ALLSEEN ALLIANCE

# Core Working Group

May 14, 2015

# Reminder:

# This call is being recorded

# Antitrust Compliance Notice

- AllSeen Alliance meetings involve participation by industry competitors, and it is the intention of AllSeen Alliance to conduct all of its activities in accordance with applicable antitrust and competition laws. It is therefore extremely important that attendees adhere to meeting agendas, and be aware of and not participate in any activities that are prohibited under applicable US state, federal or foreign antitrust and competition laws.

- Examples of types of actions that are prohibited at AllSeen Alliance meetings and in connection with AllSeen Alliance activities are described in the AllSeen Alliance Antitrust Policy. If you have questions about these matters, please contact your company counsel, or if you are a member of AllSeen Alliance, feel free to contact Lee Gesmer or Andrew Updegrove, of the firm of Gesmer Updegrove LLP, which provides legal counsel to AllSeen Alliance.

# Agenda

1. 15.08 Features
2. SRP deprecation request
3. Changing Windows to TCP/9955
4. JIRA severity
5. Configuration identification
6. Supported bindings
7. Changing APIs
8. Review Action Items

# 15.08 Features

- Need to firm on feature list
  - https://jira.allseenalliance.org/issues/?filter=11008
  - Current committed features
    - Security 2.0 (MSFT, QEO, QCE)
      - https://jira.allseenalliance.org/browse/ASACORE-1393
    - Commercialize UDP Transport for TC <-> RN connections (QCE)
      - https://jira.allseenalliance.org/browse/ASACORE-1686
- Need to firm on supported platforms
  - Supported platforms for 15.04
    - https://wiki.allseenalliance.org/core/core_15.04_release_review#quality_assurance
    - https://allseenalliance.org/developers/download/supported-platforms
  - Dino (MSFT) asks to add VS 2015 for 15.08
  - Chris (QCE) will send to mail list to get decisions for 15.08 platforms and toolchains

# SRP deprecation request

- From Greg Zaverucha (MSFT) posted to Core WG mail list on 5/8/15
  - SRP is an authentication mechanism in AllJoyn that allows two endpoints to establish a shared secret knowing only a password. Unlike ECHE_PSK, the pre-shared value in SRP may have low entropy (like a 4-digit PIN printed on the box of a Thing). This is a useful feature, but SRP is not the best way to realize it, for the following reasons
    - SRP is not supported on the thin client. It's also not a good fit for low-power devices, as it's computationally more expensive than elliptic-curve (EC) based primitives.
    - SRP uses a separate crypto stack from the ECDSA and ECDH. To implement SRP requires large integer arithmetic (bignum) and SHA-1. SRP is only auth mechanism using these. (the others share core the EC code, and use SHA-256).
    - The current SRP implementation needs work, it lacks protections against side channel attacks. The considerable investment improving it is better spent elsewhere.
  - In place of SRP I will propose an alternative protocol to get the same functionality that is a good fit for the thin client, i.e., use the same underlying EC code and hash function. I am currently reviewing the password-authenticated key exchange protocols specified in IEEE 1363.2, one of these protocols will form the basis of my proposal. The design and implementation of the new mechanism will target the 15.08 release.
- Tentative Core WG agreement, will give one more week for feedback
- This will need to be presented and voted by the TSC

# Changing Windows to TCP/9955

- Pros
- Cons
  - Potential interop if developers hard coded other ports
    - Bus attachment to daemon is hard coded as 9956
  - Potential firewall issue
- Impact
  - Firewall issue may be only impact
- Next steps
  - Dan (MSFT) will send mail to Core WG, discuss, and TSC about this change going into 15.04a
  - Marcello (QCE) will add this to the release notes.

# JIRA severity discussion

- https://wiki.allseenalliance.org/core/overview/jira_process
- David (QCE) to update the page with the details and send mail to Core WG
- Final review next week.

# Supported bindings

- Discuss policy for supported bindings
- Existing bindings in Core
  - C++
  - Obj-C
  - Java
  - C
  - Javascript NPAPI

# Proposal to outline the process for changing APIs

- Question: Who should lead effort to craft proposal?
  - Gavin (MSFT) will craft proposal for review by Core WG and then presented to TSC

# Configuration identification

- Result of email conversation regarding security samples for 15.04
- Need to identify the following
  - List of SDKs released
  - Contents of individual SDKs
  - Changes
    - SDKs
    - Platform support

# Action Items

- Need to schedule – will send out email asking for times
  - 15.08 backlog
  - 15.04 post mortem
- IPv6 discussion
  - Dino (MSFT) has set up initial meeting to discuss
  - Action: Marcello to share in email affected components before meeting
- David (QCE) to lead team crafting testing proposals
  - Proposal presented to alliance
    - Budget approved at TSC meeting - Needs to be approved by the board
  - David leading the effort
    - Assisting includes Arvind, Marcello, Chris, Dino, Gavin
- Marcello (QCE) to send IOS language binding proposal to WG mail list
- Gavin (MSFT) to see if someone from Microsoft can assist with notes from core WG meetings after 15.04 release

# Thank You

Follow Us On 

- For more information on AllSeen Alliance, visit us at: allseenalliance.org & allseenalliance.org/news/blogs

# Language bindings discussion 5/7/15

- Need a formal policy to support language bindings
  - Came up at last TSC F2F
- SCL binding proposal
  - Required
    - C++ and C
  - Optional
    - Java, NPAPI, ObjC?
- TCL binding proposal
  - No proposal
  - Should we consider JavaScript?
- Need separate policy for platforms
  - May need to consider binding platform and language binding
- Next steps
  - Action: Marcello (QCE) to send proposal to the mail list

# Notes from 14.12 Post Mortem

# 14.12 Post Mortem Improvement Items (1/3)

- Aligning date & the end game (lockdown) schedule of AllJoyn releases with release schedule of the contributing member companies if it happens to be in close proximity of AllJoyn release
  - **Action**: Arvind to send proposal to Core WG mail list
- Consistent and enforced definition/bar for code freeze
  - Need crisp definitions for "incremental bug bars“ (normal, tell, ask)
  - Need approval granularity (approval on merge)
  - Need process for how to deal with large last-minute changes
    - Suggestion – only high priority issues “ask” are added one week before release
  - **Action**:
    - Marcello to send current milestone definition to Core WG mail list
    - Gavin to send proposal to Core WG mail list based on Marcello’s email
- Need processes for breaking changes
  - Regarding protocol, API syntax, behavior
  - Mitigation: Proposed changes should be advertised
  - **Action**: Chris to add the process to this to the existing process draft

# 14.12 Post Mortem Improvement Items (2/3)

- Need agenda and slides 48 hours ahead of core WG meetings
  - Best effort to send slides by COB Friday
- Need notes from core WG meetings sent more consistently
  - Note: Linux foundation unable to assist
  - **Action**: Gavin to see if someone from Microsoft can assist
- For TSC: PR coordination for releases
  - More an issue for marketing committee
  - **Action**: Chris to discuss this with Philip
- Engage system test during feature testing
  - More members conducting system test is preferred
- Testing needs to be better distributed across members
- E2E testing is needed
  - **Action**: David and Arvind will make a proposal
- More frequently merge feature branches so that deltas can be kept to a reasonable minimum
  - **Action**: Chris to add process to the Wiki process draft

# 14.12 Post Mortem Improvement Items (3/3)

- May need more frequent but shorter Core WG meetings
  - WG meeting immediately following triage meeting for 30 minutes
  - **Action**: Chris to change Core WG status meetings to 30 minutes after the Thursday triage
- Increase frequency of triage meetings earlier in the process
  - **Action**: Chris to set up biweekly triage 2 weeks prior to branch date
    - For 15.04 it will begin week of March 9
- Define JIRA severity vs. priority process
  - **Action**: David & Arvind to set up discussions to craft proposal
- To be discussed at next meeting
  - JIRA label to identify contributing organization taking ownership of the item
  - Need process for managing the platform matrix
  - Revisit code style guidelines, rules, and enforcement