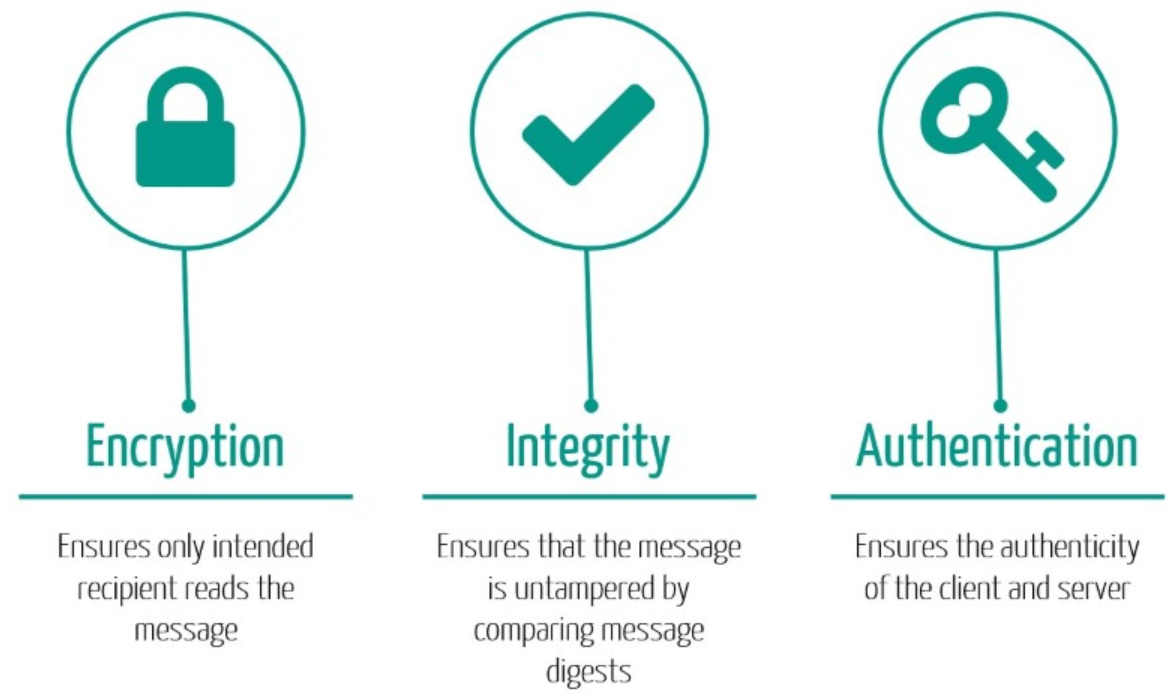
**Weblogic SSL, Keystore & Certificate**

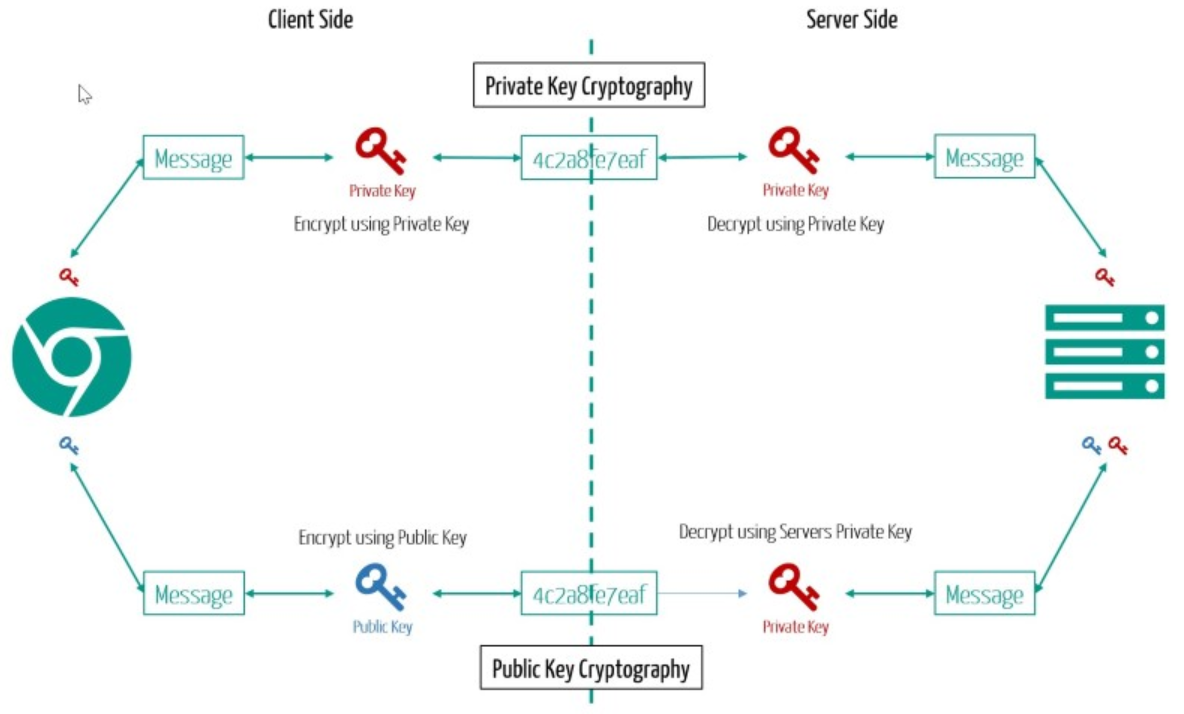
**Agenda:**

* SSL and Keystores Overview
* SSL & Its Capabilities

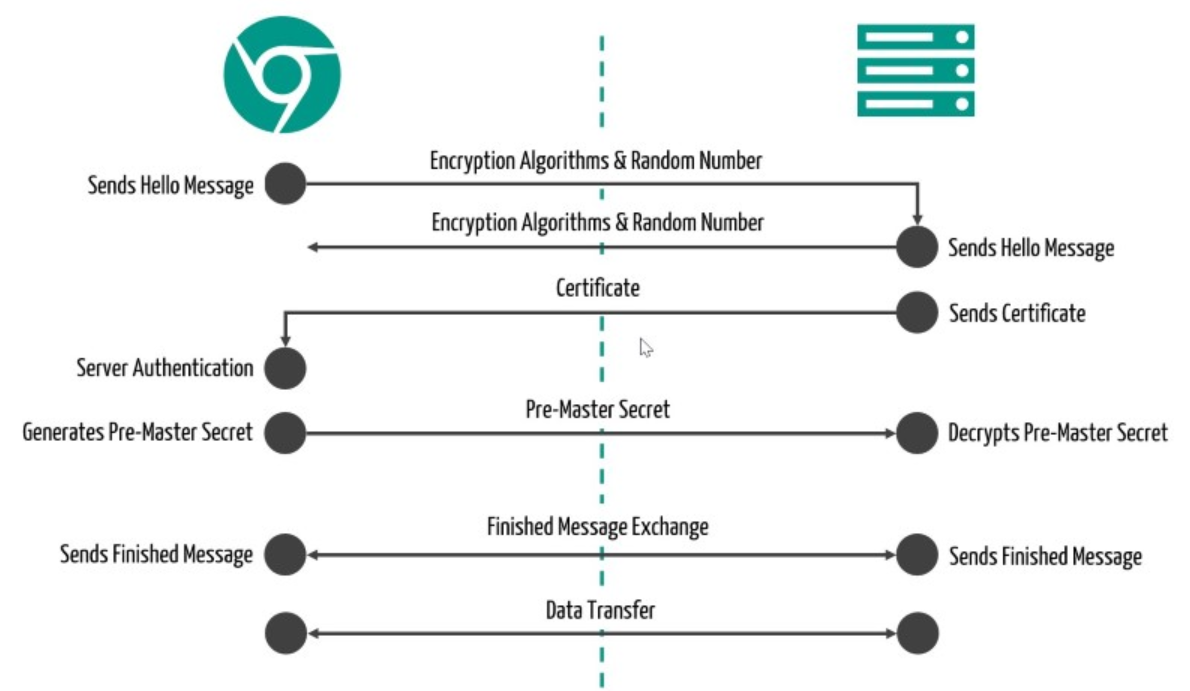
SSL is an industry standard for securing communications between client and server (In most cases it will be between your browser and the webserver)



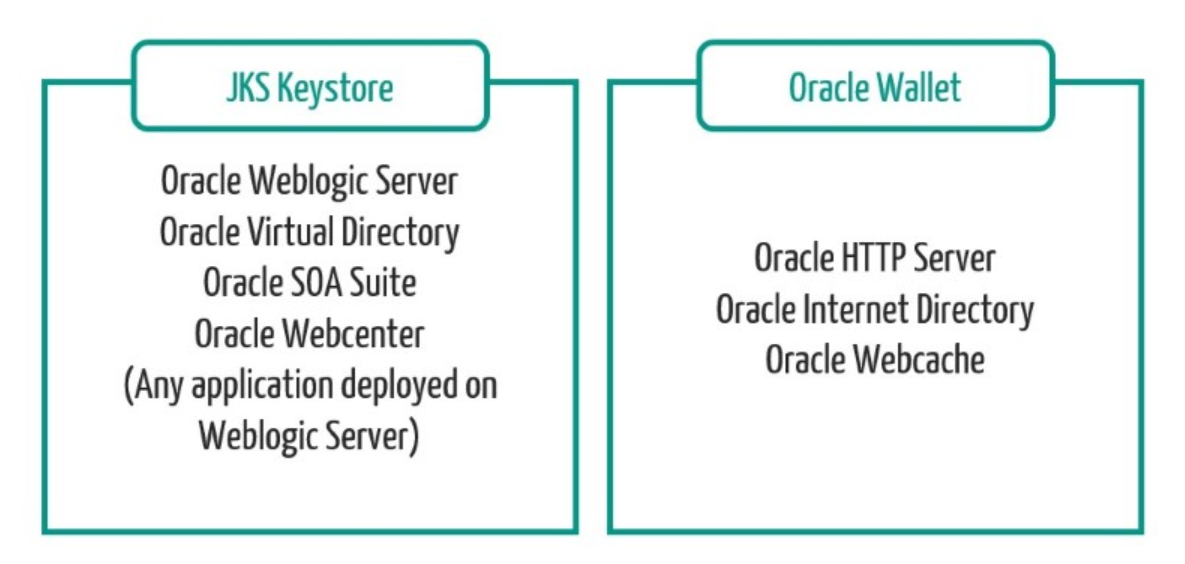
* Public & Private Key Cryptography



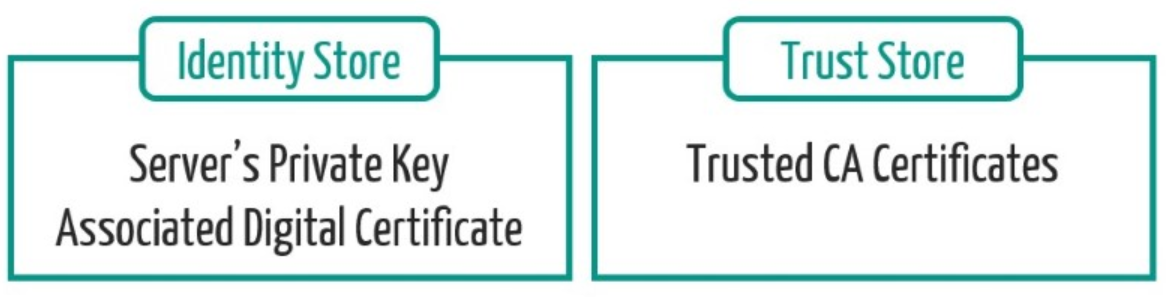
* SSL Handshake Request Flow



* Keystore Providers

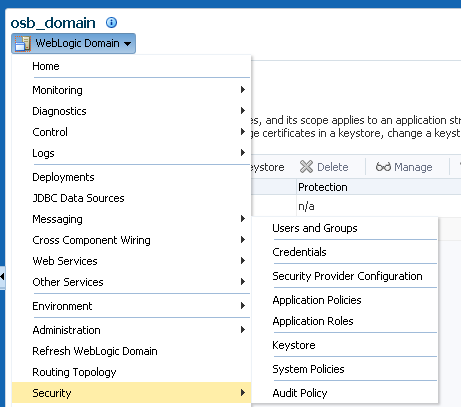


* Keystore Types



**Keystore Creation Using EM Console**

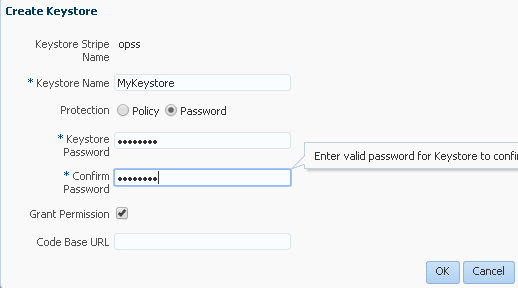
1. Login to Fusion Middleware EM Console using below URL and Weblogic administrator credentials
2. Navigate to Weblogic Domain -> Security -> Keystore:



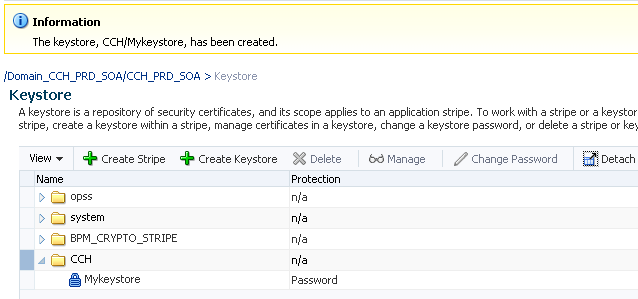
1. Click Create Keystore button



1. Provide new Keystore details and click OK

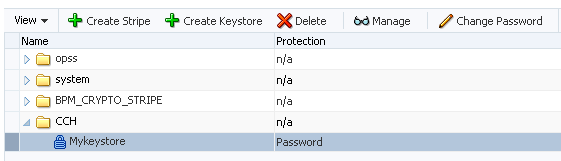


1. Verify new Keystore under your stripe:



**Keypair & CSR Creation Using EM Console**

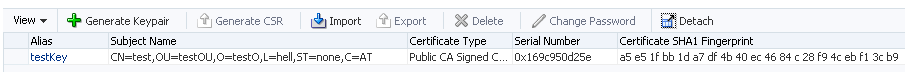
1. Select the new Keystore and click Manage:



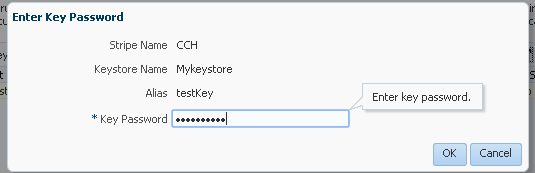
1. Click Generate Keypair which creates a public-private keypair



1. Provide details for your new keypair and click OK. Verify the new keypair details. Select it and click Generate CSR to generate a Certificate Signing Request



1. Provide password when prompted

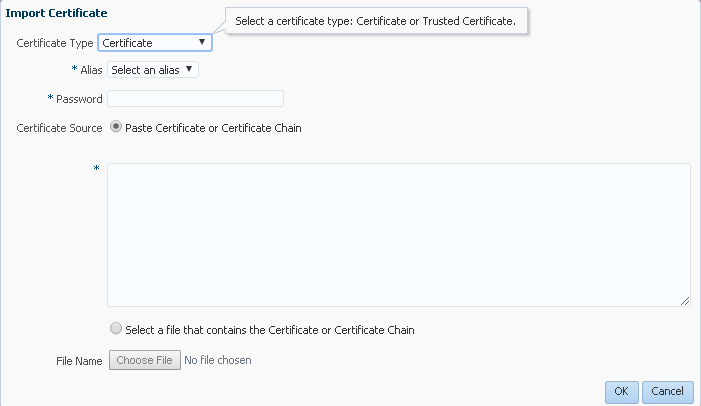


1. Copy the CSR content or export it to local machine to send it to third party Certificate Authority who will provide with a digitally signed certificate and trust certificates



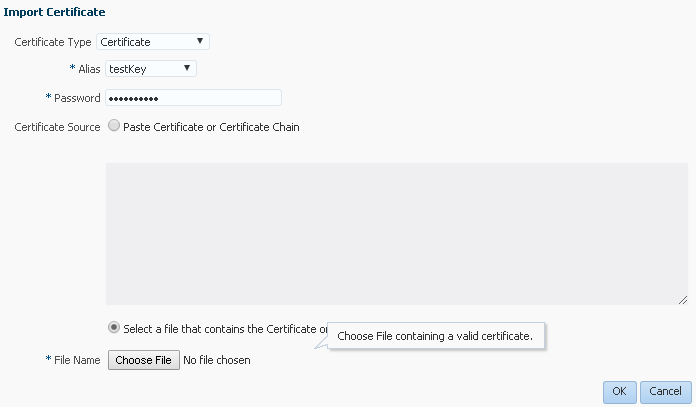
**Import Certificates Using EM Console**

1. Select alias on click Import on EM Console. Provide Keystore password when prompted



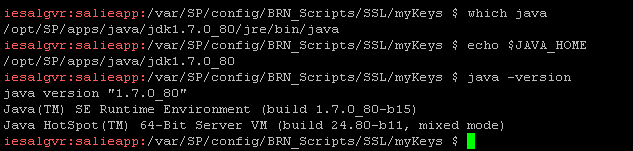
1. Provide details of the received certificates and click OK:

* Select either Trusted Certificate or Certificate depending on the type of certificate you are importing
* Select the alias from the drop down. Please select the same alias used while generating the CSR
* Provide the password for your Keystore
* For Certificate Source, you can either paste the certificate content directly or select the file received from the CA

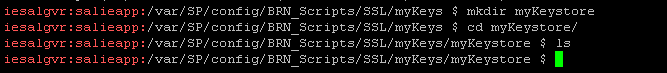


#### Keystore Creation Using JAVA Keytool

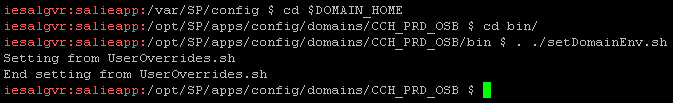
1. Keytool is a key and certificate management utility which comes with JDK
2. Make sure JAVA executable is added to PATH environment variable



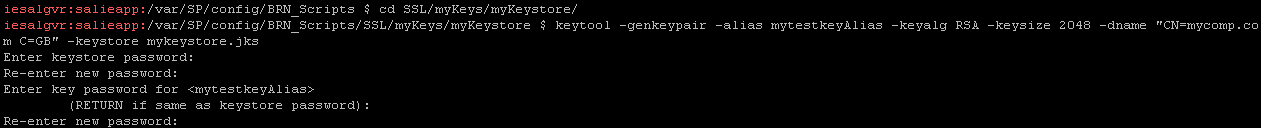
1. Create a directory to store your keystores



1. Navigate to DOMAIN\_HOME/bin and set domain environment variables

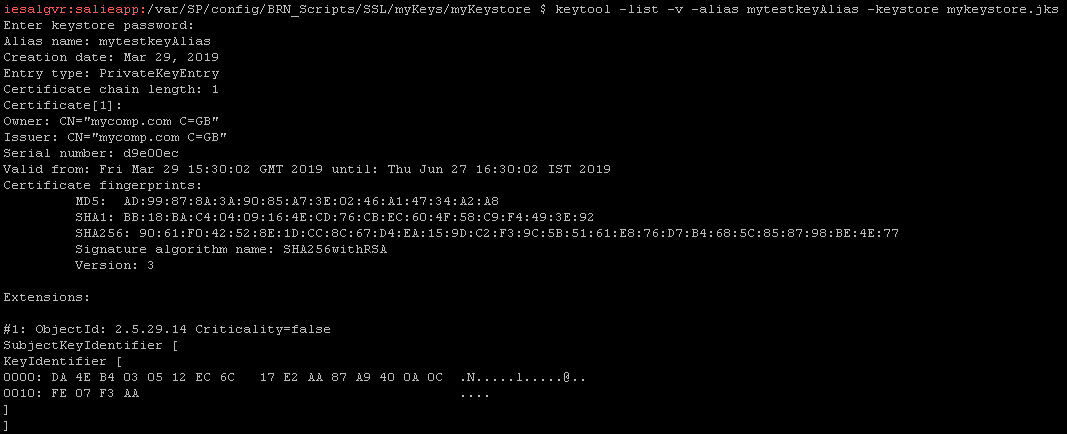


1. Navigate to the keystore directory created earlier and execute keytool command to create a keystore. Provide required passwords when prompted



**Command**: **keytool -genkeypair -alias mytestkeyAlias -keyalg RSA -keysize 2048 -dname "CN=mycomp.com C=GB" -keystore mykeystore.jks**

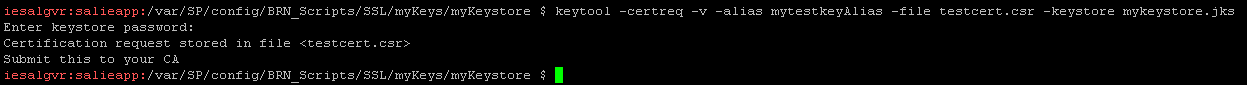
1. Make sure mytestkeystore.jks file is created. The details of the keystore can be viewed using below command



**Command:** **keytool -list -v -alias mytestkeyAlias -keystore mykeystore.jks**

**CSR Creation Using JAVA Keytool**

1. Make sure JAVA executable is added to PATH environment variable & domain environment is set as mentioned in above section
2. Navigate to the keystore directory and execute below keytool command to generate CSR



**Command: keytool -certreq -v -alias mytestkeyAlias -file testcert.csr -keystore mykeystore.jks**

1. This is the CSR file generated



**Import Certificates Using JAVA Keytool**

1. Make sure JAVA executable is added to PATH environment variable & domain environment is set as mentioned in above section
2. Navigate to the keystore directory and execute below keytool command to import Root / Trust Certificates received from CA
   * Cacert : Name of CA’s signed public certificate
   * Cacert-alias : Alias of CA’s signed public certificate
3. Navigate to the keystore directory and execute below keytool command to import Server Signed Certificates received from CA
   * mytestalias : Alias of the keypair used while generating the CSR
   * server\_signed\_cert : Server Signed Certificate received from CA

**Weblogic Keystore Configuration using Administration Console**

1. Login to Weblogic Administration Console using below URL and Weblogic Admin Credentials
2. Navigate to Environment -> Servers -> ServerName -> Configuration -> Keystores. By default DemoTrust and DemoIdentity stores will be used
3. Click on Change button. Select “Custom Identity and Custom Trust” and click Save
4. Provide details of the Custom Keystore
   * For Oracle Keystore Service (KSS), ie the Keystore created using EM console
     + Custom Identity Key Store : kss://system/MyTestKeyStore
     + Custom Identity Key Store Type: kss
     + Custom Identity Key Store Passphrase : Keystore Password
     + Confirm Custom Identity Key Store : Confirm Keystore Password
   * For JAVA Keystore Service (JKS), ie the Keystore created using JAVA Keytool

* Custom Identity Key Store : /u01/app/oracle/product/fmw/mykeystore/mytestkeystore.jks
* Custom Identity Key Store Type: jss
* Custom Identity Key Store Passphrase : Keystore Password
* Confirm Custom Identity Key Store : Confirm Keystore Password

If you are using same Keystore for Trust and Identity, provide same details in both Trust and Identity sections. If you are using different Keystores (preferred method in production environments), provide respective Keystore details

Save and activate the changes. Restart the Managed / Admin server where ever Keystore changes have been done