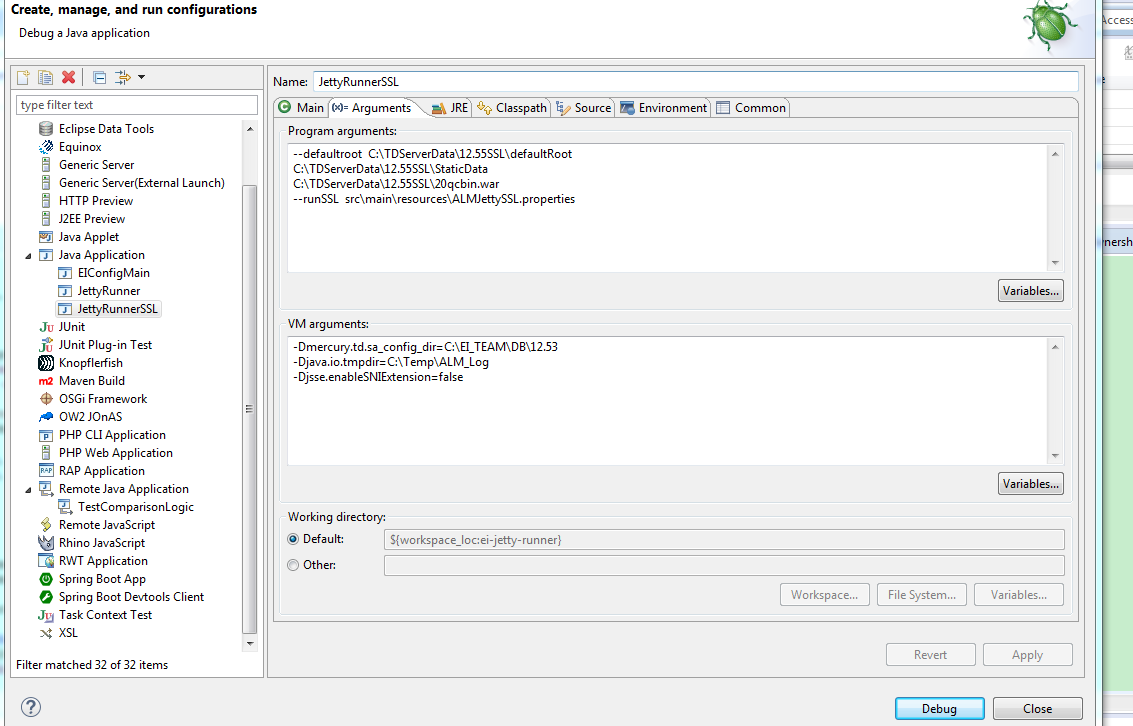
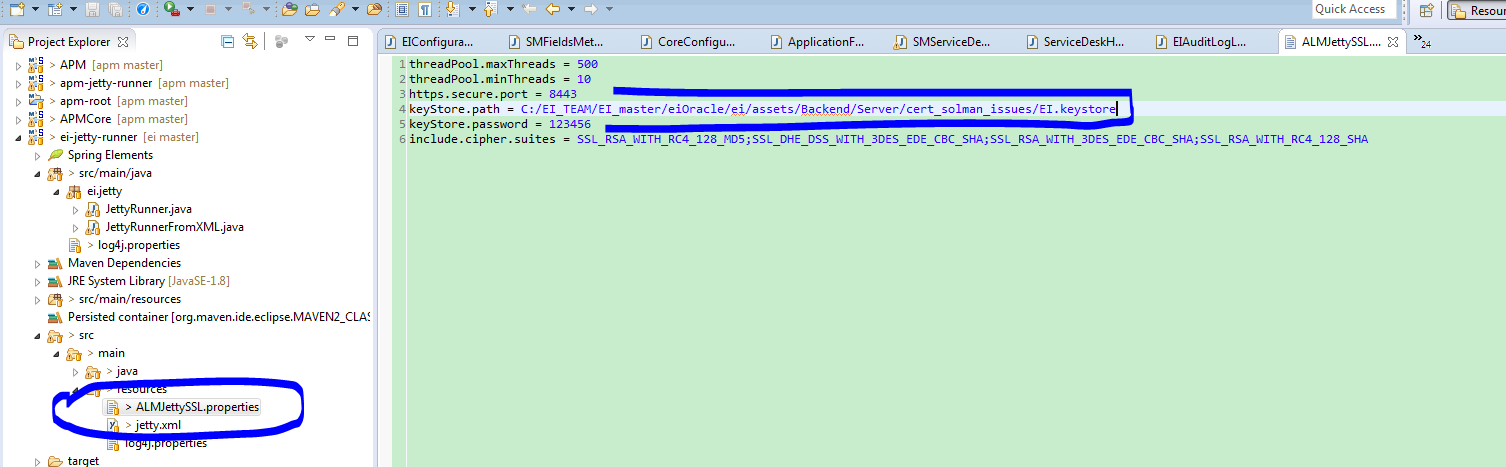
**Part 1: start ei-jetty-runner with SSL mode**

there are an additonal argument you need to add.

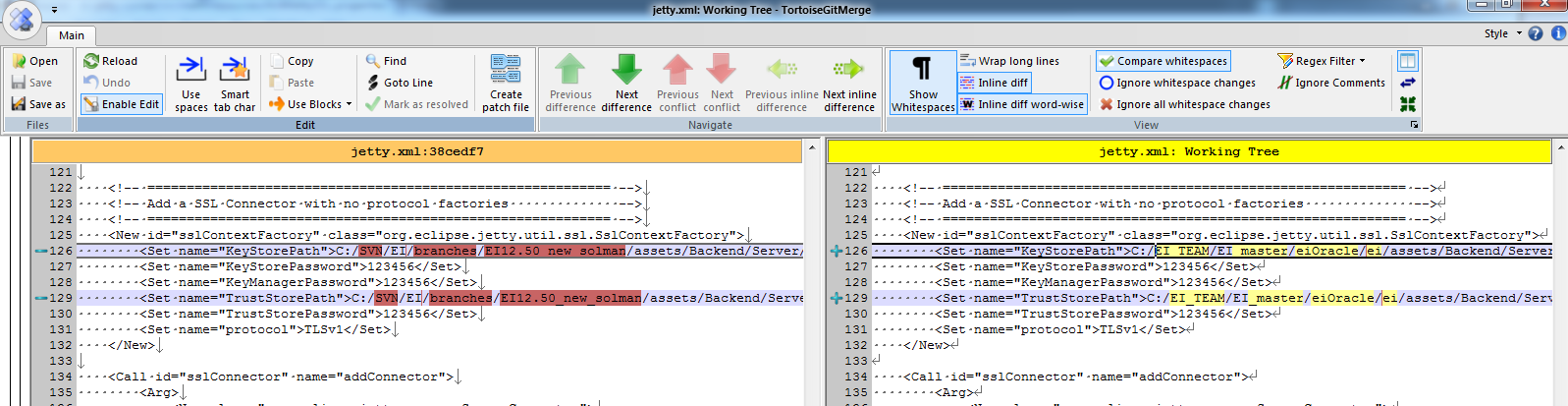
--runSSL src\main\resources\ALMJettySSL.properties



in ALMJettySSL.properties file, there are keystore.path you need to configure with right path like the following snapshot



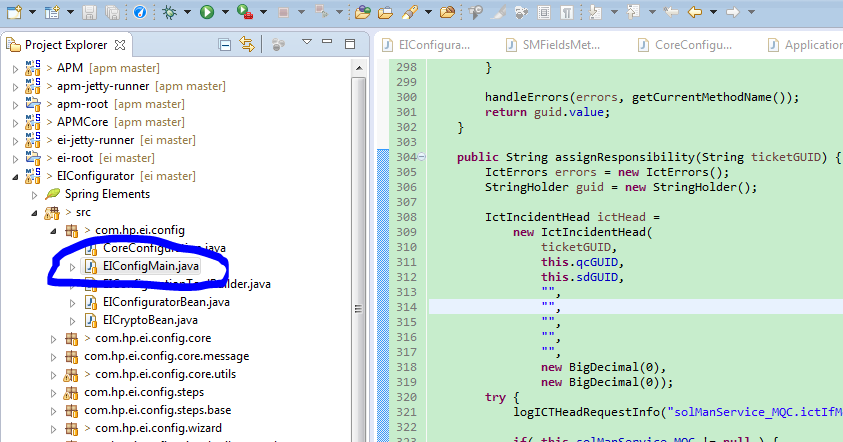
in Jetty.xml file you also need do some changes. Change KeystorePath and TrustStorePath with right value.

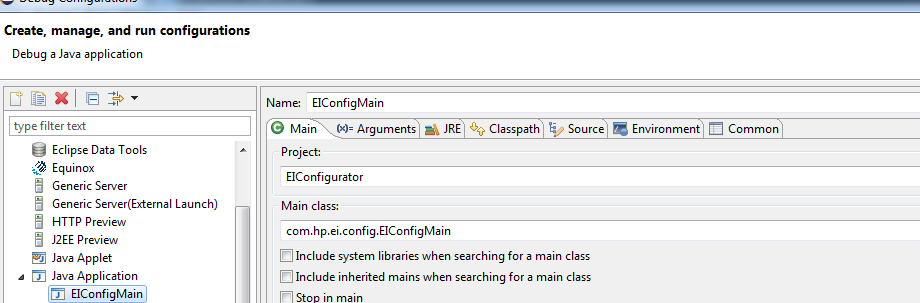


then you can run ei-jetty-runner with SSL mode

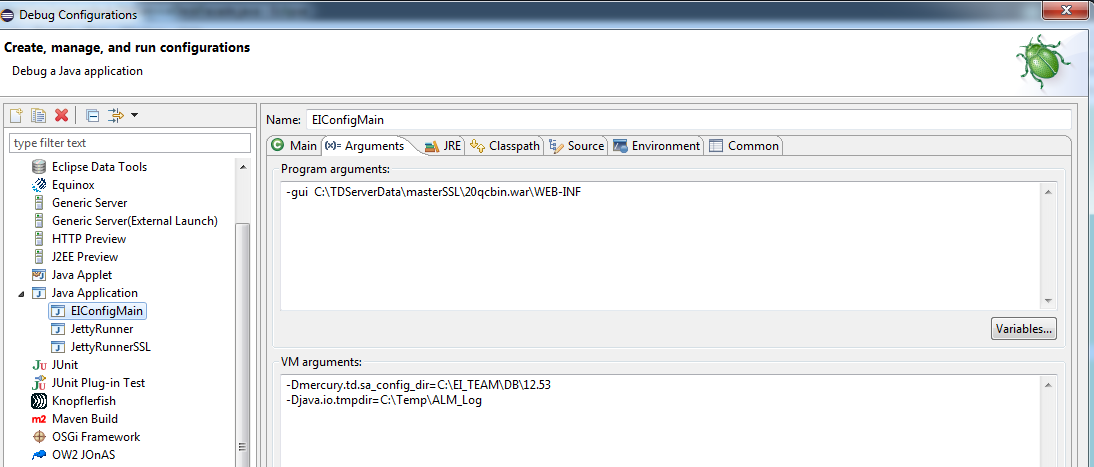
**Part 2: config dev SSL+SAML mode.**

**need to run EIConfigmain. the following snapshot is about how to run EIConfigurator in dev environment.**



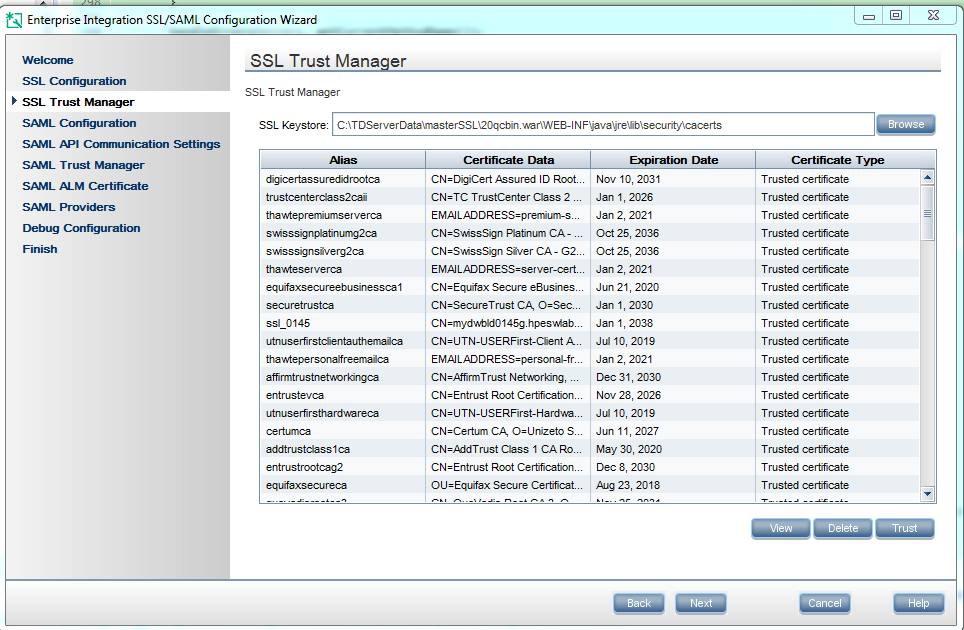


in the agruments is about the 20qcbin.war path you config when you configure ei-jetty-runner . VM arguemnts is about SiteAdmin.xml path you configuree in JettyRunner

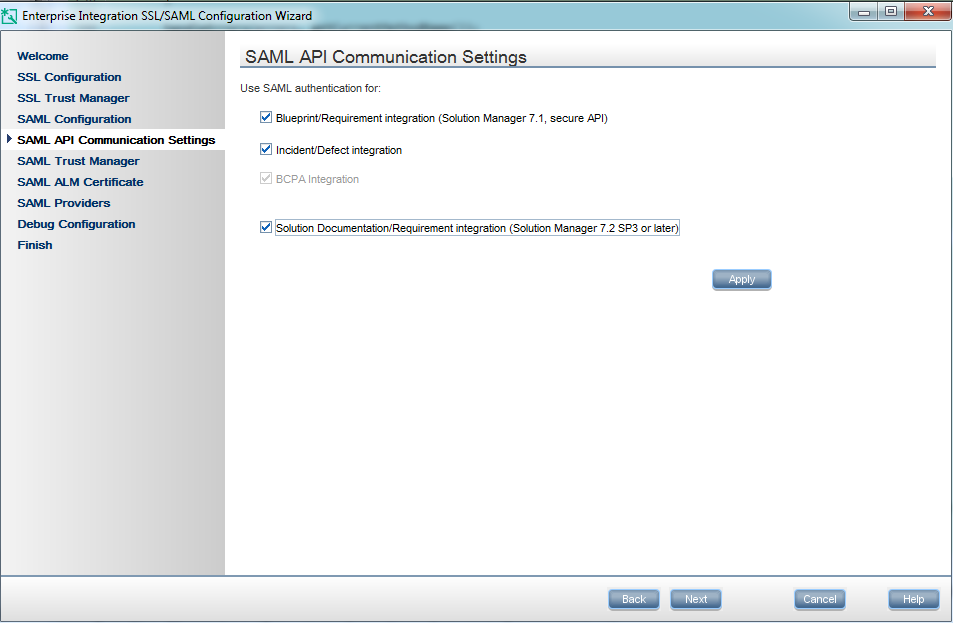


there is one file named: **Configuration of EI.xmind** you need to install XMindPro to open it. in this documentation,there are some all steps about how to config SSL+SAML mode.

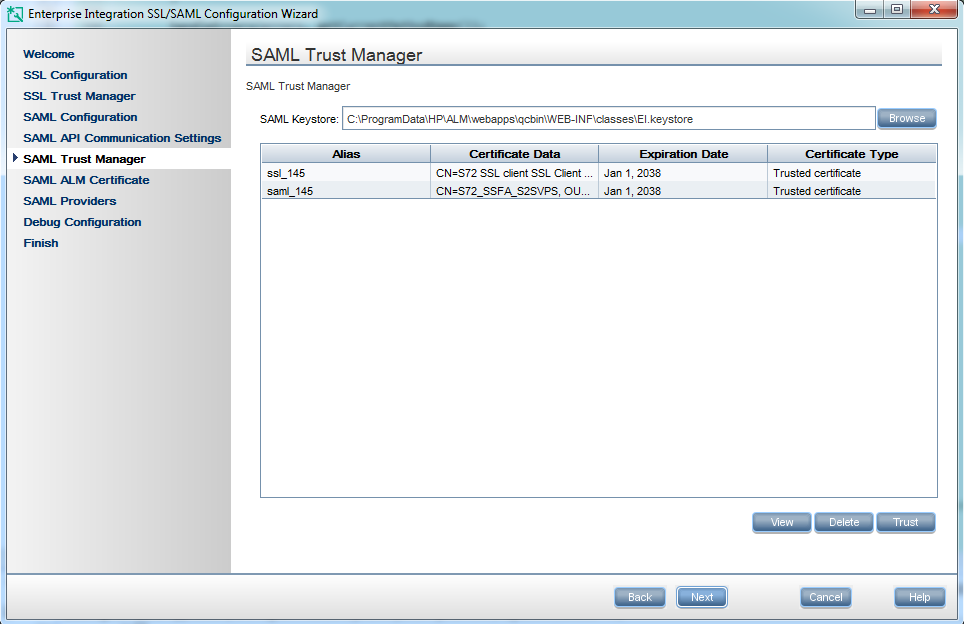
1: after running EIconfigurator like the following snapshot,trust solman SSL.



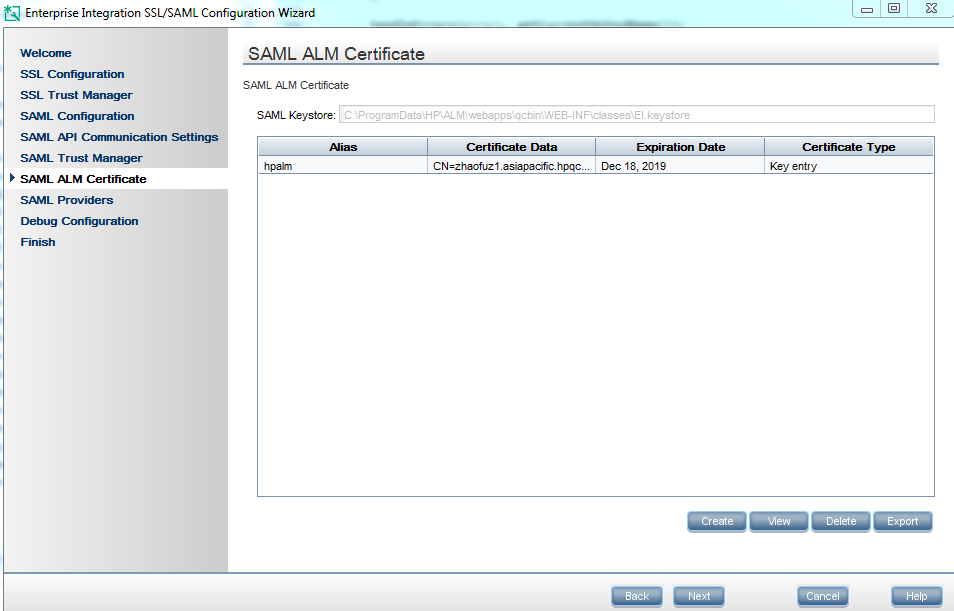
2: enable SAMLmode for blueprint defect and so on. click apply button.



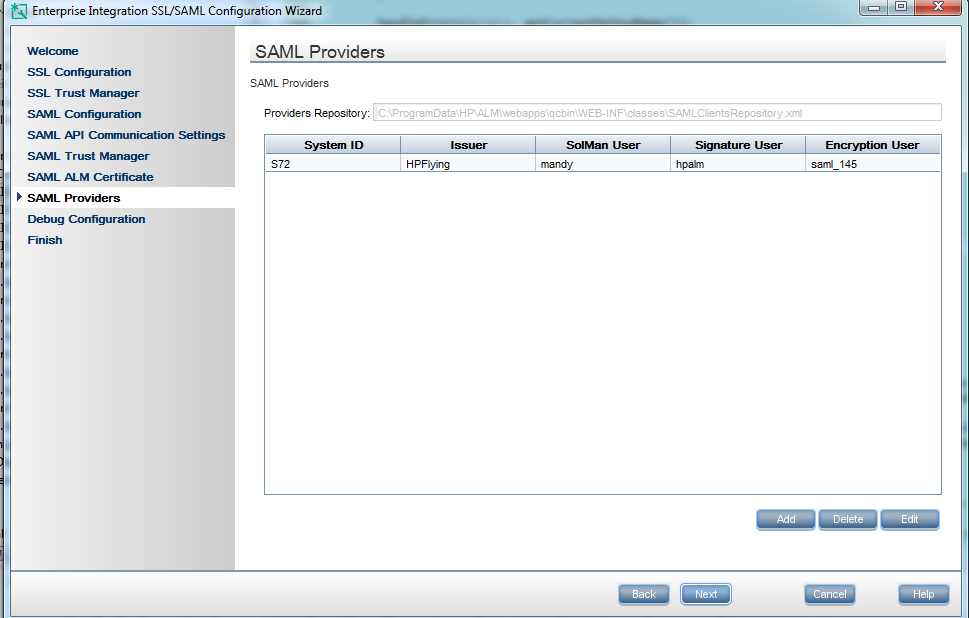
3: Trust Solman's exported SAML certificate.



4: create ALM SAML certificate and export it out.

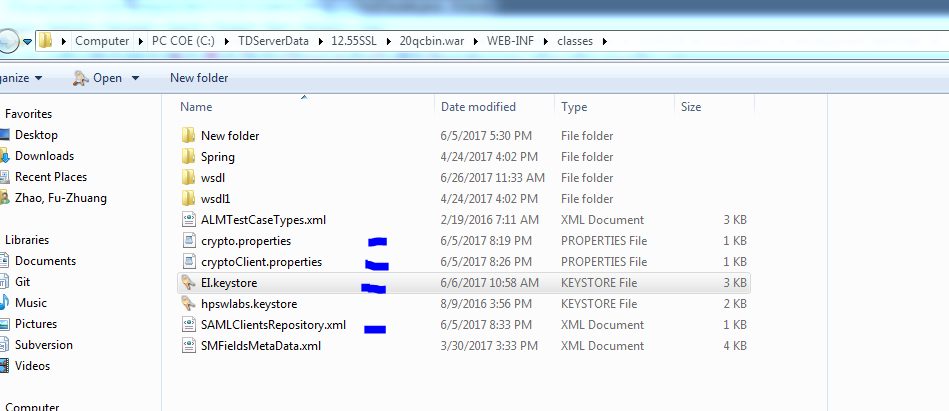


5: Add providers: the Issuer name shoud be same with SAML2 transaction's provider you added.



After finish all those steps, you will find some files you created or modified in -gui **arguments path\classes. like** C:\TDServerData\12.55SSL\20qcbin.war\WEB-INF\classes

you need to copy that four files to your code path: like: C:\EI\_TEAM\EI\_master\eiOracle\ei\assets\Backend\Server\cert\_solman\_issues



<https://rndwiki.corp.hpecorp.net/confluence/display/UFT/Secure+API+Configuration+Guide>

In dev environment. when config \*TESTRESULT\* in soamanager. set the bindingname with **AGS\_SM\_TESTRESULT\_API Not**

**AGS\_SM\_TESTRESULT\_API\_SAML**

**Then config in SPRO. config corresponding parameters.**

**copy SAMLClientsRepository.xml to**

**SAMLClientsRepository.class compile file path target/..../**

**copy clientRepository.xml and other files to the right place in code folder near SMFieldsMetaData.xml**

**replace cxf-rt-ws-security.jar in .m2 with corresponding file in code path, search by everything.**

**create keywords in Strust transaction.**

**don't forget replace accerts file to java/security/accerts**