Zoom Meeting Interface and Basic Logistics

- **VIDEO**: Please enable your video using **bottom left video button with camera icon**. Video sharing capability is accessible for SMEs and Panelists.

- **AUDIO**: Adjust your audio settings as needed (choose computer audio, call in, mute, etc.) using **audio button bottom left, microphone icon**

- **PLEASE MUTE WHEN NOT SPEAKING**: Click on your video box to mute yourself or use the audio button, bottom left

- **CHAT**: Chat function allows communication directly with all participants or privately with a specific person (bottom, middle right, highlighted in orange in this image), then use the drop down to choose visibility of message

*image above is a publicly available tutorial image obtained from Zoom website*
FAST SME Session
Scalable Security Solutions
The ONC FHIR At Scale Taskforce (FAST) (Hereinafter “Taskforce”) is committed to full compliance with existing federal and state antitrust laws.

All members involved in the Taskforce effort, including its advisory groups, will comply with all applicable antitrust laws during the course of their activities. During Taskforce meetings and other associated activities, including all informal or social discussions, each member shall refrain from discussing or exchanging competitively sensitive information with any other member. Such information includes, but may not be limited to:

- Price, premiums, or reimbursement charged or paid for products or services
- Allocation of customers, enrollees, sales territories, sales of any products or contracts with providers
- Any other competitively sensitive information that is proprietary to a member company

If you have any specific questions or concerns, seek guidance from your own legal counsel.

Members should not bring confidential information or intellectual property (hereinafter “Intellectual Property”) owned by their respective member companies into Taskforce meetings. To the extent such Intellectual Property is shared with the Taskforce that shall not be construed as a waiver of member company’s rights to, or ownership in, the Intellectual Property.
## Welcome

### SME Participants

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Matt Randall</td>
<td>Cerner</td>
</tr>
<tr>
<td>Joshua Mandel</td>
<td>Microsoft Healthcare</td>
</tr>
<tr>
<td>Jason Vogt</td>
<td>CommonWell</td>
</tr>
<tr>
<td>Catherine Schulten</td>
<td>AllClear ID</td>
</tr>
<tr>
<td>Avinash Shanbhag</td>
<td>HHS</td>
</tr>
<tr>
<td>Mark Scrimshire</td>
<td>NewWave</td>
</tr>
<tr>
<td>Calvin E Beebe</td>
<td>Mayo Clinic</td>
</tr>
<tr>
<td>Aman Raheja</td>
<td>Humana</td>
</tr>
<tr>
<td>Mike Donnelly</td>
<td>Epic</td>
</tr>
<tr>
<td>Scott Stuewe</td>
<td>DirectTrust</td>
</tr>
</tbody>
</table>

### FAST Facilitators

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Stephen Konya</td>
<td>ONC, FAST Lead</td>
</tr>
<tr>
<td>Patrick Murta</td>
<td>Humana, FAST Chief Architect</td>
</tr>
<tr>
<td>Paul Oates</td>
<td>Cigna, FAST Chief Architect</td>
</tr>
<tr>
<td>Brett Stringham, CISSP</td>
<td>Optum</td>
</tr>
<tr>
<td>Luis C. Maas III, M.D., Ph.D.</td>
<td>FAST Security Tiger Team Co-Lead</td>
</tr>
</tbody>
</table>

SK
# FAST Security Team Members

<table>
<thead>
<tr>
<th>Name</th>
<th>Organization</th>
</tr>
</thead>
<tbody>
<tr>
<td>Luis C. Maas III, M.D., Ph.D. (Co-Lead)</td>
<td>EMR Direct</td>
</tr>
<tr>
<td>Brett Stringham (Co-Lead)</td>
<td>Optum</td>
</tr>
<tr>
<td>Rose-Marie Nsahlai (Co-Lead)</td>
<td>ONC</td>
</tr>
<tr>
<td>Aaron Seib</td>
<td>Onyx</td>
</tr>
<tr>
<td>Kathleen Connor</td>
<td>US Dept. of Veterans Affairs/Book Zurman</td>
</tr>
<tr>
<td>David Kibbe</td>
<td>The Kibbe Group</td>
</tr>
<tr>
<td>Ali Massihi</td>
<td>ONC</td>
</tr>
<tr>
<td><strong>Debbie Bucci (past member and Co-Lead)</strong></td>
<td>ONC</td>
</tr>
</tbody>
</table>
• Welcome
• Session Goals
• Proposed Solution Overview: Trusted Ecosystem
  – Trusted Dynamic Client Registration
  – JWT-Based Client Authentication & Authorization
• Discussion: Trust Ecosystem
  – Feedback on the Overall Solution Approach
  – Trust Frameworks
  – X509 Certificates
  – JWT-Based Authorization
  – Multiple Networks/ Trust Frameworks
• Discussion: Stakeholder Readiness
• Discussion: Industry Path Forward
  – Implementation Guides
  – Regulations and Other Considerations
• Action Items
• Next Steps
SME Role

• You were selected for your domain expertise and the FAST team encourages you to provide input and perspective based upon your experience in your own field

• You will be asked to evaluate proposed solutions and provide your expert opinion and guidance on feasibility, unintended consequences, stronger alternate approaches and best implementation path forward

Session Logistics

• Place yourself on mute when not speaking

• Video is encouraged to enhance engagement with your peers, though not required, especially if you have any bandwidth or other issues that would prevent its use

• All ideas are good and valid – your questions, comments, and critiques will only enhance our work!
Session Goals

1. Obtain Feedback on Solution Approach of Adapting Existing Standards

2. Define and Apply Principles of Trust Ecosystem
   - Role of Trust Frameworks
   - X509 Certificates
   - Scopes and authorization metadata

3. Identify Path Forward
   - Stakeholder readiness
   - Regulatory impact
   - Path forward to gain consensus on the proposed security patterns
Example FHIR Transaction Journey

**REQUESTING SYSTEM**
1. Formulates FHIR Request
2. Looks Up the FHIR Endpoint for Recipient
3. Receives Transaction, Validates Requestor, Validates Version
4. Performs Patient Matching and Sends Back Not Found If Unable To Do So
5a. Authenticates FHIR User’s Role
5b. Filters Out Data That Does Not Have Consent
6. Generates & Returns FHIR Response

**DIRECTORY**
7. Requesting System Receives Data

**RECEIVING SYSTEM**
3. Transaction Information (e.g., Header) Appropriately Configured
4. Validates Requestor, Validates Version
5a. Authenticates FHIR User’s Role
5b. Filters Out Data That Does Not Have Consent
6. Generates & Returns FHIR Response

**IDENTITY**

**VERSIONING**

**EXCHANGE**

**DIRECTORY**

**CONFORMANCE & CERTIFICATION**

**SECURITY**

**PILOTS**
FAST Solutions

Recommended Infrastructure Solutions

• Tiger Teams
• TLC
• SME

FAST Solution Input

Ecosystem Use Cases

- Identity
- Directory, Version & Scale

Technical Barriers

- Core Capabilities
- Exchange Process
- Testing & Certification
- Pilots

Proposed Infrastructure Solutions

Core Capabilities

Evaluation, Feedback, and Pilots

Recommended Infrastructure Solutions

- Standards
- Process
- Regulation

Operationalize Solutions

PM
There is a significant amount of prior work in the industry that has specified security guidelines.

We do not need to replicate this work. Rather, we need to apply current security rules to FHIR use and identify gaps where scale is needed.

Today, we have limitations on our ability to ensure, in a scalable way, that the requestor of information using a FHIR based information exchange is appropriately authenticated and has the authorization to see the data requested.

How do we know the FHIR consumer has permission to ask or see?

We need a scalable solution that works for hundreds of millions of patients/insured and millions of requesting organizations and individual providers.
# Problems to be Solved

<table>
<thead>
<tr>
<th>Problem</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>CREDENTIAL SPRAWL</td>
<td>How can we minimize the number of credentials the requestor and responder are required to securely maintain?</td>
</tr>
<tr>
<td>CLIENT APPLICATION SPRAWL</td>
<td>How can we streamline the registration and user of client applications across multiple endpoints?</td>
</tr>
<tr>
<td>AUTHENTICATION &amp; AUTHORIZATION</td>
<td>How can we increase assurance that the requestor is appropriately authenticated and has the authorization to review and use the data requested?</td>
</tr>
<tr>
<td>EXISTING PROCESSES &amp; TOOLS LIMIT SCALABILITY</td>
<td>Techniques such as Open Authorization (OAuth 2.0) are widely accepted but can they be extended to improve scalability in FHIR?</td>
</tr>
</tbody>
</table>
| HIPAA MINIMUM NECESSARY                    | When payers have access to patients’ medical records using FHIR, the question of “minimum necessary” will become a significant issue since the current human mediated response will no longer take place.  
However, having direct access to clinical data allows the industry to reduce provider burden by decreasing the number of manual interventions providers need to manage to exchange data with payers and other providers.  
Instead of setting the bar at the “minimum necessary,” which can be interpreted differently by different stakeholders, the industry will need to move away from concerns about data access and shift toward defining the stated purpose for using the data (e.g., “I need access to these data for quality reporting measures”), which then becomes the approved use. |
FAST Solution Approach

- **Leverage existing credentials and authorizations**
  - Enabled by portable electronic requestor certifications
  - Securely communicate the verified attributes behind a requestor’s digital identity to responder

- **Enable federated access**
  - Federated use of credentials
  - Federated authorization servers

- **Leverage best practices (existing standards) — workable solutions**
  - OAuth 2.0 Authorization Framework
  - OpenID Connect
  - Unified Data Access Profiles
  - PKI-Based Health Information Networks

- **Facilitate automated exchange (i.e., reduce bottlenecks)**
  - Minimize time for participants to actively exchange with a new endpoint
  - Identify areas where solutions to authorization and authentication can be reused in more than one technical exchange protocol

- **Implement Role Based Access (where necessary)**

- **Reuse existing infrastructure where possible**
Proposed Solution: Trusted Ecosystem

UDAP Trusted Dynamic Client Registration

UDAP Tiered OAuth

User Authentication

Trusted DCR

Authorization Assertions

UDAP JWT-Based Authorization Assertions

UDAP JWT-Based Client Authentication

Client Authentication
Proposed Solution 1:

Trusted Dynamic Client Registration
**Proposed Solution: Trusted Dynamic Client Registration – Overview**

**Solution Summary**
For larger ecosystems with numerous requestors and responders a distributed system of authoritative information can be leveraged through the use of digital certificates to enable a scalable dynamic solution to client (i.e., requestor) registration. Requestor and Responder Actor pairs can be represented by provider/provider, provider/payer, and payer/payer pairings.

**In Scope**
- Establishing Identity of Network Participants
- Client App Registration
- Authentication (via digital certificates)
- Authorization (via verifiable attributes/endorsements from trusted 3rd parties)

**Assumptions**
- Registration will be completed before accessing resources
- Registration may be initiated by a system or by an individual/organization, but will always be performed by a **system to system communication**

**Out of Scope**
- Directory, Endpoint Discovery
- Trust Policy Governance
- Requirements for a specific architecture
- Patient/provider or provider/patient (for now)

*Requester must be able to protect the private key used to sign software statements

**Complexity Rating**
**Medium:** Extends existing OAuth 2.0 specifications; reuses existing technologies to validate JWTs & X.509 Certificates
Proposed Solution: Trusted Dynamic Client Registration & Token Request

**Prerequisites:**
- Client app obtains a trusted digital certificate and end user at requestor organization is authorized to use the app.
- Endpoints support DCR and policy logic identifies trusted applications and ecosystem participants.

**Requestor Actor**
1. UDAP Dynamic Client Registration request (signed with client’s certificate-backed key)
2. Authorization and/or Authentication JWT using client_id (signed with same key) e.g. UDAP JWT-Based Client Authentication
3. FHIR Transaction Request

**Registration Endpoint**
4. Access Token
5. FHIR Transaction Request

**Responder Actor**
- **Authenticate/Authorize (CC2)**
- **Reliable Provider Identity Management (CC6)**
- **Synchronous Transaction Support (CC12)**
- **Role/Context Identification (CC9)**

```
UDAP Dynamic Client Registration request (signed with client's certificate-backed key)
Authorization and/or Authentication JWT using client_id (signed with same key) e.g. UDAP JWT-Based Client Authentication
FHIR Transaction Request
Access Token
FHIR Transaction Response
```
Proposed Solution: Trusted Dynamic Client Registration

In Scope

Requestor Actor

1. UDAP Dynamic Client Registration request (signed with client's certificate-backed key)

Registration Endpoint

2. client_id

Responder Actor

3. Authorization and/or Authentication JWT using client_id (signed with same key) e.g. UDAP JWT-Based Client Authentication

4. Access Token

5. FHIR Transaction Request

6. FHIR Transaction Response

Prerequisites: Client app obtains a trusted digital certificate and end user at requestor organization is authorized to use the app

Data Provenance (CC5)

Prerequisites: endpoints support DCR and policy logic identifies trusted applications and ecosystem participants

Role/Context Identification (CC9)
Proposed Solution: Trusted Dynamic Client Registration

Trusted Dynamic Client Registration enables:

• Public Key registration for JWT-Based Authentication of Client Apps
  – for client credentials flow OR authorization code flow

• Server Validation
  – including multi-tenant environments

• Certifications and Endorsements
  – for tailored scopes

• Tiered OAuth for User Authentication
  – with authorization code flow
  – Identity provider as trusted network participant
Starting From Standard OAuth User Authorization

1. **Requestor Actor (Client App)**
   - User’s Browser
     - App sends User to authorization endpoint
     - Server redirects User Back to App
     - App receives code

2. **Responder Actor (Authorization Endpoint)**
   - Authenticate/Authorize (CC2)
   - Role/Context Identification (CC9)

3. **Responder Actor (Token Endpoint)**
   - Access Token

- **Step 3a**: App sends User to authorization endpoint
- **Step 3b**: Server redirects User Back to App
- **Step 3c**: App authenticates to responder and exchanges authorization code for access token
Starting From Standard OAuth User Authorization

Requestor Actor
Client App

User’s Browser

Responder Actor
Authorization Endpoint

Responder Actor
Token Endpoint

3a
App sends User to authorization endpoint

3b
Server redirects User Back to App

3c
App authenticates to responder and exchanges authorization code for access token

Authenticate/Authorize (CC2)

Access Token

Role/Context Identification (CC9)
Proposed Solution: Trusted Dynamic Client Registration & Tiered OAuth

Requestor Actor
Client App

User’s Browser

Responder Actor
Authorization Endpoint

Responder Actor
OIDC Endpoints

3a
App sends User to authorization endpoint

3b
Server redirects User Back to App

App receives code

Responder uses OpenID Connect to authenticate User

Authentication Response

Authenticate/Authorize (CC2)

Role/Context Identification (CC9)
The interaction between Responder Actor & Requestor Actor’s OIDC endpoint can be based on dynamic client registration of the Responder Actor (as an OIDC client) with OIDC endpoint.

For example...

• the Requestor Actor’s client app can ask the Responder Actor to use the Requestor’s own OIDC endpoint with this workflow...
• even if the Responder Actor has not previous registered with that endpoint
Proposed Solution 2:
JWT-Based Client Authentication & Authorization
Proposed Solution: JWT-Based Client Authentication & Authorization – Overview

Solution Summary
Many organizations have established digital identities that can be reused within a trust community to facilitate a request to a responder’s endpoint. JWT-based client authentication leverages existing public key infrastructure and validated identities to help scale authentication and authorization.

Assumptions
• The request for authentication and authorization may be initiated by a system or by an individual/organization (i.e., Requestor must be able to protect the private key used digital signatures)
• Authentication and authorization transactions will be synchronous
• Patient is known/consent has been granted in requests that obtain sensitive health data from responder
• Directory available to find provider/payer related endpoints
• Responder does not need to validate that the sharing of the data conforms to HIPAA as it already falls under the three acceptable uses for HIPAA (Treatment, Payment, and Operations)

In Scope
• Authentication (via digital certificate – X.509)
• Authorization (via OAuth2 Extensions such as verified claims, certifications & endorsements)

Out of Scope
• Directory, Endpoint Discovery
• Trust Policy Governance
• Requirements for a specific architecture
• Patient/provider or provider/patient (for now)

Complexity Rating
Medium: Extends existing OAuth2 specifications (e.g., access token); reuses existing technologies to validate JWTs & X509 Certificates
Proposed Solution: JSON Web Token-Based Client Authentication – Process Flow

Prerequisites: Client app obtains a trusted digital certificate and end user at requestor organization is authorized to use the app.

Data Provenance (CC5)

In Scope

Out of Scope

Requestor Actor

1. UDAP Dynamic Client Registration request (signed with client’s certificate-backed key)

Registration Endpoint

- client_id

2. Authorization and/or Authentication JWT using client_id (signed with same key) e.g. UDAP JWT-Based Client Authentication

3. 

Responding Actor

- Authenticate/Authorize (CC2)
- Reliable Provider Identity Management (CC6)
- Synchronous Transaction Support (CC12)
- Access Token
- FHIR Transaction Request
- FHIR Transaction Response

Role/Context Identification (CC9)

Prerequisites: endpoints support DCR and policy logic identifies trusted applications and ecosystem participants.

Prerequisites:
- endpoints support DCR and policy logic identifies trusted applications and ecosystem participants.
- Requester organization is authorized to use the app.
Proposed Solution: JSON Web Token-Based Client Authentication – Process Flow

**Prerequisites:**
- Client app obtains a trusted digital certificate and end user at requestor organization is authorized to use the app.

**Requestor Actor**
1. UDAP Dynamic Client Registration request (signed with client’s certificate-backed key)
2. Authorization and/or Authentication JWT using `client_id` (signed with same key) e.g. UDAP JWT-Based Client Authentication

**Registration Endpoint**
- `client_id`

**Responder Actor**
- **Authenticate/Authorize (CC2)**
- **Reliable Provider Identity Management (CC6)**
- **Synchronous Transaction Support (CC12)**

**In Scope**
- Prerequisites: endpoints support DCR and policy logic identifies trusted applications and ecosystem participants

**Out of Scope**
- Prerequisites: endpoints support DCR and policy logic identifies trusted applications and ecosystem participants

Data Provenance (CC5)

Role/Context Identification (CC9)
Support real-time assessment of the request’s trust & scope

1. Can the FHIR endpoint trust the identity associated with the request to access protected information?
2. What attributes (e.g., requesting organization) are linked to the requestor’s identity that will inform this real-time trust assessment?
3. What is the scope of the request (e.g., read, update, specific patient)?

An authorization server (AS) provides an access token to the requestor (i.e., answers to the questions above have been verified)

1. Assurance levels are satisfied that the request originates from a trusted requestor
2. Scope of the request has been authorized
3. The access token will be compatible with FHIR responding server
JWT-Based Client Authentication & Authorization

**Relationship to Existing OAUTH2 Standards**

- This security solution is defined as an extension to the OAuth 2.0 authorization framework defined in RFC 6749, based in part on the profiles defined in RFC 7521 and RFC 7523 for assertion based authentication

- RFC 7521 enables OAuth2 to work with other identity systems using assertions and to allow for alternative client authentication mechanisms

- The RFC 7523 standard allows new extensions (i.e., new JWT profile)
  - Example (for this solution): A requestor in a FHIR transaction will utilize semantics of the JWT to express an existing trust relationship (e.g., is authorized to access certain data)
Trust Communities

Reusing established digital identities (i.e., leverage existing PKI infrastructure)

- Many organizations have established digital identities that can be reused within a trust community for FHIR transactions.
- Digital identities, expressed in digital X509 certificates, enables the requestor to authenticate itself to a responder’s endpoint.
- The use of these digital identities helps to remove the burden of credentials management among FHIR transaction participants – paving the way for scalability within the FHIR ecosystem.
What is an Assertion?

• Assertions are statements from one party (i.e., issuer) that allow a relying party (RP) to make authorization decisions regarding access to resources held by the responder.

• For example, attributes tied to a digital identity, purpose/scope of a given request, authorization (e.g., consent) has been granted to access certain information.
JWTs & Assertions

**JSON Web Tokens (JWT)**

- Structured way to sign and package assertions
- Serves as a security token that contains information which has been asserted by the issuer (could include information verified by the 3rd party)
- Signed with a digital signature
  - Protects token from tampering
  - Provides high assurance that the token was produced by a trusted party
- Two types are leveraged in this solution:
  1. JWT-based authentication
  2. JWT-based authorization
**Basic Scenario:** Requestor is a privileged application (applies when certificate contains necessary attributes for the token endpoint to also make an authorization decision in addition to authentication)

3. Requestor first prepares an authentication token (AnT) for inclusion in the request to the token endpoint. The AnT is a JWT that serves to purposes...
   1. Establishes requestor’s control of the private key
   2. Provides the certificate necessary for the token endpoint to validate the signature and establish trust

---

**Diagram:**
- **3** Requestor prepares an authentication token (AnT) for inclusion in the request to the token endpoint.
- **4** Token Endpoint issues an Access Token.

**Details:****
- Authentication and/or Authorization JWT using `client_id` (signed with same key)
- e.g. UDAP JWT-Based Client Authentication

**Text:**
- Authentication and/or Authorization JWT using client_id (signed with same key)
- e.g. UDAP JWT-Based Client Authentication
The AnT is a digitally signed JWT containing the following claims:

- **Issuer** (iss): unique identifying (URI) of the client token service for the assertion signer
- **Subject** (sub): the client ID issued by the AS to the client application
- **Audience** (aud): token endpoint (URI) of the authorization server
- **Expiration time** (exp): token expiration time expresses as second since epoch (should be short-lived)
- **Issued at time** (iat): issued at time expressed as seconds since epoch
- **JWT ID** (jti): token identifier used to detect a token replay
**Alternate Scenario:** Requestor first obtains a digitally signed Authorization Assertion (AzA) from resource owner / authorized party

- Once received, the requestor may then include this AzA with in the same JWT that will also contain an AnT to the token endpoint.
The Requestor May Use an Aza to Communicate to the Token Endpoint...

**Examples**

- That the requested resource will be used for a specific purpose permitted by a data use agreement
- Information will only be shared with a certain class of users
- That the request is being made on behalf of a particular organization or person
- Consent has been obtained
The AzA is a digitally signed JWT containing the following claims:

- **Issuer** (iss): unique identifying (URI) of the client token service for the assertion signer
- **Subject** (sub): the authorized requestor for which the access token is being requested
- **Authorized Party** (azp): equal to the client application (i.e., requestor) identifying URI
- **Audience** (aud): token endpoint (URI) of the authorization server
- **Resources**: optional - array of URIs of specific resources authorized by the assertion signer (i.e., resource owner/authorized party); when absent implies requestor has access to all resources issuer has access to
- **Scope**: optional - delimited list of scopes requested by the client application (i.e., requestor)
- **Extensions**: if required by the authorization server (AS) – for example, the purpose (e.g., payment, treatments, etc.) for which information is requested and the user who initiated the request / query.
**JWT-Based Client Authentication With Authorization**

**Alternate Scenario:** Requestor has received an authorization token (AzA) from a trusted party

1. Requestor prepares a signed JWT that includes an authentication token (AnT) as well as the authorization token (AzA) that was received.

2. The authorization server (AS) receives the signed JWT at the access token endpoint.
   - Validates the JWT’s digital signature and the AnT (i.e., is the requestor trusted?)
   - Validates the AzA (i.e., signed by a trusted party)

Diagram:
- AnT + AzA (from trusted party)
- Access Token
- AS - Token Endpoint
- Authenticate/Authorize (CC2)
Discussion Topic

Feedback on the Overall Solution Approach
Discussion: Proposed Solution Approach

Does the overall approach of adapting existing standards make sense?

- UDAP Tiered OAuth
- UDAP Trusted Dynamic Client Registration
- UDAP JWT-Based Authorization Assertions
- UDAP Trusted Dynamic Client Registration
- UDAP JWT-Based Client Authentication
Discussion: Proposed Solution Approach

Are there broad areas that are not covered by the solution, but should be?
Break: 5-10 minutes
Discussion Topic

Trust Frameworks

A principle of the solution is that parties’ roles and security assertions are based on their belonging to a trust framework.
What are the “rules of the road”? 
• Will an organization join multiple trust frameworks? 
• Who can build a trust framework?
Discussion: Trust Across Frameworks

How can participants trust across frameworks?

- What role do you see for formal trust framework definitions? E.g., to govern how you federate across frameworks, especially with respect to authorization?
- Is there a need for an “umbrella” framework above, or do participants work across?
  - Defining agreement / contract? What’s the minimum that needs to be included? What’s optional?
    - E.g., ability to segment data
    - Federation or cross-network?
- What “scope of authorization” is a participant working under at any given point in time
Discussion: Trust Frameworks – Integrating Existing Networks

How readily can existing interoperability networks fit into the model?
Discussion Topic

X509 Certificates

The solution uses X509 certificates to represent a party’s scope
Discussion: X509 Certificates – Information Needs

What information needs to be included in the X509 certificate?

- Identification of the organization responsible for that application or server?
- HIPAA status such as covered entity?
- ?
What level of certificate issuance granularity is needed?

- Domain name vs. URIs to identify participants
- Certificates for organizational participants (e.g., hospitals, payers) vs. users
- Apps (software) vs. users of the software
- Apps vs. operators (responsible for operation of the software)
Polling Question: What client application attributes are most important for a responder to authorize a FHIR transaction (choose all that apply)?

• Developer Name
• Application Web Site
• Application Operator’s Privacy Policy
• Application Operator’s HIPAA status
• Other (please indicate in comment box)
Solution strategy - building on existing standards

Trusted Dynamic Client Registration vs Open Dynamic Client Registration

Allowance for less automated registration methods where needed

Use of PKI infrastructure, with multiple issuers (solution doesn’t require all participants to sign up with a single PKI vendor or network)

Role of certifications and endorsements in the framework

Trust across frameworks: Collaboration between existing trust frameworks versus use of an umbrella trust framework

Use of X509 certificates in the solution

Discussion of certificate content – may be use case and participant-specific
Polling Summary from the First Session

<table>
<thead>
<tr>
<th>Question</th>
<th>Yes</th>
<th>Somewhat</th>
<th>No</th>
</tr>
</thead>
<tbody>
<tr>
<td>Do you agree with the proposed solution approach?</td>
<td>67%</td>
<td>33%</td>
<td></td>
</tr>
</tbody>
</table>

**“Somewhat” comments:**
- Commenter: Standards need to be piloted for practical implementation experience
- Commenter: Policies seem to be an issue to flesh out further
- Commenter: Concerned about OpenID Connect-related protocols. *Discussion: The FAST team will reevaluate emerging standards/technology more thoroughly as they come to completion*

<table>
<thead>
<tr>
<th>Question</th>
<th>Developer Name</th>
<th>Application Web Site</th>
<th>Application Operator’s Privacy Policy</th>
<th>Application Operator’s HIPPA Status</th>
<th>Other</th>
</tr>
</thead>
<tbody>
<tr>
<td>What client application attributes are most important for a responder to authorize a FHIR transaction? (choose all that apply)</td>
<td>55%</td>
<td>45%</td>
<td>82%</td>
<td>64%</td>
<td>45%</td>
</tr>
</tbody>
</table>

**“Other” comments:**
- Commenter: This is very context-dependent
- Commenter: Terms of Service, Certification to trust frameworks e.g., CARIN
- Commenter: Depends on use case, individual / organizational choices, perspective, values
Discussion Topic

JWT-Based Authorization

Scopes and Authorization Metadata
What information needs to be included in the software statement?

- What adjunct information about the application itself may be useful? (e.g., patient disclosure, privacy policy, etc.)
**Discussion: JWT Authorization – Additional Authorization Metadata**

**Additional authorization metadata a responder will need from the requestor to...**

Authorize the transaction or record in the audit log? E.g., user role, purpose of use, consent references...

---

**Requestor Actor**

- UDAP Dynamic Client Registration request (signed with client’s certificate-backed key)
- Authorization and/or Authentication JWT using client_id (signed with same key) e.g. UDAP JWT-Based Client Authentication
- FHIR Transaction Request

**Responder Actor**

- Authenticate/Authorize (CC2)
- Reliable Provider Identity Management (CC6)
- Synchronous Transaction Support (CC12)
- Access Token
- FHIR Transaction Response

**Prerequisites:**
- Client app obtains a trusted digital certificate and end user at requestor organization is authorized to use the app
- Prerequisites: endpoints support DCR and policy logic identifies trusted applications and ecosystem participants

---

**Data Provenance (CC5)**

- In Scope
- Out of Scope
Discussion: JWT Authorization – Scope vs. Authorization

The proposed solution differentiates between scope and authorization metadata.

What concepts are better expressed as OAuth scope vs. authorization metadata?

Proposal:

**OAuth Scope answers:** What do I want? What do I want to do? For example:
- Read access
- Condition resource

**Authorization metadata answers:** Why do I want it? What do I want it for? Why should you give it to me? For example:
- Purpose of use (individual right of access, treatment, payment, etc.)
- “Break the glass”
Polling Question: Do you agree with the approach discussed regarding scopes and authorization metadata?

- Yes
- No (please enter comments in the chat box)
- Somewhat (please enter comments in the chat box)
Discussion Topic

Multiple Networks

How could multiple networks or trust frameworks share a common foundation that implements these extensions?
Discussion: Multiple Networks or Trust Frameworks

How could multiple networks or trust frameworks share a common foundation that implements these extensions?

- What are the minimum policy & technical requirements to support cross-network exchange or cross-framework exchange?
- Minimum assertions in the JWT needed for effective cross network exchange?
Polling Question: Do you agree that the proposed solution can express the necessary information to enable cross-network exchange?

- Yes
- No (please enter comments in the chat box)
- Somewhat (please enter comments in the chat box)
Discussion Topic

Stakeholder Readiness

Readiness of payers, providers and vendors to implement these extensions
Discussion: Stakeholder Readiness

- Readiness of trust networks to support these use cases
- Technical readiness
- Policy readiness (e.g., legal agreements)

Readiness of payers, providers, vendors, others to implement these extensions?
Polling Question: Rate the technical and operational readiness of trust networks, payers, providers and vendors to implement these extensions. Please enter additional comments in the chat box.

• Completely ready
• Somewhat ready
• Not at all ready
Discussion Topic

Industry Path Forward

What is the path forward to gain consensus around the proposed security patterns?
Various FHIR Implementation Guides are being drafted today. Authors are grappling with security guidance.

What is the right output of this group, to provide to the industry?

How can the guidance be made most consumable by implementers and IG writers?

Where is the logical home for the work of creating and maintaining the guidance?

Ballot guidance through HL7 or other standards body?
Discussion: Other adoption considerations

Are there legal, regulatory, or standards aspects that need to be considered to support adoption and implementation of the proposed security patterns?
Polling Question: What type of legal, regulatory or standards aspects come to mind?

*Please provide your top three in the chat box*
Action Items/ Next Steps
• *Summary of key takeaways from this SME session*
FAST Next Steps

- FAST Report-Out to summarize SME Session discussion, decisions, and next steps will be posted in August: FAST Scalable Security Proposed Solution - Expert Panel Discussion

- FAST Action Plan to define proposed solution path (standard, regulation and/or process)

In the meantime, please reach out to the FAST team with additional feedback or questions!

CONTINUE THE CONVERSATION!

Join the Technical Learning Community to stay up to date – receive updates about FAST presentations & events, provide additional input and follow our progress.

JOIN THE LINKEDIN GROUP & SIGN UP FOR THE TLC
Thank You – Today’s Presenters

Patrick Murta
FAST Chief Architect

Paul Oates
FAST Chief Architect

Stephen Konya
ONC FAST Lead

Brett Stringham, CISSP
FAST Security Tiger Team Lead

Luis C. Maas, III, M.D., Ph.D.
FAST Security Tiger Team Lead

Connect with us on LinkedIn to stay informed

For more information on the FAST Initiative, visit the FAST Project Page or https://tinyurl.com/ONC-FAST

Have any further questions/suggestions?

Please contact Stephen Konya at Stephen.Konya@hhs.gov
& Diana Ciricean at Diana.Ciricean@hhs.gov