



***FAST* Focus Webinar**

Secure Healthcare Data Exchange - *FAST* Security IG
Supports Scalable and Secure Healthcare Systems

May 2024



HL7 Antitrust Statement



Professional Associations, such as HL7, which bring together competing entities are subject to strict scrutiny under applicable antitrust laws.

HL7 recognizes that the antitrust laws were enacted to promote fairness in competition and, as such, supports laws against monopoly and restraints of trade and their enforcement.

Each individual participating in HL7 meetings and conferences, regardless of venue, is responsible for knowing the contents of and adhering to the HL7 Antitrust Policy as stated in §05.01 of the Governance and Operations Manual (GOM).



Agenda & Speakers



Welcome

FAST Security Implementation Guide
(IG) Overview

Industry Policy and Use

FAST Implementer Panel

How You Can Engage/Call to Action

Q&A

- Luis Maas, Chief Technology Officer, EMR Direct
- Brett Stringham, Distinguished Engineer - Platform Security, Optum
- Joseph Shook, Senior Software Architect, Surescripts LLC
- Jason Vogt, Development Manager, APIs and Structured Documents, MEDITECH
- Tom Loomis, Enterprise Architecture, Interoperability, Evernorth
- Dan Cinnamon, Principal Solutions Architect, Okta, Inc.
- David Pyke, *FAST* Technical Director, Standards Architect, Audacious Inquiry, a PointClickCare Company

Facilitated by:

- Alix Goss, Senior Consultant, Point-of-Care Partners

FAST Security IG





Overview – Security for Scalable Registration, Authentication, and Authorization



BARRIER

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. Current registration processes are manual and too time-consuming to support expected growth



SOLUTION

Leverage existing credentials and authorizations and best practice standards to establish common security processes that facilitate automated exchange and reuse existing infrastructure where possible



IN SCOPE

Trusted Dynamic Client Registration using Unified Data Access Profiles (UDAP)

JWT-Based Client Authentication & Authorization



OUT OF SCOPE

Directory for Endpoint Discovery, Trust Policy Governance, Requirements for a specific architecture, Patient/provider or provider/patient



Security for Scalable Registration, Authentication, and Authorization

[JWT-Based Client Authentication:](#)

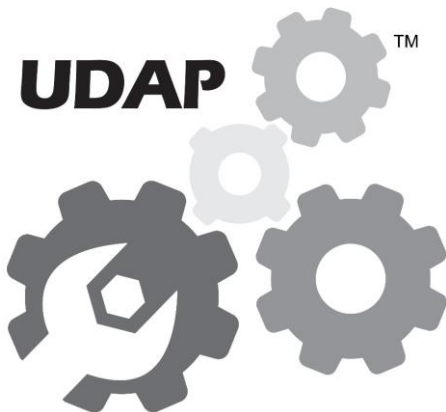
Uses asymmetric cryptography to authenticate client apps

[Server Metadata:](#)

Endpoint validation for added confidence

[Trusted Dynamic Client Registration:](#)

Identify and dynamically register trusted client applications, streamlining app management



[JWT-Based Authorization Assertions:](#)

Extensible JWT-based client authorization grants & other claims incidental to a token request

[Certifications & Endorsements:](#)

Trusted informational assertion

[Tiered OAuth:](#)

Reusable identities via scalable, dynamic, cross organizational use

Connectathon Track Page:
[2024 - 05 FAST Infrastructure \(Security & Identity\)](#)

Project Scope Statement:
[Scalable Registration, Authentication, and Authorization for FHIR Ecosystem Participants](#)

Implementation Guide:
[Security for Scalable Registration, Authentication, and Authorization](#)



UDAP Trusted Dynamic Client Registration

- For larger ecosystems with numerous requestors and responders a distributed system of authoritative information can be leveraged through the use of digital certificates
- This enables a scalable dynamic solution to client (i.e., requestor) registration
- The solution extends OAuth 2.0 workflows and Dynamic Client Registration to add assurance for and about all parties involved in the API ecosystem

- Automated registration API
 - Replace (and standardize) manual developer registration processes
- Trusted app operator identities
 - Reusable credentials



UDAP JWT-Based Client Authentication

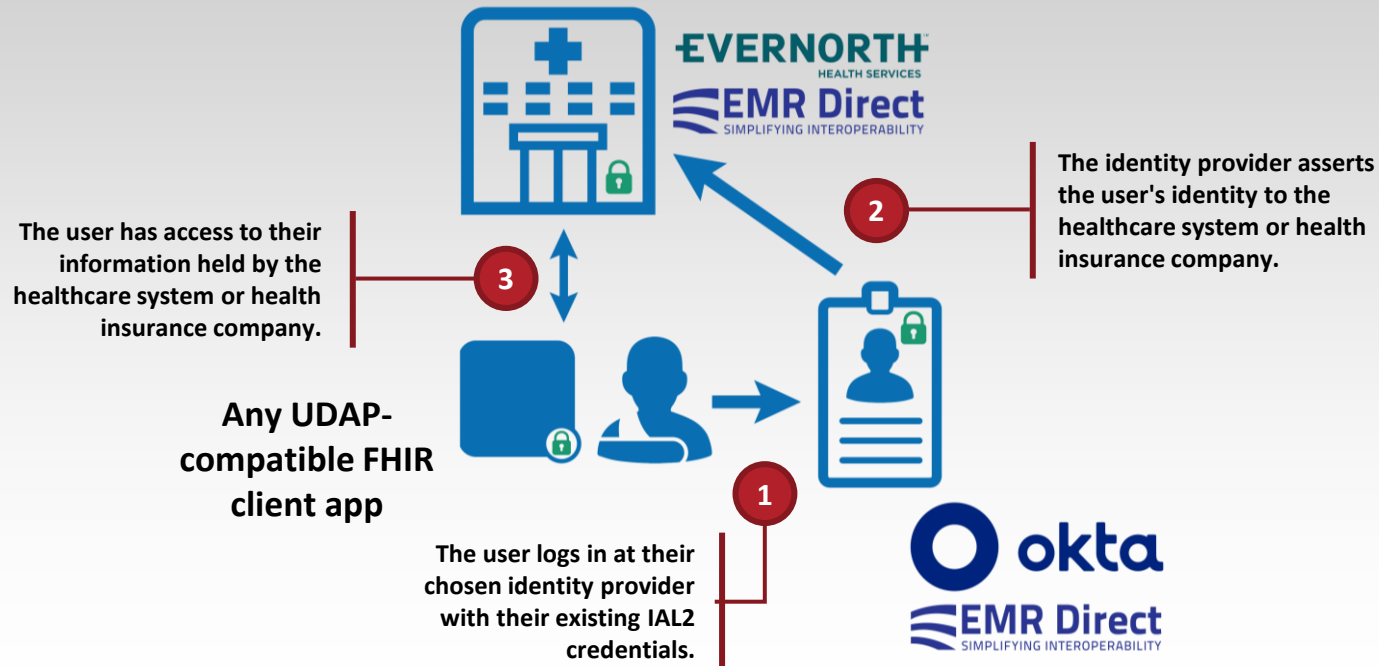


- Increased security over shared secrets
 - E.g., RSA, Elliptic Curve
- Simplified Key Management
 - Public Key Infrastructure
- Increased confidence for actions beyond read-only access
- Authorization Extension Objects
 - Allows for extension of authorization data as required by workflows



UDAP Tiered OAuth

The user wishes to access their data held by a system where they don't have credentials.
They specify an approved identity provider for authentication.





UDAP Tiered OAuth Benefits



- No advance testing or integration is required by ecosystem participants (client app, relying party data holder, and credential service provider implement UDAP profiles and use in real-time discovery and trust validation) for true scalability.
- Patients can use one trusted set of credentials representing their identity to interact with multiple healthcare systems/fewer credentials to maintain.
- Health record systems have a high level of confidence about which patient has been authenticated, as well as protection from breach severity knowing they are using publicly-available security and patient matching standards, particularly if the hl7_identifier is used for more perfect patient matching.



Ecosystem Benefits



- Scalability
 - Frictionless app onboarding & life cycle management; automated discovery
 - Reusable credentials for apps, servers, & users
- Security
 - Trusted apps and servers are identified through digital certificates, eliminating
 1. app impersonation due to a compromised secret
 2. server impersonation leading to compromised user's or app's credentials or compromised PII or PHI, and
 3. data provenance and credential trust issues
 - Exchange health data directly between trusted endpoints & trust the source of assertions made, e.g. Purpose of Use, HIPAA Authorization, verified Identity Attributes
 - Identity information is exchanged directly from IdP to FHIR server using Tiered OAuth
 - Verifiable directory information and endpoint identity



Standards Alignment



- Requirements/reliance on UDAP
 - FHIR Security specification for R5
 - HL7 FAST Interoperable Digital Identity and Patient Matching IG
 - Da Vinci HRex
- Support for UDAP
 - CARIN Blue Button IG
- Implementations utilizing FAST Security
 - TEFCA Facilitated FHIR
 - Carequality FHIR IG
 - CommonWell FHIR IG
 - eHealth Exchange Authorization Framework



Industry Implementation & Testing



- Implementations
 - Diverse industry efforts
 - HL7 FHIR Connectathon Testing
 - IHE/Carequality Connectathon Testing
 - Commonwell Connectathon Testing
 - Open-Source Reference Implementations (next slide)
 - CARIN POC tested UDAP Tiered OAuth and *FAST* Identity concepts, and the [final report](#) recommended this approach as one of two preferred paths toward digital identity federation



Open-Source



Evernorth/Okta Reference UDAP client app, client SDK, and server:

<https://github.com/Evernorth/hl7-fhir-udap-docs>

Opensource Spring Boot – UDAP Client (client_credentials grant)

<https://github.com/udap-tools/udap-spring-boot>

.NET Reference Implementation covering the full implementation guide. [NuGet packages](#) for building Client, Metadata Server, Auth Server and Tiered OAuth (IdP).

Stable Home: [udap-tools/udap-dotnet: reference implementation for .NET \(github.com\)](https://github.com/udap-tools/udap-dotnet)

Daily development: <https://github.com/JoeShook/udap-dotnet/tree/develop>

Open-Source / UDAP Education

• <https://udaped.fhirlabs.net> is a visualization of UDAP.

- Explore the home page to find negative use cases to experiment with.
- Experience the Implementation Guide in action with UdapEd.

• Examples of how build clients and servers with .NET UDAP NuGet packages. Developers can spin up a lab environment locally covering the whole Implementation Guide.

- <https://github.com/JoeShook/udap-devdays-2023>
- <https://github.com/JoeShook/udap-devdays-2024>

• The Interoperable Digital Identity and Patient Matching RI is using the .NET UDAP RI for their implementation of UDAP.

=>

The screenshot displays the UdapEd application interface. On the left is a navigation sidebar with options like Home, Discovery, Registration, B2B, Consumer, Tiered OAuth, SMART Area, Patient, Search, Match, Directory, and Todo. The main content area is titled 'Udap Metadata' and features a 'QUERY' button and a 'REMOVE BASE URL' button. Below these is a 'Choose Trust Anchor Certificate' section with buttons for 'LOAD EMR DIRECT TEST CA' and 'UPLOAD'. A dropdown menu shows 'Community' selected. The bottom part of the interface is split into two panels: 'Discovery / Metadata / Signed / Communities' and 'SIGNED SOFTWARE STATEMENT / CERTIFICATES'. The left panel shows a JSON object representing UDAP metadata, including supported versions, profiles, extensions, and signing algorithms. The right panel shows a 'Decoded software statement' with a header 'Algorithm & Token Type' and a 'SIGNED STATEMENT' section containing a large block of base64-encoded data.



FAST Security IG Status



- Discussions around the use of the Security IG continue and have increased with the adoption of the IG by TEFCA
- The co-leads have been categorizing updates to be part of an STU Update or STU2
- The FHIR Connectathon wrapped up with testing done using the updated RI and new test scripts. As with Identity we are looking into the results of testing, including what we tested and what issues came up, to refine the Track description for July / September

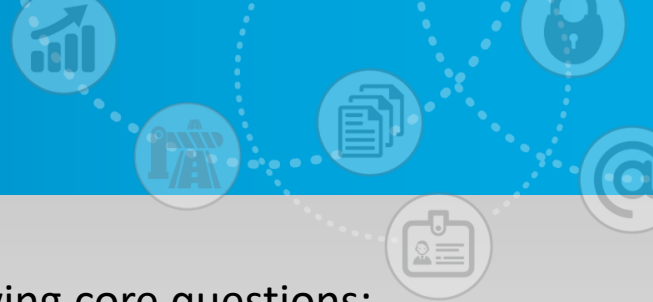
REQUESTS



- Meets on the 2nd & 4th Tuesdays of the month at 2pm ET, get involved to help make STU2 ([HL7 Conference Call Center](#))
- Confluence space: <https://confluence.hl7.org/display/FAST/Security+for+Scalable+Registration%2C+Authorization%2C+and+Authentication>



Implementer Panel



Implementers will share their stories and answer the following core questions:

- Why did you implement the *FAST* Security IG?
- What value are you getting from it?
- What have folks already implemented that provides a glidepath to implementation?

Q&A



Engaging with *FAST*





Simple Ways to Join *FAST's* Work



<i>FAST</i>: Security for Scalable Registration, Authentication, and Authorization	<i>FAST</i>: Directory	<i>FAST</i>: Interoperable Digital Identity & Patient Matching	<i>FAST</i>: Consent
<p>HL7 Project Page Security for Scalable Registration, Authentication, and Authorization</p>	<p>HL7 Project Page Directory</p>	<p>HL7 Project Page Interoperable Digital Identity & Patient Matching</p>	<p>HL7 Project Page Consent</p>
<p>Public Meetings the 2nd and 4th Tuesdays Each Month at 2PM ET https://hl7-org.zoom.us/j/99770852614?pwd=Sk1QUDBiY0huSDNxYVQ4YW5KNkpidz09_</p>	<p>Public Meetings: Biweekly meetings on Mondays at 3pm ET as of April 29th https://hl7-org.zoom.us/j/95314390248?pwd=QUhvNktmTVJiWUk2ZnRHSmdWcHpmdz09</p>	<p>Public Meetings the 1st and 3rd Thursdays Each Month at 2PM ET https://hl7-org.zoom.us/j/99145025586?pwd=bE01OFVHZkVta051S1RjbjZMTFRQT09</p>	<p>Public Meetings: Launched April 5th and calls to be held 2nd and 4th Fridays at 2 pm ET https://hl7-org.zoom.us/j/93156049340?pwd=UmpibnBHNONSZThmZUhpdkppWE5tdz09</p>
<p>Chat.fhir Stream https://chat.fhir.org/#narrow/stream/294749-FHIR-at.20Scale.20Taskforce.20.28FAST.29.3A.20Security</p>	<p>Chat.fhir Stream https://chat.fhir.org/#narrow/stream/283066-united-states.2Fnational.20directory</p>	<p>Chat.fhir Stream https://chat.fhir.org/#narrow/stream/294750-FHIR-at.20Scale.20Taskforce.20.28FAST.29.3A.20Identity</p>	<p>Chat.fhir Stream https://chat.fhir.org/#narrow/stream/426241-FHIR-at-Scale-.28FAST.29.3A-Consent-Management</p>

Implementer Support Office Hours are on the first Tuesday each month from 1 – 2 pm ET

[Join the Implementer Support Hours Conference Call](#)



FAST Artifacts and Resources



Want to learn more about becoming a member of the HL7 *FAST* FHIR Accelerator?

Want to work with us to implement and test the *FAST* Security IG?

Contact fast@hl7.org

**CONTINUE THE
CONVERSATION!**



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

[VISIT FAST PROJECT PAGE](#)

[JOIN FAST LISTSERV](#)

[JOIN THE LINKEDIN GROUP](#)



Thank You

For more information on the *FAST* Initiative,
visit the *FAST* [Project Page](#)

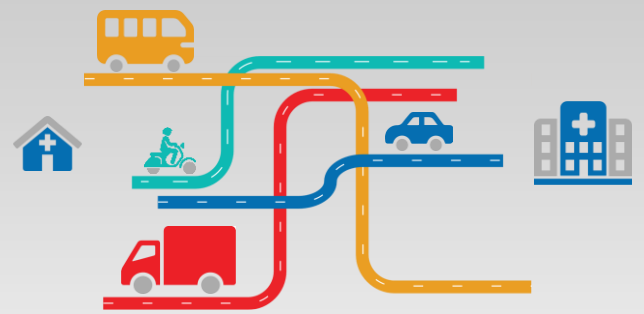
Have any further questions/suggestions?
Please contact fast@hl7.org

FAST – Level Setting





What is the Problem?



TODAY - Exchange

Exchange characterized by point-to-point interfaces
Adoption trajectory is slow, expensive, and fragmented



FUTURE - Interoperability

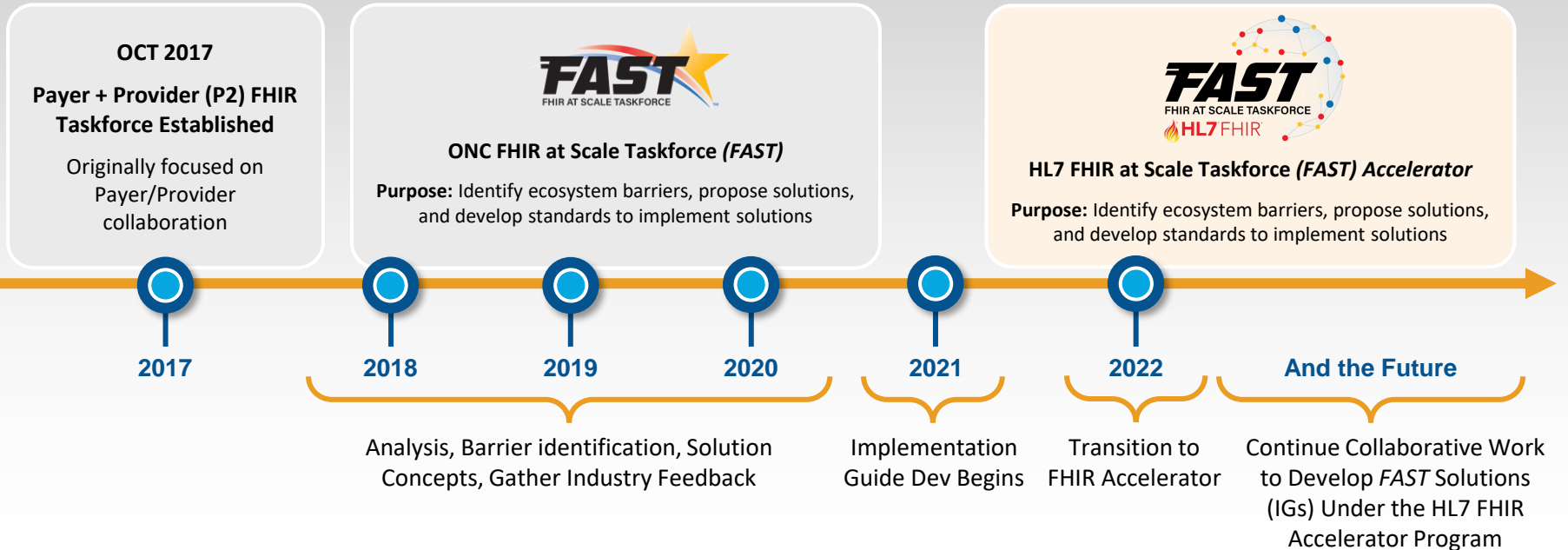
A common & consistent infrastructure approach to API implementation
Consensus on implementation guides for key enablers, such as directory, security, patient matching, exchange and testing

DESIRED RESULT:
A national interoperability approach that enables consistent data exchange via API. We have this for administrative transactions (X12, clearinghouses, WEDI) and pharmacy transactions (NCPDP, Surescripts). We do not have this for HL7-FHIR.

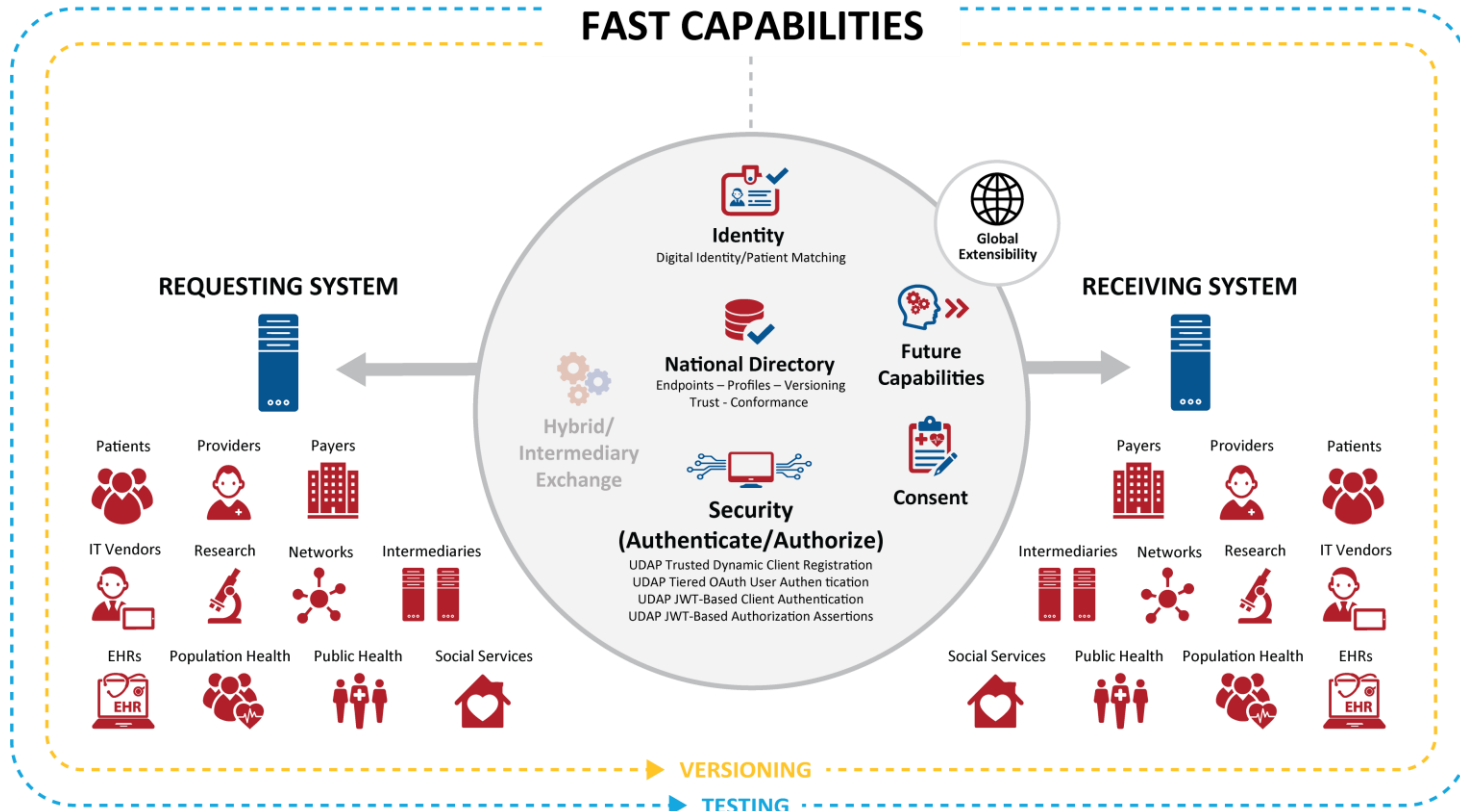


What is FAST?

The *FHIR at Scale Taskforce (FAST)* is a representative community of motivated healthcare industry stakeholders and health information technology experts who have identified HL7® Fast Healthcare Interoperability Resources (FHIR®) scalability gaps and are actively working on solutions to address current barriers to enable scalable data exchange using FHIR APIs



Conceptual Architecture





FAST 2024 Members

