Argonaut Project:
Security SME Team

September 21, 2015
Agenda

- Alternative approaches to Argonaut SMART on FHIR authorization specification
- Authorization profile implementation update
- Use Case 5 update
Alternative Approaches to Argonaut Authorization Specification

• SMART on FHIR authorization specification for Argonaut use cases #1-4 (i.e., provider/patient app access to EHR)
  – http://fhir-docs.smarthealthit.org/argonaut-dev/authorization/

• Some sponsors expressed a desire for more formal specification similar to IETF RFCs
  – Matt Randall (Cerner) developed draft of more formal specification, based on SMART on FHIR authorization specification for Argonaut use cases #1-4
  – http://fhir-docs.smarthealthit.org/argonaut-dev/specification/
  – Identified a number of questions and areas needing further specification
Sponsor Preferences

- We currently have a working draft of a SMART on FHIR OAuth 2.0 profile for an EHR-to-EHR exchange (use case #5)

- Before we proceed further, we are asking for your thoughts on the type of specification that will be most useful to your developers
Argonaut Implementation Program: Authorization

• Implementation Program wiki
  – https://github.com/argonautproject/implementation-program/wiki

• Sprint 1 authorization:
  – Focused on getting data services up and running
  – Each server published its FHIR endpoint URL along with an access token (OAuth bearer token) that clients could include in an HTTP Authorization header with each API call:
    • Authorization: Bearer {server-specific-token-here}

• Sprint 1 results:
  – 18 servers and 18 clients signed up for Sprint
  – Testing results reported by 4 clients against 13 servers
  – Reporting light
Argonaut Implementation Program: Authorization

• Sprint 2 introduced basic authorization:
  – Standalone launch sequence only
  – Public clients and confidential clients are both supported
  – Access scopes are limited to: `user/*.read`, meaning that a client can read any data that the authorizing user is permitted to see
  – No launch context is returned to the app
  – No single-sign-on (OpenID Connect) is required

• Sprint 2 results to date
  – Minor issues encountered and resolved
Argonaut Implementation Program: Authorization

• Sprint 3 (just beginning)
  – Adds support for apps that require access to only one record, rather than everything the authorizing user is permitted to see
  – Accomplished through launch scope
  – Assumptions
    1. Standalone launch sequence only
    2. Both public clients and confidential clients are supported
    3. Access scopes include:
       – launch/patient (indicates to the EHR that a single patient must be selected to complete the launch process)
       – patient/*.read (to ensure a patient-specific access token)
    4. One context parameter is returned to the app upon successful authorization:
       – patient (indicates the patient currently open in the EHR)
    5. No single-sign-on (OpenID Connect) is required
Use Case #5 Activity: DirectTrust Consideration

• Held initial meeting with DirectTrust to discuss potential synergies and capabilities Argonaut could leverage
  – Direct has spent years on trustworthy proof of organizational identity – all of the pre-conditions for use case #5 have been addressed by DirectTrust
  – DirectTrust agreed to come back to Argonaut authorization team with recommendation

• Follow-on meeting
  – DirectTrust presented its scalable trust model
  – Direct email messages contain digital signature of sender generated using X.509 certificates
  – Certificate Trust Chaining is used to trace an end-user’s certificate back to a Trust Anchor from which it was generated
  – Initially, HISPs would sign agreements with each other => proved not to be scalable
Use Case #5 Activity: Direct Trust Consideration

• (Follow-on meeting cont.)
  – Adopted “Trust Bundle” approach in which Trust Anchor certificates for a Trust Community are bundled and distributed (~certificate bundles used for SSL)
  – Attempted to address bridging across Trust Communities => unsuccessful, so single certificate can be in multiple Trust Communities
  – Plan to address EHR-to-EHR exchange
Use Case #5 Activity: Direct Trust Consideration

• Argonaut Conclusion
  – Agree that DirectTrust model could be extended to apply to the EHR-to-EHR use case Argonaut is addressing
  – Argonaut EHR-to-EHR approach uses digital certificates as part of trust infrastructure
    • For secure SSL transport
    • For digitally signing authorization JWT sent from EHR-A to EHR-B
    • For digitally signing authentication JWT sent from EHR-A to EHR-B
  – Focus is on API between EHR desiring access to a FHIR resource, and the EHR holding that resource
  – Argonaut does not address policy rules enforced within either enterprise, or their processes for distributing, sharing, and validating digital certificates
  – Argonaut interests are best served by continuing to focus exclusively on the enterprise-to-enterprise API
Next Steps

• Ascertain sponsor needs and preferences for specification
• Proceed with further refinement of specifications, based on sponsor needs