Security 2.0 and 2.1 Feature Matrix

ID	HLD	Feature	Version	JIRA ASACORE	CC Date	Interfaces	Contributor	Notes
1	2.3.1.1	Claim factory-reset device without out-of-band registration data	2	1446	done	PermissionMgmt::Claim	QCE	
2	2.3.1.2	Claim factory-reset device using out-of-band registration data	2	1447	done		QCE	No work required in Core. Responsibility for the Security manager and/or app developer to use either PSK or NULL. Action: Need to discuss best practice for Security manager and/or app developer to use either PSK or NULL Need to consider 2.1 feature for core to manage pre shared keys. This will require design discussions.
3	2.3.3	Example of building a policy	2	1448	done	PermissionPolicy object	QCE	QCE: Built object. Responsibility of security manager to write the UI
4	2.3.4	Install a policy	2	1449	done	PermissionMgmt::InstallPolicy	QCE	
5	2.3.5	Add an application to a guild	2	1450	done	PermissionMgmt::InstallMembership, PermissionMgtm::InstallMembershipAuthData	QCE	
6	2.3.6	Add a user to a guild	2	1451	done	PermissionMmgt::InstallMembership	QCE	
7	2.3.7	Delegating membership certificate	2	1427	2/9/2015		QCE	
8	2.3.8	Add a guild equivalence certificate to an application	2.1	1452	UNK			Covered on item #32 Need detail design
9	2.3.9	Certificate revocation	2.1	1453	UNK			2-3-15: QEO asks if it is worthwhile to have Security 2.0 for 15.04 without this feature. Concerned about not being able to keep rogue devices out of the system without this feature. QEO believes expiring certificates is not adequate. One amenable for QEO is the option is to use the deny flag for the 2.0 release. QCE will post proposed update for checking for deny to the mail list. Need to clearly document the process flow QCE believes this need more design discussion
10	2.3.10	Distribution of policy updates and membership certificates	2.1	1454	UNK			For core, the implementation is: The PermissionMgmt::InstallEncryptedPolicy still need design decision regarding which key material to use to encrypt the data Option to not encrypt the policy - only sign. Otherwise this may require security manager to be always on. Action: Chris to se t up time for Thurs @ 1pm Feb 5 for deeper dive on this item.
11	2.3.11.1	Manifest Format	2	1455	done	PermissionMgmt::GetManifest, API call PermissionConfigutor::SetPermissionManifest	QCE	
12	2.3.11.2	Trusted Description	2		UNK		QEO MSFT	This is done by the Security Manager
13	2.3.11.3	Manifest enforcement	2	1456	done		QCE	
14	2.3.11.4	Generating Policy and Membership Based on Manifest	2	1457	done		QCE	QCE: Built enforcement of the policy in core. There is no enforcement of the manifest. It is the responsibility of the security manager to build the policy based on the manifest.
15	2.4.1	Validation flow	2	1459	done		QCE	
16	2.4.2	Validating a consumer policy	2	1426	2/9/2015		QCE	
17	2.4.3	Exchanging the membership certificates during session establishment	2	1458	done		QCE	

Security 2.0 and 2.1 Feature Matrix

ID	HLD	Feature	Version	JIRA ASACORE	CC Date	Interfaces	Contributor	Notes
18	2.4.4	Anonymous session	2.1	1460	UNK			In the current codes, once the app/device is claimed it requires that any user must provide an identity certificate that it can trust. The app has a number of trust anchors to verify the identity trust. We don't allow an anonymous user to access a claimed app. QEO is okay with this being a post 2.0 feature
19	2.4.5	Validating an admin user	2	1384	done		QCE	
20	2.4.6	Emitting a session-based signal	2	1461	done		QCE	
21	2.5.1	The format is binary and exchanged between peers using AllJoyn marshalling	2	1462	done	PermissionPolicy object	QCE	
22	2.5.2.1	Authorization data field definition	2	1463	done	PermissionPolicy object	QCE	
23	2.5.2.2	Enforcing the rules at message creation or receipt	2	1464	done		QCE	
24	2.5.2.3	Search Algorithm	2	1465	done		QCE	
25	2.5.2.4	Matching Algorithm within a Policy Term	2	1466	done		QCE	
26	2.5.2.5	Search Priorities for Policy Terms	2	1467	done		QCE	
27	2.5.3	Policy Templates	2.1	1468	UNK			
28	2.6.1	Main Certificate Structure	2	1469	done		QCE	
29	2.6.1.1	Security 2.0 Custom OIDs	2	1470	done		QCE	
30	2.6.2	Identity certificate	2	1471	done		QCE	
31	2.6.3	Membership certificate	2	1472	done		QCE	
32	2.6.4	Guild equivalence certificate	2.1	1473	UNK			QEO asks if it is worthwhile to have Security 2.0 for 15.04 without this feature. defined. No enforcement codes.
33	2.6.5	User equivalence certificate	2.1	1474	UNK			
34	2.7.2	Users set up by Dad	2	1475	done		QCE	Security manager will handle this use case. Core work implemented
35	2.7.3	Living room set up by Dad	2	1476	done		QCE	Security manager will handle this use case. Core work implemented
36	2.7.4	Son's bedroom set up by son	2	1477	done		QCE	Security manager will handle this use case. Core work implemented
37	2.7.5	Master bedroom set up by Dad	2	1478	done		QCE	Security manager will handle this use case. Core work implemented
38	2.7.6	Son can control different TVs in the house	2	1443	2/9/2015	PermissionMgmt::InstallCredential, PermissionMgmt::InstallMembership	QCE	
39	2.7.7	Living room tablet controls TVs in the house	2	1443	2/9/2015	PermissionMgmt::InstallCredential, PermissionMgmt::InstallMembership	QCE	
40	3.1	Crypto Agility Exchange	2.1	1479	UNK			
41	3.2	Permission NotifyConfig Announcement	2	1480	done		QCE	
42	4.1	Broadcast signals and multipoint sessions	2.1	1481	UNK			
43	??	Manufacturer certificates (Symantec)	2.1	1482	UNK			
44	??	Issue with certificate date validity check need time check when we have trusted time	2	1484	2/9/2015		QCE	Need to update HLD
45	??	Issue with certificate date validity check when trusted time is not available	2	1485	2/9/2015		QCE	Need to update HLD

Security 2.0 and 2.1 Feature Matrix

ID	HLD	Feature	Version	JIRA ASACORE	CC Date	Interfaces	Contributor	Notes
46	Part of 2.3.10	The PermissionMgmt::InstallEncryptedPolicy still need design decision regarding which key material to use to encrypt the data	2.1	1483	UNK		QCE	Covered in #10
47	N/A	Hook to replace the default key store implementation.	2	1429	2/9/2015		QCE	