A White Paper on

Integration Patterns for Federated Identity Management in CMS patient access FHIR APIs: A State Medicaid Agency Use Case

Ryan M. Harrison
Pavan Jagalur
Mukundan Srinivasan

Amida Technology Solutions, Inc.
December 2021

Summary

The CMS Interoperability and Patient Access Final Rule (CMS-9115-F) requires commercial payers, Medicaid Advantage plans and state Medicaid agencies to provide a patient access API, which will allow patients to delegate access to their claims and clinical records to third-party applications. While the access and identity landscape vary widely between enterprises, we have identified three integration patterns that will cover most payer use-cases for CMS patient access FHIR-API compliance. In this white paper, we use a state Medicaid agency use-case to demonstrate the application of these three integration patterns.

Problem

On May 1, 2020, the CMS[1] and ONC[2] interoperability rules were published on the Federal Register. These rules require individual patient access (2021) and payer-to-payer exchange (2022) via API (Application Programming Interface) without special effort. The mandates from CMS cover both Medicaid's Fee-For-Service (FFS) and Medicaid Managed Care Organization (MCO) programs.

Medicaid programs are administered by 55 distinct state and territorial entities, each of which has its own assortment of IT systems.[3] Each state Medicaid program in turn contracts with multiple companies with theirown siloed identity system (Figure 1). Hundreds of entities – from state agencies to their contractual partners, including fiscal agents, Medicaid Management Information System (MMIS), Eligibility and Enrollment (E&E), and MCOs – will have to comply with the CMS and ONC interoperability mandates starting in late 2020. For example, Virginia Medicaid has two fiscal agents, four MMIS vendors, two E&E vendors,[4] one Enrollment Broker System (EBS) vendor, one

[1] 85 FR 25510 [federalregister.gov/documents/2020/05/01/2020-05050/medicare-and-medicaid-programs-patient-protection-and-affordable-care-act-interoperability-and]

[2] 85 FR 25642 [federalregister.gov/documents/2020/05/01/2020-07419/21st-century-cures-act-interoperability-information-blocking-and-the-onc-health-it-certification]

[3] CMS maintains a list of MMIS and E&E contracts by state, updated quarterly. [medicaid.gov/medicaid/data-and-systems/mmis/contract-status-report/index.html]

[4] Virginia Medicaid eligibility is integrated with the Department of Social Services (DSS) eligibility for CHIP, TANF, SNAP. State-wide integrated eligibility determination programs were a requirement of the 2013 PPACA regulation.

FFS Non-Emergency Medical Transportation (NEMT) broker, six state-contracted MCOs, seventeen help desks, and countless FFS providers.

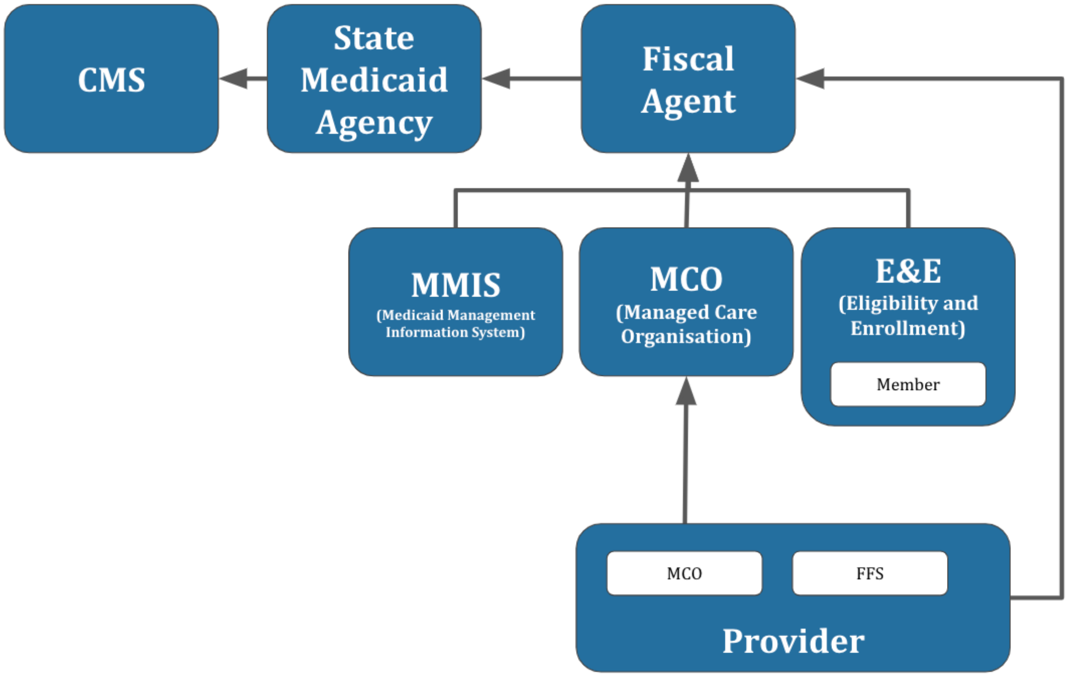
CMS
State Medicaid Agency
Fiscal Agent
MMIS
(Medicaid Management Information System)
MCO
(Managed Care Organisation)
E&E
(Eligibility and Enrollment)
Member
MCO
FFS
Provider

Figure 1 – Summary of Medicaid reimbursement entities by contractual relationship. *A typical state Medicaid agency administers its programs but outsources more than 90 percent of the tasks to various entities. Outsourcing includes member and provider enrollment, claims adjudication, payments, help desk and IT systems.*

Because of the byzantine identity landscape, a typical Medicaid member could be forced to navigate more than a half-dozen identity systems to enroll and ultimately see a physician. Federated identity systems with SSO offer a solution; a member is provided one login for access to multiple disparate systems. The systems themselves remain siloed, but the member's identity is shared and administered from one central location.

The Substitutable Medical Apps Reusable Technology (SMART) on Fast Healthcare Interoperability Resource (FHIR) and FHIR Bulk Access standards are the leading mechanisms to facilitate individual access and payer-to-payer exchange. A SMART on FHIR solution for delegated individual access requires, at a minimum, identity management for members and third-party applications. In complying with the CMS and ONC access mandates, state Medicaid agencies have the opportunity to both address the immediate regulatory requirement for member access and to modernize their member identity solutions.

Solution Patterns

Given the heterogeneous identity landscape of state Medicaid agencies, we classify three integration approaches based on the existence of an SSO solution and state-wide Medicaid Member Portal (Table 1).

		Single Sign-On (SSO)	
		Yes	No
State Medicaid Member Portal	Yes	Pattern 1	Pattern 2
	No	Pattern 1	Pattern 3

***Table 1 – Summary of state Medicaid integration patterns.** Each of the three integration approaches is described in a subsection.*

Pattern 1: Existing SSO

Architecture Building Block

In pattern 1 (Figure 2), the state Medicaid agency integrates with an existing IdP, which may be provided by the state or the state Medicaid agency itself.

SMART on FHIR specifies both authentication and authorization, using OpenID Connect (OIDC) claims (authentication) and OAuth2.0 scopes (authorization). A SMART on FHIR `id_token` includes OIDC claims; the `access_token` contains FHIR-specific OAuth2.0 scopes; and the `refresh_token` is used to request a new `access_token` without prompting the user for another login.

Rather than add SMART on FHIR scopes to the existing portal, we would federate the identity to a FHIR Auth server. In a federated architecture, the only high-level requirements of the IdP would be to support either OIDC or SAML. To conform with SMART on FHIR, downstream applications would consume identity as OIDC, regardless of whether the upstream IdP used OIDC or SAML.

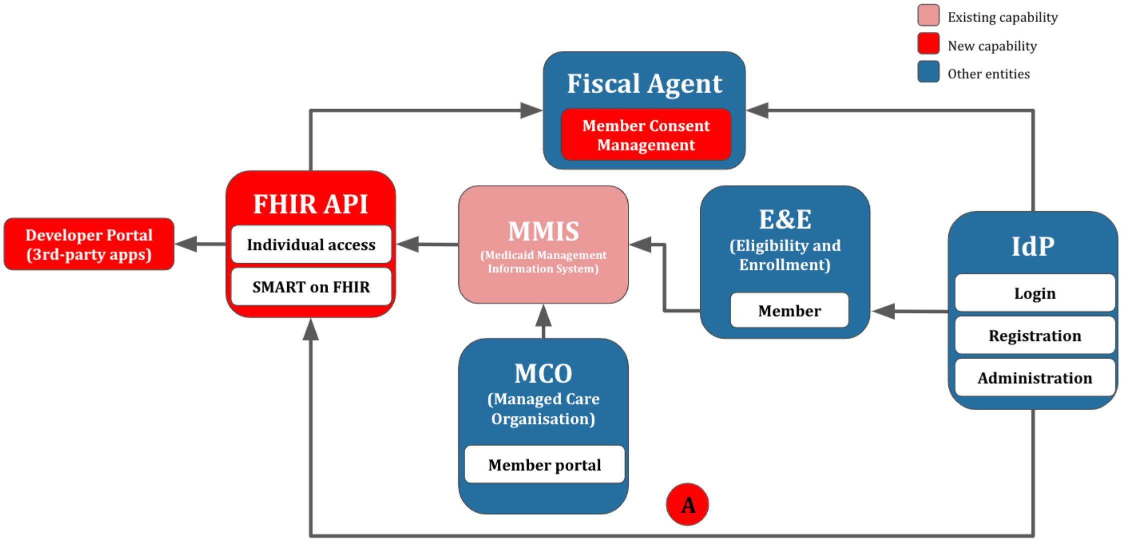

***Figure 2 – Component architecture with existing identity provider**. A sequence diagram showing the authentication and authorization flow are shown in Figure 3.*

Solution Building Block: SecureAccess Washington using SAML and AWS Cognito (OIDC)

AWS Cognito, like other identity management solutions, supports both authentication and authorization. Identities are managed via either Cognito User Pools or Identity Pools. Both pool types support federation from OIDC and SAML providers, such as SecureAccess Washington. As Medicaid users would not require direct access to underlying AWS resources, Cognito User Pools are often the more appropriate choice.

A Cognito User Pool may back multiple resource servers, and each can be configured with a distinct set of allowed authorization scopes. The `access_token` is retrieved with an appropriate OAuth2.0 flow — for example, an "Authorization Code" flow for mobile apps. The service provider – for example, a third-party FHIR application – may then use the `access_token` for delegated access to a resource server.

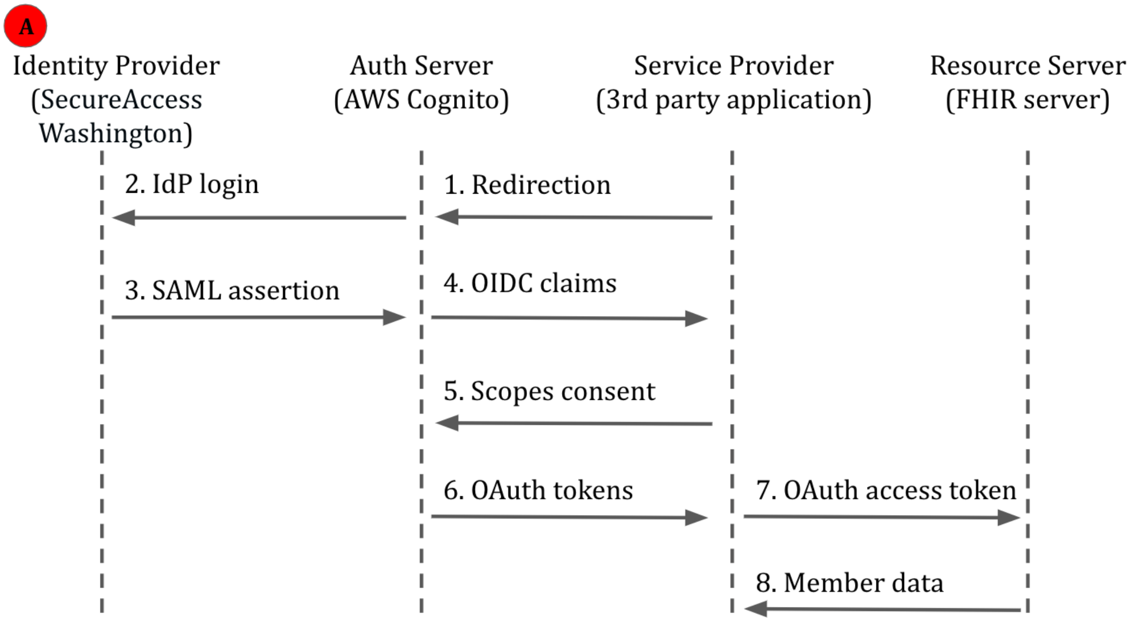
A
Identity Provider (SecureAccess Washington)
Auth Server (AWS Cognito)
Service Provider (3rd party application)
Resource Server (FHIR server)
2. IdP login
1. Redirection
3. SAML assertion
4. OIDC claims
5. Scopes consent
6. OAuth tokens
7. OAuth access token
8. Member data

Figure 3 – Sequence diagram depicting simplified authentication (1-4) and authorization (5-8) flows*.* *Since SecureAccess Washington (SAW) does not support OIDC directly, AWS Cognito converts the SAML assertions returned from SAW (2) into OIDC claims used by the FHIR application (3). SMART on FHIR authorization scopes are stored within AWS Cognito, not SAW. Arbitrary metadata (key/value attributes) may be stored in either the IdP or Auth server. As a guideline, attributes specific to the application should be stored within the Auth server, whereas attributes about the individual should be stored in the IdP. AWS Cognito supports attribute mapping between IdP attributes and AWS Cognito user attributes.*

Pattern 2: No SSO, Existing State Medicaid Member Portal

In pattern 2 (Figure 4), no SSO is available, but there is an existing Fiscal Agent member portal. Here, the state Medicaid agency *may* be able to use the same *non-SSO* identity as the existing member portal. This represents a stop-gap arrangement that avoids the deployment of a full-fledged SSO solution, at the expense of substantial technical debt. Member consent management can be added to the existing state Medicaid member portal.

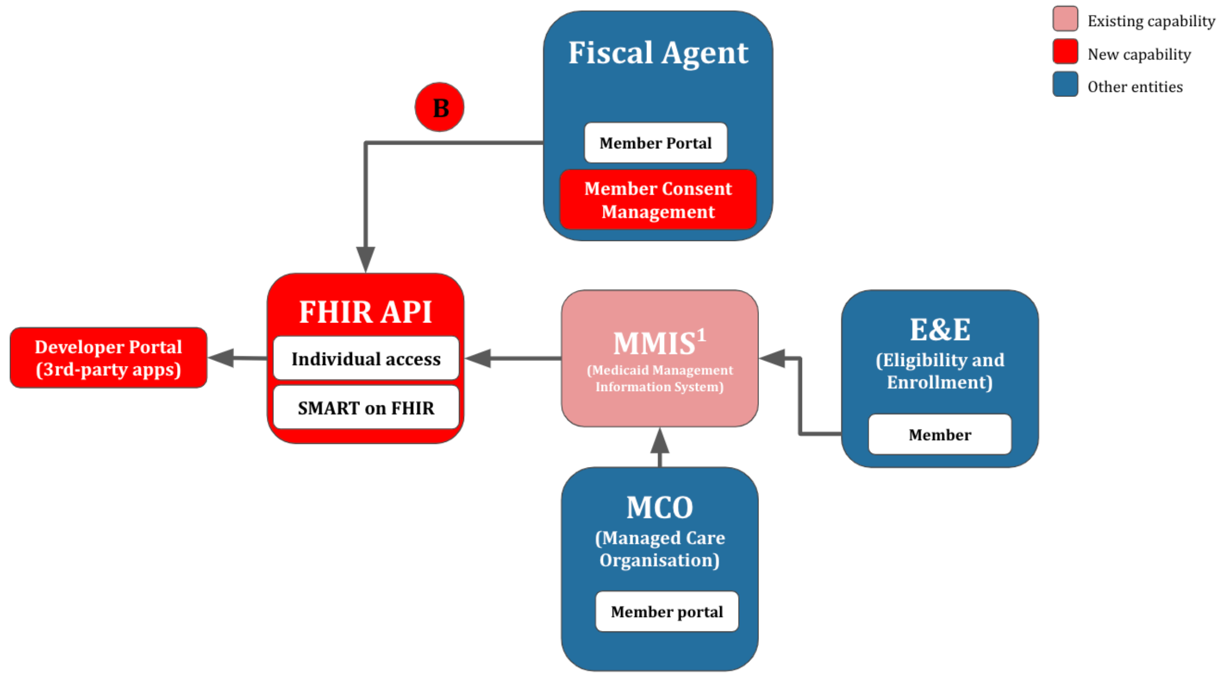
Existing capability
New capability
Other entities
Fiscal Agent
Member Portal
Member Consent Management
B
FHIR API
Individual access
SMART on FHIR
Developer Portal (3rd-party apps)
MMIS1
(Medicaid Management Information System)
E&E
(Eligibility and Enrollment)
Member
MCO
(Managed Care Organisation)
Member portal

Figure 4 – Component architecture with existing state Medicaid member portal and without SSO. *The detailed architecture of (B) will depend on the authentication implementation of the existing member portal.*

Pattern 3: No SSO, No State Medicaid Member Portal

In pattern 3, neither SSO nor a state Medicaid member portal are available. A less sustainable option would be to build a member directory into the Auth server used by the FHIR server. This would require either: 1) having members create an account before sharing data via FHIR, or 2) provisioning accounts in the Auth server for every member. A more sustainable option (Figure 5) would entail providing an SSO-supporting IdP to the state Medicaid agency, which would be similar to the pre-existing IdP depicted in Pattern 1 (Figure 3).

Although most modern IdPs support the open standards SAML and OIDC, many IdPs remain closed-source. Selecting a FLOSS (Free/Libre and Open-Source Software) IdP avoids vendor-locking both the IdP vendor proper and IdP-related professional services such as integration and long-term support. Further, selecting a FLOSS IdP serves as a form of futureproofing. In a worst-case pattern, where the IdP vendor is either unable or unwilling to support future use-cases, a FLOSS IdP can be unilaterally extended by a state Medicaid agency or integration partner (although this comes at the expense of long-term support for the extension). A common criticism of FLOSS solutions is that they lack enterprise support; however, within the IdP space, enterprise backing is provided by firms such as Apereo (educational institutions), the Open Identity Platform Community, Shibboleth, and Redhat/IBM.

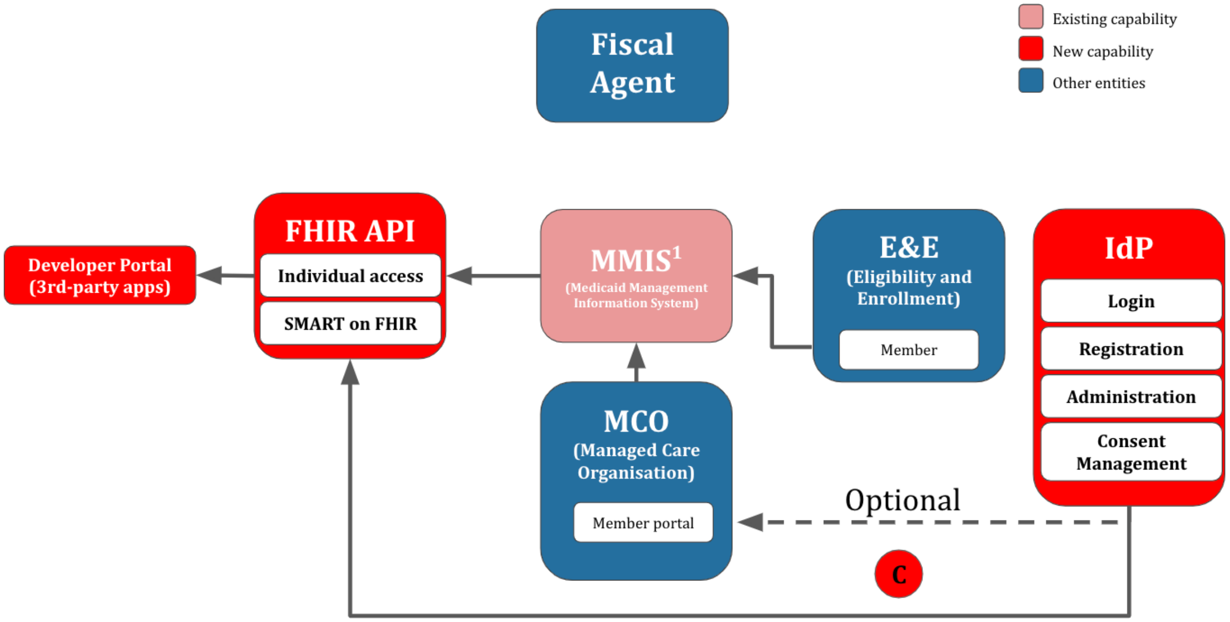

Figure 5 – Component architecture without state Medicaid member portal and without preexisting SSO. *Unlike Pattern 1 (Figure 2) and Pattern 2 (Figure 4), in Pattern 3 there are no member consent flows to the Fiscal Agent. Therefore, there are no lines connecting to the Fiscal Agent from the FHIR API, E&E or IdP. The state Medicaid agency would be responsible for deploying and configuring an IdP to support the SSO. SAML-based SSO in (C) could follow the same flow as in Figure 3. If there is no member portal available, as a stop-gap arrangement, consent management could be handled within the IdP by revoking access to the member identity. Optionally, the IdP could also be used for SSO in the MCO member portals.*

Recommendations

1. Use enterprise wide SSO, for your CMS FHIR patient access API solution. Although SAML-based SSO configurations will vary by IdP, integrating with an existing IdP via SAML (Pattern 1) will be much less effort than building an ad hoc solution (Pattern 2) or providing a full-fledged IdP (Pattern 3).
2. Integrate consent management with existing member-portal workflows. Members must have a mechanism to revoke consent to third-party applications. Members should also be able to conveniently view their consents and see, at a minimum, the last time each third-party application accessed their data. Consent management can be provided by a stand-alone application linked by SSO; however, administering their account should be seamless to the users. For example, it is more user-friendly to update address, revoke consent, and add a new household member from within one user flow, as opposed to three distinct flows.
3. Prioritize FLOSS (Free/Libre and Open-Source Software) and open standards in vendor procurement. Vendor-locking to a closed standard is a death knell to innovation. Indeed, SAML and OpenID Connect (OIDC) were born out of a frustrating landscape of competing proprietary authentication protocols.
4. Plan for an increase in HelpDesk activity for third-party access. In pattern 1, members will need to remember their login credentials to consent to third-party access. Expect increased HelpDesk volume for password resets and questions about what information is being shared with third-party providers. First- and second-tier HelpDesk employees will require

training on common member inquiries related to FHIR. For third-tier support, an escalation path to your internal development team or contractor will also be needed. User guides, including a FAQ, are recommended for stakeholders such as members, third-party FHIR application developers, and HelpDesk staff.

About Amida

Amida is a software company focused on enterprise data management, cybersecurity, and digital platform strategies. We design, develop, and deploy systems that enable the secure and reliable exchange of sensitive information. Amida builds open-source solutions that collect and prepare data from a variety of sources – independent of structure, format, provenance, and schema – for applications like business intelligence, predictive analytics, and downstream transactions. We are especially known for open data architectures and production services that are scalable, efficient, modular, and secure. Our software engineers and data scientists have extensive experience in data modeling, governance, interoperability and exchange, and visualization, especially in health IT.

Amida's founding team co-conceived and led the design, implementation, and production deployment of the Blue Button personal health record at the Department of Veterans Affairs (VA) and supported its development and deployment at the Centers for Medicare & Medicaid Services (CMS) and the Department of Defense's (DOD) Military Health System. They co-conceived and led the creation of the Joint Legacy Viewer, a clinician portal used by hundreds of thousands of VA and DoD healthcare providers every day, and which is the cornerstone of both agencies EHR modernization efforts. They also led the design and prototype construction (the "Virtual Regional Office") of the service-connected disability claims platform still in enterprise service today.

Appendix: Identity Providers (IdP)

Federal Identity Providers: Login.gov

In the Federal Government, the General Services Administration (GSA)[5] has deployed the login.gov SSO portal. Rather than build and support their own identity solutions, federal agencies have the option to use the login.gov SSO.[6] Following a one-time integration with login.gov, federal agencies outsource the non-differentiated work of maintaining a secure, National Institute of Standards and Technology(NIST)-compliant identity management solution that automatically stays up-to-date with the latest best practices.

Where token-based authentication is used, establishing a federated Identity Provider (IdP) allows agencies to leverage each other's personnel security and background investigation processes. This avoids duplicate background screenings, facilitates moves between agencies, and reduces the use of policy exemptions to Multi-Factor Authentication (MFA) requirements when generating temporary accounts. In short, smoother end-user interactions (e.g. obviating the need to juggle multiple logins), better security (e.g. built-in identity-proofing and MFA), lower cost (e.g. amortizing the expense of the identity management system over many agencies), and the facilitation of cross-agency knowledge-sharing (e.g. reusing software components from other agencies). Although login.gov does not support state and local users, it nonetheless serves as a reference model for SSO within government.

State Identity Providers: North Carolina, Washington, Michigan

At the state level, North Carolina has introduced the **N**orth **C**arolina **Id**entity Management Service (NCID) for state and local SSO.[7] Importantly, the NCID system supports state and local employees, as well as individual citizens and business users, within the same SSO system. NCID supports SAML 2.0.[8]

The state of Washington hosts two distinct SSO systems — Enterprise Active Directory[9] for state and local employees, and SecureAccess Washington (SAW)[10] for the general public. For example, Washington Connection (cash assistance, food assistance), Unemployment and Licensing (including motor vehicles) uses SAW to authenticate the general public. Washington Healthplanfinder (Medicaid, CHIP) does not appear to use SAW on its public site. Cloud-hosted agency applications using SAW must authenticate via SAML 2.0.

Michigan hosts the general-public-facing MILogin[11] SSO system, which supports both individual Michigan citizens and businesses/organizations. MIBridges, the state's consolidated benefits portal

[5] Specifically, the GSA Technology Transformation Service component 18F and the US Digital Service (USDS).

[6] Adoption of login.gov varies greatly by federal agency. Indeed, one risk factor in offering a centrally administered SSO solution is that agency adoption will be low. Fortunately, high-profile adoptions of login.gov include USAJOBS (Office of Personnel Management), the System for Award Management (General Services Administration), and the Trusted Traveler Programs (Homeland Security). Other agencies have not readily adopted SSO via login.gov. For example, at Veterans Affairs, software applications are waitlisted for ninety days before any SSO integrations are allowed.

[7] North Carolina Identity Service (NCID) [it.nc.gov/ncid]

[8] NCID Integration Forms [it.nc.gov/services/service-directory/core-services/nc-identity-management-ncid/ncid/ncid-integration-forms]

[9] WaTech Enterprise Active Directory via Active Directory Federation Services (ADFS) [watech.wa.gov/services/Enterprise-Active-Directory-Services]

[10] WaTech SecureAccess Washington [watech.wa.gov/services/SecureAccess-Washington]

[11] Michigan MILogin [michigan.gov/MILogin]

(Medicaid, cash assistance, childcare, emergency relief, food assistance), uses MILogin. Michigan Medicaid's myHealthPortal (web) and myHealthButton (mobile) applications also use MILogin.[12]

Product	Vendor	Licensing	Notes
Login.gov	US Government	Closed source	Production availability for Federal agencies. Pilot availability for state and local governments.[13]
MILogin	Michigan	Closed source	Used by MIBridges, which includes Michigan Medicaid.
NCID	North Carolina	Closed source	
SecureAccess Washington	Washington	Closed source	Used by Washington Connection assistance programs.
Auth0	Auth0	Closed source	
AWS Cognito	AWS	Closed source	Lacks some governance and user-management features commonly found in identity management solutions. Does not support SMART on FHIR.[14]
Igia on Keycloak	Persistent	Open source	Specific to SMART on FHIR.
Keycloak Redhat-SSO	Redhat	Open source	Keycloak is the community-supported upstream, while Redhat-SSO is the enterprise-supported downstream.
IBM IAM	IBM	Closed source[15]	
Okta	Okta	Closed source	Used by CMS Quality Payment Program. Okta has an unofficial and unsupported SMART on FHIR reference implementation.[16,17]

Table 2 – Selected government and commercial identity providers. *Most identity providers (IdP) follow a per-user pricing model, with modest monthly rates per active (and sometimes inactive) user. Commercial providers have à la carte pricing, with minimums and a separate fixed-price enterprise agreement.*

[12] Michigan myHealthPortal Registration User Guide [myhb.state.mi.us/myHBPublic/pages/doc/myHPRegistrationUserGuide.pdf]

[13] Login.gov pilot available for state and local governments as of February 2021 [partners.login.gov/product/#state-and-local]

[14] A detailed memo on why Cognito does not support SMART on FHIR is available on the FHIR Chat registration required [chat.fhir.org/#narrow/stream/179170-smart/topic/SMART.20on.20FHIR.20with.20AWS.20Cognito]

[15] IBM IAM Is licensed under the IBM International Program License Agreement. Publication ENUS216-290 [ibm.com/common/ssi/printableversion.wss?docURL=/common/ssi/rep_ca/0/897/ENUS216-290/index.html&amp;request_locale=en]

[16] Okta unofficial and unsupported SMART on FHIR reference implementation [github.com/oktadev/okta-smartfhir-docs]

[17] FHIR chat discussion of Okta's SMART on FHIR reference implementation, registration required [chat.fhir.org/#narrow/stream/179170-smart/topic/Keycloak.20for.20SMART.20authz/near/214251419], and recorded FHIR chat discussion [openaccessvideos.blob.core.windows.net/openaccessvideos/20210218-SMART-Okta-720p.mp4]

Overview of Identity Protocols

Recall that authentication is about *who* the user is, and authorization is about *what* a user is allowed to do. Identity providers and identity protocols address the *who*; JSON Web Token (JWT) scopes, such as those used in SMART on FHIR, address the *what*.

Lightweight Directory Access Protocol (LDAP), OpenID Connect (OIDC), and Security Assertion Markup Language (SAML) are three common authentication protocols. These protocols are used to authenticate transactions between a User Agent (e.g. an internet browser), a Service Provider (e.g. a web application), and an Identity Provider (which includes a directory service)(Figure 6). LDAP is most commonly used for on-premises applications (e.g. signing into a remote desktop), whereas SAML and OIDC are most commonly used for web applications. In practice, most enterprises will use both LDAP (SSO for employees)[18] and SAML/OIDC (SSO for customers).

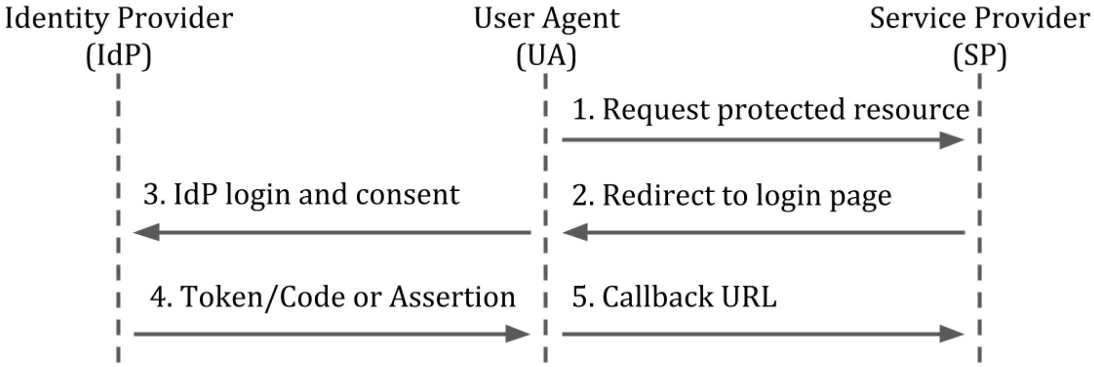

Figure 6 – Simplified OIDC[19] authentication flows *Steps 1-5 are ordered sequentially. (1) The user requests a protected resource, e.g. a web page displaying information about the patient. (2) The user is redirected to an IdP login page; users never share credentials with the Service Provider. (3) The user enters their credentials on the IdP login page. A consent page is also displayed, summarizing which information is about to be shared with the third party. Service Providers should only ask for the information they require to service the user. (4) Both OIDC and SAML return proof that the user consented. OIDC relies upon a JWT token (`id_token`) or code (which is used to request a token). SAML relies upon an XML assertion. While both OIDC and SAML support arbitrary metadata, which may be used by the Service Provider in making authorization decisions, neither OIDC nor SAML performs authorization directly. (5) The User Agent forwards the IdP response to the Service Provider via a callback URL.*

[18] Active Directory is not an identity protocol in and of itself; rather, it is an IdP directory service that is commonly used with the LDAP protocol. Active Directory Federation Services (AD FS) allows for the use of Active Directory with SAML and, more recently, OIDC.

[19] Strictly speaking, the OIDC roles are OpenID provider, end-user, and relying party.