HL7® FHIR® Security

Education Event

May 2024

HL7 International

ASTP Assistant Secretary for Technology Policy

ONC Office of the National Coordinator for Health Information Technology

Imp[lamenting Secure Healthcare Data Exchange

FAST Security IG Supports Scalable and Secure Healthcare Systems

HL7® International

ASTP
Assistant Secretary for Technology Policy

ONC
Office of the National Coordinator for Health Information Technology

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

- 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
- David Pyke, *FAST* Technical Director

Slides and recording to be posted: https://confluence.hl7.org/display/FAST/FAST+Calendar

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

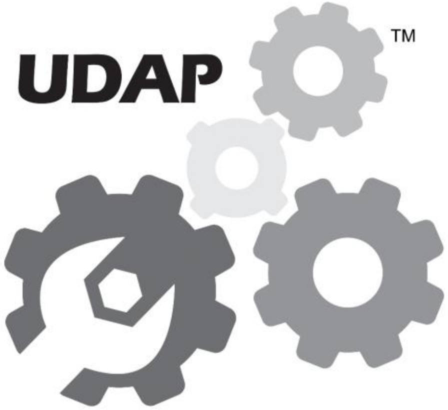
JWT-Based Client Authentication:

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

BS

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

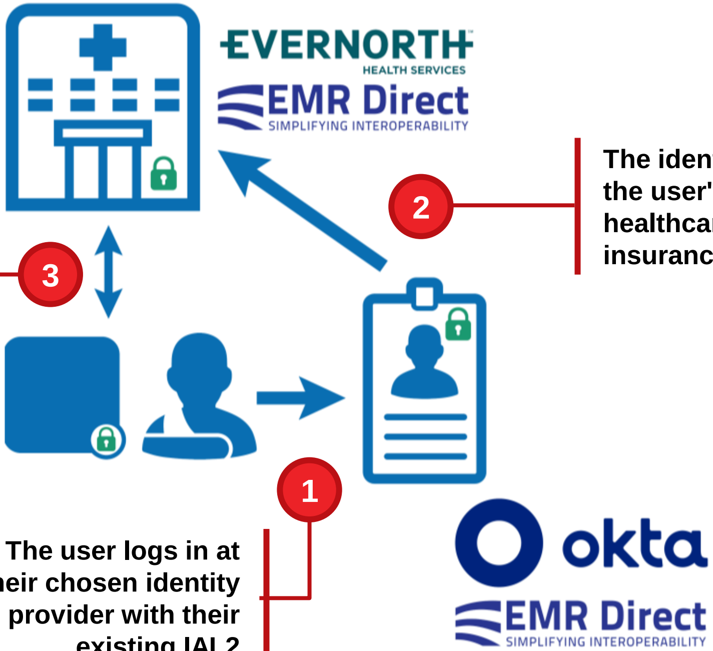
UDAP JWT-Based Client Authentication

- 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

~~BS~~

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.



Any UDAP-compatible FHIR client app

1 The user logs in at their chosen identity provider with their existing IAL2 credentials.

2 The identity provider asserts the user's identity to the healthcare system or health insurance company.

3 The user has access to their information held by the healthcare system or health insurance company.

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

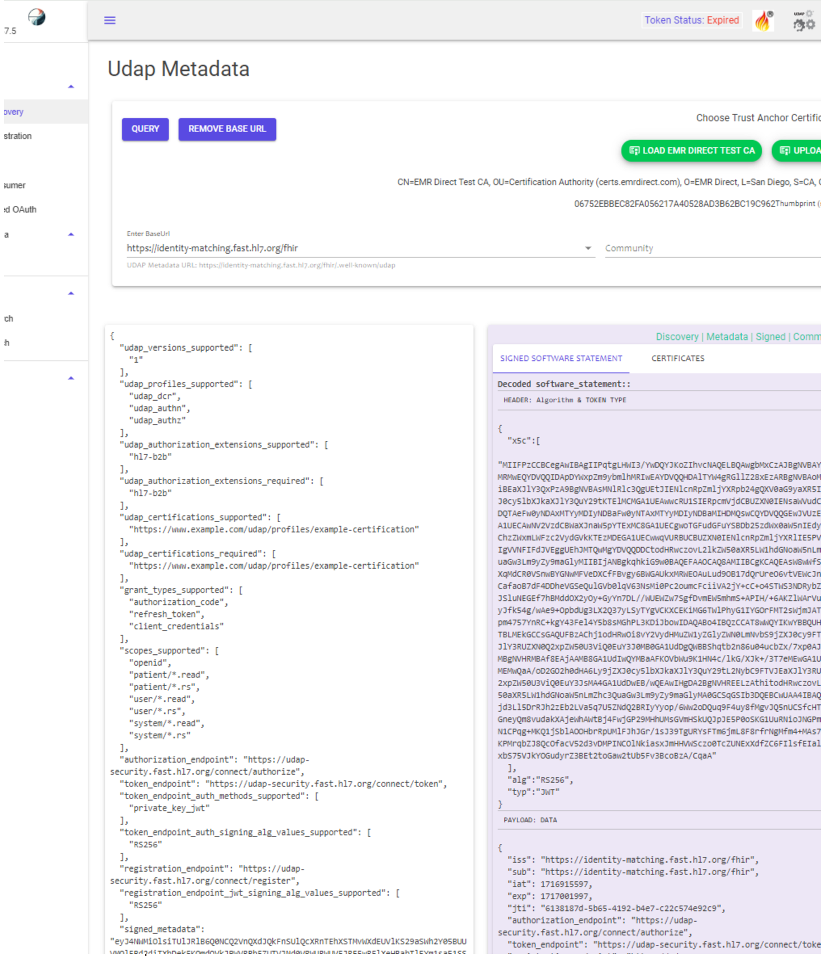
- Implementations
  - Diverse industry efforts
  - HL7 FHIR Connectathon Testing
  - IHE/Carequality Connectathon Testing
  - Commonwell Connectathon Testing
  - Open-Source Reference Implementations (next slide)
  - CARIN POC tested UDAP Tiered OAuth and *FAST* Identity concepts, and the final report 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)
Daily development: https://github.com/JoeShook/udap-dotnet/tree/develop



Udap Metadata

Choose Trust Anchor Certific

CN=EMR Direct Test CA, OU=Certification Authority (certs.emrdirect.com), O=EMR Direct, L=San Diego, S=CA, (

06752EBBEC82FA056217A40528AD3B62BC19C962Thumbprint (

Enter BaseUrl: https://identity-matching.fast.hl7.org/fhir

Community

UDAP Metadata URL: https://identity-matching.fast.hl7.org/fhir/.well-known/udap

```
{
  "udap_versions_supported": [
    "1"
  ],
  "udap_profiles_supported": [
    "udap_dcr",
    "udap_authn",
    "udap_authz"
  ],
  "udap_authorization_extensions_supported": [
    "hl7-b2b"
  ],
  "udap_authorization_extensions_required": [
    "hl7-b2b"
  ],
  "udap_certifications_supported": [
    "https://www.example.com/udap/profiles/example-certification"
  ],
  "udap_certifications_required": [
    "https://www.example.com/udap/profiles/example-certification"
  ],
  "grant_types_supported": [
    "authorization_code",
    "refresh_token",
    "client_credentials"
  ],
  "scopes_supported": [
    "openid",
    "patient/*.read",
    "patient/*.rs",
    "user/*.read",
    "user/*.rs",
    "system/*.read",
    "system/*.rs"
  ],
  "authorization_endpoint": "https://udap-
security.fast.hl7.org/connect/authorize",
  "token_endpoint": "https://udap-security.fast.hl7.org/connect/token",
  "token_endpoint_auth_methods_supported": [
    "private_key_jwt"
  ],
  "token_endpoint_auth_signing_alg_values_supported": [
    "RS256"
  ],
  "registration_endpoint": "https://udap-
security.fast.hl7.org/connect/register",
  "registration_endpoint_jwt_signing_alg_values_supported": [
    "RS256"
  ],
  "signed_metadata":
"eyJ4NWMiOlsiTUlJRlB6Q0NCQ2VnQXdJQkFnSUlQcXRnTEhXSTMvWXdEUVlKS29aSWh2Y05BUU
```

```
Decoded software_statement::
 HEADER: Algorithm & TOKEN TYPE
```

```
{
  "x5c":[

"MIIFPzCCBCegAwIBAgIIPqtgLHWI3/YwDQYJKoZIhvcNAQELBQAwgbMxCzAJBgNVBAY
MRMwEQYDVQQIDApDYWxpZm9ybmlhMRIwEAYDVQQHDAlTYW4gRGllZ28xEzARBgNVBAoM
iBEaXJlY3QxPzA9BgNVBAsMNlRlc3QgUEtJIENlcnRpZmljYXRpb24gQXV0aG9yaXR5I
J0cy5lbXJkaXJlY3QuY29tKTElMCMGA1UEAwwcRU1SIERpcmVjdCBUZXN0IENsaWVudC
DQTAeFw0yNDAxMTYyMDIyNDBaFw0yNTAxMTYyMDIyNDBaMIHDMQswCQYDVQQGEwJVUzE
A1UECAwNV2VzdCBWaXJnaW5pYTExMC8GA1UECgwoTGFudGFuYSBDb25zdWx0aW5nIEdy
ChzZWxmLWFzc2VydGVkKTEzMDEGA1UECwwqVURBUCBUZXN0IENlcnRpZmljYXRlIE5PV
IgVVNFIFdJVEggUEhJMTQwMgYDVQQDDCtodHRwczovL2lkZW50aXR5LW1hdGNoaW5nLm
uaGw3Lm9yZy9maGlyMIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEAsW8wWfS
XqMdCR0VSnwBYGNwMFVeDXCfFBvgy6BWGAUkxMRWEOAuLud9OB17dQrUreO6vtVEWcJn
CafaoB7dF4DDheVGSeQulGVb0lqV63NsMi0Pc2oumcFciiVA2jY+cC+o4STWS3NDRybZ
JSluNEGEf7hBMddOX2yOy+GyYn7DL//WUEWZw7SgfDvmEW5mhmS+APIH/+6AKZlWArVu
yJfk54g/wAe9+OpbdUg3LX2Q37yLSyTYgVCKXCEKiMG6TWlPhyG1IYGOrFMT2sWjmJAT
pm4757YnRC+kgY43Fel4Y5b8sMGhPL3KDiJbowIDAQABo4IBQzCCAT8wWQYIKwYBBQUH
TBLMEkGCCsGAQUFBzAChj1odHRwOi8vY2VydHMuZW1yZGlyZWN0LmNvbS9jZXJ0cy9FT
JlY3RUZXN0Q2xpZW50U3ViQ0EuY3J0MB0GA1UdDgQWBBShqtb2n86u04ucbZx/7xp0AJ
MBgNVHRMBAf8EAjAAMB8GA1UdIwQYMBaAFKOVbWu9K1HN4c/lkG/XJk+/3T7eMEwGA1U
MEMwQaA/oD2GO2h0dHA6Ly9jZXJ0cy5lbXJkaXJlY3QuY29tL2NybC9FTVJEaXJlY3RU
2xpZW50U3ViQ0EuY3JsMA4GA1UdDwEB/wQEAwIHgDA2BgNVHREELzAthitodHRwczovL
50aXR5LW1hdGNoaW5nLmZhc3QuaGw3Lm9yZy9maGlyMA0GCSqGSIb3DQEBCwUAA4IBAQ
jd3Ll5DrRJh2zEb2LVa5q7U5ZNdQ2BRIyYyop/6Ww2oDQuq9F4uy8fMgvJQ5nUCSfcHT
GneyQm8vudakXAjeWhAWtBj4FwjGP29MHhUMsGVmHSkUQJpJE5P0oSKG1UuRNioJNGPm
N1CPqg+MKQ1jSblAOOHbrRpUMlFJhJGr/1sJ39TgURYsFTm6jmL8F8rfrNgMfm4+MAs7
KPMrqbZJ8QcOfacV52d3vDMPINCOlNkiasxJmHHVWSczo0TcZUNExXdfZC6FIlsfEIal
xbS75VJkYOGudyrZ3BEt2toGaw2tUb5Fv3BcoBzA/CqaA"
  ],
  "alg":"RS256",
  "typ":"JWT"
}
```

```
 PAYLOAD: DATA
```

```
{
  "iss": "https://identity-matching.fast.hl7.org/fhir",
  "sub": "https://identity-matching.fast.hl7.org/fhir",
  "iat": 1716915597,
  "exp": 1717001997,
  "jti": "6138187d-5b65-4192-b4e7-c22c574e92c9",
  "authorization_endpoint": "https://udap-
security.fast.hl7.org/connect/authorize",
  "token_endpoint": "https://udap-security.fast.hl7.org/connect/toke
```

=>

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.

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*

***FAST*: Security for Scalable Registration, Authentication, and Authorization**	***FAST*: Directory**	***FAST*: Interoperable Digital Identity & Patient Matching**	***FAST:* Consent**
HL7 Project Page **Security for Scalable Registration, Authentication, and Authorization**	**HL7 Project Page** **Directory**	**HL7 Project Page** **Interoperable Digital Identity & Patient Matching**	**HL7 Project Page** **Consent**
Public Meetings the 2nd and 4th Tuesdays Each Month at 2PM ET https://hl7-org.zoom.us/j/99770852614?pwd=Sk1QUDBjY0huSDNxYVQ4YW5KNkpjdz09	**Public Meetings: Biweekly meetings on Mondays at 3pm ET** as of April 29th https://hl7-org.zoom.us/j/95314390248?pwd=QUhvNktmTVJiWUk2ZnRHSmdWcHpmdz09	**Public Meetings the 1st and 3rd Thursdays Each Month at 2PM ET** https://hl7-org.zoom.us/j/99145025586?pwd=bE01OFVHZkVta051SlRjbjJZMTFRQT09	**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=UmpibnBHN0NSZThmZUhpdkppWE5tdz09
Chat.fhir Stream https://chat.fhir.org/#narrow/stream/294749-FHIR-at.20Scale.20Taskforce.20.28FAST.29.3A.20Security	**Chat.fhir Stream** https://chat.fhir.org/#narrow/stream/283066-united-states.2Fnational.20directory	**Chat.fhir Stream** https://chat.fhir.org/#narrow/stream/294750-FHIR-at.20Scale.20Taskforce.20.28FAST.29.3A.20Identity	**Chat.fhir Stream** https://chat.fhir.org/#narrow/stream/426241-FHIR-at-Scale-.28FAST.29.3A-Consent-Management

FAST Artifacts and Resources

Want to learn more about becor *FAST* FHIR Accelerator?

Want to work with us to implem 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