Security 2.0 Remaining Core Items 1-20-15

ID	Must for 15.04	Implemented (Y/N)	Feature	HLD Section	Notes	Status	Total Dev LOE	Calendar Dev LOE
1	Y	N	Guild Equivalence	2.6.1	Can become part of policy, but client needs to interpret this correctly	Not Implemented	2w	1w
2	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. QCE recommend punt for future release	2w	1w
3	N	Y	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	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	?	?
4	Y	N	Certificate revocation	2.3.9	Support in client is a must have. Risk of backward compatibility issues	Not Implemented. 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.	5w	2.5w
5	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	4w	2w
6	N	N	Policy templates	2.5.3	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.**	Policy templates are implemented as the PermissionConfigurator::SetPermisionManifest()	?	?
7	Y	N	Accepting identity certificate chain to allow the use case of a son claim his own TV in this bedroom	2.7.4	Needs to be designed. Discovered when creating the test plan.	Not Implemented	6d	3d
8	Y	N	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.	Not Implemented	6d	3d
9	N	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	Not Implemented	6d	3d
10	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	UNK	UNK
11	N	N	Add some additional names for existing key exchange algorithms as described in the section 3.1 on Crypto Agility	3.1		Not Implemented	6d	3d

12	Y	N	The PermissionMgmt::InstallEncryptedPolicy still need design decision whether which key material to use to encrypt the data	To support 2.3.11	3 days to 2 weeks calendar time depending on which key material to use.	Not Implemented	4w	2w
13	Y	?	Delegation	2.3.7	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?		?	?

Action Items

Techicolor to send details to wg mail list regarding #3
Techicolor to document how security manager will handle #6
Symantec to send technical proposal to wg mail list regarding #5 once TSC approves approach
QCE to make feature matrix for core
Techicolor to make feature matrix for Security manager
Chris to set up technical meetings at 1pm alternate Tuesdays
Chris to send times to core WG mail list about times for security manager call at 8am
Phil to update HLD regarding what happens when trusted time is not available (related to #10)
Phil to send design to Core WG mail list regarding #12
Phil to answer questions posed in #13