Digital Signature and Implementation in DataPower

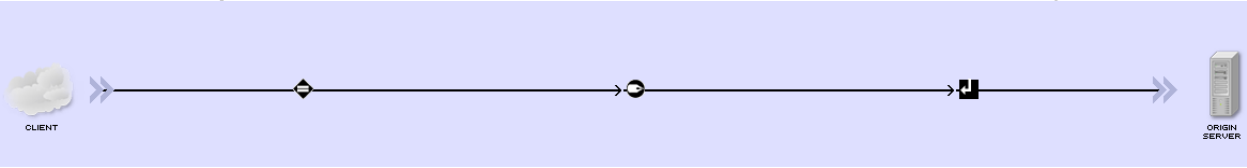
First one should understand what is Digital Signature and why enterprise level applications use this.
Digital Signature is an electronic signature which used to authenticate the sender of the message and ensure the message content is unchanged.We can ensure the original signed message because the sender cannot easily repudiate it later.

These are widely used in most secured transactional applications like credit card,bank loan,other financial and health applications where confidentiality is strictly maintained.It doesnt mean that other industries may not use them.Every application which need the high security level will use digital signatures. Concept of Digital Signatures: There are few simple steps to explain how Digital Signature works.
Step 1:
Ram sends email with stamping his digital signature by using his private key to Sita
Step 2:

Up on receving email Sita verifies the digital signature in the email with the Ram public Key.
So once both keys matched and verified Sita able to read the message and she can confirm that message was unchanged.
DataPower Implementation: We can validate the digital signature or sign the digital signatiure on document with the processing actions and public and private self signed certs. Once we created the private and public key for the digital signature from the crypto tools in DP.We are almost ready to implement the Digital Signature in our Processing Policies. Example any web services which involved in transmission of highly confidential data.We create a multi-protocal gateway or WSP based on the requirements and after that To Verify: 1. Go to Processing Policy

2. drag and drop the "verify" Action
3. Create the vliadation credentials and insert the public key for the verification

To Sign 1. Go to Processing Policy
2.Drag and Drop "Sign" Action
3.Create the Key and Certificate with the private key and public cert.
4.Share the public cert with the receiver so that he can verify



How AAA action works

AAA,Authenticaion Authorization and Audit.This is the one of the most important security feature provided by DataPower. Every time if we want to secure a web service and we want to let the authorized user to access that service we use AAA mechanism. There is a step wise process AAA working flow Extract the Identity credentials from the input message or request Authenticate the credentials extracted from payload Maps the credentials with the authorization server credentials Extract the resource from the input message or request Map the resource with the authorization server which the credentials are assigned it to Authorize the credentials from the first 3 steps with the resource in 4th and 5th one. Post Processing of the request

Creating a FTP Poller in Datapower

DataPower provides functionality for FTP and SFTP ing of files.Before going to creation of poller let us look at brief description for FTP and SFTP.

FTP:
File transfer protocol exchanges data in 2 seperate channels
Command channel
Data channel
Command Channel:
It is responsible for creating client conenction,authentication and exchange of simple FTP commands.It will be open until it gets QUIT command.
Data Channel:
It is responsible for exchanging data like listing,uploading and dowloading the files.Data channel will be closed once the transfer completes.

SFTP:
SSH File Transfer Protocol is based on SSH protocol which provides more security to access the remote servers.
SFTP doesnt exchange data in separate channels but exchanges in packets over a single connection.Data will be transferred in encryption using agreed encryption cipher.

FTP Poller in DataPower:
Step-1:
Go to Objects->Protocol Handlers->Ftp protocol front side handler
Step-2:
Give the name for the handler
Step-3:
Carefully assign required configuration settings
Target Directory: It is specified for giving the target server and directory where the poller will pick the file
Delay Between the polls: It is used to specify time to wait for next polling cycle,time is in milliseconds
Input File match pattern: It is used to specify the regular expression to let poller know which file it has to pick up from the directory

If you choose off for Generate Result file pattern it will enable two required options
Processing Seize Timeout: It is used to specify the time to wait before processing the file that is already in processing state

Processing Seize Pattern: PCRE expression to find which files are in being processed state but not completly processed.
XML Manager: Assign it to an XML manager where it carries the maximum file size settings and User agent which controls the authentication information of FTP servers and client policies.

PG which will be enabling the poller to start the file transfer process.

SSL proxy in DataPower

Secure socket layer is a security enhancement to to establish the encrypted communication between web browser and web server. Lets see the difference between http and https protocols before going to SSL proxy configuration.

HTTP:
Hyper text transfer protocol is application level and stateless protocol which is used for data transmission over world wide web.The three main features are it is connection less,media independent and stateless.
HTTPS:
Hyper text transfer protocol secure is the secure version of HTTP. HTTPS will encrypt the session with the digital certificate.The secure socket layer is the sub-layer which is used under regular http.SSL will encrypt and decrypt the information passed with the public and private keys.All the websites which are needed to transfer the sensitive data will use this protocol to avoid man-in-middle attacks.
SSL proxy profile:
SSL proxy can be assigned to web service proxy,multiprotocol gateway or web application firewall when you need to secure the communication between the clients,service and the remote server.Crypto profile objects in the ssl proxy will define the way of communication.
Steps to create the SSL Proxy
· Open object->crypto configuration->SSL proxyo profile
· Name the proxy

· SSL direction: to secure communivation with requesting clients then it is reverse ssl,to secure the commincation with remote server it is forward ssl,to secure both client and remote server communication it is both

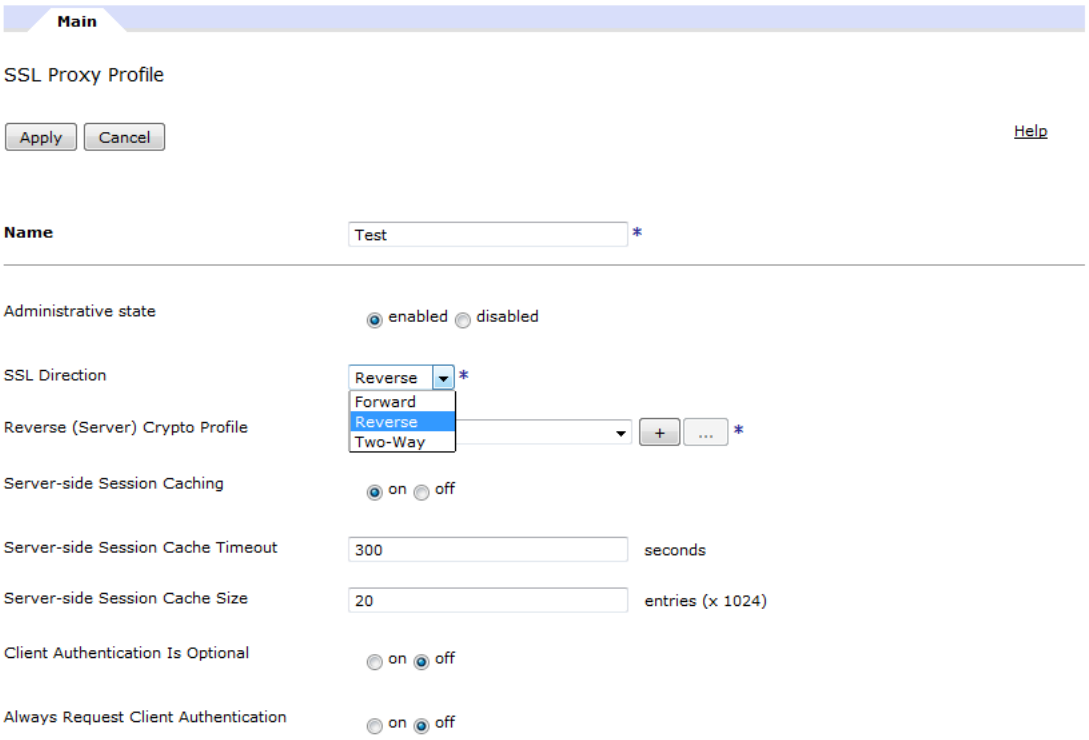
· Create a crypto profile which holds the validation and identity credentials

1. Name the profile
2. Identity credentials uses the crypto key and certificate to use identify itself to the remote server which authenticates the user
3. Validation credentials uses the crypto certs and which authenticates the certificate sent by remote server
4. Leave the rest of the options as default

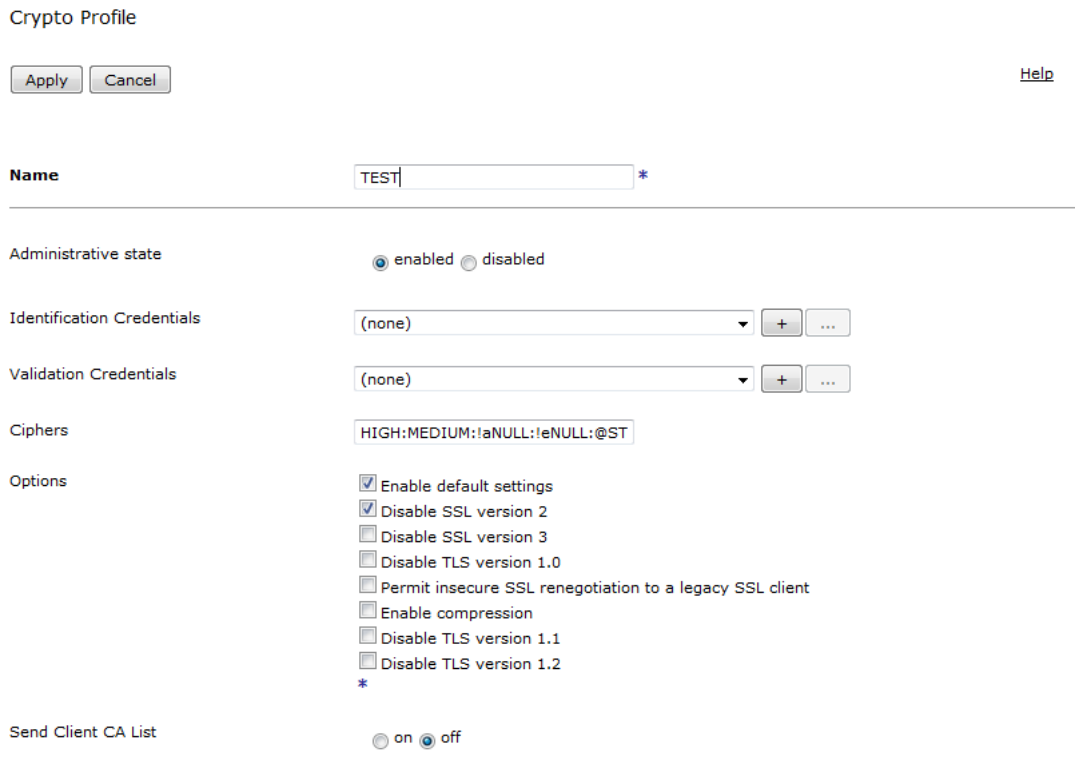
· You can leave rest of the options as defaults

Assign this to the gateway or procy or firewall object to enable the communication over ssl.

SSL Proxy profile



Crypto profile:



"Network Error (Connection hangup) on Back interface"-Solution

In DataPower firmware version 7 most of the SSL proxy profile objects have been affected with the titled error. All the certificates are validated even though you would see the Connection Hangup error. The main reason for this error is,

·Crypto Profile object in DataPower have the series of open SSL options which modify the behavior of SSL hand shake,

·From version 7 DataPower supporting the TLS v1.1 and 1.2 protocols. As we all know SSL is being replaced by TLS due its high security, but most of the servers are still using the combination of SSl v3.0 and TLS 1.0 for the SSL negotiation.

·There are explicit options available on the crypto profile object to disable the TLS v1.1 and 1.2 if these options not checked then the SSL handshake will take the highest security protocol TLS 1.1 or TLS 1.2 by default and cannot complete the SSL handshake due the server was expecting the SSL v3 and TLS 1.0.

Solution: Check the Disable TLS v1.1 and TLS v1.2 options. By default they were enabled. If the server is configured with TLS v1.1 and v1.2 capability then you wouldn't find this issue at all.