HHS / CARIN DIGITAL IDENTITY FEDERATION
PROOF OF CONCEPT KICKOFF MEETING

LEAVITT
PARTNERS

Agenda

Today's kickoff will address the following:

- PURPOSE AND VISION
- TECHNICAL APPROACH – HHS XMS AND UDAP TIERED OAUTH
- PARTICIPATION
- PROJECT MANAGEMENT AND NEXT STEPS

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

Commonwell and Carequality : IAL2 requirements

- Commonwell and Carequality, two of the largest health information exchange networks in the country, enable the exchange of clinical data for specific use cases
  - Carequality is a subsidiary of The Sequoia Project which is the Recognized Coordinating Entity (RCE) who is working with the Office of National Coordinator to implement the Trusted Exchange Framework and Common Agreement (TEFCA). Carequality has been leading the work related to the technical components of the TEFCA.
- Commonwell is going to require third-party applications to ensure their consumer has been identity proofed to an IAL2 level with a credentialing service provider who has been certified by Kantara or DirectTrust in order to connect to their FHIR ecosystem

  (Source: https://www.commonwellalliance.org/connect-to-the-network/#core-services)
- Carequality is still discussing their requirements for applications who want to connect to their FHIR ecosystem but current in-flight discussions appear to be arriving at the same conclusion as Commonwell

Why?

- It's incredibly important for covered entities to ensure they are sending health care information to a specific, unique individual to avoid any disclosure issues under HIPAA

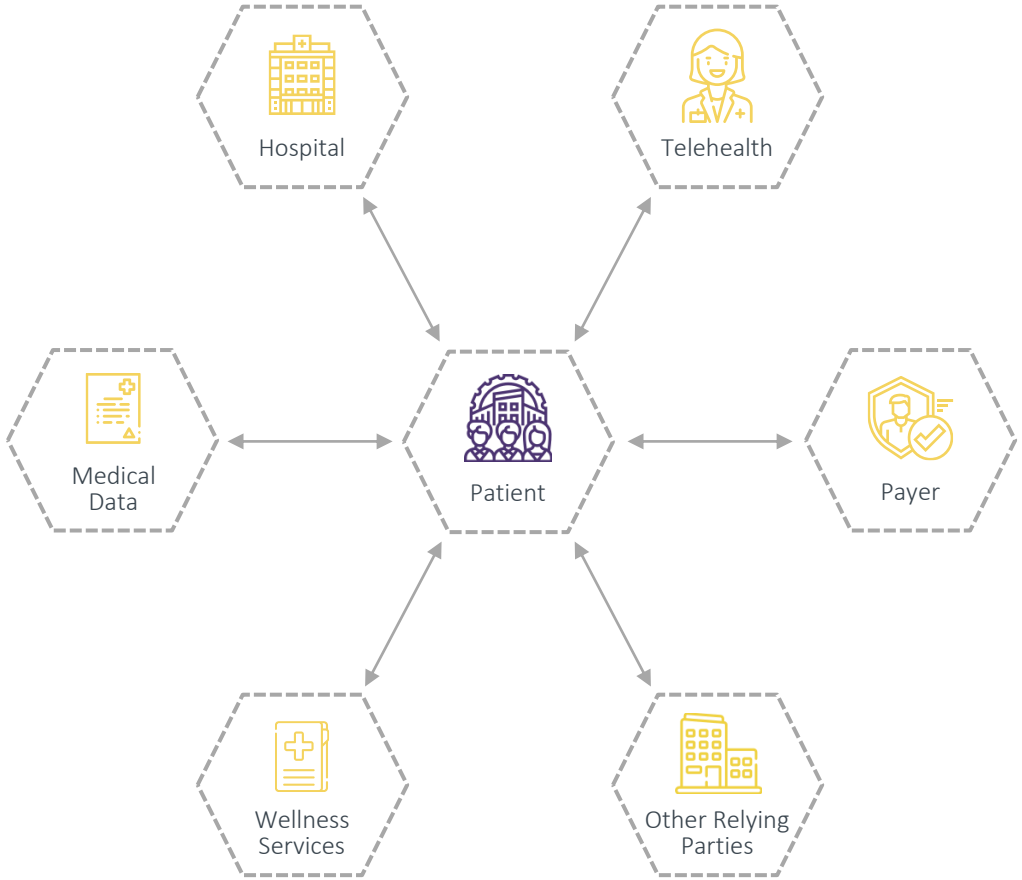
Purpose & Vision

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/

A Person-Centric Approach to Health Data



Give prior authorizations, sign HIPPA disclosures and communicate other information with healthcare providers

Engage in telehealth or renew prescriptions with a physician

Obtain and exchange health information with HDOs, payers, health management apps and other businesses a patient chooses to engage with

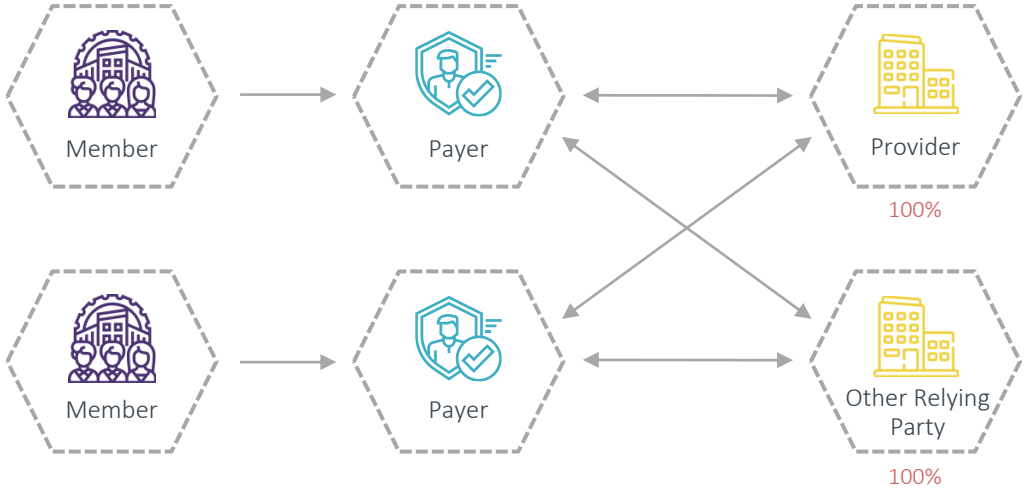
Interact with payers or change payers as patients move between employers, get married or undergo other life changes

Engage with online wellness services, mental health, and other health and healthcare related software systems

Interact with other relying parties that may not be involved in healthcare (e.g., community-based organizations) but are willing to consume identity assertions from health or healthcare-oriented identity providers

The Current State of Identity

Current State

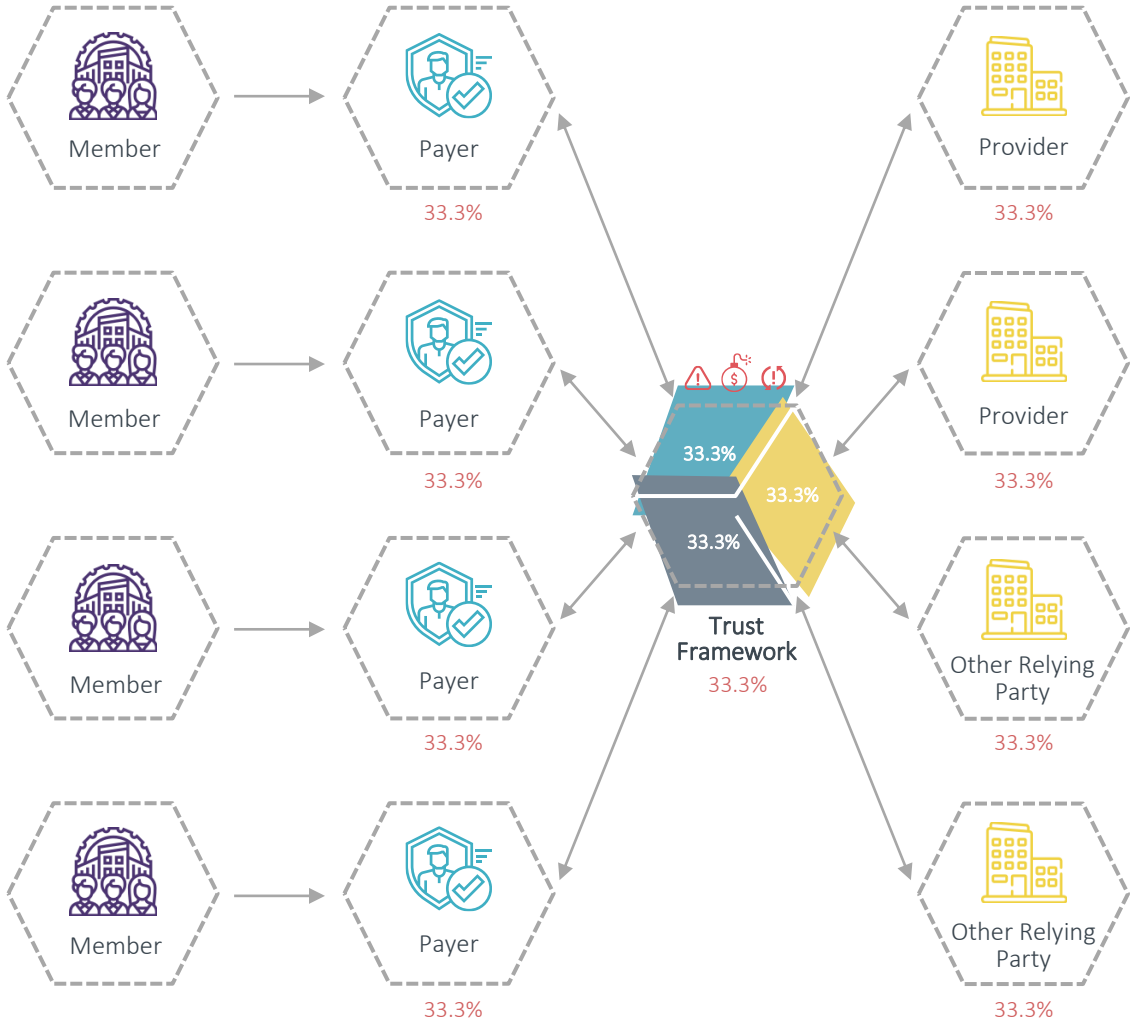


Risk
Unmanaged or unknown risk that fluctuates between each identity provider

Liability
Unmanaged or unknown legal liability unless defined in bi-lateral agreements with each identity provider

Technical Interoperability
Technical interoperability achieved by working with each external entity independently

Future State



Federating Trust is What a Trust Framework Does

Current Approach

- Number of federations increases quadratically for vendors and buyers
- Most security auditors don't know how to audit identity systems
- Establishing legal and liability agreements with all entities is very expensive for both parties
- Lack of global governance leads to inconsistent identity assurance between companies
- Evaluating annual audits of 10s or 100s of identity providers is not viable with limited resources

Trust Framework Approach

- Federate Trust rather than identities
- Enables participants to buy products that support standards in identity and cryptography
- One industry-led governance body to aggregate and manage federations between organizations
- Require vendors to procure or issue their own credentials when engaging in business with you that you can rely on
- Support all identity use cases to include authentication, digital signatures, encryption and IoT for your entire supply chain
- Consolidate liability, warranties indemnification and other legal matters across all vendor identity credentials

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

Technical Approach – HHS XMS and UDAP Tiered OAuth

Scope

HHS XMS

HHS XMS is an identity federation broker tool that enables individuals to choose to log in by selecting from multiple CSPs that have been certified by a trust framework organization.

Standards

The proof of concept will use NIST-800-63-3, Open ID Connect (OIDC), SMART on FHIR / OAuth 2.0, UDAP, and other open standards.

Credential Policy

CARIN is drafting a federated credential policy which outlines the technical, policy, legal and certification guidelines necessary to create trust so digital identity credentials can be used and accepted even when they are issued and certified by different credentialing providers and trust framework organizations.

Participants

The proof of concept will include applications, health plans, providers, credential service providers, relying parties, and trust frameworks.

HHS NextGen External User Management System (XMS)

NextGen XMS is a scalable, cloud-based solution that allows HHS Operational Divisions to focus on their mission and takes into consideration:

- Alignment with Digital Identity guidelines, ICAM and Cloud modernization efforts
- Security and compliance with federal standards (NIST, OMB, HHS EPLC requirements, etc.)
- Identity and Access Governance and delegated administration model
- Enterprise service that can secure access to external HHS applications
- Centralized platform that is flexible to integrate with third-party providers and services

Capabilities & Benefits

Secure Access:	***Enables external users to access protected applications using credentials issued by the General Services Administration's (GSA's) Login.gov or other agency's PIV/CAC***
NIST 800-63-3 Compliance:	***IAL1, IAL2, and IAL3, and AAL2 and AAL3***
Identity Proofing/Delegated Proofing:	***Remote ID proofing using Login.gov; and delegated proofing for users that affiliate with an organization that's managed within NextGen XMS.***
Organization Affiliation:	***Ability to create and manage organization affiliations within NextGen XMS***
Access Requests/Approvals:	***Configurable access request framework for an application***
Organization Relationship Management:	***Ability to create organizations and manage affiliations to those organizations***
Accredited Platform and Helpdesk:	***NextGen ATO in place which includes Login.gov; no impact to integrated application's ATO, only ISA/MOU required***

How XMS Works

- Upon successful integration, users wanting to access the relying party application will be routed to XMS for authentication.
- Within XMS, users will be presented with a list of CSPs they can choose from.
- If the user is required to complete identity proofing (IAL2), XMS will include this information in the authentication request to the CSP.
- Post successful authentication, XMS will share the user information with the relying application party to initiate the application session.

Technical Workflow

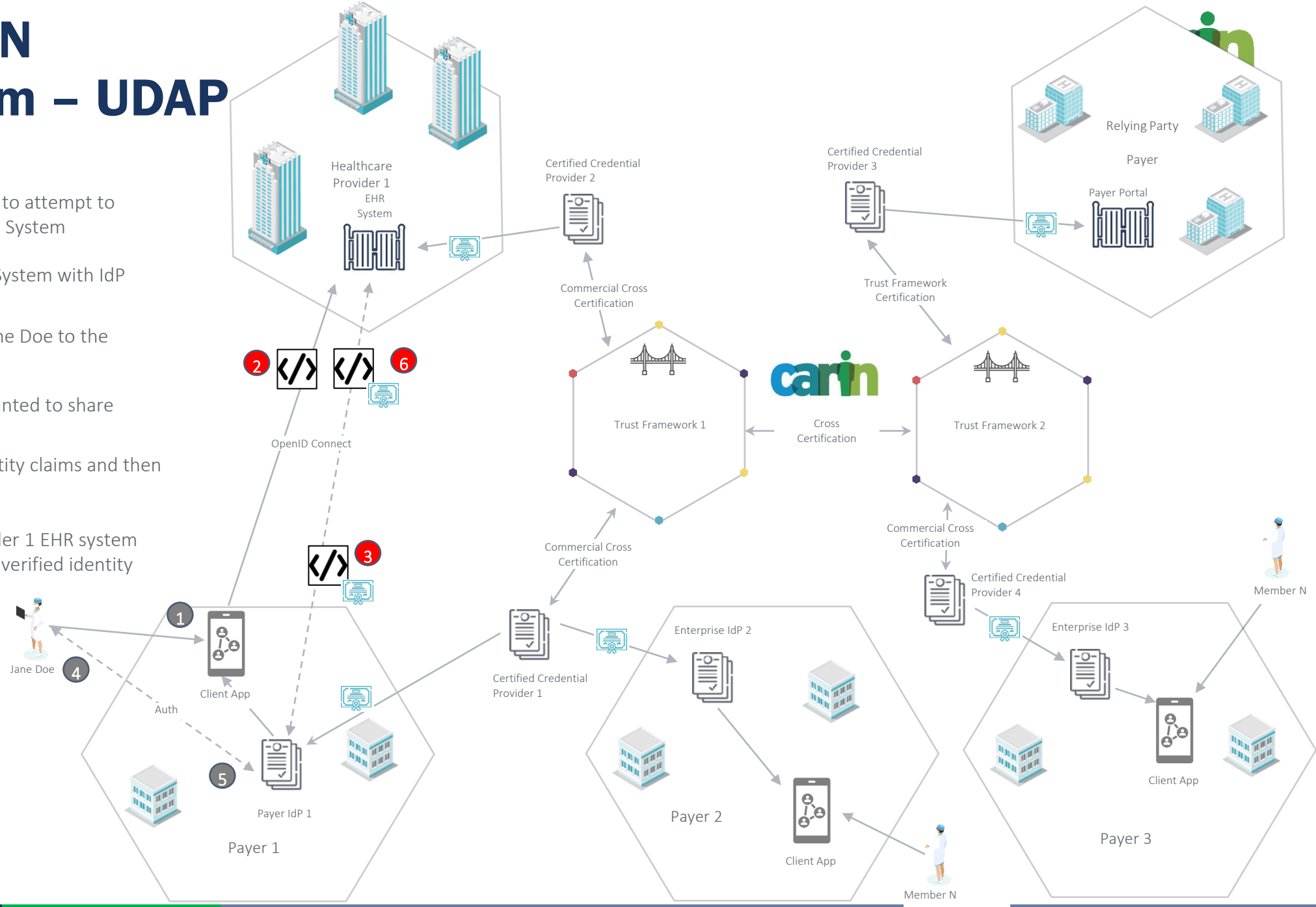
XMS integrates with relying party applications using standards-based protocols (SAML, OIDC):

- The relying party application team and XMS team align on prerequisites, timelines, and resources, including user acceptance testing (UAT) testers.
- The relying party application team and XMS team exchanges single sign-on configuration metadata for their identified non-production environment.
- The relying party application team completes Identity Provider (IdP) configuration updates and development (if applicable). In parallel, the XMS team completes service provider (SP) configuration.
- The XMS team and relying party application team conducts integration testing.
- UAT Testers complete UAT testing, coordinated via the relying party application team.

The CARIN Ecosystem – UDAP

1. Jane Doe uses Payer 1 Client App to attempt to access Healthcare Provider 1 EHR System
2. Client App sends request to EHR System with IdP hint
3. EHR System uses hint to direct Jane Doe to the Payer 1 IdP
4. Payer 1 IdP asks Jane Doe if she wanted to share her identity info with EHR System
5. Jane Doe approves sharing of identity claims and then authenticates to Payer 1 IdP
6. Payer 1 IdP responds to the Provider 1 EHR system with an OIDC_ID token containing verified identity claims

**When applicable, Jane Doe approves the sharing of their PHI by Provider 1 EHR system



Participation

Interested Participants

INTERESTED PARTICIPANTS	
Aetna	AllClearID
b.well	BCBSA
Cambia Health Solutions	Centene
DirectTrust	DrFirst.com
EMR Direct	Express Scripts
Graphite Health	HHS XMS
Humana	ID.me
Inovalon	Intermountain
iShare Medical	Kantara
Login.gov	Massachusetts Health Data Consortium
Mastercard	MaxMD
Microsoft	OneRecord
Patient Centric Solutions	Premera Blue Cross
Providence Health Systems	Security Health Plan
Optum Health / UnitedHealthcare	xCures
ZenKey	

How Interested Participants Can Prepare

- **Consumer-facing Applications:** Ensure you are partnered with a CSP that issues IAL2 digital credentials and are certified by DirectTrust, Kantara Initiative, or TDRAAP program.
- **Health Plans, Providers, EHR systems:** Determine whether you will use a CSP or whether you will be a relying party or both. Determine whether you have a CSP solution that is part of or separate from your core system.
- **Credential Service Provider (CSPs):** Get certified with the Kantara Initiative, DirectTrust, or TDRAAP program.
- **Relying Parties:** Consider what questions you need to get answered internally before you can participate in the proof of concept and trust an identity coming from another source?
- **Trust Framework Organizations:** Participate on our tiger team.

Resources Needed

Relying party application engineers with experience in configuring identity and access management

Project management, Business, and coordination support

User Acceptance Testing (UAT) testers

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

Project Management and Next Steps

Cadence and Communication

- The proof of concept will create a private chat through chat.fhir.org as a primary way of communication and will meet bi-weekly for one hour.

- The bi-weekly meetings will feature technical and policy and governance workstreams:
  - The technical workstream will address how/whether the proof of concept is working between the relying parties, CSPs, XMS, and Tiered OAuth providers as appropriate.
  - The policy workstream will ensure the proof of concept is considering the business questions related to what participants need to go live with the digital identity federation.

- The proof-of-concept leadership team will hold one-on-one meetings with participants as needed.

Directional Timeline

- Q1 : Kickoff meeting, secure confirmation from interested parties, Use Case Development, XMS onboarding, UDAP Tiered OAuth preparation, identify and begin to onboard IAL2 CSPs

- Q2 / Q3: Testing of the use cases and documenting lessons learned and key relying party questions

- Q4: Develop interim report/results from the proof of concept and discuss next steps

Next Steps