Security 2.0 Remaining Core Items 1-26-15

ID	Assessment For 15.04				Feature	HLD Section	Notes	Design	Status
	Team Initial Review	Microsoft	QCE	Technicolor					
1	Y	Y	N	?	Guild Equivalence	2.6.1	QCE: Recommend punt. This does not change the wire protocol Can become part of policy, but client needs to interpret this correctly	As described in section 2.3.9 of the HLD rev 1.6: An admin can add a guild equivalence certificate to the application so the membership certificates issued by other certificate authorities (like friends) can be trusted. These certificate holders would only have access to permissions assigned to that specific guild. **However, we have not work out the details on how the local device trusts the guest's device during ECDSA key exchange. We still need additional design discussion on this topic.**	Not Implemented
2	N	N	N	N	User Equivalence	2.5.3 in V1.3 of HLD and removed in newer versions	Technicolor comment: Scenario is not clearly defined in HLD, but should be supported by client. QCE reponse: Because the section 2 was in progress, when it was updated with the X.509 information (as of version 1.4), the User Equivalence is taken out because it is not clearly defined.		Not Implemented.
3	N	N	N	N	Out-of-Band claiming	2.3.1.2	Negotiation to use OoB vs. always-accept Need way to determine if you need a pre-shared key If pre-shared key is chosen, the security mangager needs to understand how to share the key NOTE: The current core codes support using ECDHE_PSK in addition to ECDHE_NULL . The app developer must provide the OOB PSK to the core layer in an AuthListener callback		Not Implemented
4	Y	Y	N	?	Certificate revocation	2.3.9	QCE : Believes secure expiration may be better - recommend punt. This may further design and, since it is an optional service, that there is no backwards compatability. This requires further discussion. Technicolor: states this is risk of backward compatibility issues	As described in section 2.3.9 of the HLD rev 1.6: The application will validate the certificate using a revocation service provided by the Security Manager. The Certificate Revocation Service is expected to provide a method call that takes in the certificate and return whether the given certificate is revoked. The application looks in the “self” section of its installed policy for the peer that provides the Certificate Revocation Service. If the application can’t locate any of the Certificate Revocation Service, the certificate revocation check will be skipped. **As the result, the certificate revocation check is not deterministic. Sometimes it does the check, sometimes it does not. Need design to reduce response time in service discovery of the Service Revocation Service in the local network as well as the certificate revocation call during session setup.**	Not Implemented.
5	N	N	N	N	Manufacturer certificates (Symantec)	Not defined in HLD	Extend PermissionMgmt interface with method to retrieve certificate Announce its availability in the NotifyConfig signal Waiting for Brian Witten’s proposal. Development includes an API change to allow for app developer to install the certificate. Multiple bindings supports (C/C++, Java, Objective C/IOS) QC recomends pushing to future release		Not Implemented
6	N	N	N	N	Policy templates	2.5.3	Policy templates are implemented as the PermissionConfigurator::SetPermisionManifest() Policy templates should be different than manifests Templates could be downloaded by Security Manager similar to manifest descriptions (easier on thin clients, can be updated, internationalization, …) <- **QCE states: This is the intention.** **In this case there is no impact for core or compatibility issue**. Technicolor asks: Does the client support this kind of certificate? Does the client check that the rights of a membership certificate are a subset of the delegated rights? **QCE answers: The manifest serves a guidance to the Security Manager. The permission module does not validate or enforce it until the rules listed in the manifest become rules inside the installed policy or membership certificates.**		Not Implemented

7	Y	N	Y	Y	Accepting identity certificate chain to allow the use case of a son claims his own smart device and use that device to control other devices in the local network that he does not claim.	2.7.4		The IntallIdentity will accept an identity cert chain. The GetIdentity will return an identity cert chain This change would allow for different people in the home can admin for their own set of devices while these devices can trust other devices inside the local network as long as any of the cert in the identity cert chain is signed by a root of trust known to each device.	Effort underway
8	Y	N	Y	Y	The current policy design does not allow for an application to be told to only send a method call to a particular peer or a particular guild	defined in 2.4.2 but was eliminated by the new design of authorizationdata	An example mentioned in meetings but not described in the HLD is the use case of an alarm system that needs to check smoke detector that belong to the home security guild. The alarm system is not allowed to check any other smoke detector. The new authorization data has eliminated the consumer policy.	replace the terms section of the current policy with two different sections: outgoing -- to control the behavior of the app when it send a message. incoming -- to control the behavior of the app when it receives a message. Refer to section 2.5.2 of the HLD rev 1.6 for more details.	Effort underway
9	Y	?	N	?	Issue with certificate date validity check need time check when we have trusted time	Not defined in HLD	Checking if the cert was revoked may be the ideal option	One idea is to make the appliction to periodically retrieve the real time from a trust source (a service in the local network). This would be done instead of revocation while we take time to consider the optimal way to manage revocation.	Not Implemented
10	N	N	N	N	Issue with certificate date validity check when trusted time is not available	Not defined in HLD	Need agreement and need to update the HLD on the decision on how to do deal with devices with no real time clock QCE recomends punting for future release		Not Implemented
11	N	N	N	N	Additional names for existing key exchange algorithms	3.1	Add some additional names for existing key exchange algorithms as described in the section 3.1 on Crypto Agility		Not Implemented
12	Y	Y	N	?	The PermissionMgmt::InstallEncryptedPolicy still need design decision regarding which key material to use to encrypt the data	To support 2.3.11	QCE: Recommend punt. QCE does not have resources to do this for the first release	As described in section 2.3.10 of the HLD rev 1.6: An admin uses the Security Manager to generate updated policy and membership certificates, encrypt the payload with a session key derived from the some nonce value and the master secret for the <sender, recipient> pair. The package including the sender public key, destination public key, nonce, and encrypted payload is sent to the Distribution Service to delivery to the target. The target uses the information in the package to locate the master secret to generate the corresponding session key to decrypt the payload. Once the decryption is successful, the target signs the hash of the package and provide the signature in the reply. **This change require additional BusAttachment API calls, thus requiring Java and iOS binding changes.**	Not Implemented
13	Y	Y	Y	Y	Delegation	2.3.7	This is not straight delegation but subset delegation Technicolor asks: Does the client support this kind of certificate? Does the client check that the rights of a membership certificate are a subset of the delegated rights?	The message is checked to ensure access is allowed by the rules in all the certs of the given membership cert chain. This eliminates the need to perform a logical diff between all the rules in the membership chain. For the thin client, this would require more memory.	Effort underway
14	Y	Y	Y	?	Hook to replace the default key store implementation.			refactor the current key store code to have the default key store listener to a separate file for linux and windows	