Objective*

Scale an open-source framework for federating trusted Identity Assurance Level 2 (IAL2) certified credentials across health care organizations using a person-centric approach and modern internet technologies.

*First announced at our Q4 2021 CARIN Community meeting: https://www.carinalliance.com/events/carin-community-meetings/

TEFCA – Launch of Digital Identity projects via FHIR

"The RCE will launch a workgroup of TEFCA stakeholders to develop a model for services that QHINs may offer to support network-facilitated FHIR exchange. The RCE will also coordinate a pilot to test the facilitated FHIR exchange model for Individual Access Services (IAS) and at least one other use case. This pilot is expected to include at least a QHIN, a provider, a payer, and an IAS provider. The results of the pilot will be published by the end of CY 2022 to support publication of the Common Agreement V1.1 and associated Implementation Guides (IGs), as needed, to support full production availability in the first half of CY 2023."

– "FHIR® Roadmap for TEFCA Exchange, Version 1", January 2022

https://rce.sequoiaproject.org/wp-content/uploads/2022/01/FHIR-Roadmap-v1.0_updated.pdf

Digital Identity Proof of Concept Participants

ANTICIPATED ROLE	ORGANIZATIONS
Application	b.Well Ciitizen / Invitae OneRecord Otis Health Patient Centric Solutions
CSP	AllClear ID EMR Direct ID.me MaxMD
Identity Broker	Department of HHS XMS team
Relying Party	Cambia Health Solutions (Health Plan) CVS Health (Health Plan) Cedars-Sinai Health System (Provider) Kaiser Permanente (Provider and Health Plan) Marshfield Clinic Health System (Provider and Health Plan) Providence Health System (Provider)
Trust Framework	DirectTrust Kantara International
Government Observer	The Office of National Coordinator (ONC) Centers for Medicare and Medicaid Services (CMS)

Additional Organizations Interested in the PoC

OTHER INTERESTED ORGANIZATIONS	
Apple	Aetna
Centene	DrFirst.com
Express Scripts	Graphite Health
Google	Humana
Inovalon	Intermountain
Interoperability Institute	iShare Medical
Login.gov	Massachusetts Health Data Consortium
Mastercard	Microsoft
Premera Blue Cross	Security Health Plan
UnitedHealthcare (Optum)	xCures

Engagement Model

XMS integrates with CSPs using standards-based protocols (SAML, OIDC). Interested CSPs must either be certified by a third party, such as DirectTrust or Kantara, or be in the process of certification. Interested CPSs can submit their requests for their inclusion in this PoC using the process outlined below:

1. Email Ashley ashley.hudak@leavittpartners.com and Ryan ryan.howells@leavittpartners.com regarding your interest

2. In the email, please provide the following:
   - Evidence of IAL2 certification (or intent to certify) with either DirectTrust, Kantara, or EHNAC's TDRAAP certification for technical UDAP and/or IdP functionality
   - Primary contact (1 person) who will take point on this proof of concept from each participating organization
   - Business and Technical contacts (multiple) who will be actively participating in the CARIN Alliance Digital Identity proof of concept workgroups

Draft Use Cases

- #1 Consumer-facing Application
  - A consumer uses an application of their choice to identity proof themselves via an IAL2 credentialing service provider and the HHS XMS flow, and then authenticates via XMS to multiple provider and payer FHIR endpoints
- #2 Health Plan Member
  - A consumer will identity proof themselves via an IAL2 credentialing service provider and the HHS XMS flow, and then authenticates via XMS to multiple applications and providers
- #3 Health System patient
  - A patient will identity proof themselves via an IAL2 credentialing service provider and the HHS XMS flow, and then authenticates via XMS to multiple payers and applications

**Similar flows would also occur using UDAP Tiered OAuth but would authenticate using OIDC

Draft Workflows

1. CSP Standalone
   - Entity has a CSP which is certified by DirectTrust or Kantara to an IAL2 or higher
   - **FOCUS:** Policy only; What does a relying party need to ask and have answered in order to accept a digital identity from another entity they do not have a relationship with?
2. CSP with HHS XMS
   - Same as #1 integrated into HHS XMS
   - **FOCUS**: Technical and Policy
3. CSP with UDAP
   - Same as #1 with CSP using UDAP Tiered Oauth
   - FOCUS: Technical and Policy