Thu 4/25/2019 1:21 PM

RE: TPM Integration and installation.

Hi Sasi,

Thanks for joining the call.

**Please find the list of points discussed in the call:**

1. Create a **utility** :
   1. to connect to the TPM and extract the EK pub key and store it [encoded format] into a particular file [pub.key]
   2. to encrypt the [DB and binary jar] symmetric key using EK pub key {which would be decrypted with in the application using the TPM EK private key}.
2. **Operator** should send the pub key to the admin person to get it inserted into the db.             - Need to discuss with Nasir and John.
3. In **machine\_master** table, should have the facility to hold the pub key instead of mac id.           - Need to discuss with Nasir and John.
4. Once the user logged into the machine [with online service], the initial master sync  to be triggered with **“pub key” in the request**. The same should be validated by kernel service while providing the master sync response.
5. We need to find the method to convert the **ASNEncoded** format to the X509 format [identify the ByteorderMark]
6. Signature validation for the all the requests from client application to be implemented at server end using the client specific pub key.   – **V2 Scope**
7. We need to use the **OpenJre** instead of Oracle jre as there could be so many license and policies are involved with respect to country.      -
8. **JRE** can be bundled part of initial setup and same can be choosen during bundle creation. Could would update the required policy in the jre and release the same part of bundle.

Thanks

R Karthik

**From:** Karthik Ramanan   
**Sent:** Wednesday, April 24, 2019 3:33 PM  
**To:** SasiKumar Ganesan <[gsasikumar@gmail.com](mailto:gsasikumar@gmail.com)>  
**Cc:** Gayathri Krishna Kumar <[Gayathri.KrishnaKumar@mindtree.com](mailto:Gayathri.KrishnaKumar@mindtree.com)>; Omsaieswar Mulakaluri <[Omsaieswar.Mulakaluri@mindtree.com](mailto:Omsaieswar.Mulakaluri@mindtree.com)>; Shravan Poorigali <[Shravan.Poorigali@mindtree.com](mailto:Shravan.Poorigali@mindtree.com)>; Balaji Sridharan <[Balaji.Sridharan@mindtree.com](mailto:Balaji.Sridharan@mindtree.com)>; Ramesh Narayanan <[ramesh@mosip.io](mailto:ramesh@mosip.io)>; John David Panneerselvam <[John.Panneerselvam@mindtree.com](mailto:John.Panneerselvam@mindtree.com)>; Nasir Khan <[Nasir.Khan@mindtree.com](mailto:Nasir.Khan@mindtree.com)>  
**Subject:** RE: TPM Integration and installation.

Hi Sasi,

              We have extracted the **TPMT\_Public** part has encoded byte and signed the data using **private key** and used the public key to validate the sign by another instance. It works fine.

**Note:** While **validating the signature** we are using the TPM libraries without having connection with the TPM. We will be using the same at server component while validating the signature.

As of now, the every individual machine id [ie: mac id] is first stored into the admin db. Whenever the sync request goes from client application, the mac id would be sent. If the mac id is present at the server db then it will allow the further process. otherwise it would reject the request.

Since Registration client is going to send the machine’s ***public key*** instead of mac id [for sync service call], the server will validate the key against DB and provided success response.

The size of public key part comes around 500 characters.

Kindly confirm our understanding whether shall we proceed with sending of ***public key*** in the **request while doing data sync from server to local**.

Thanks

R Karthik

**From:** Karthik Ramanan   
**Sent:** Tuesday, April 23, 2019 1:18 PM  
**To:** SasiKumar Ganesan <[gsasikumar@gmail.com](mailto:gsasikumar@gmail.com)>  
**Cc:** Gayathri Krishna Kumar <[Gayathri.KrishnaKumar@mindtree.com](mailto:Gayathri.KrishnaKumar@mindtree.com)>; Omsaieswar Mulakaluri <[Omsaieswar.Mulakaluri@mindtree.com](mailto:Omsaieswar.Mulakaluri@mindtree.com)>; Shravan Poorigali <[Shravan.Poorigali@mindtree.com](mailto:Shravan.Poorigali@mindtree.com)>; Balaji Sridharan <[Balaji.Sridharan@mindtree.com](mailto:Balaji.Sridharan@mindtree.com)>; Romila Mattu <[Romila.Mattu@mindtree.com](mailto:Romila.Mattu@mindtree.com)>; Resham Chugani <[Resham.Chugani@mindtree.com](mailto:Resham.Chugani@mindtree.com)>; Vivek Srinivasan <[Vivek.Srinivasan@mindtree.com](mailto:Vivek.Srinivasan@mindtree.com)>  
**Subject:** RE: TPM Integration and installation.

Thanks for joining the call.

Please find the list of points discussed in the call.

1. **EK public key** will be sent to the server, through the existing ‘SyncData [MasterSync]’ service after user’s successful login [with online connectivity].
   1. Sync service will accept this key and store it into the existing table where the machine detail is stored.  – **need to discuss with DB and Kernel team to get their concurrence**.
   2. All the request from client machine, should be signed with the TPM private key.
2. **EK public key** – **[backup plan]**
   1. Encrypt the db and jar keys using this public key and write the same into the local client properties.  When the application started, get the respective private key from TPM and decrypt the same to connect to the database and unencrypt the jar.
3. **AES – Symmetric key** –>
   1. This key [db and jar] should be loaded into the local TPM.              - currently dev team is facing problem to store the key into TPM. Code should be shared with Sasi for further support.
4. **Currently for V1 release**, we will not make any major changes at Server modules [Pre. Reg, REg processor and IDA] to validate the signed request sent by the client application.

Thanks

R Karthik

99628 20585

-----Original Appointment-----  
**From:** Karthik Ramanan   
**Sent:** Tuesday, April 23, 2019 12:21 PM  
**To:** SasiKumar Ganesan; Omsaieswar Mulakaluri; Shravan Poorigali; Balaji Sridharan  
**Cc:** Gayathri Krishna Kumar  
**Subject:** TPM Integration and installation.  
**When:** Tuesday, April 23, 2019 12:30 PM-1:30 PM (UTC+05:30) Sri Jayawardenepura.  
**Where:** Conference Bridge : 1800 120 1331 / 7045671331 Guest code :  4219789#

**Guest code update >>>**

**Conference Bridge** : 1800 120 1331 / 7045671331 Guest code :   4219789#

Hi Sasi,

Kindly join this call to discuss about the following points:

* How do we store the EK public key into the Server [New machine / old machine key update]? Is there any UI to be developed in Admin portal to update key in server?
* Approach to sign the individual request from Registration client.  Whether **all** the requests from TPM client to server should be signed and validated by Server component?
* Need to finalize the approach to manage [Generate, download, store and replace] the Session key [Symmetric key] for **derby DB data encryption** and decryption [at local machine].
* Need to finalize the approach to manage  [Generate, download, store and replace] the Session key [Symmetric key] for **binary jars encryption** and decryption.
* We have already tried with ***LoadExternal*** method, but we are unable to load the Symmetric key into TPM. We will discuss about the same.
  + Exception in thread "main" tss.TpmException: TPM Exception: {AUTH\_UNAVAILABLE}

    at tss.TpmBase.DispatchCommand(TpmBase.java:383)

  at tss.Tpm.EncryptDecrypt(Tpm.java:491)

at samples.Samples.symmetricKeyInsertion(Samples.java:679)

at samples.Samples.doAll(Samples.java:129)

* Which feature should be considered as Vital, Essential and Desired?
* Run through the Initial setup and update process.

Thanks

R Karthik

99628 20585