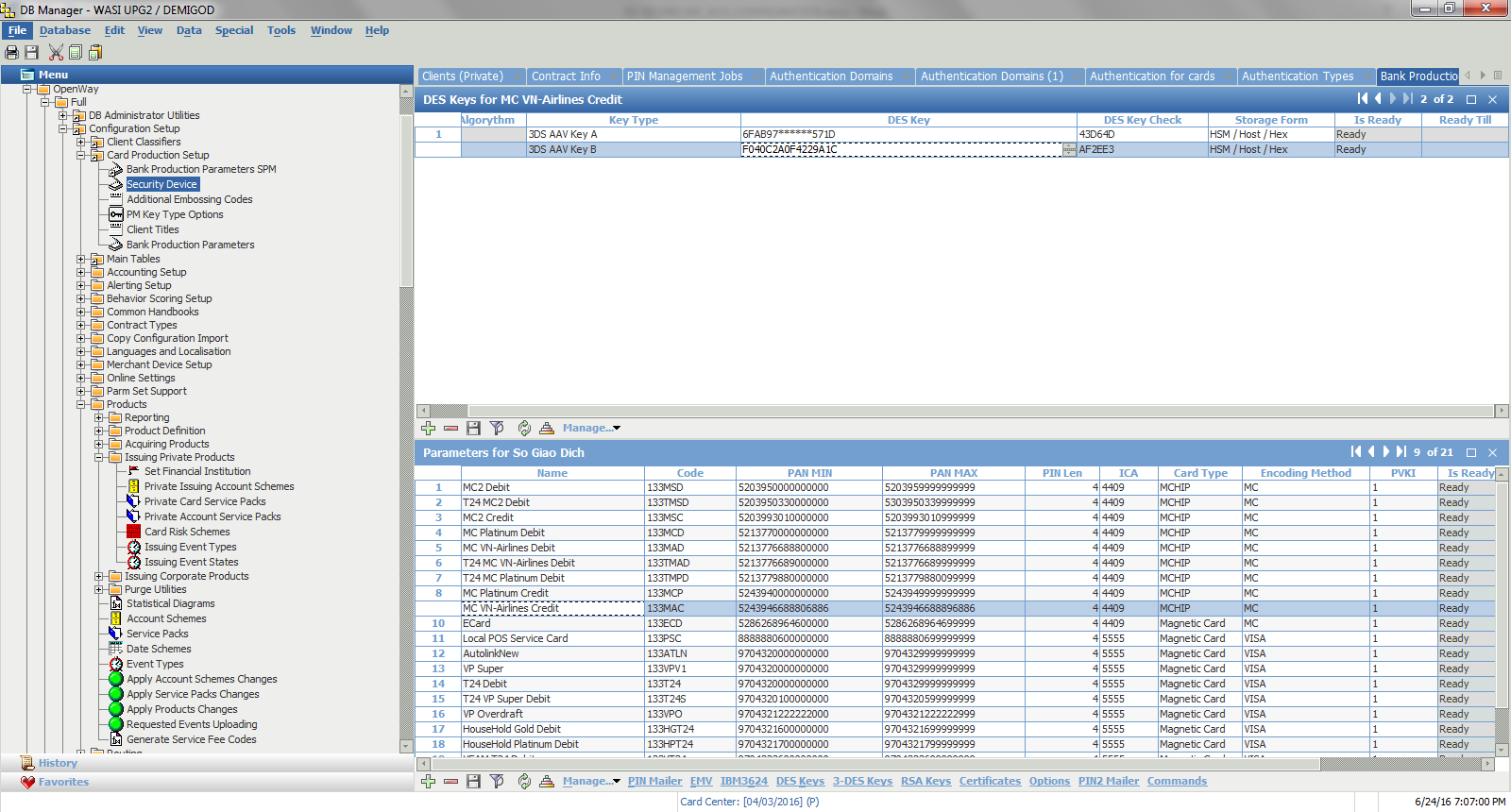


Click Ins to insert two CAVVK



Click Manage and choose Generate Key





New keys are generated and then choose Manage under parameter to verify

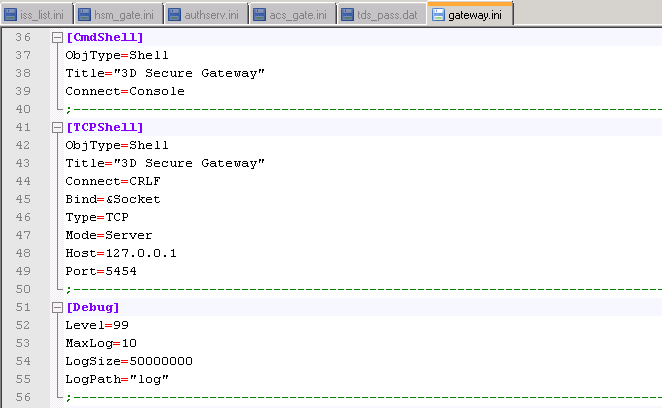
# Configure EGATEWAY

**Remember do all configuration under way4 user**

## Edit log level of Egateway

Specify logging parameters in /opt/egateway/gateway.ini

|  |
| --- |
| [Debug]  Level=99  MaxLog=10  ... |



## Configure netserv.ini

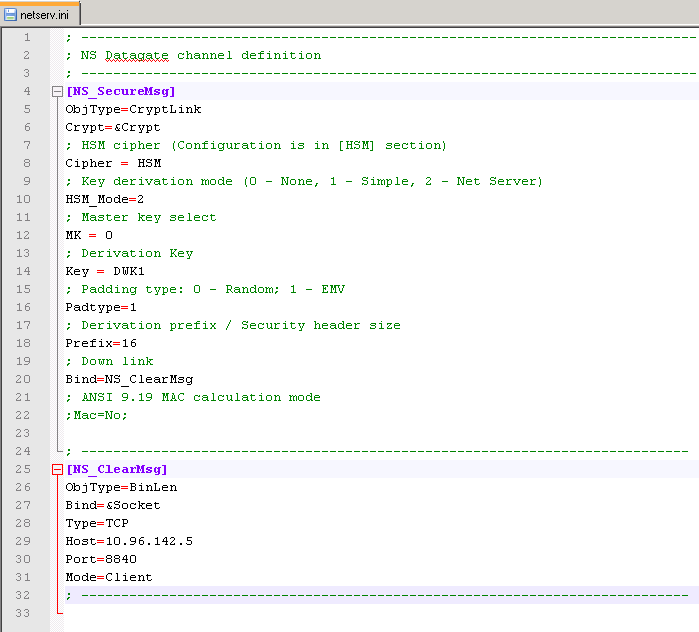
Specify Transaction Switch’s DATAGATE\_3DS channel connection parameters

Edit the following file

opt/egateway/datagate/netserv.ini:

Edit the Host, Port to the value of yours. In the testing environment Transaction Switch is deployed in 10.96.142.5. Port 8840 is open for connection with Egateway

|  |
| --- |
| [NS\_ClearMsg]  ObjType=BinLen  Bind=&Socket  Type=TCP  Host= 10.96.142.5  Port=8840  Mode=Client |



## Configure authserv.ini

Edit the following file

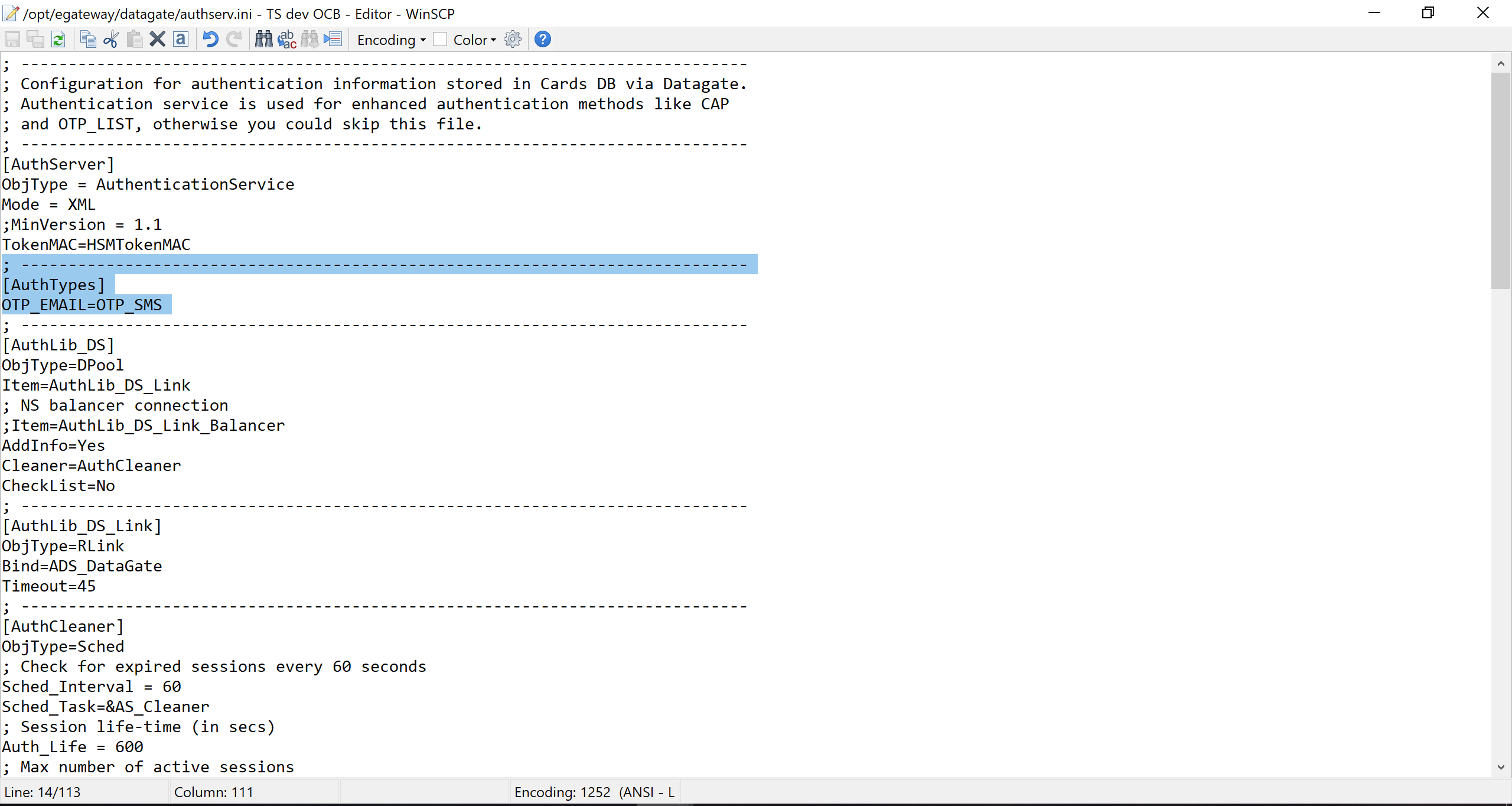
opt/egateway/datagate/authserv.ini

Add in

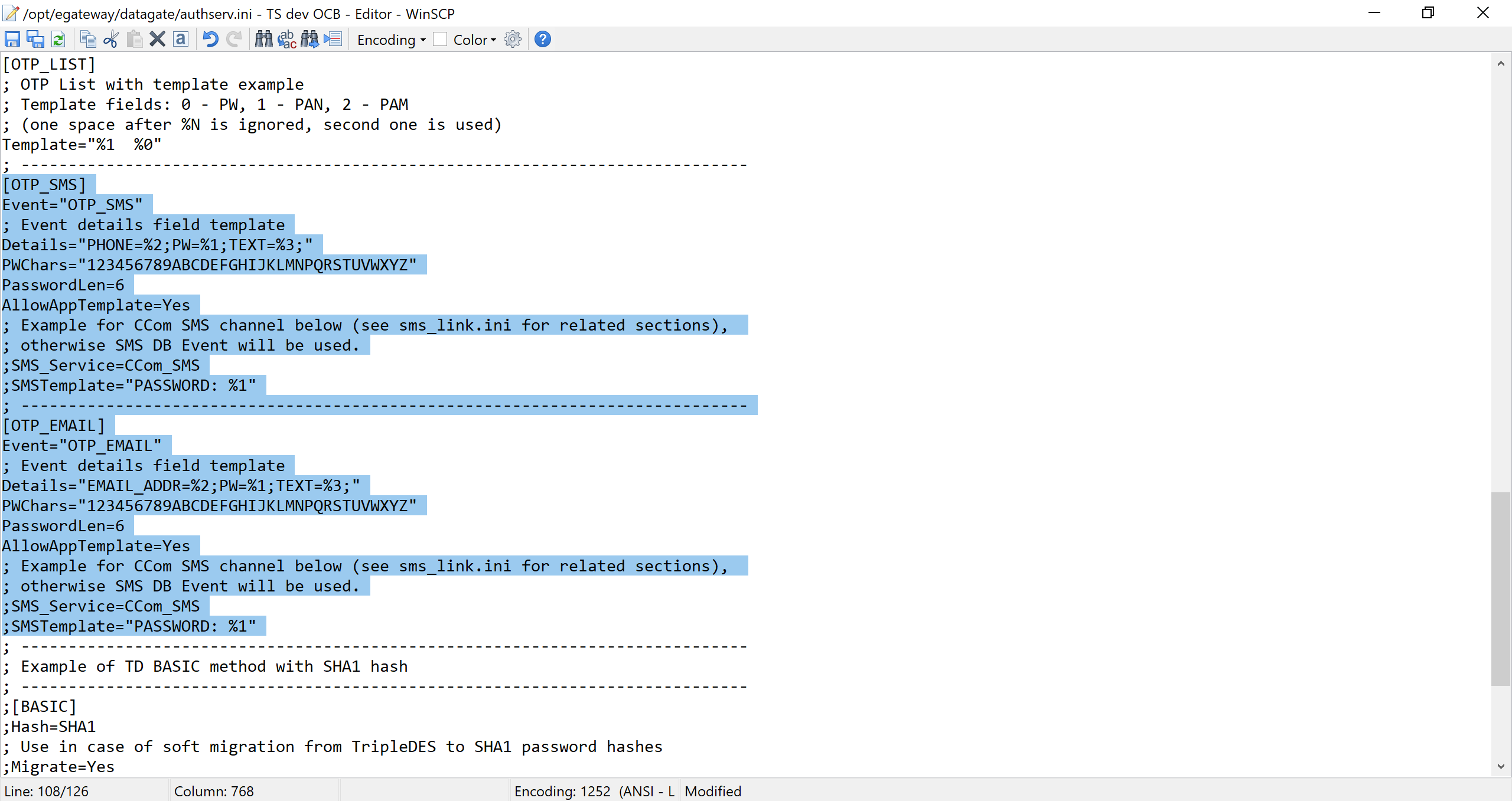
; -----------------------------------------------------------------------------

[AuthTypes]

OTP\_EMAIL=OTP\_SMS



And then edit



[OTP\_SMS]

Event="OTP\_SMS"

; Event details field template

Details="PHONE=%2;PW=%1;TEXT=%3;"

PWChars="123456789ABCDEFGHIJKLMNPQRSTUVWXYZ"

PasswordLen=6

AllowAppTemplate=Yes

; Example for CCom SMS channel below (see sms\_link.ini for related sections),

; otherwise SMS DB Event will be used.

;SMS\_Service=CCom\_SMS

;SMSTemplate="PASSWORD: %1"

; -----------------------------------------------------------------------------

[OTP\_EMAIL]

Event="OTP\_EMAIL"

; Event details field template

Details="EMAIL\_ADDR=%2;PW=%1;TEXT=%3;"

PWChars="123456789ABCDEFGHIJKLMNPQRSTUVWXYZ"

PasswordLen=6

AllowAppTemplate=Yes

; Example for CCom SMS channel below (see sms\_link.ini for related sections),

; otherwise SMS DB Event will be used.

;SMS\_Service=CCom\_SMS

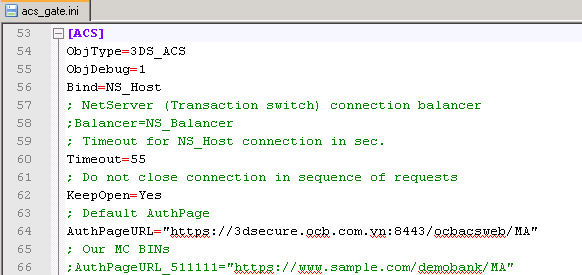
;SMSTemplate="PASSWORD: %1"

## Configure acs\_gate.ini

### Link to Authentication Page

Open the file opt/egateway/datagate/acs\_gate.ini.

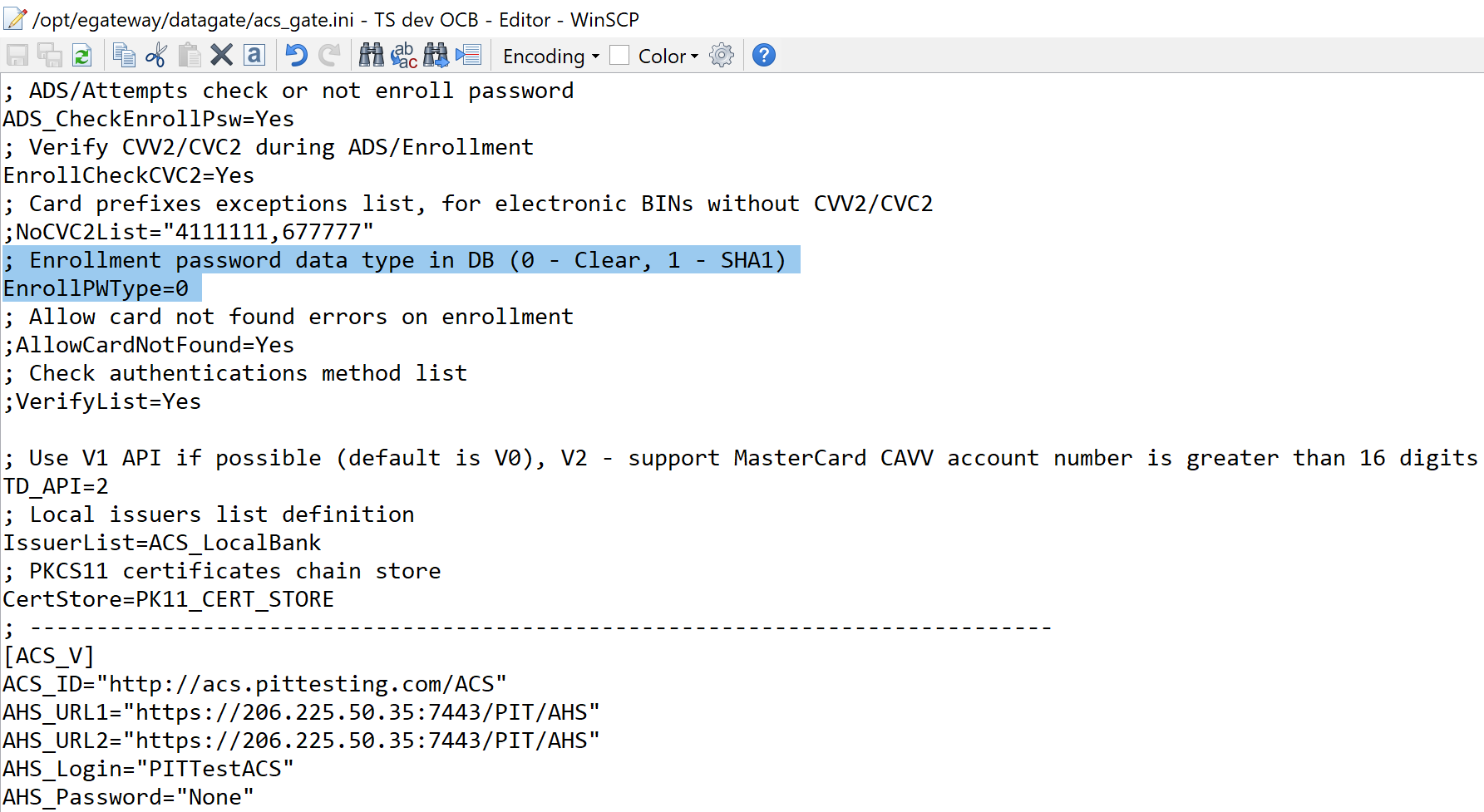
Go to [ACS] section and edit this section as the following



|  |
| --- |
| AuthPageURL=<https://3dsecure.ocb.com.vn:8443/ocbacsweb/MA> |

### Setup a non-hashed password for enrolment

Continue change the following parameter in the [ACS] section



|  |
| --- |
| ; Enrollment password data type in DB (0 - Clear, 1 - SHA1)  EnrollPWType=0 |

### Uncomment CertStore



### Configure the rest parameters

**ACS\_CHANNELS="E"**

**ACS\_CH\_NAMES="MC\_SecureCode”**

**AuthList = "OTP\_SMS,OTP\_EMAIL,BASIC"**

**[ACS\_E]**

**AHS\_URL1="https://mcahs.securecode.com:443"**

**AHS\_URL2="https://mcahs.securecode.com:443"**

**ACS\_ID="https://3dsecure.ocb.com.vn/way4acs/ve"**

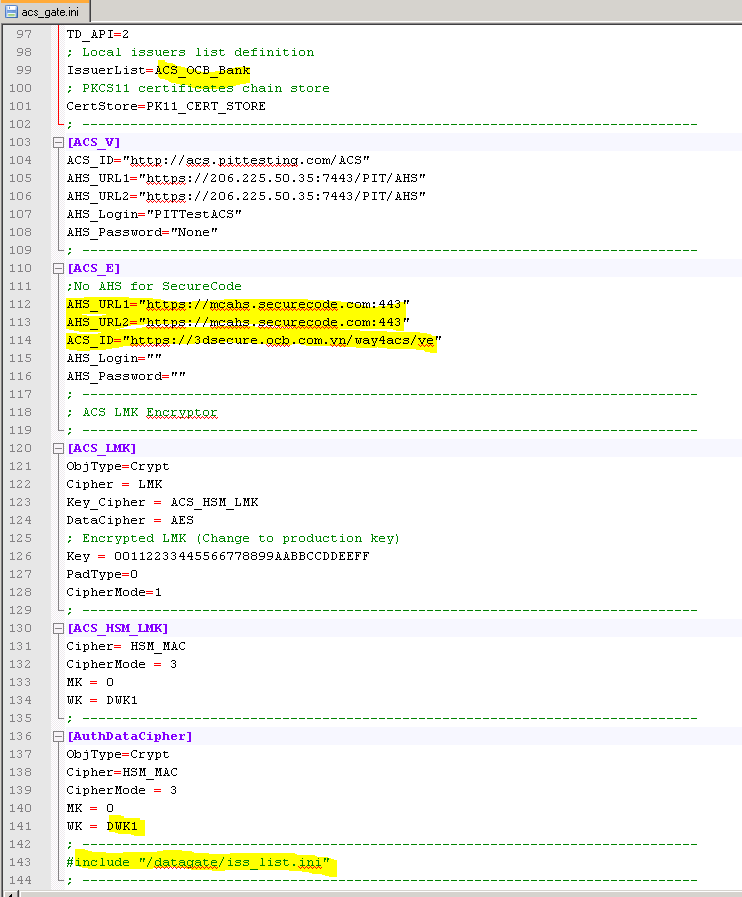
In the acs\_gate.ini IssuerList must be configured. There are two parameters: IssuerList, CertStore.

IssuerList: This parameter is linked to the iss\_list.ini file. See detail configuration of this file in the next section

CertStore: With the paremeter **CertStore=PK11\_CERT\_STORE**. It means that all certificates are stored in the ERACOM's HSM

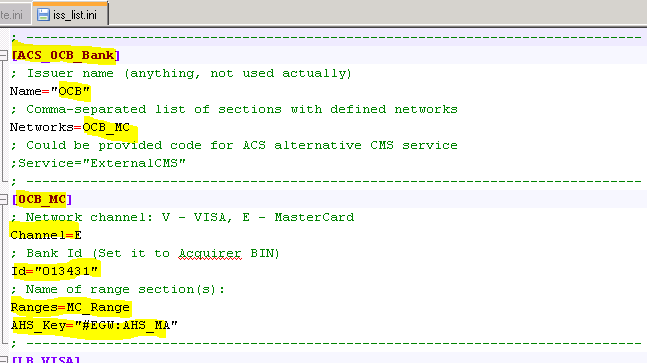
**Issuer List = ACS\_OCB\_BANK**

Addrow **#include "/datagate/iss\_list.ini”**

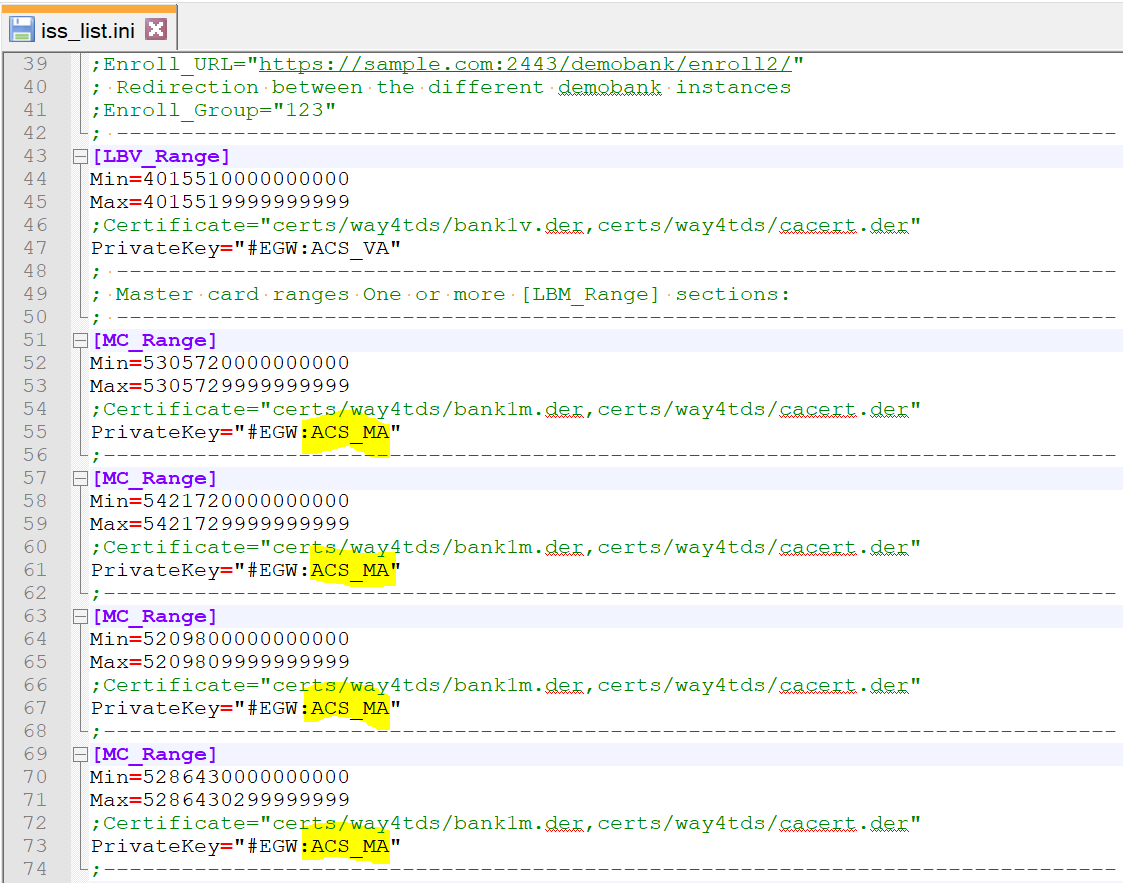


`

In the iss\_list.ini the ACS\_OCB\_BANK section must be configured.

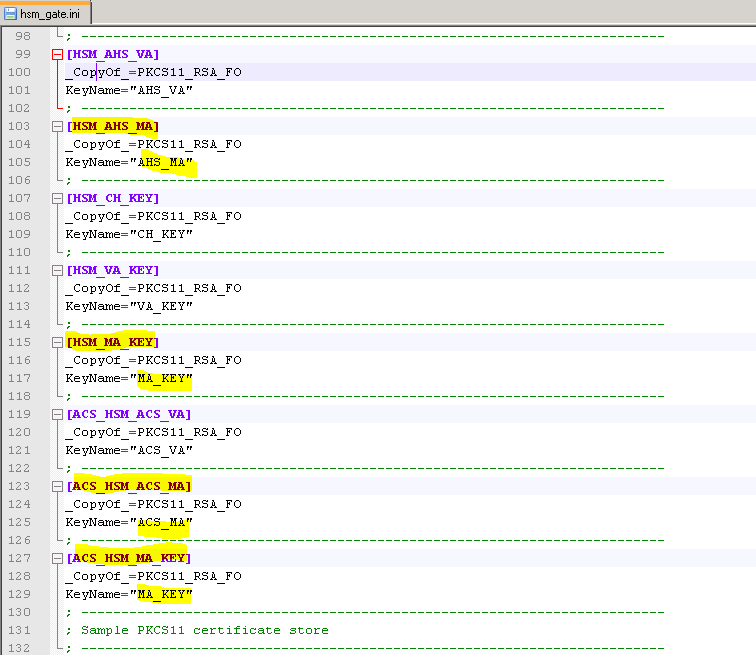


Configure [MC\_Range] add BIN Range for 3D, in Private Key have to set **#EGW:ACS\_MA**



## Configure hsm\_gate.ini

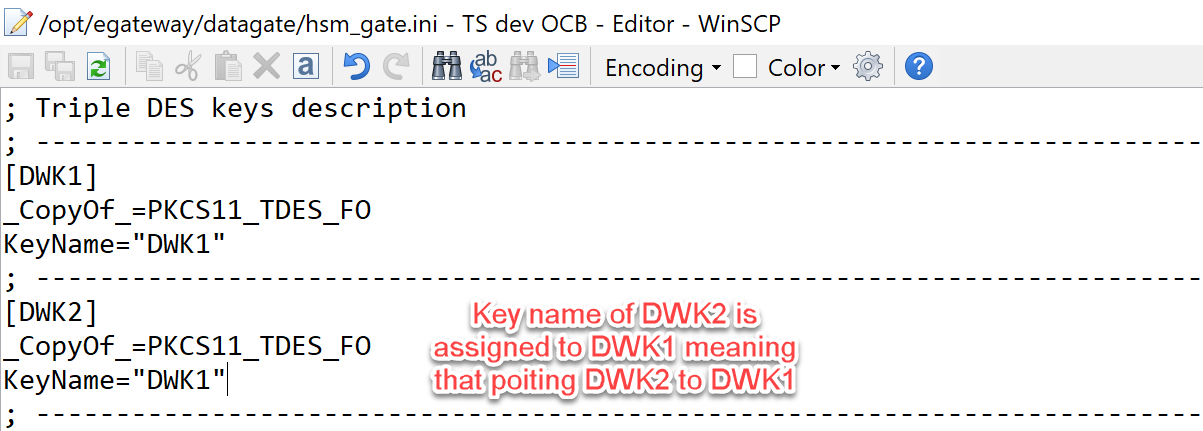
### Configure RSA key



### Configure DWK2 point to DWK1

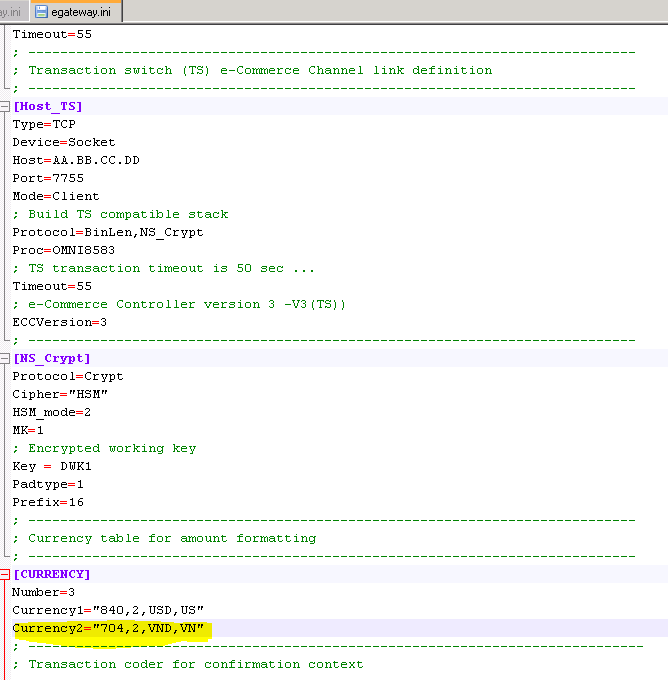
In the standard document, we need to create two keys DWK1, DWK2 and place those keys in the E-COMMERCE and DATAGATE respectively. However, we should generate only one key with KG command, then DWK2 will point (references) to DWK1. The activity of pointing DWK2 to DWK1 is configured as the following

|  |
| --- |
| ; -------------------------------------------------------------------------  ; Triple DES keys description  ; -------------------------------------------------------------------------  [DWK1]  \_CopyOf\_=PKCS11\_TDES\_FO  KeyName="DWK1"  ; -------------------------------------------------------------------------  [DWK2]  \_CopyOf\_=PKCS11\_TDES\_FO  KeyName="DWK1"  ; ------------------------------------------------------------------------- |



### Configure currency

Edit: /opt/egateway/egateway/egateway.ini



## Copy \*.mod file

Copy all of \*.mod files from addon folder of egateway to /opt/egateway/bin/mod folder where you installed egateway using way4 user

Make sure that owner of all \*.mod files is way4 user

If you have error regarding gdbmlib.so when starting EGATEWAY, please check that library libgdbm.so.2.0.0 and libgdbm.so.2 is included in Linux libraries. If not, install these libraries.

# Configure Transaction Switch

Go to /home/way4/appserver/applications/ts/webapps/ts/WEB-INF/conf/application

Create new file DatadGateAdapter.s.xml to open port 8840 and add in DWK which will be created in **Generate Keys** section

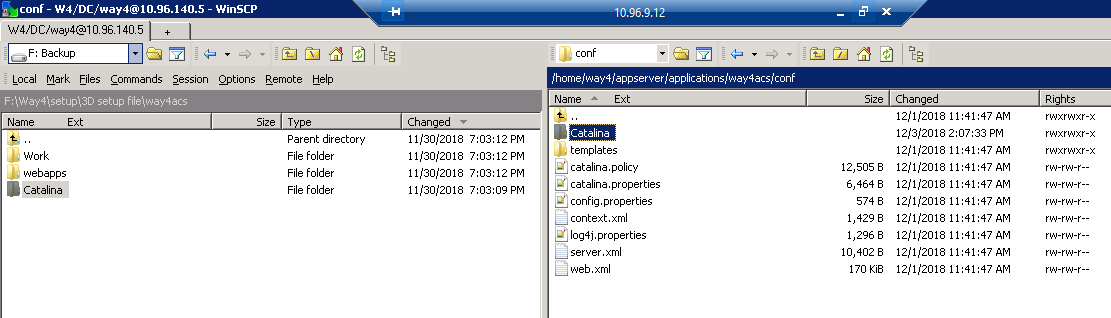


# Configure WAY4ACS

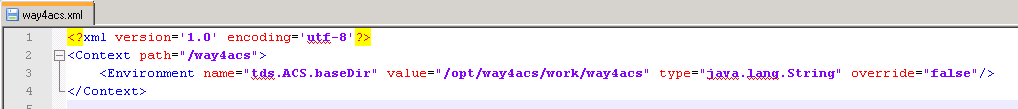
## Configure way4acs

### Copy Catalina folder

Under the way4 user, copy the Catalina/localhost/way4acs.xml file in way4acs setup folder to /home/way4/appserver/applications/way4acs/conf/Catalina/localhost/way4acs.xml.



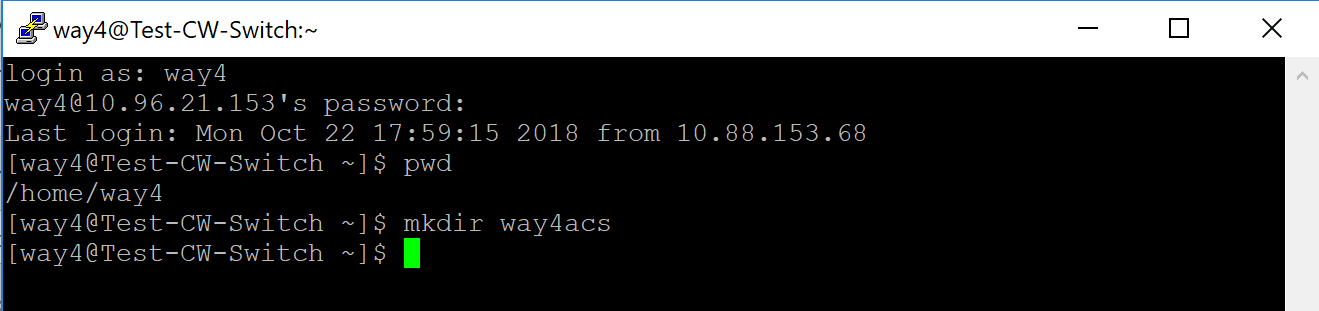
Edit the content of the way4acs.xml as the following



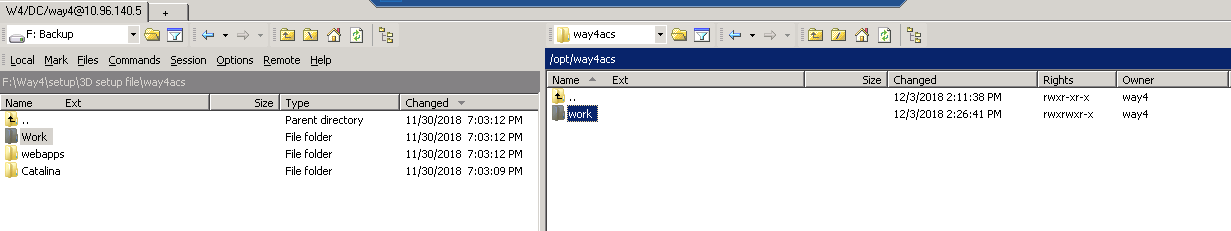
### Create way4acs folder in opt directory

* Login as way4
* Go to the directory /opt
* Run the following command to create way4acs directory under way4

|  |
| --- |
| [way4@Test-CW-Swtich ~]# mkdir way4acs |



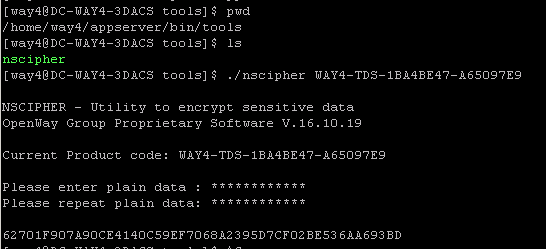
Copy the work folder from the distribution package to /opt/way4acs folder created in the previous step. After copy, the content as the following

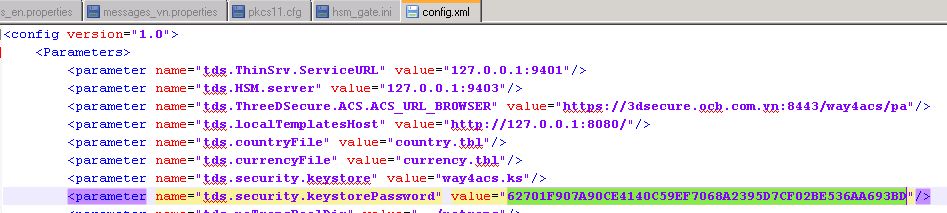


### Add parameters to ACS configuration (opt/way4acs/work/way4acs/config.xml)

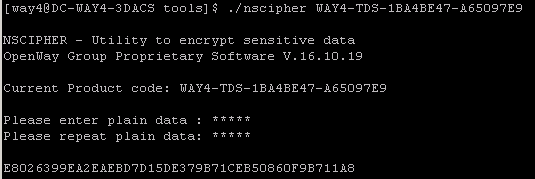
KeystorePassword and pin are encrypted password for the store, encrypted by the command "nscipher <product code>" (the product code is WAY4-TDS-1BA4BE47-A65097E9)

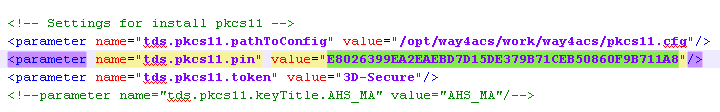
Keystore password: k4kwqoUe4eL#





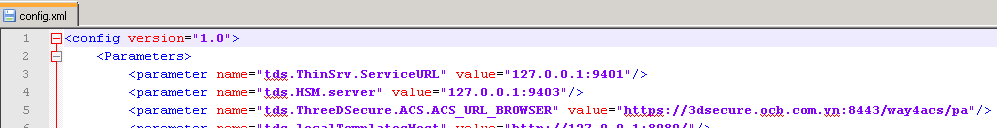
Pkcs11.pin: pin of hsm token 12345





* CH.tunnel – for cardholders during registration and authentication at the time of the transaction. This tunnel is public, it must be sent to the http port of the Apache Web server (see <AS\_HOME>/conf/webserver/httpd-main.conf, in the example – 8080). Apache is better supported in terms of security and works better with static content.
* MA.tunnel – tunnels for payment system DS servers, not public, require client SSL authentication. They must be sent directly to the WAY4 ACS http port. Payment systems can work on HTTP 1.0 and not send Host headers (DS MC works this way, for example), which is mandatory for working with virtual hosts. That is, sent to Apache, these connections will be refused, since configuration of virtual hosts on the Application Server and Web Server Apache is now mandatory

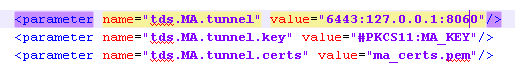
<parameter name="tds.ThreeDSecure.ACS.ACS\_URL\_BROWSER" value="https://3dsecure.ocb.com.vn:8443/way4acs/pa"/>



<parameter name="tds.MA.tunnel" value="6443:127.0.0.1:**8060**"/>

<parameter name="tds.MA.tunnel.key" value="#PKCS11:TEST\_MA\_KEY"/>

<parameter name="tds.MA.tunnel.certs" value="ma\_certs.pem"/>



<!-- OTP\_SMS settings (Example for external SMS delivery service) -->

<parameter name="AS.OTP\_SMS.select" value="PHONE=\*;TEXT=%description% (%amount%);"/>

<parameter name="AS.OTP\_SMS.verify" value="PASSWORD"/-->

<parameter name="AS.OTP\_SMS.select" value="PHONE=\*;TEMPLATE:=sms\_text.jsp;"/>

<parameter name="AS.OTP\_SMS.service" value="PHONE=\*;TEMPLATE:=sms\_text.jsp;"/>

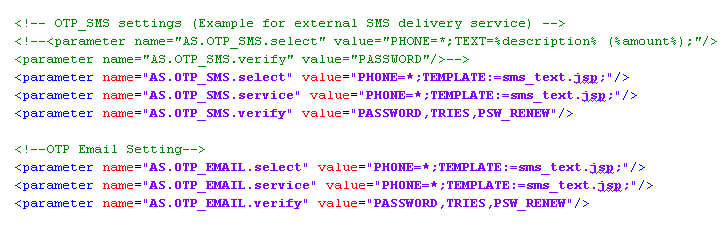
<parameter name="AS.OTP\_SMS.verify" value="PASSWORD,TRIES,PSW\_RENEW"/>

<!--OTP Email Setting-->

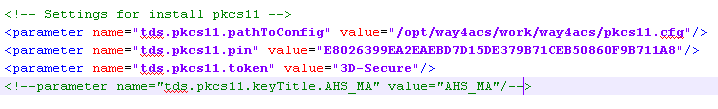
<parameter name="AS.OTP\_EMAIL.select" value="PHONE=\*;TEMPLATE:=sms\_text.jsp;"/>

<parameter name="AS.OTP\_EMAIL.service" value="PHONE=\*;TEMPLATE:=sms\_text.jsp;"/>

<parameter name="AS.OTP\_EMAIL.verify" value="PASSWORD,TRIES,PSW\_RENEW"/>

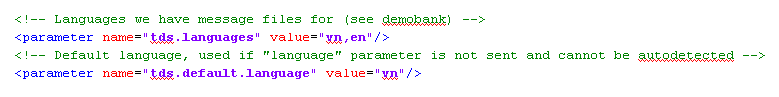


<parameter name="tds.pkcs11.pathToConfig" value="/opt/way4acs/work/way4acs/pkcs11.cfg"/>



To support Vietnamese language please add in vn

<parameter name="tds.languages" value="vn,en "/>



You can find the code of language in folder

**/home/way4/appserver/applications/demobank/webapps/demobank/images/flags**

### Set LD\_LIBRARY\_PATH and full log:

**Add parameter** in acs config.properties (/home/way4/appserver/applications/way4acs/conf/config.properties)

OS\_LD\_LIBRARY\_PATH=/opt/safenet/protecttoolkit5/ptk/lib

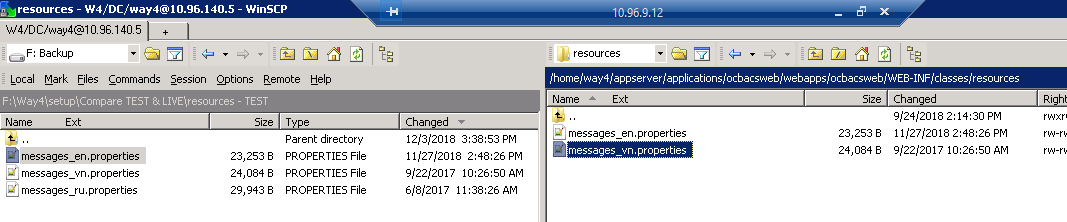
*jvm\_params=-Xmx512m -Xms128m -Djavax.net.debug=ssl:handshake:trustmanager -> to get full log*

# Configure WAY4 ACS Web

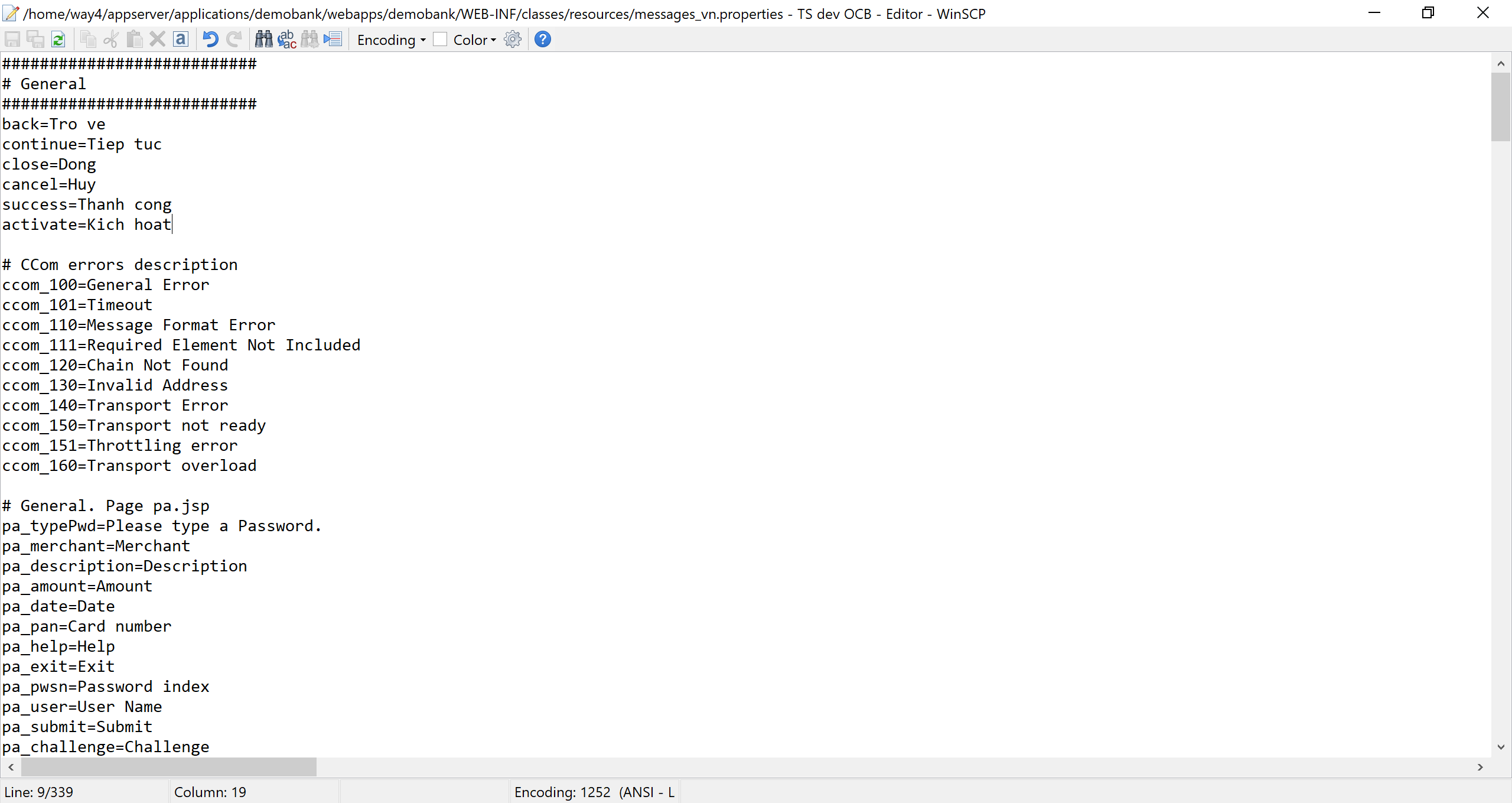
## Languages

Access folder**: /home/way4/appserver/applications/ocbacsweb/webapps/ocbacsweb/WEB-INF/classes/resources**

Create new file message\_vn.properties by duplicating message\_en.properties



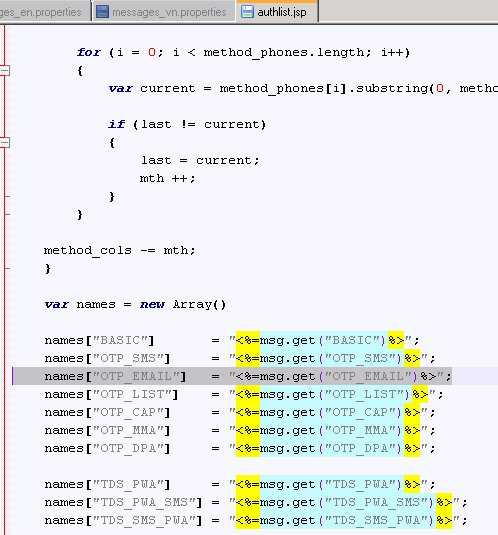
And then you can edit this file to display Vietnamese language



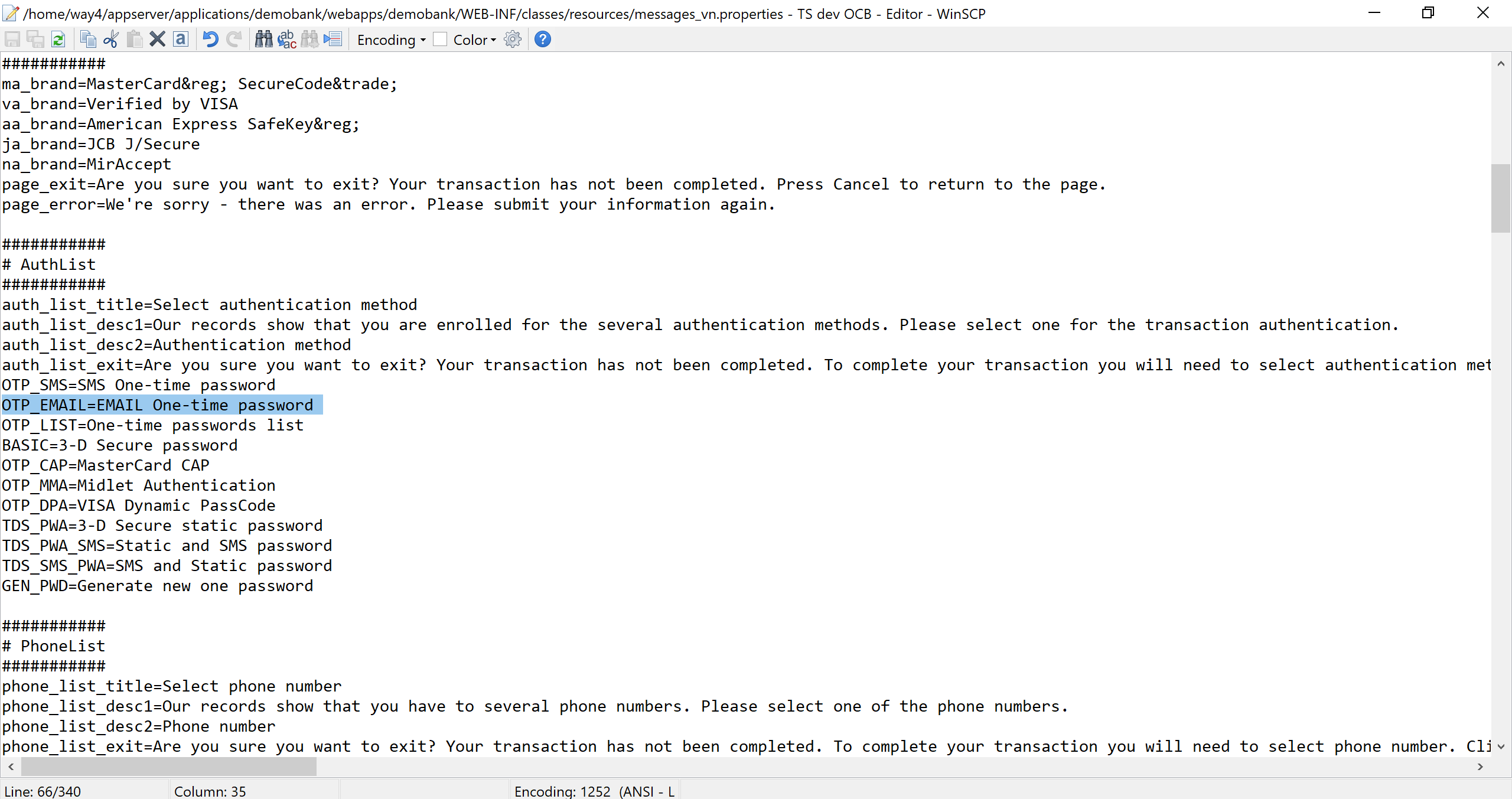
## OTP Email

**Go to** /home/way4/appserver/applications/ocbacsweb/webapps/ocbacsweb/common folder and edit authlist.jsp to insert

names["OTP\_EMAIL"] ="<%=msg.get("OTP\_EMAIL")%>";

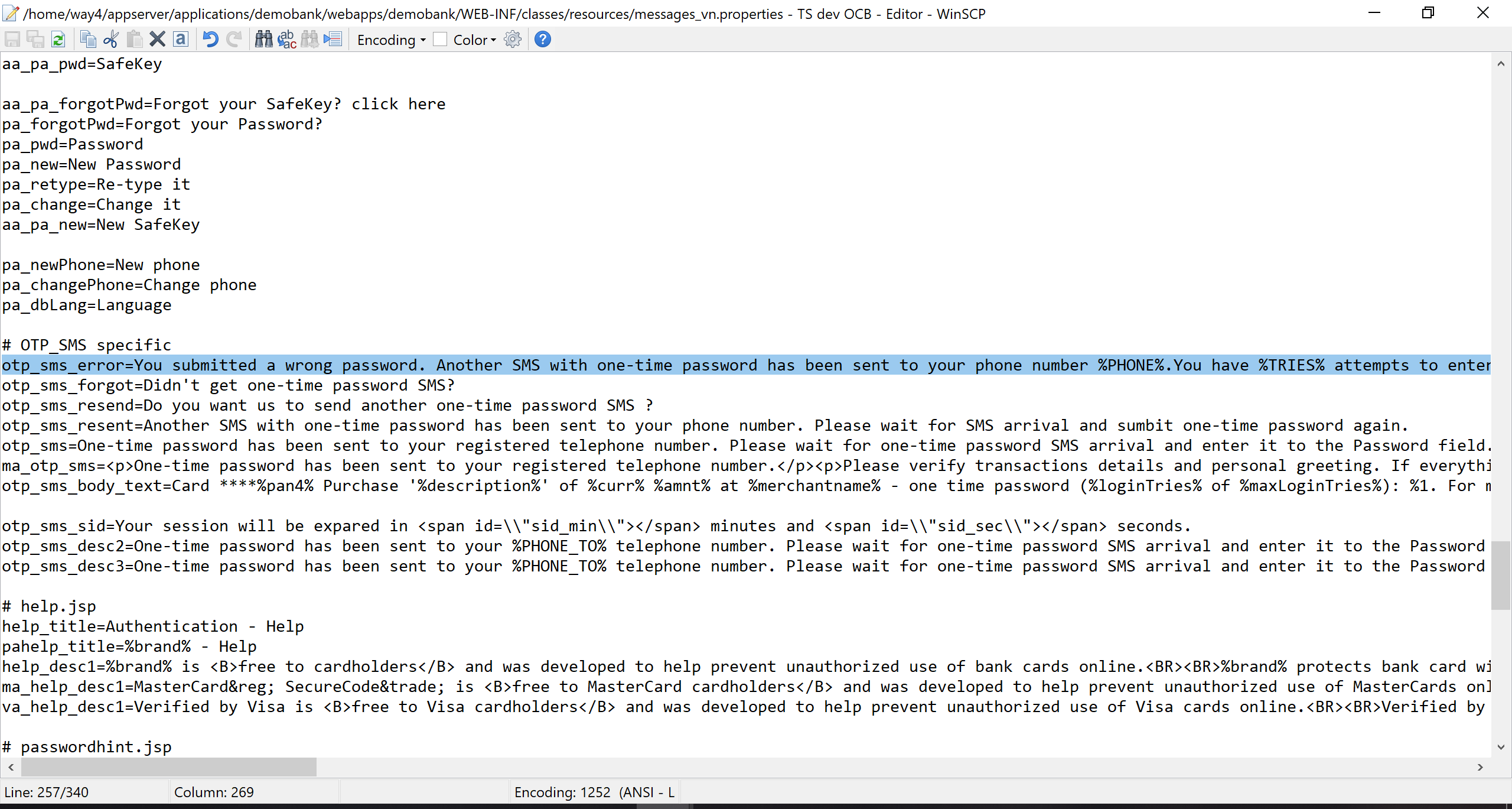


Edit above **message\_vn.properties** and **message\_en.properties** to support OTP Email



OTP\_EMAIL=Email One-time password

Please change below to support display email/phone in OTP form



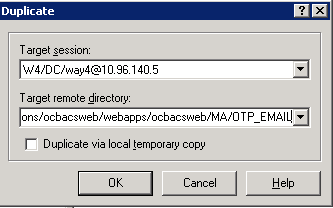
otp\_sms\_error=You submitted a wrong password. Another SMS with one-time password has been sent to your phone number **%PHONE%.**You have ***%TRIES%*** attempts to enter password and **%SMS\_TRIES%** to request new one. Please wait for SMS arrival and sumbit one-time password again.

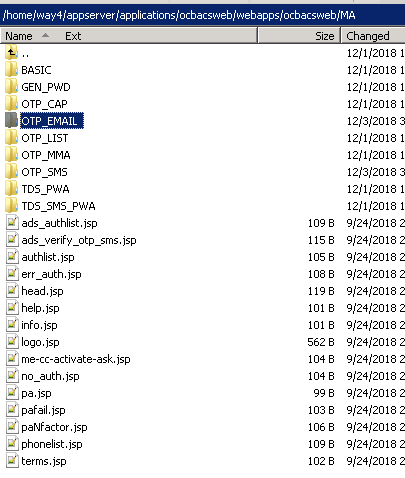
otp\_sms\_resend=Do you want us to send another one-time password SMS ?

otp\_sms\_resent=Another SMS with one-time password has been sent to your phone number. Please wait for SMS arrival and sumbit one-time password again.

otp\_sms=One-time password has been sent to your registered telephone number/email **%PHONE%.** Please wait for one-time password SMS arrival and enter it to the Password field.

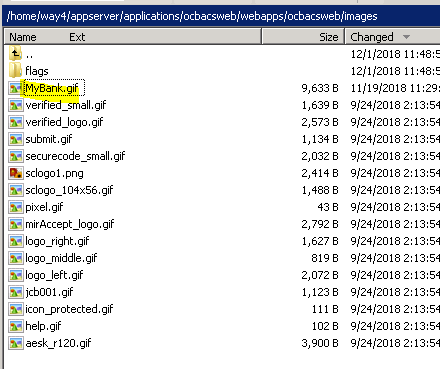
**Go to** /home/way4/appserver/applications/ocbacsweb/webapps/ocbacsweb/MA to create OTP\_EMAIL folder by duplicating existing OTM\_SMS folder





## OCB Logo

Go to /home/way4/appserver/applications/ocbacsweb/webapps/ocbacsweb/images



**Please copy logo file of the bank into this folder and rename it to MyBank.gif**

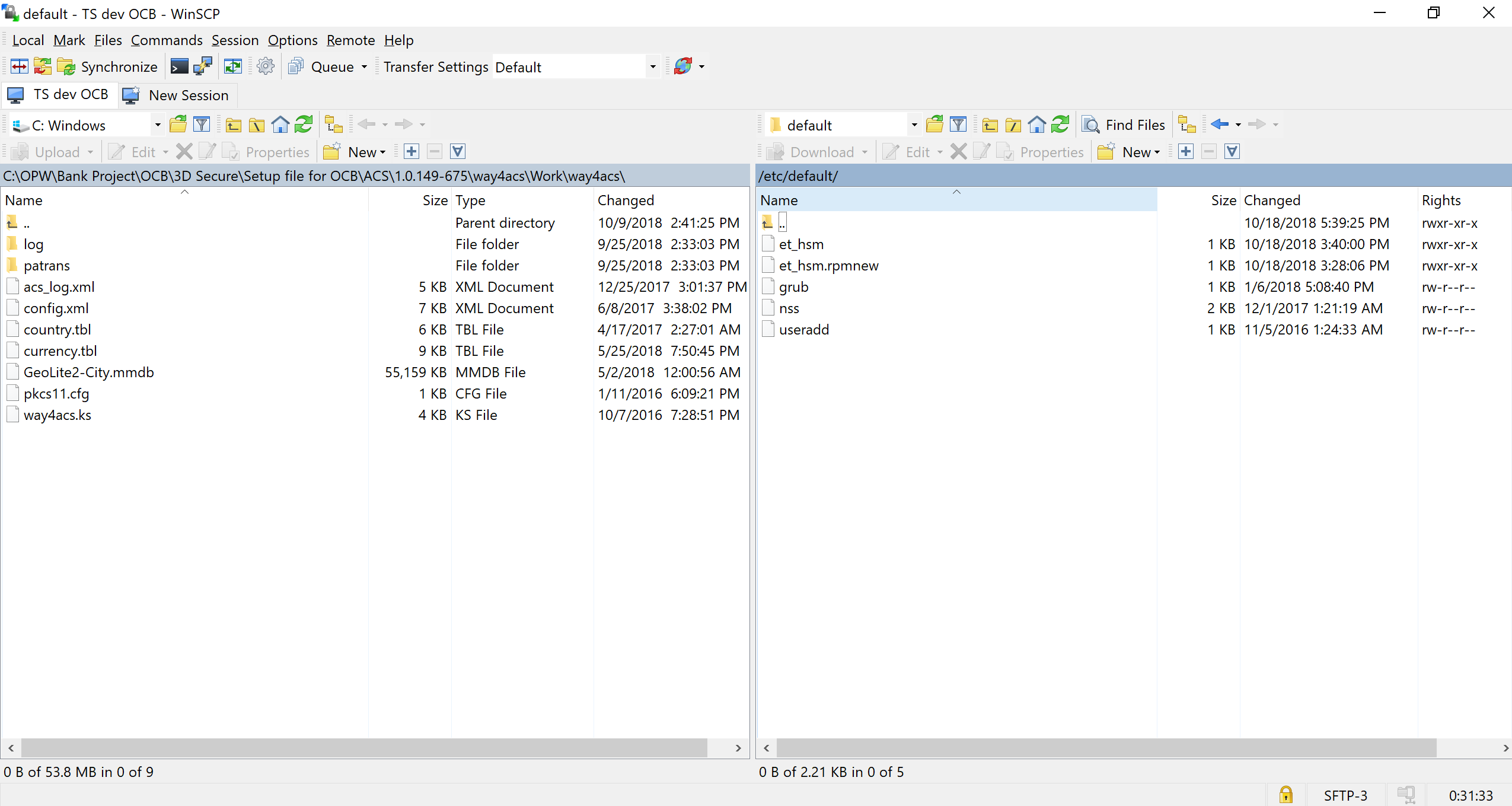
# Configure to support Eracom HSM connection

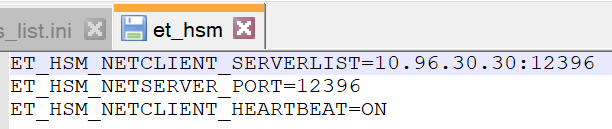
**Access parameters** must be put in a variable environment or in the file /etc/default/et\_hsm:

ET\_HSM\_NETCLIENT\_SERVERLIST=[host[:port]]

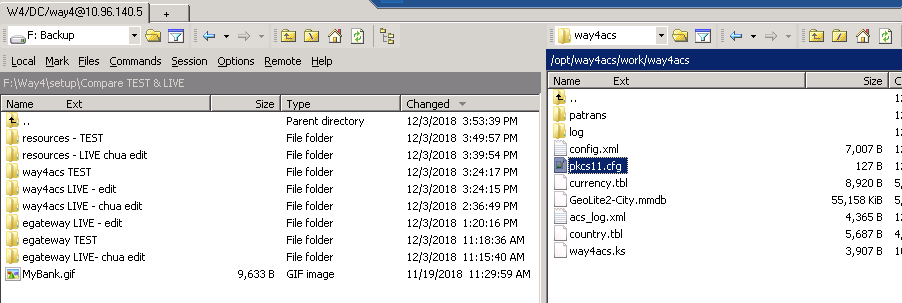
ET\_HSM\_NETSERVER\_PORT=[port]

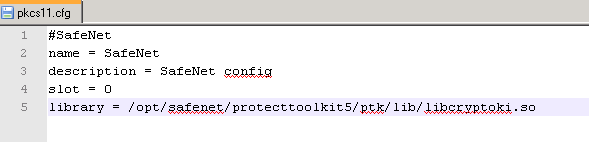
ET\_HSM\_NETCLIENT\_HEARTBEAT=ON





**Creating a PKCS#11 configuration file in /opt/way4acs/work/way4acs folder (pkcs11.cfg file)**





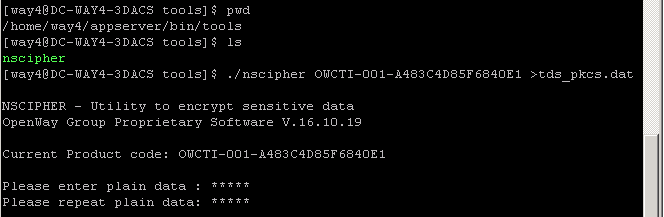
* Install the module support libraries. For external Eracom, install "Protect Toolkit C" and "Network HSM Access Provider".
* The "User password" for the device is set in /opt/egateway/datagate/hsm\_gate.ini:

...

Password="@datagate/tds\_pkcs.dat"  
...

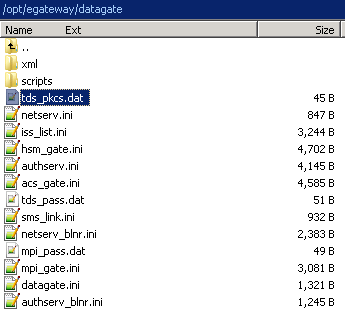
A file with the password is generated by the command:

nscipher OWCTI-001-A483C4D85F6840E1 >tds\_pkcs.dat

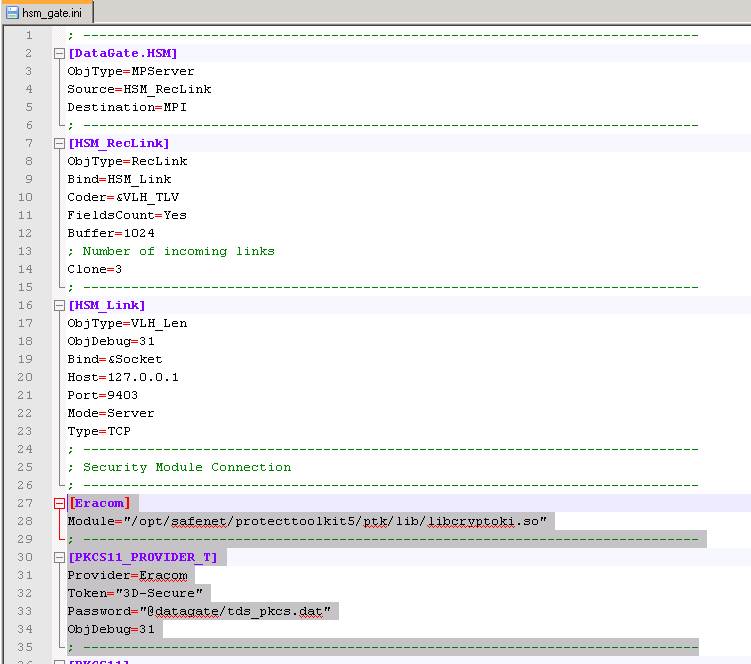


Plain Data should be user PIN of SO in Eracom (plain data = 12345)

Copy new tds\_pkcs.dat file from /home/way4/appserver/bin/tools to /opt/egateway/datagate folder



Edit hsm\_gate.ini



[Eracom]

Module="/opt/safenet/protecttoolkit5/ptk/lib/libcryptoki.so"

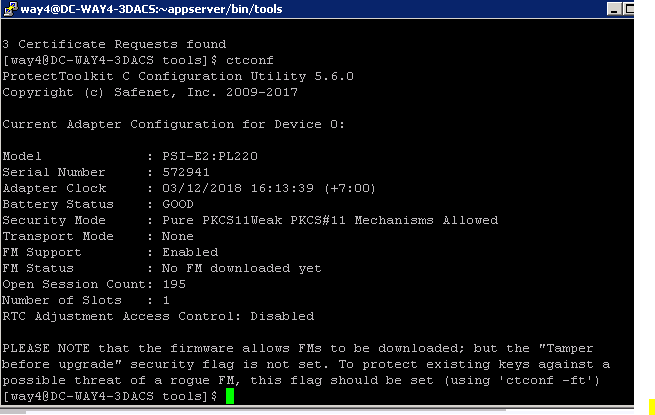
## Check the connection to Eracom Hsm

Login under way4 user

go to /opt/safenet/protecttoolkit5/ptk/bin

Run the ./ctconf command to view Eracom HSM information.

If you see the information as the following picture, the connection is good.



# Generate keys

A 3-D Secure product uses two main key types:

* Symmetric Triple DES keys for Secure ISO needs and internal data encryption
* Asymmetric RSA keys for SSL/TLS authentication and 3-D Secure digital signature of PaRes messages

Generate ZMK

## Generate 3DES Keys under Online HSM

### Creating components of a zone master key (ZMK) used to import working keys

The follwing commands is executed in the Online HSM under "Online HSM" mode

|  |
| --- |
| Online-AUTH>gc  Enter LMK id [0-4]: 0  Enter key length [1,2,3]: 2  Enter key type: 000  Enter key scheme: U  Clear component:  =====>>> **Will be used to import in the 3DSECURE ERACOM HSM**  Encrypted component:  Key check value:  **Component 2:**  Online-AUTH>gc  Enter LMK id [0-4]: 0  Enter key length [1,2,3]: 2  Enter key type: 000  Enter key scheme: U  Clear component:  =====>>> **Will be used to import in the 3DSECURE ERACOM HSM**  Encrypted component:  Key check value: |

gc - key type 000

Clear Component: 3257 1334 9DEA FE51 2F80 1358 2F89 0167

Encypted component: UBCA5 EACB CE67 4E9F EC3E 5CBE FA12 4EC5

Key check value: 4FC4AF

gc - key type 000

Clear Component: 0E0D BF1C 9B23 DC0B 46DA 94B0 6EE9 804C

Encypted component: U0D3E 73C3 4B55 92DD B480 CE90 F7FC 93A5

Key check value: E4E4C9

### Form ZMK key from two components generated in the previous step (Form ZMK key from ZMK1, ZMK2)

Component 1, and Component 2 are the two Encrypted component in the previous step

|  |
| --- |
| Online-AUTH>fk  Enter LMK id [0-4]: 0  Enter key length [1,2,3]: 2  Enter key type: 000  Enter key scheme: U  Enter component type [X,H,T,E,S]: X  Enter number of components [1-9]: 2  Enter component 1:  Enter component 2:  Encrypted key:  =======>>>>> **ENCRYPTED ZMK, This key will be used to encrypt DWK**  Key check value: |

fk - key type 000

Encypted key: U94DC 62AB 48DF E4E2 6A77 5466 67D8 77E0

Key check value: 905FD4

### Generate working key (DWK) in HSM online (Thales)

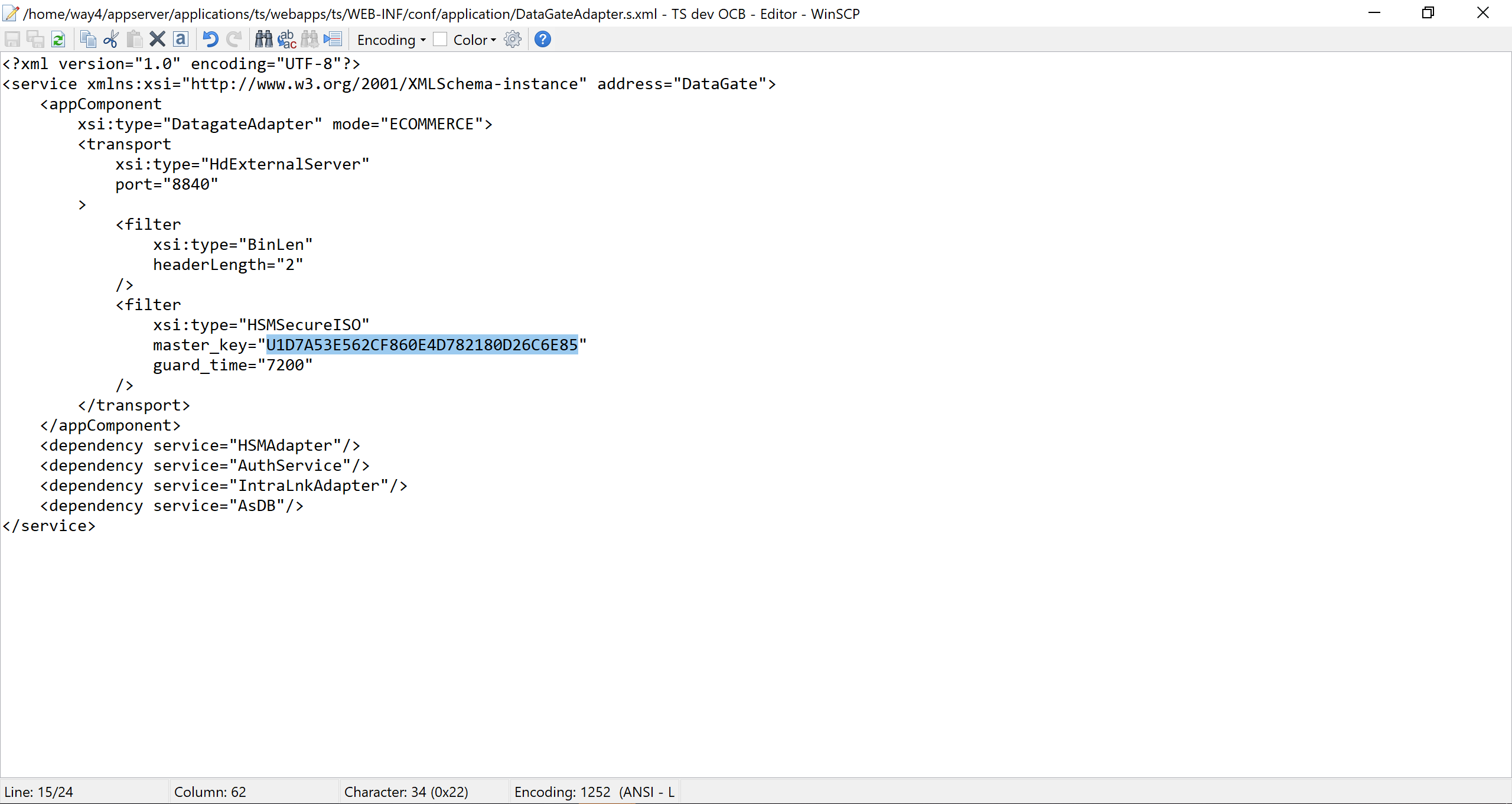
ZMK created in the previous step will be used in this step to create working key

In the standard document, we need to create two keys DWK1, DWK2 and place those keys in the E-COMMERCE and DATAGATE respectively.

|  |
| --- |
| Online-AUTH>KG  Enter key length [1,2,3]: 2  Enter key type: 008  Enter key scheme (LMK): U  Enter key scheme (ZMK): X  Enter ZMK: U94DC 62AB 48DF E4E2 6A77 5466 67D8 77E0  Key under LMK: U1D7A 53E5 62CF 860E 4D78 2180 D26C 6E85//**Put into Datagate Adapter of** Transaction Switch  Key under ZMK: A2DA E5A4 A309 AB85 2CBA 598A 1F34 C609 // **DWK 1 to import into Eracom**  Key check value: D2A8F8 |

### Add DWK1 working key created in the above step to the channel in Transaction Switch

Working Key under LMK (U1D7A 53E5 62CF 860E 4D78 2180 D26C 6E85) will be used to configure master key in the channel datagate adapter of Transaction Switch



### Import Zone Master Key (ZMK) to Eracom HSM

[way4@Test-CW-Switch ~]$ ctkmu c --slot-num=0 --type=des2 --name=ZMK1 --num-comp=2 --attributes=RTEPDWU

ProtectToolkit C Key Management Utility 5.6.0

Copyright (c) Safenet, Inc. 2009-2017

Enter user PIN for slot 0:

Enter Key Component 1 (Need to enter 32 HEX chars):

Component 1 KCV : 4FC4AF

Is this correct? [Y/n]: y

Enter Key Component 2 (Need to enter 32 HEX chars):

Component 2 KCV : E4E4C9

Is this correct? [Y/n]: y

Key 'ZMK1' KCV : 905FD4

Is this correct? [Y/n]: y

Key "ZMK1" was created

### Import working key (DWK1) to Eracom HSM

|  |
| --- |
| ctkmu i --slot-num=0 --type=des2 --name=DWK1 --wrap-key=ZMK1 --attributes=TEPS --console |

[way4@Test-CW-Switch ~]$ ctkmu i --slot-num=0 --type=des2 --name=DWK1 --wrap-key=ZMK1 --attributes=TEPS --console

ProtectToolkit C Key Management Utility 5.6.0

Copyright (c) Safenet, Inc. 2009-2017

Enter user PIN for slot 0:

Choose Mechanism to Wrap with

0. Mechanism DES3\_ECB

1. Mechanism DES3\_ECB\_PAD

2. Mechanism DES3\_CBC

3. Mechanism DES3\_CBC\_PAD

4. Mechanism WRAPKEY\_DES3\_ECB

5. Mechanism WRAPKEY\_DES3\_CBC

6. Mechanism WRAPKEYBLOB\_DES3\_CBC

7. Mechanism DES3\_DDD\_CBC

Enter number of item OR q to quit: 0

Item ID of 0 has been selected. Is this correct? [Y/n]: y

Enter key cryptogram

Read data from a file? no

Enter data (HEX or Base64):

A2DAE5A4A309AB852CBA598A1F34C609

More data (or RETURN to finish):

0x10 bytes entered

KCV : D2A8F8

Is this correct? [Y/n]: y

New key generated successfully.

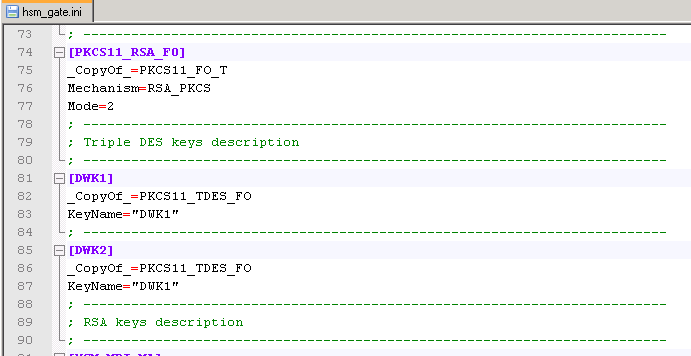
Check all keys imported/generated in ERACOM's HSM



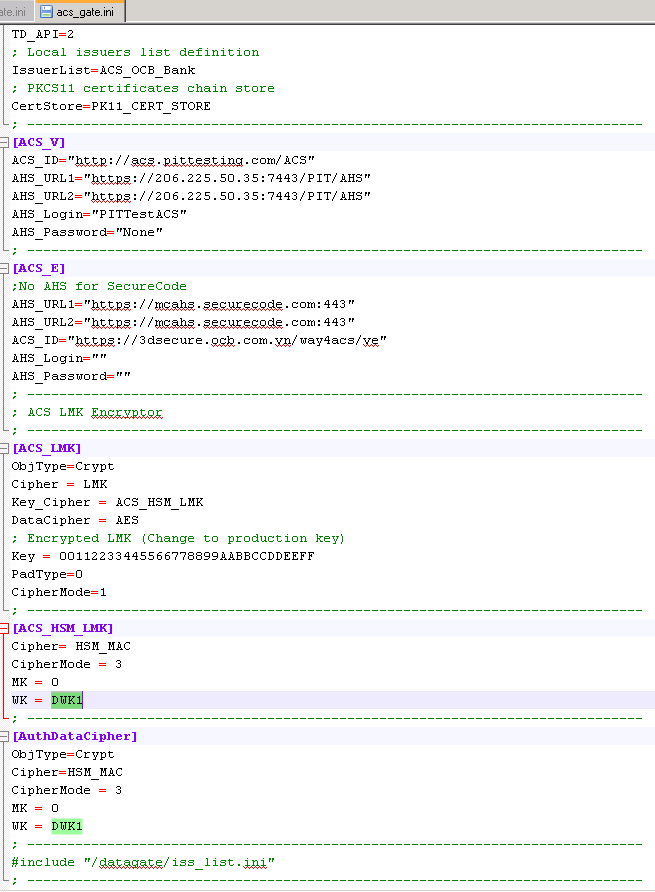
### Check the link in the 3D-Secure Gateway configuration file:

Go to /opt/egateway/datagate/datagate/hsm\_gate.ini

|  |
| --- |
| [HSM]  HSM=Switch  Keys="DWK1,DWK2"  [DWK1]  \_CopyOf\_=PKCS11\_TDES\_FO  KeyName="DWK1" |



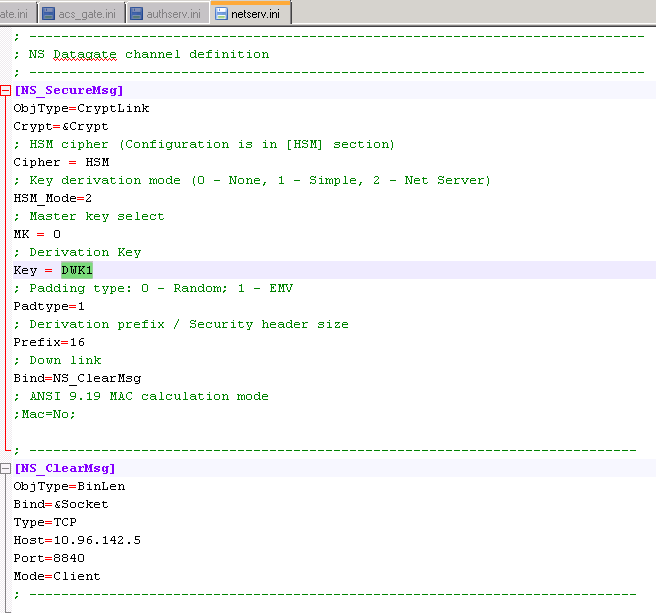
Edit /opt/egateway/datagate/acs\_gate.ini



/opt/egateway/datagate/authserv.ini



/opt/egateway/datagate/netserv.ini



## Generate RSA keys to support SSL/TSL and digital signature of PaRes

Login to ERACOM HSM Server under root user

Go to the following folder:

|  |
| --- |
| /opt/ETcpsdk/bin/linux-i386 |

Refer to MC\_KEY\_safenet version 5.6 - Live env.docx

## Check the key after import to the ERACOM's hsm

Run command ctkmu l –s0



# Network configuration

The bank need to configure the network to expose the following address to the internet so that MC DS can send message to ACS.

https://3dsecure.ocb.com.vn:6443/way4acs/pa

Noted that 3dsecure.ocb.com.vn is mapped to 10.96.140.5 in OCB

# Configure Application Server

## Edit virtual host name and address

appserver/conf/webserver/httpd-main.conf

