

Security 2.0 Combined High Level Schedule 02/04/15

- October
 - Technicolor
 - Proxy distribution agent – API definition - DONE
 - QCE
 - Functional test planning begins Oct 13
- November
 - Technicolor
 - Security manager utility v0.5 Nov 3 - DONE
- December
 - QCE
 - JIRA
 - ASACORE-1170 (additional API calls) Dec 12
 - ASACORE-1256: Install Identity Certificate in Claim method Dec 19
 - ASACORE-1259: Add method to retrieve peer's public key from DSA session Dec 19
 - ASACORE-1260: Use public key to identify peers in Policy Dec 19
 - Microsoft
 - Finalize Threat Analysis & Security Code review
 - Completed and addressed in 14.12 ([ASACORE-1194](#))
 - Technicolor
 - Android sample v0.5 Dec 19
 - One patch pending approval will be complete week of Jan 5
- January
 - QCE
 - Finalize test plan and test cases Jan 12
 - Functional Core testing begins Jan 12
 - Release to alliance by Jan 23
 - Rebaseline with master by Jan16
 - Microsoft
 - Network Isolation
 - ASACORE-935
 - About Interface privacy improvements
 - [ASACORE-1288](#)
 - Header Encryption
 - TBD (pending confirmation from Gateway Working Group that they are ready for this change after 14.12)
 - Design Documents for February work
 - Design Reviews with Alliance
 - Technicolor
 - Vulnerability testing around January 19
- February
 - QCE
 - Permission management (SC) DC Feb 9
 - Permission management (TC) DC Feb 9

Security 2.0 Combined High Level Schedule 02/04/15

- Unit tests applications Feb 27
 - Technicolor
 - Security Manager Utility v1.0 Feb 20
 - Android sample v1.0 Feb 20
 - Microsoft
 - Windows Keystore Implementation
 - Qualcomm will provide the necessary hooks in the AllJoyn core services to allow implementers to replace the default key store. Microsoft will update our AllJoyn services in Windows to use these hooks to replace the default key store with secure Windows APIs including the use of TPMs on Windows devices.
 - Dependency: QCOM keystore hooks for Core Services
 - Federated user identity prototype
 - Microsoft will provide a generic prototype that will allow the use of federated user IDs with AllJoyn security. The goal is to provide an implementable prototype to allow security managers and apps to accept Federated ID credentials to allow users access across any number of services they have been authorized to use simply by having the service reference the current user's federated ID.
 - Windows Security Manager sample app
 - Security manager will be an app experience that allows the user to manage security policies and credentials on devices that support AllJoyn Security 2.0. AllSeen Alliance partner Technicolor is providing sample Security Managers for Android and iOS. Microsoft will provide the analogous sample app for Windows.
 - Dependency: collaboration with Technicolor building Android/iOS Security Managers.
 - Integration testing needs to begin
 - Requires additional planning and coordination between contributors
- March
 - Microsoft
 - Optional credential management plug-in model
 - Microsoft proposed a security plug-in model for AllJoyn devices. This plug-in would allow for optional credential managers and even enterprise management to be added to AllJoyn devices.
 - Test Case documentation
 - Windows Telemetry
 - Test effort completes Mar 13
 - Feature branch merged with master
- April
 - Security 2.0 included as part of the 15.04 Core release