ALLSEEN ALLIANCE

# Core Working Group

May 21, 2015

The contents of this document, and the interfaces described, and all the information herein, are the result of collaborative discussions by the Core Working Group. This summary documents the final consensus of the team.”

# 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. Resolve side-effect of releasing TC 15.04a before SC 15.04a
2. 15.08 Features
3. SRP deprecation request
4. JIRA severity
5. Configuration identification
6. Supported bindings
7. Review Action Items

# Resolve side-effect of releasing TC 15.04a before SC 15.04a

- Note
  - the 15.04a sample routing node binary will not be available for the Windows TC SDK.
- We have two options
  - Create the 15.04a Windows TC SDK with the 15.04 sample routing node. The sample is only for dev use. Maybe the 15.04a SC fixes aren't important for the routing node anyway.
  - Update the 15.04a Windows TC SDK with the 15.04a sample routing node when SC 15.04a releases.
- Core WG decision
  - Do not update the 15.04a Windows TC SDK with the 15.04a sample routing node when SC 15.04a releases.

# Discussion: BusAttachment::Connect(connectspec)

- MSFT discussion about possible deprecation of ajn::BusAttachment::Connect(connectspec) overload
- Next steps
  - MSFT to submit proposal to Core WG mail list

# 15.08 Features

- Need to firm on feature list from all contributors
  - 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, no opposition after 1 week of requesting feedback
- Note: This will need to be presented and voted by the TSC
- Next steps:
  - MSFT to understand the ecosystem and impact before making proposal (reach out to LIFX)
  - Chris (QCE) to move this to the action item list

# 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 this week.

# Supported bindings

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

# 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 (1/2)

- Need to schedule – will send out email asking for times
  - 15.08 backlog
  - 15.04 post mortem
- 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

# Action Items (2/2)

- Marcello (QCE) to send IOS language binding proposal to WG mail list
- Changing Windows to TCP/9955
  - Dan (MSFT) will send mail to Core WG, discuss, and TSC mail list about this change going into 15.04a
  - Marcello (QCE) will add this to the release notes.
- Proposal to outline the process for changing APIs
  - Gavin (MSFT) will craft proposal for review by Core WG and then presented to TSC
- 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