ALLSEEN ALLIANCE

# Technical Steering Meeting

June 09, 2015

# 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.

# Reminder:

# This call is being recorded

1. Approve minutes from previous meeting
2. Core 15.08 Update
3. SRP deprecation request
4. Webdocs maintainer and committers
5. Common Frameworks
   - Vote on Base Services 15.04 release
6. HAE Project Progress Update
7. Overseas trip recap

# Core 15.08 Update

# Core 15.08

- Scheduled release date
  - August 28
- Features
  - Major features (Committed for the release)
    - AJCORE-1393 Security 2.0 (MSFT, QEO, QCE)
    - AJCORE- 1686 Commercialize UDP Transport for TC <-> RN connections (QCE)
  - Minor features (Best effort – not committed)
    - ASACORE-2034 Deadlock if max BusAttachment concurrency is reached (MSFT)
    - ASACORE-2029 Add About feature to JavaScript binding (LG)
    - ASACORE-1813 Change Win7 LN-side Standard Client to connect to the Win10 named pipe… (MSFT)
    - ASACORE-1556 Fix the Logger so it can work with ETW on Windows (MSFT)
    - ASACORE-1060 Add non-variadic functions to marshal/unmarshal multiple message args (MSFT)
  - Full list of features
    - https://jira.allseenalliance.org/issues/?filter=11008

# SRP deprecation request

# SRP deprecation request (1/2)

- Background
  - 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.

# SRP deprecation request (2/2)

- Proposal
  - In place of SRP, MSFT via the Core WG 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.
  - MSFT is currently reviewing the password-authenticated key exchange protocols specified in IEEE 1363.2, one of these protocols will form the basis of the proposal.
  - The design and implementation of the new mechanism will target the 15.08 release.
- Implications
  - Apps using SRP will have to migrate to another auth. Mechanism
  - Apps that only support SRP, and are not updated will not be able to connect with newer apps.
    - Those supporting SRP and other auth mechanism(s) may negotiate to a mechanism supported by both sides
  - Our codebase will get smaller, and have less crypto code (we can remove SRP, Bignum and SHA-1)
- TSC Vote

# Webdocs maintainer and committers

# Webdocs maintainer and committers

- The webdocs.git project was originally under the documentation subcommittee, but is now part of the Developer Support Working Group.
- Please approve the following roles:
  - Maintainer:
    - George Nash
  - Committers:
    - Brian Spencer
    - Jan Lissens
    - Mathew Martineau

# Common Frameworks: Base Services 15.04 release

# Common Frameworks
# Base Services 15.04 release

- Fully tested platforms
  - Linux Ubuntu (64 bit x86) (SCL & TCL)
  - Android Lollipop (ARM7) (SCL only)
  - OpenWRT Barrier Breaker (SCL only)
- Informally tested, not verified
  - Windows
  - iOS

# Base Services TC Summary

- No new features
- Bug fixes for thin core
  - ASABASE-503 TCL Control Panel Generator '.c' file does not include the generated '.h' file
  - ASABASE-498 base_tcl sample apps fail on darwin
  - ASABASE-249 Cannot onboard when the WiFi credentials set to WEP with security ASCII and the client uses ANY
  - ASABASE-241 TCL apps do not handle AJ_ERR_WRITE. Leading to application Announcement infinite loop

# Base Services SC Summary

- No new features
- Bug fixes for standard core
  - ASABASE-231 Config client crashes on gingerbread android version
  - ASABASE-345 Config service sample code error, authentication failure
  - ASABASE-452 Deprecate older About related base service APIs
  - ASABASE-479 1504 SC ConfigClient sample memory leak
  - ASABASE-482 1504 SC Linux ControlPanel controller sample memory leak
  - ASABASE-454 NotificationDismisserSender and NotificationDismisserReceiver bus objects have the same path
  - ASABASE-470 Remove SuperAgent from Notification service
  - ASABASE-489 Notification service reports bad introspection XML
  - ASABASE-345 Config service sample code error, authentication failure
  - ASABASE-453 The Onboarding Daemon should not use hard-coded device ID and App I

# Base Services 15.04 release vote to approve

- Full text of resolved and open bugs:

  https://jira.allseenalliance.org/secure/ReleaseNote.jspa?projectId=10103&version=10901

- Call for vote to release Base Services 15.04 for the CBI
  - The 30 day review period starts on notification to the board

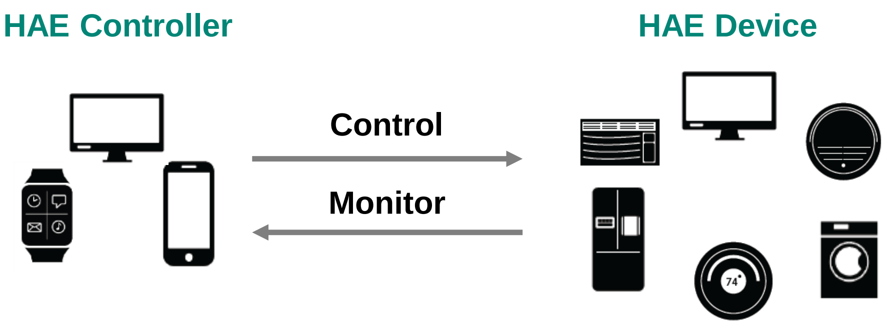
# HAE Project Progress Update

- Inhwan Choi, LG Electronics
- Project Maintainer

# Overview of HAE Service Framework

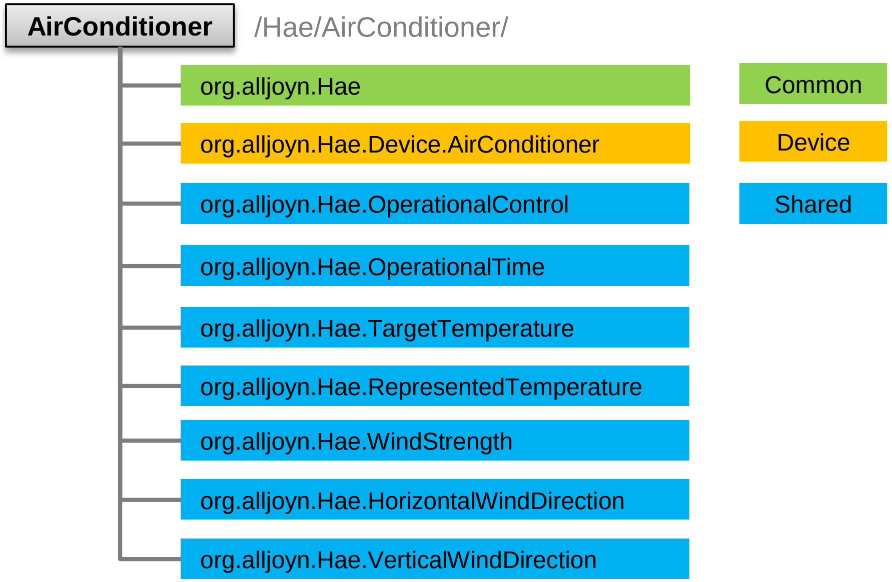
The HAE service framework project develops the common way of controlling and monitoring Home Appliances & Entertainment (HAE) category devices, regardless of device manufacturers.

## Use Cases and Benefits



- Cross-Vendor Interoperability
- True Machine-to-Machine Interaction

## AllJoyn Representation



**AirConditioner** /Hae/AirConditioner/

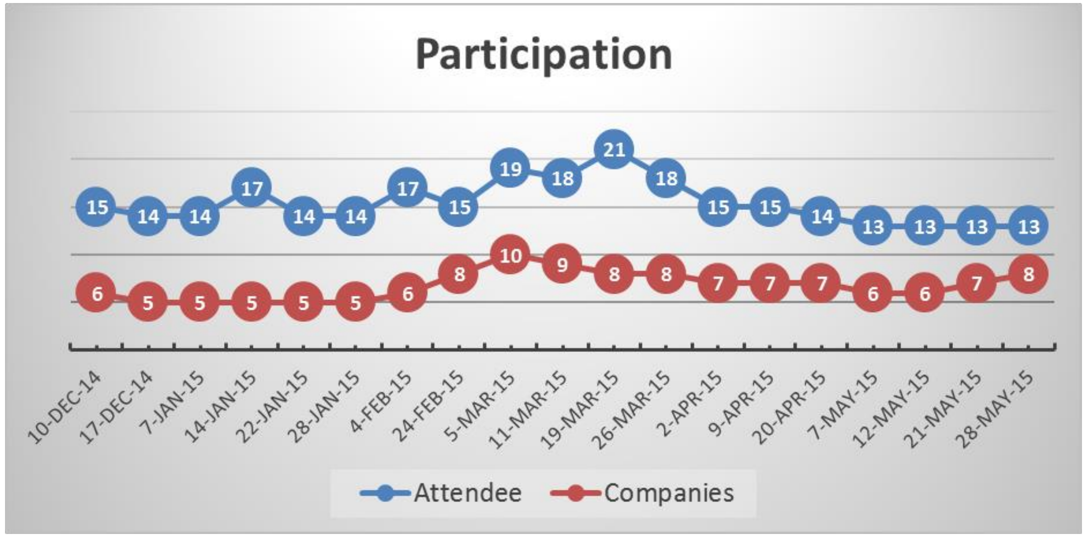
- org.alljoyn.Hae
- org.alljoyn.Hae.Device.AirConditioner
- org.alljoyn.Hae.OperationalControl
- org.alljoyn.Hae.OperationalTime
- org.alljoyn.Hae.TargetTemperature
- org.alljoyn.Hae.RepresentedTemperature
- org.alljoyn.Hae.WindStrength
- org.alljoyn.Hae.HorizontalWindDirection
- org.alljoyn.Hae.VerticalWindDirection

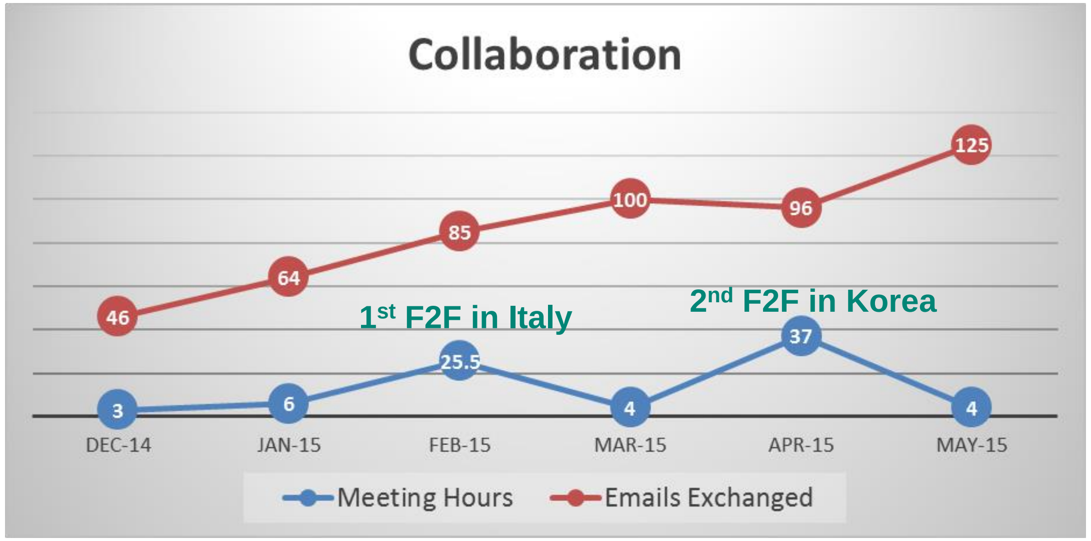
🟩 Common
🟨 Device
🟦 Shared

※ **Example Representation**

# Consistent Efforts

**Members are making consistent efforts to deliver AllJoyn interface definitions for flexible representation of HAE devices while complying with IRB guidelines.**





- Participation hit record-high in March.
- Consistent participation by 7 companies.

Electrolux Haier Honeywell LG Panasonic SHARP SONY

- Target schedule for interface definitions
  - Submit to IRB by early July.
  - Get approval by early August.
    (before summer vacation)

# Current Progress

- “Common” interface
  - Contains common part for All HAE devices.
  - Per About announcement, one and only one shall be found under the root HAE bus object.
  - https://jira.allseenalliance.org/browse/ASAHAE-3 (under comments & resolutions)
- “Shared” interfaces
  - Sharable or Reusable interfaces across HAE devices.
  - 36 interfaces are developed and converting those into AllJoyn-syntax version are under way.
  - A few more are expected to be added.

※ AllJoyn syntax independent device models have been developed first to help identify common/reusable features across device types and separate optional features from mandatory ones.

※The final total number of interface definitions are subject to change.

- “Device” interfaces
  - 20 interfaces will be developed. (one per each standard HAE device type)
  - Refrigerator, Fridge, Freezer, Ice Maker, Air Conditioner, Humidifier, Dehumidifier, Air Purifier, Electric Fan, Air Quality Monitor, Thermostat, Washer, Dryer, Washer Dryer, Dish Washer, Oven, Cooker Hood, Cooktop, Robot Cleaner, TV.
- Link to interface definitions for internal review will be available shortly here (ASAHAE-16).
  - Use of Git /Gerrit was adopted for further comments & resolutions of developed interface definitions in markdown format (@ June 21st call).

# Next Step

- Updated milestones

| Milestone | Original (Dec-14) | 1st Update (Feb-15) | 2nd Update (May-2015) |
|---|---|---|---|
| AllJoyn interface specifications | Feb. 2015 | Apr. 2015 | Submission to IRB by July 8, 2015<br>IRB Approval by August 5, 2015 |
| High-level design (HLD) documents | Mar. 2015 | May. 2015 | End of August, 2015 |
| Foundational component implementations for Linux (C/C++) | Jun. 2015 | Jul. 2015 | End of October, 2015 |
| Certification test suite | Aug. 2015 | Sep. 2015 | End of December, 2015 |
| Reference controller applications for Android & iOS | Sep. 2015 | Oct. 2015 | End of December, 2015 |

- To finish our work on interface definitions, 3rd F2F meeting will be held in Beijing during 6/23 ~ 26.

# Open Points and Call for Advice

- List of general open points is available here.
  - https://jira.allseenalliance.org/browse/ASAHAE-13
- While resolving some of open points, inquiries and requests were made to IRB, Core and Common Frameworks WGs.
  - A new feature Jira ticket (ASACORE-1811) to add support for generic error message delivery for Properties was created.
  - A question on the availability and its current status of “Time Service” was asked, and one of HAE participants volunteered to take over the project.
  - A question on the reusability of the org.alljoyn.Control.Volume was asked, it was recommended to redefine the volume control interface of HAE’s own since that interface violates some of IRB guidelines.
- Some of points are still open and they are not HAE-specific. Your advice or consultation would be greatly appreciated.
  - [ID 6] Is it legal to reply to a method call or SetProperty before applying a set-point value internally ?
  - [ID 8] Too frequent emission of property changed signal should be avoided. Any guideline or minimum requirements on frequency or interval ?
  - [ID 10] Identifying semantic meanings of multiple instances of an interface.

# Overseas trip recap

# Thank You

Follow Us On

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