HHS/CARIN DIGITAL IDENTITY PROOF OF CONCEPT

Overview

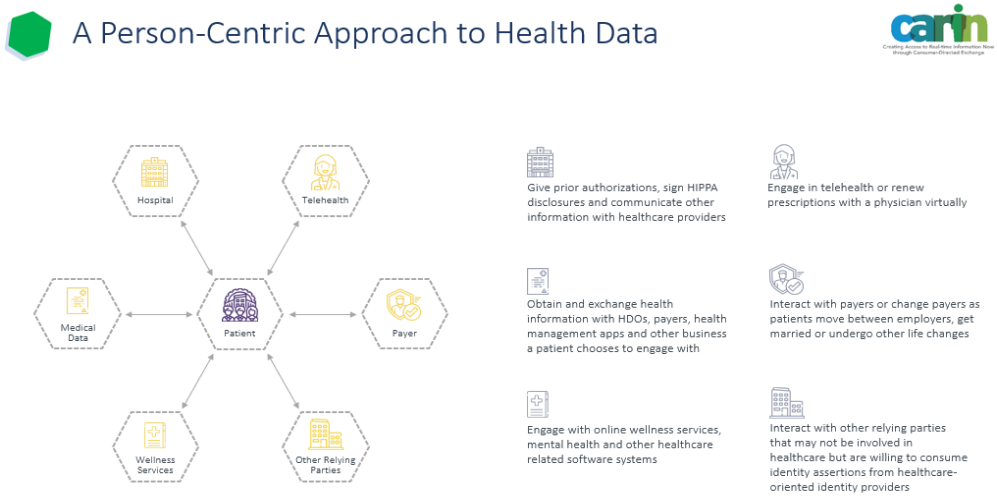
The 21st Century Cures Act, the ONC Cures Act Final Rule, and the CMS Interoperability and Patient Access rule have accelerated the ability for an individual to access their personal health information via an application of their choice by leveraging HL7® FHIR® Application Programming Interfaces or APIs. Currently, the use of SMART on FHIR® allows for an individual to use their provider or payer portal username and password to authenticate themselves and retrieve their personal health information. While the CARIN Alliance strongly endorses the current implementation of SMART on FHIR® by stakeholders in the health care ecosystem to ensure individuals have immediate access to their health information, we also want to advance a future vision for how we could as an industry digitally authenticate individuals in a trusted way without being tied to the creation of portal accounts, and then allow an individual to use that same trusted authentication event to access their health information across multiple payers and providers.

In addition, the Office of National Coordinator released the "FHIR Roadmap for TEFCA Exchange – Version 1" in January 2022 which discussed the following digital identity pilot:

> "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."

CARIN is working with the RCE to ensure the proof of concept meets the needs outlined in the pilot discussed above including drafting a report of the results that will support the publication of the Common Agreement v1.1. CARIN's approach is also in line with current guidelines from Commonwell and in-flight conversations within Carequality regarding how they are approaching digital identity for individual access services (IAS).

CARIN is pursuing a person-centric approach to health data, which would allow a consumer to prove their identity once, and have this credential accepted across systems. Trust is necessary for this to occur, and organizations that federate trust across multiple parties have the ability to scale this approach.



Trust is necessary for a person-centric approach. In the current system, it is the responsibility of the two parties involved to make federation happen. This is not scalable. In a point-to-point approach, if a payer wants to exchange data with a provider/relying party, they would need to talk directly with one another. With a trust framework, the liability is shared among all participants in a way that is consistent with the responsibilities they take on as a participant in the trust framework. Organizations that federate trust across multiple parties have the ability to scale this approach. This is why the CARIN digital identity proof of concept will utilize existing trust framework organizations (e.g., DirectTrust, Kantara, etc.) to federate trust and liability across participating entities.

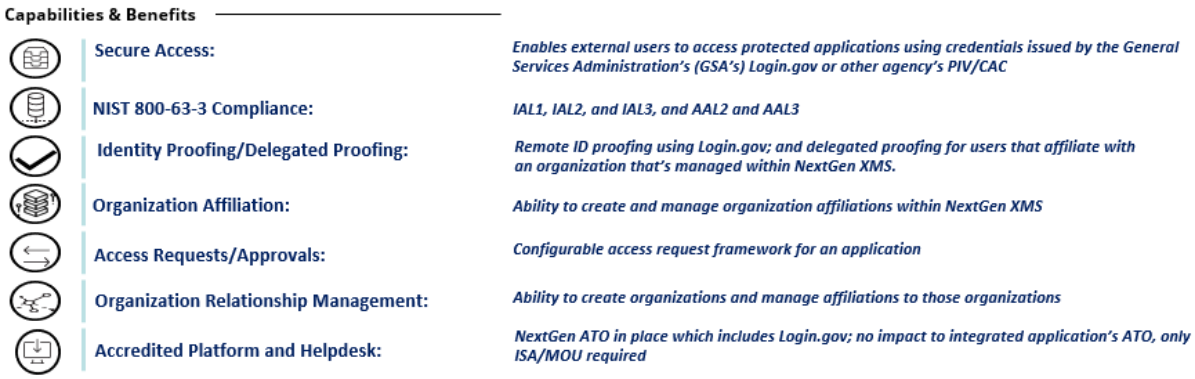
CARIN/HHS Proof of Concept

In working to achieve a person-centric approach and federate trust, CARIN and the Department of Health and Human Services (HHS) are partnering together to lead a digital identity federation Proof of Concept (POC). The goal of the POC is to scale an open framework for federating trusted Identity Assurance Level 2 (IAL2) certified credentials using a person-centric approach across health care organizations leveraging modern internet technologies.

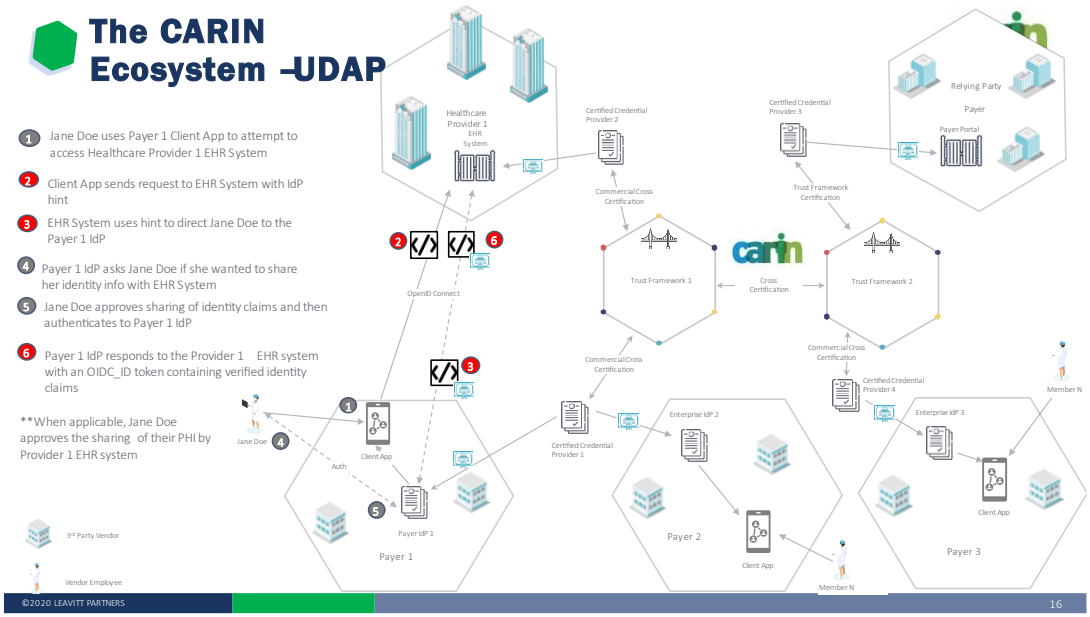
The POC will use HHS' External User Management System (XMS). XMS is an identity federation broker tool that enables individuals to voluntarily choose to log in by selecting from multiple credential service providers (CSPs) that have been certified by a trust framework organization. The XMS platform can:

- Integrate with trusted CSPs to enable "Bring your own trusted identity."
- Integrate with relying parties to enable seamless federated access – "Login once, access multiple applications."

XMS capabilities and benefits include:



In parallel to the HHX XMS proof of concept, we will also be conducting a proof of concept that leverages the UDAP Tiered OAuth specification. A high level workflow can be found below.



Project Details

Scope of the Proof of Concept

The proof of concept will:

- Partner with HHS' External User Management System (XMS) and the UDAP Tiered OAuth teams and include apps, health plans, providers, IdPs, relying parties, and trust frameworks.
- Use NIST-800-63-3, RFC 3647, Open ID Connect (OIDC), SMART on FHIR/OAuth 2.0, UDAP Tiered OAuth, and other open standards.
- Use the CARIN 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.

Project 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 (30 minutes) and policy and governance (30 minutes) workstreams. The leadership team will hold one-on-one meetings with participants as needed.

- The technical workstream will address how/whether the proof of concept is working between the relying parties, CSPs, and XMS.
- 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.

Use Cases

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

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

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 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.

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 (IAL 2), 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.

A demo of the XMS platform can be viewed here.

How Credential Service Providers (CSPs) Join XMS

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:

- Email Ashley Hudak (ashley.hudak@leavittpartners.com) and Ryan Howells (ryan.howells@leavittpartners.com) regarding your interest

- 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

Desired Outcomes

- Prove that federation broker technology can enable a single patient digital identity that can be used to access digital resources across payers and providers (relying parties).

Prerequisites to participate

- **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 for the Proof of Concept (6-12 months)

- Relying party application engineers with experience in configuring identity and access management services
- Project management and coordination support
- User Acceptance Testing (UAT) testers

Next Steps

1. **Deadline to respond: We are looking for organizations to respond by Friday, February 11 COB to signal their interest in participating in the proof of concept**
2. Finalize the Credential Policy.
3. Establish proof of concept participants.
4. Determine the high-level success criteria.
5. Determine the high-level timeline, including roles and responsibilities. It is anticipated this proof of concept will take at least 6-12 months to complete.
6. Scheduling workgroup discussions