FHIR AT SCALE TASKFORCE

FHIR at Scale Taskforce *(FAST)*

SME Session Summary Report

National Standards Based Approaches
for Scalable Security Solutions

Session 1: June 3, 2020
Session 2: July 26, 2020

Meeting Introduction

The FHIR at Scale Taskforce (*FAST*) sought and obtained industry subject matter expert (SME) input to further refine the Taskforce's proposed solutions to FHIR scalability challenges.

Fifteen SMEs from across the healthcare ecosystem participated in the *FAST* Scalable Security Proposed Solutions Expert Panel Discussion on June 1, 2020, providing feedback based on their individual expertise and domain knowledge. The security scalability needs and challenges of a broad range of stakeholders were represented, including medical and quality associations, interchange associations/Health Information Exchanges (HIEs), security vendors/developers in both healthcare and non-healthcare industries, The Office of the National Coordinator for Health Information Technology (ONC), providers, payers, electronic health record (EHR) vendors, and researchers. The SMEs shared their expertise and input with ONC *FAST* facilitators, concerning proposed solution approaches for security processes including authentication; application registration and data request authorization; open questions and discussion topics specific to each solution; as well as learnings from the SMEs' individual and organization implementation experiences. The *FAST* security team received positive feedback on this session and the participating SMEs decided to continue the conversation in a second session which took place on July 26, 2020.

To learn more about the *FAST* solutions development process as well as the objectives and meeting materials for each SME Session, please visit the *FAST* Proposed Solutions – Subject Matter Expert Panel Sessions Confluence pages.

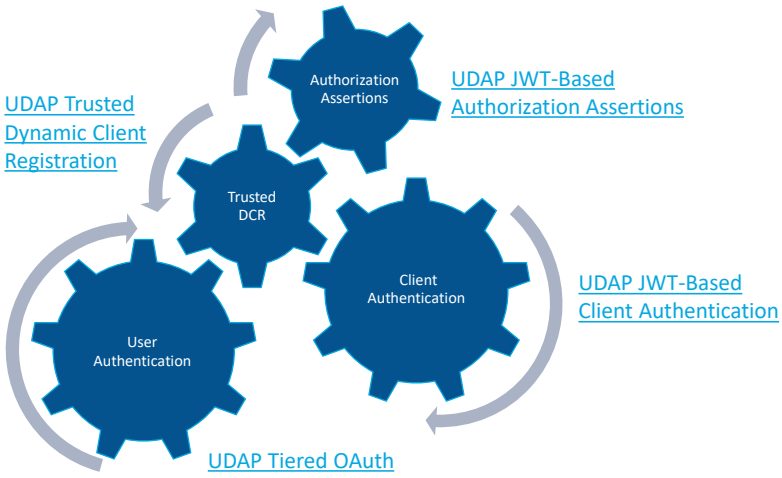
Solution Overview

The *FAST* Scalable Security solutions are intended to address potential limitations of FHIR-based information exchange to appropriately authenticate entities (confirm they are who they say they are) and authorize them (confirm they have required permissions) to see the data they request. Furthermore, methods to speed the process of granting client system access to FHIR data servers—while still vetting the client's identity and trustability—must be implemented so that this registration step doesn't become a bottleneck that delays availability of new patient-facing and business healthcare applications.

Authentication and authorization functions must be scalable to support millions of users and billions of transactions. And client system registration must be scalable to support the proliferation of new applications that seek to leverage healthcare data for the benefit of consumers and the organizations that serve them.

The recommended *FAST* Scalable Security solutions aim to minimize the number of credentials requestors and responders are required to securely maintain, reduce client application sprawl and increase confidence the requester is appropriately authenticated and authorized to view the data being requested.

During the SME sessions, the *FAST* Security Tiger Team reviewed two proposed solutions to address the challenges and goals identified above: (1) Trusted Dynamic Client Registration and (2) JSON Web Token (JWT)-Based Client Authentication & Authorization.



1. *FAST* proposed Trusted Dynamic Client Registration streamlines the registration and use of client applications across multiple endpoints. It provides a way to leverage a distributed system of authoritative information to enable fast and secure client system registration—removing process roadblocks that hinder scaling today.

2. *FAST* proposed JWT-Based Client Authentication & Authorization enables industry participants to use existing public key infrastructure and validated digital identities to authenticate system access and authorize information requests. It assures that an information requestor is appropriately authenticated and has the authorization to review and use the data requested.

Both approaches are based on existing, best standards including OAuth 2.0 Authorization Framework, OpenID Connect, Unified Data Access Profiles (UDAP), and best practices employed by PKI-Based Health Information Networks. The *FAST* security solutions aim to facilitate automated exchange and minimize the number of credentials that requestors and responders are required to securely maintain, reusing existing infrastructure where possible.

The Unified Data Access Profiles work together to accomplish the goals of the two *FAST* Security solutions. UDAP Tiered OAuth and UDAP JWT-Based Client Authentication underlie both solutions, reducing "credential sprawl" by enabling credentials to be maintained by a smaller set of trusted entities. UDAP Trusted Dynamic Client Registration is the foundation of the solution to reduce the burden associated with granting client system access to FHIR data servers. UDAP JWT-Based Authorization Assertions provide the means to enable more informed authorization decisions in the Authentication and Authorization proposed solution.

To learn more about these proposed solutions, please review the pre-reading and presentation materials available on the *FAST* Scalable Security Proposed Solution - Expert Panel Discussion Confluence page.

Discussion Topics

During two sessions (for a total of five hours) the group discussed various aspects of the proposed *FAST* security solutions. While the discussions touched on a range of related challenges and security approaches, eg, user-level authentication and identity proofing, the conversation focused primarily on the following topics:

1. Trust Frameworks

Trust frameworks are important in today's digital healthcare ecosystem. They are a set of rules and procedures to authenticate the data sender and receiver, verify ownership of the data that are being exchanged, and ensure secure and accurate data transmission. Use of several existing frameworks was explored as examples during the sessions, including those implemented by DirectTrust, Carequality and CommonWell.

The group discussed the minimum technical requirements and related policy considerations necessary to support cross-network exchange and cross-framework exchange. Both system and business challenges were identified by the group, such as the potential for trust frameworks to set different identity proofing or authentication conventions, presenting an obstacle to use of the authentication mechanisms included in the *FAST* security solution. The group explored the "rules of the road" needed to ensure compatibility among trust frameworks, including use of common technical components and consistent governance rules. Participants noted that cross-framework exchange is occurring today to a limited extent, enabled by discussion and agreement between the frameworks involved.

The group agreed with the proposed solutions' requirement that each participant belong to a trust framework, which will define its roles and security assertions. Participants also raised additional points to which the group agreed, including that further exploration of the topic is needed, especially in the following areas: essential policy and technical requirements; standard transactional metadata covering the "80%" uses; guidance on a minimum set of JWT security assertions for frameworks to support; and use case-specific requirements.

2. X509 Certificates

Digital identities, expressed in digital X509 certificates, enable the requestor to authenticate itself to a responder's endpoint. Many organizations have established certificate-based digital identities that can be reused within a trust community for FHIR transactions. The use of these digital identities helps to remove the burden of credentials management among FHIR transaction participants. This helps pave the way for scalability within the FHIR ecosystem. This is important, for example, for the numerous applications that are in the market or are being developed to enable patients' access and exchange of their data.

The group confirmed the appropriateness of using the x509 standard in the proposed security solutions to represent the characteristics of entities that operate application servers and client applications.

The *FAST* Security Tiger Team brought forward discussion points to gain insights on the types of information needed in X509 certificates to support registration, authentication, and authorization in various scenarios. Participants agreed that certificate content proposed by the *FAST* Security Tiger Team would be useful, including identification of the organization responsible for an application or server and a party's status as a covered entity under provisions of the Health Insurance Portability and Accountability Act (HIPAA).

Beyond what was proposed by the *FAST* Security Tiger Team, the group identified opportunities to include additional information in X509 certificates that could inform end-users' decisions on whether to use an application. Suggestions from the group included the application operator's policies on data use and retention and its organizational relationships.

Participants identified other new possibilities that arise when an application has a digital "identity" with which many network participants interact—from being able to share an application's popularity with potential users, to detecting and alerting on improper behavior.

3. Authorization Data

The group considered the types of information that information holders would need to receive with a request to make informed decisions about:

- whether to reply with patient information
- the amount or type of information that could be appropriately released.

Discussion touched on both the content of this "authorization metadata" and the technical means for conveying it in an information request (as "scopes" vs "additional authorization metadata"). The group recognized that conventions exist for representing these data, and that proposing changes to those conventions would incur costs. Discussion didn't resolve to an agreed answer, but the *FAST* Security Tiger Team identified the need to explore further with respect to the "80%" common content.

4. Stakeholder Readiness

The readiness of industry participants to adopt the proposed solutions was discussed as a focus topic and also arose naturally in relation to other session topics. Session participants considered the readiness of standards underlying the proposed solutions, current opportunities for (and obstacles to) exchange across trust frameworks, and stakeholder ability to adopt the solutions.

They agreed that many stakeholders would lack the operational and technical readiness to adopt the proposed solutions in the immediate future. That is because not all process, regulatory, and policy pieces are in place; many are still under development. Small payers and vendors might have a heavier lift.

In addition to the factors noted above, multiple participants noted that implementing the proposed security solution would need to follow other priorities in their organizations' development queues—including those related to recent federal rules.

5. Industry Path Forward

The session participants considered the steps necessary to adopt the proposed solutions, including education and guidance for the FHIR implementer community—eg, in the form of implementation guides or other materials—as well as potential legal and regulatory needs.

The group discussed that additional, real-world implementation experience could enable the solution to be solidified prior to being established as standard. Participants cited the complexity of the combined solutions and the benefit of iterative implementation, learning, and refinement.

Moving Forward

After two productive SME sessions, the *FAST* Security Tiger Team is analyzing the feedback they received and working to incorporate what they learned into the next iteration of their solution documentation. As the team further develops their action plan, they will take the following SME perspectives into account:

Immediate Next Steps

- Cross walk the overlaps with the other Tiger Teams on Security aspects
  - Action: Schedule working session with the Identity Tiger Team
  - Action: Discuss *FAST* Ecosystem Security Framework & *FAST* Security Solutions with the Chief Architects to identify other Tiger Teams where coordination may be needed
- Review feedback on use of the UDAP Tiered OAuth profile and make proposals related to privacy
  - Action: Reference topic among areas considered in version 3 solution documentation and re-assess these concepts as they mature
- Discuss W3C Verifiable Credentials
  - Action: Concept reviewed and determined it has low maturity. Reference topic among other areas considered in version 3 solution documentation
- Add CMS BB2.0 statistic re: years of effort for app registration
  - Action: Add statistics to version 3 solution documentation

Path Forward

- Identify actions to ascertain the "80%" standard authorization metadata items
  - Action: Review the SME-suggested items and determine which to include in version 3 of the solution
- Consider running vocabulary to be used across trust frameworks through HL7 so that it can be referenced in regulation
  - Action: Review and propose relevant work to support Implementation Guide writers or further development of the solution by the "landing place/ home"
- Provide IG writers direction to enable them to start off in the same way
  - Action: Address in version 3 of the solution (output is self-contained, team not to assume ownership or maintenance)
- Consider/propose incremental solution approach
  - Action: Make proposals regarding what is core (everyone should do) and what is not necessary immediately (optional but valuable in certain instances)
- Engage implementer community
  - Action: Consider appropriate stakeholders and timeframe for engagement