Prepaid Online Vending System

XMLVend 2.1 Test Suite Setup Instructions

Contents

Document Title	Prepaid Online Vending System - XMLVend 2.1 Test Suite Setup Instructions
Document Number	
Document Issue	
Compiled By	M Masoleng
Issue Date	31 October 2012
Controlled By	M Masoleng

Approval

Position	Name	Signature	Date
Prepayment Development Manager	Deon van Rooi		

Amendment History

Doc. Issue	Date	Changed Chapter / Topic / Page	No. of Pages	Checked by Name Initial

Distribution List

Distribution Control: This document will be under distribution control to the following persons:

Copy No.	Person	Organisation	Distr. Control	Signature

Software required

1) Ant
2) JDK
3) Tomcat
4) Novell plugin for IE
5) XMLVend server (***.war**)
   + Eskom Server Responses
6) XMLVend Client (***.war**)
7) Eskom XMLVend client (***.war**)
8) Interceptor
9) Cmdhere.reg to be able to open folders in Command prompt

Setup Java JDK

1. Extract ANT files and copy to **c:\ant**
2. Create ANT_HOME variable **c:\ant**
3. Add **c:\ant\bin** to PATH
4. Setup the following:
   JAVA SDK, JAVA_HOME and set PATH to Java as User and System variables

Set up user variables:

a) Variable name – JAVA_HOME
   Variable value – **C:\Program Files\Java\jdk1.5.0_02**
b) Variable name – path
   Variable value – **C:\Program Files\Java\jdk1.5.0_02\bin;C:\Ant\apache-ant-1.8.2\bin**

System variables to add:

a) Variable name – JAVA_HOME
   Variable value – **C:\Program Files\Java\jdk1.5.0_02**
b) Variable name – path
   Variable value – **C:\Program Files\Java\jdk1.5.0_02\bin;C:\Ant\apache-ant-1.8.2\bin**

Note: Select path by copying the path wherever the JDK and Ant is located

TOMCAT Setup for XML

1. Extract Tomcat file. Copy files to **c:\jakarta-tomcat-5**
2. Copy the "**c:\jakarta-tomcat-5\server\lib\catalina-ant.jar**" file to the **c:\ant\lib**
3. Copy the xmlvend client **and** server war file to the "**C:\tomcat\jakarta-tomcat-5.0.27\webapps**" folder
4. Startup Tomcat from **C:\tomcat\jakarta-tomcat-5.0.27\bin\startup.bat.**

   The service can be stopped by shutting it down from
   C:\tomcat\jakarta-tomcat-5.0.27\bin\shutdown.bat

5. To run the test Client/Server, enter the following in the web browser:-

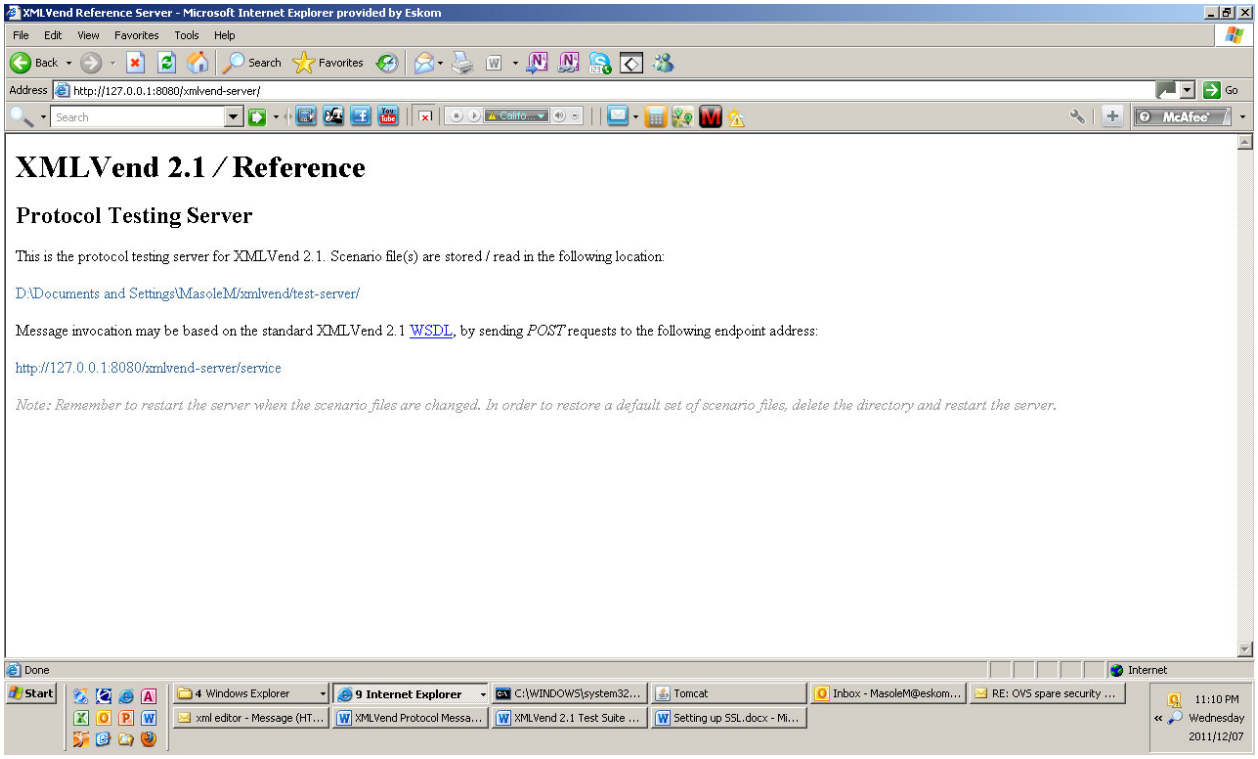
http://localhost:8080/xmlvend-server/

http://localhost:8080/xmlvend-client/

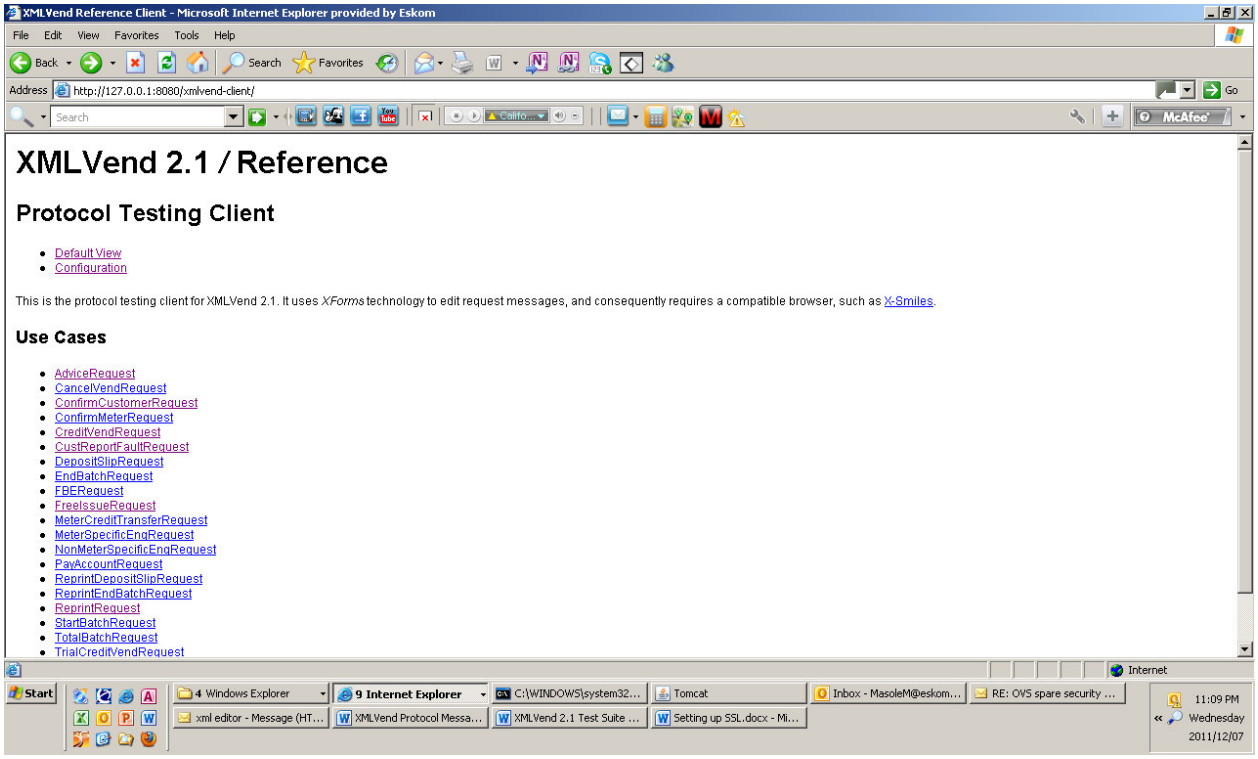
http://localhost:8080/xmlvend-server-eskom/

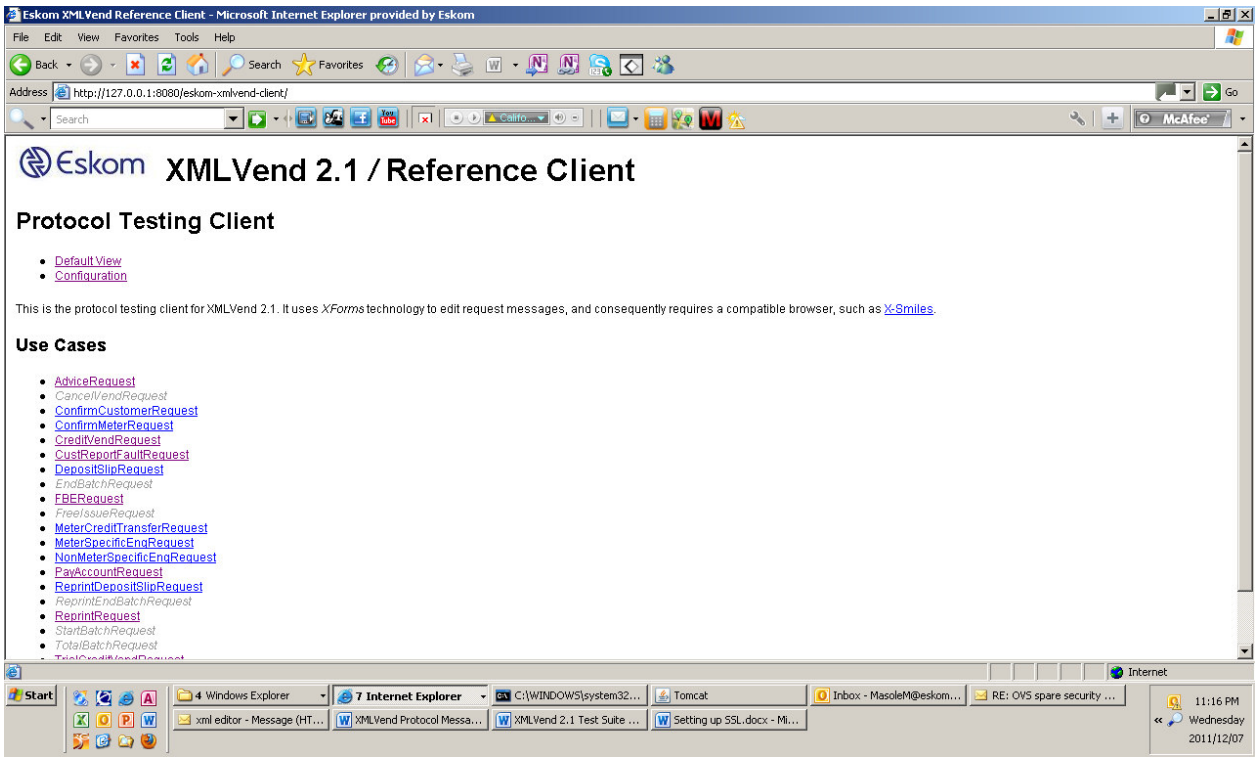
Use **C:\tomcat\jakarta-tomcat-5.0.27\bin\startup.bat** to create a short cut for start-up.

Use **C:\tomcat\jakarta-tomcat-5.0.27\bin\shutdown.bat** to create a short cut for shutdown



http://127.0.0.1:8080/xmlvend-client/





Interceptor

1. Extract interceptor zipped folder into the root directory.
2. For information on how to set up the message interceptor, see the **XMLVend message validation suite** document.
3. Configurations to note is that for the interceptor to recognise the full xml message, remove the compression request [must be false].
4. The XMLVend Server URL: http://localhost:8082/xmlvend-server/service/ for the listening port or it will be set automatically.

Setting up SSL

1. Install Active Perl.
2. Setup OpenSSL
    a. Install OpenSSL
    b. Install Visual C++ Redistributables
3. Create new system variable - OPENSSL_CONF c:\opensssl-win32\bin\openssl.cfg
4. Add to PATH c:\openssl-win32\bin\ to the system variable PATH.

Setting up the SSL – CA environment

i) Create CA

1) create dir **c:\ca**

2) copy the CA.pl file from the openssl-win32 bin folder to c:\ca

3) open **c:\ca** folder in Command Prompt

4) execute the command **c:\ca>perl CA.pl –newca**, then press “enter”

5) **NB:** Do not specify a filename name, just Press "Enter".

6) Supply PEM Passphrase for the certificate = "testca", enter again to verify the Passphrase

7) Enter the following

    (a) Country code

    (b) Province name

    (c) Locality

    (d) Organisation name

    (e) Organisational Unit

    (f) Common Name, CA name

    (g) Email address

    (h) Challenge password

8) Enter passphrase for certificate. This will confirm all the details entered when creating of the certificate.

ii) Add the CA cert in Java Trusted Store

You can check this by typing in the command prompt **c:\>set** and then enter.

Look for where Java_Home is in your system variables to check the exact location of Java.

Add the testCA root certificate in Java trusted store (do this on client and server machines), on JDK or JRE installations (depending on where Java_Home is located) by following these steps:-

- copy **c:\ca\demoCA\cacert.pem** to **c:\%JAVA_Home%\jre\lib\security**
- cd to **c:\%JAVA_Home%\jre\lib\security**
- enter, **keytool -import -keystore cacerts -file cacert.pem**

password="**changeit**".

NB: If an error message displays "keytool error: java.lang.Exception: Input not an X.509 certificate", you need to edit the cacert.pem file and remove the entries from the first line in the file up to the part before "

-----BEGIN CERTIFICATE-----
MIICzDCCAjWgAwIBAgIJALHI+ZVypJMEMA0GCSqGSIb3DQEBBQUAMH8xCzAJBgNV
BAYTAnphMRAwDgYDVQQIDAdnYXV0ZW5nMQ4wDAYDVQQKDAVFc2tvbTETMBEGA1UE
CwwKUEREIFRlc3RDQTEVMBMGA1UEAwwMTWFydGluVGVzdENBMSIwIAYJKoZIhvcN
AQkBFhNtYXNvbGVtQGVza29tLmNvLnphMB4XDTEyMDcyNjA5MjUxNloXDTE1MDcy
NjA5MjUxNlowfzELMAkGA1UEBhMCemExEDAOBgNVBAgMB2dhdXRlbmcxDjAMBgNV
BAoMBUVza29tMRMwEQYDVQQLDApQREQgVGVzdENBMRUwEwYDVQQDDAxNYXJ0aW5U
ZXN0Q0ExIjAgBgkqhkiG9w0BCQEWE21hc29sZW1AZXNrb20uY28uemEwgZ8wDQYJ
KoZIhvcNAQEBBQADgY0AMIGJAoGBALQPJCT19Yp0jCPOmY3998JS3ZeBCikcpn0O
HZyXvZSOnZOA77kw00aign10SbklM0yb7Ae6vTJhb3yA3dXSEBrtQH/myC8tjGxq
2LQ7EWKesOkU/cMcAzubUc9c9AAwgnTLxVBuXxkOfP8R3qhQXHkcax3bP/frAu1o
lN0rHuN5AgMBAAGjUDBOMB0GA1UdDgQWBBT5xyXGKjzkK8qHpyUiye+WzY7DZzAf
BgNVHSMEGDAWgBT5xyXGKjzkK8qHpyUiye+WzY7DZzAMBgNVHRMEBTADAQH/MA0G
CSqGSIb3DQEBBQUAA4GBAD9oKjlle/cEKyXAOrlzVvXVqd6lDqi71YONoa+S+iXs
GIvDVYgH4sYgKHSf1t1KqkF18WuBASAD0Y2kK4z3/lFWB2GKNPtHguB4WGSDaqUw
PNkkUGil2mA1LMRjqCuttnl4XHDph2v6TYGpGWkmw1DCj9ZboZNg9AL5tgKPcrfn
-----END CERTIFICATE-----".

Save the file after editing and run the command again.

- alias set to "mykey" ??

to check if the cacert has been added into the keystore, enter "**keytool –list –keystore cacerts**"

Setting up the SSL – Server Environment

1. Create server keystore

- create a directory to store server key **c:\onlinevending\security**
- open the folder form the command prompt
- enter "**keytool -genkey -keystore xmlvendserver -keyalg rsa -alias xmlvendserver -storepass testserver"**
- enter "**keytool -list -keystore xmlvendserver** to check if the keystore has been created

2. Create server CSR

- From the directory created for the security, open command prompt and then enter "**keytool -keystore xmlvendserver -keyalg rsa -certreq -alias xmlvendserver -file xmlvendserver.csr -storepass testserver**"
- Send the .csr file to the CA for signing and create a server certificate. Copy the **xmlvendserver.csr** file into the demoCA\ folder

3. Sign the server CSR in CA

- open **c:\TestCA\demoCA** from command prompt
- enter "**C:\ca\demoCA>openssl x509 -req -CA cacert.pem -CAkey private/cakey.pem -extensions v3_ca -in xmlvendserver.csr -inform DER -out xmlvendserver.cer**"
- If error message display "**cacert.srl: no such file or directory**" looking for a ***.srl** file then enter the command below
- **C:\testCA\demoCA>openssl x509 -req -CA cacert.pem -CAkey private/cakey.pem -extensions v3_ca -in xmlvendserver.csr -inform DER -out xmlvendserver.cer –CAserial serial**
- password = "**testca**"

4. Send signed certificate to server

Send the signed .csr back to the server to load

5. Load signed certificate in server

- copy **xmlvendserver.cer** to **c:\onlinevending\security**
- open folder from command prompt
- enter "**C:\OnlineVending\security>keytool -import -alias xmlvendserver -keystore xmlvendserver -trustcacerts -file xmlvendserver.cer**"

ERROR - **keytool error: java.lang.Exception: Failed to establish chain from reply** means the CA certitificate is not installed in the trusted cacerts store as per **2**.

- Re-enter "**C:\OnlineVending\security>keytool –keyalg rsa -import -alias myxmlvendserver -keystore xmlvendserver -trustcacerts -file xmlvendserver.cer**"

6. Configure Tomcat for SSL in the server

1) edit the **server.xml** in /conf dir
2) Uncomment SSL connector.
3) Set clientAuth="**true**", this ensures that client authentication is done.
4) The password and location of the server keystore must be specified, see example below.

```
<!-- Define a SSL Coyote HTTP/1.1 Connector on port 8443 -->

<Connector port="8443"

maxThreads="150" minSpareThreads="25" maxSpareThreads="75" enableLookups="false"
disableUploadTimeout="true" acceptCount="100" debug="0" scheme="https" secure="true"
clientAuth="true" sslProtocol="TLS" KeystoreFile="D:\OnlineVending\security\xmlvendserver"
keystorePass="online" />
```

Setting up the SSL – Client Environment

1. Create client environment

1) Create Certificate on Client machine.

Create directory for client, eg. C:/onlinevending_dev/security

Open from command prompt,

Then enter, **>keytool -genkey -keyalg rsa -keystore xmlvendclient -alias xmlvendclient -storepass online**

Enter **>keytool -list -keystore xmlvendclient**

Enter **>keytool -keystore xmlvendclient -keyalg rsa -certreq -alias xmlvendclient -file xmlvendclient.csr -storepass online**

2) Add the CA cert in Java Trusted Store

You can check this by typing in the command prompt **c:\>set** and then enter.

Look for where Java_Home is in your system variables to check the jdk or jre file in the folder for the correct location.

Add the testCA root certificate in Java trusted store (do this on client and server machines), on JDK or JRE installations (depending on where Java_Home is located) by following these steps:-

- copy **c:\ca\demoCA\cacert.pem** to **c:\%JAVA_Home%\jre\lib\security**
- cd to **c:\%JAVA_Home%\jre\lib\security**
- enter, **keytool -import -keystore cacerts -file cacert.pem**

password="**changeit**".

NB: If an error message displays "**keytool error: java.lang.Exception: Input not an X.509 certificate**", you need to edit the **cacert.pem** file and remove the entries from the first line in the file up to the part before -------BEGIN CERTIFICATE---------.

Save the file after editing and run the command again.

- alias set to "**mykey**" ??

To check if the cacert has been added into the keystore, enter "**keytool –list –keystore cacerts**"

3) Send the **.csr** file to CA to be signed and create a certificate

C:\ca\demoCA>openssl x509 -req -CA cacert.pem -CAkey private/cakey.pem -extensions v3_ca -in xmlvendclient.csr -inform DER -out xmlvendclient.cer

4) Send signed certificate back

To import the certificate into the client keystore, enter
C:\OnlineVending_dev\security>keytool -import -alias xmlvendclient -keystore xmlvendclient -trustcacerts -file xmlvendclient.cer

2. Client SSL configuration

1) In the client configuration screen, ensure the that URL is updated as follows:

https://localhost:8443/xmlvend-server/service/. The "s" in https:// must be added to enable SSL. In case there will be two systems that will interface with each other, use the IP address of the machine that will be hosting the server.

2) Specify the client keystore location and password, eg.

C:\onlinevending_dev\security\testclient password "**online**"

3) Verify that in the server.xml that the SSL connector is commented out!!!

Windows

1. Copy CA.pem (CA self signed certificate) to temp dir.
2. Rename to CA.cer.
3. Import into Trusted stored.
4. The certs must be in DER format for windows.

Windows Client

1. The hosts file must refer the IP to the server name???

Other

1. Creating an expired cert. Change CA pc date

"openssl x509 -days 30 -req -CA cacert.pem -CAkey private/cakey.pem

-extensions v3_ca -in bluelable2.csr -inform DER -out bluelable2.cer"

2. Deleting a cert out of the JAVA CACERTS

C:\Program Files\Java\jdk1.5.0_02\jre\lib\security>keytool -delete -alias mykey -keystore cacerts

Enter keystore password: changeit

C:\Program Files\Java\jdk1.5.0_02\jre\lib\security>keytool -import -keystore cacerts -file lawtrustca.cer -alias lawtrust

serverID: 6004708001998

ClientID: 6004708001981

CRL generation

1. openssl ca -cert cacert.pem -keyfile private/cakey.pem -revoke xmlvendclient_act.cer -config openssl.cnf

?Creates an entry in the index.txt file - note openssl.cnf points to the index.txt

2. openssl ca -cert cacert.pem -keyfile private/cakey.pem -gencrl -out ca-crl.pem -config openssl.cnf

?Create the CRL, "ca-crl.pem"

3. openssl crl -in ca-crl.pem -text -noout

?Display CRL, note only the revoked certs serial number is displayed.

DISPLAY contents of a Certificate

openssl x509 -text -in xmlvendclient_act.cer