EMR EHR Connectivity

Federation Identity and Single Sign-On – Business View

May 21, 2021

Document Version & Status: 2.1 – DFU (Draft for Use)

Table of Contents

1. INTRODUCTION 3

1.1 OVERVIEW 3
1.2 RELATED DOCUMENTS, REFERENCES, AND SOURCES 3

2. BUSINESS VIEW 4

2.1 BUSINESS DRIVERS 4
2.2 FEDERATED IDENTITY 4
2.3 BINDING EMR CREDENTIALS TO FEDERATED IDENTITY AND SSO 4
2.3.1 SSO Implementation within the EMR Offering 5
2.3.2 User Stories 6

3. SYSTEM VIEW 8

3.1 FEDERATED IDENTITY 8
3.2 SINGLE SIGN-ON (SSO) 8
3.3 SEQUENCE FLOW 9
3.4 IMPLEMENTATION OF SSO PROTOCOLS 10
3.4.1 OAuth2 Protocol 10
3.4.2 Federated IDP vs. Local EMR Credential Workflows 11

4. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS 13

4.1 ACRONYMS AND ABBREVIATIONS 13

5. APPENDIX C: SAML WORKFLOW FOR EMR USERS WITH MULTIPLE RIDS ..... ERROR! BOOKMARK NOT DEFINED.

1. INTRODUCTION

1.1 Overview

Integrating federation identity and single sign-on (SSO) functionality into an EMR Offering allows for a user to experience seamless access to EHR products and services through their EMR. Simplifying authentication with a single user account using a federated identity reduces the need for clinicians to manage multiple user accounts to access different systems, while promoting greater adoption and use of EHR products and services that provide clinicians with greater access to information and the ability to coordinate with other care providers.

1.2 Related Documents, References, and Sources

ID	DOCUMENT NAME	VERSION	PUBLICATION DATE
2	ONE ID Oauth2/OpenID Specification (Ontario Health Digital Services, 2020) https://www.ehealthontario.on.ca/en/standards/view/one-id-openid-connect-specification	1.2	2020-05-20

2. BUSINESS VIEW

2.1 Business Drivers

Clinicians can provide enhanced patient care with improved access to information and the ability to coordinate patient care. Integrating EMR Offerings with provincial EHR products and services makes it easier for clinicians to access, helping clinicians achieve this goal.
The provincial ONE Access Provider Gateway (OAG) is the primary means for a point-of-service system (such as an EMR) to access products and services, available in the provincial EHR.
EMR Offerings can connect to multiple EHR products or services through the OAG which is a common access point, removing the need to implement connectivity for each EHR product or service individually. The requirements are provided to ensure a consistent and repeatable way to authenticate EMR users and connect to the OAG. Once authenticated, EMR users can access the EHR products and services they are authorized to use. This document focuses on user authentication using a federated IDP, such as Ontario Health (Digital Services) (OHDS) ONE ID, to access EHR products and services. Implementers may opt to integrate ONE ID into their EMR Offering's authentication service for SSO to integrate seamless access from logging into the EMR Offering to using EHR products and services.

2.2 Federated Identity

Anyone accessing provincial EHR products or services must be authenticated (to ensure certainty about the person's identity) and authorized (to ensure they have appropriate access to the EHR product or service). Authentication requires a person to provide one or more pieces of information to self-identify, such as something that the user:

- knows (e.g., password)
- has (e.g., a digital certificate)
- is (e.g., fingerprint)

However, requiring people to remember multiple usernames and passwords has shown to be a barrier to the adoption of new technologies. A federated identity links the user's multiple credentials to enable the user to use a single assigned credential to be authenticated for access to multiple EHR products and services, such as an OHDS ONE ID account. Integrating federated identity within an EMR Offering enables the EMR user to access different EHR products with the same federated credentials.

2.3 Binding EMR Credentials to Federated Identity and SSO

OHDS provides the ability for implementers to associate or bind an EMR user's EMR Offering credentials to their ONE ID federated service credentials. Once this binding occurs, the EMR user can leverage their Federated ONE ID account to log into the EMR Offering. This allows for a more seamless interaction between logging into their EMR Offering and access EHR products and services integrated in the EMR Offering without having to enter multiple credentials. Implementers have the option whether or not to build functionality to be able to bind EMR credentials to the OHDS' ONE ID federated ID credentials.

SSO allows a user to authenticate once with a federated IDP (e.g., ONE ID) to be able to access to all EHR products and services to which they are entitled. Access to EHR products and services is available without having to re-enter their credentials for each EHR product or service accessed during that active session. SSO functionality exists regardless of whether EMR binding occurs. When a user attempts to access EHR products or services, if the user is not logged into the EMR Offering with Federated IDP credentials, they will be prompted to authenticate themselves in order for SSO to be achieved.

2.3.1 SSO Implementation within the EMR Offering

SSO can be achieved through two different workflows where an EMR user will require their federated identity credentials. Binding EMR credentials to federated IDP (e.g., ONE ID) is optional and is implemented as part of the EMR Offering's login process.

1. **(SSO With Binding - Optional) User logs into EMR using ONE ID credentials** – The EMR Offering provides functionality to bind credentials. The EMR user selects a federated IDP (e.g., ONE ID) to log into the EMR Offering and enters their federated identity credentials. Once the EMR user is authenticated using their (ONE ID) federated identity credentials, they will have access to EMR functionality as well as all EHR products and services they have entitlements to without having to enter their credentials again. Binding EMR credentials to federated identity credentials achieves SSO at the time of EMR login. The EMR user will only need to remember their federated identity credentials (ONE ID Account) since it grants them access to both their EMR and to EHR products and services.

2. **(SSO Without Binding) User logs into EMR with local credentials** – The EMR Offering either does not provide functionality to bind credentials, or the EMR user opts to not use their federated identity credentials to log into the EMR. The EMR user logs into the EMR Offering using their EMR credentials and gains to all the EMR functionality to which they are authorized. When the EMR user requests access to an EHR product or service, they are prompted to provide their federated identity credentials (e.g., ONE ID credentials) before they are granted access. Once granted, the EMR user has access to all EHR products and services they are authorized to. SSO is achieved when the EMR user successfully authenticates their federated identity credentials to accessing an EHR product or service. SSO is active for the duration of the EMR user's session. In order to achieve SSO without binding The EMR user needs to remember two sets of credentials -- their EMR credentials to log into the EMR Offering, and the federated identity credentials to access EHR products and services.

The following stakeholder roles are required to authenticate and authorize EMR users to consume EHR products and services from their EMR.

STAKEHOLDER ROLE	DESCRIPTION
EMR user	Sometimes called a "principal" in OHDS specifications, they use an EMR Offering to access EHR products and services. Examples include a clinician, physician, nurse, or delegate.
Federated Identity Provider (IDP)	Provides the business services to assign credentials to healthcare providers and provide the identity management applications that authenticate credentials.
EHR Service / Service Providers / Line of Business (LOB)	Manage the business service to grant and authorize EMR users' access to a given EHR asset or service and provide applications that provide EHR products or services.

2.3.2 User Stories

Accessing EHR Services with Local EMR Credentials

- At the login screen to the EMR Offering, a clinician is presented with an option to either log in with their EMR credentials or federated IDP credentials.
- The clinician enters their EMR credentials and is authenticated.
- The clinician uses their EMR Offering to view a patient record and decides they would like to access an EHR service (e.g., Request an eConsult, or access the ConnectingOntario Portal).
- When the clinician attempts to access the EHR service, the EMR Offering informs them that they need to be authenticated using credentials from a federated IDP.
- The EMR Offering redirects the clinician to the Federated Identity Broker where they are prompted to select his federated IDP. Upon selection, they are redirected to the selected federated IDP's login page.
- The clinician enters their federated IDP credentials (e.g., ONE ID) and has access to the requested EHR service.

Initial Credential Binding from the EMR Login Screen

- At the login screen to the EMR, a clinician is presented with an option to either log in with their EMR credentials or federated IDP credentials.
- The clinician selects the federated IDP and is redirected to the Federated Identity Broker where they are prompted to select their IDP from a list of approved federated IDPs. Upon selection, they are redirected to the selected federated IDP's login page.
- The clinician enters their credentials and upon successful authentication, the EMR alerts the clinician that they can bind the EMR credentials to the federated IDP credentials.
- The clinician interacts with the EMR to agree to binding their credentials.
- Upon completion of the credential binding, the clinician has access to their EMR as they normally would.

Initial Credential Binding from an EHR Service Request

- At the login screen to the EMR Offering, a clinician is presented with an option to either log in with their EMR credentials or federated IDP credentials.
- The clinician enters their EMR credentials and is authenticated.
- The clinician is using their EMR Offering to view a patient record and decides she would like to access an EHR Service (e.g., Request a consult, access the ConnectingOntario Portal, etc.).
- When the clinician attempts to access the EHR Service, the EMR Offering informs them that they need to be authenticated using credentials from a federated IDP.
- The EMR Offering redirects the clinician to the Federated Identity Broker where they are prompted to select their federated IDP from a list of approved federated IDPs. Upon selection, they are redirected to the selected federated IDP's login page.
- The clinician enters their credentials and upon successful authentication, the EMR Offering alerts the clinician that they can bind their EMR credentials to the federated IDP credentials.
- The clinician interacts with the EMR Offering to agree to bind their credentials.
- Upon completion of the credential binding, the clinician has access to their EMR Offering as they normally would.

Federated IDP to EMR Offering and EHR Services

- At the login screen to the EMR Offering, a clinician is presented with an option to either log in with their EMR credentials or federated IDP credentials.
- The clinician selects the federated IDP and is redirected to the Federated Identity Broker where they are prompted to select their federated IDP from a list of approved federated IDPs. Upon selection, they are redirected to the selected federated IDP's login page.
- After the clinician is successfully authenticated by the federated IDP, they have access to their EMR Offering as they normally do.
- The clinician uses their EMR Offering to view a patient a record and decides they would like to access an EHR Service (e.g., Request a consult, access the ConnectingOntario Portal, etc.)
- The clinician launches the EHR Service without entering any additional credentials.

3. SYSTEM VIEW

3.1 Federated Identity

EHR products and services leverage OHDS' ONE ID federated service to delegate services to identify the EMR user who requests access to those EHR products and services. The ONE ID federated service accomplishes this securely using the OAuth2 open standard. Below is a sequence diagram to illustrate the communications between the EMR Offering and the different services to grant the EMR user access to an EHR product or service.

Figure 1 - EMR user access to an EHR product or service Patterns

3.2 Single Sign-On (SSO)

SSO is mandatory but an implementer has the option whether or not to implement binding EMR credentials to OHDS' ONE ID federated identity to achieve SSO.

3.3 Sequence Flow

Depending on whether the implementer opts to implement binding for SSO or not, there are different workflows. The following diagrams conceptually depict how EMR users interact with an EMR Offering to access EHR products and services where ONE ID federated identity is implemented with binding and where it is not.

Figure 2 - Business Context Diagram

3.4 Implementation of SSO Protocols

EHR products or services follow the Open Authentication 2.0 (OAuth2) open standard to integrate SSO with an EMR Offering.

3.4.1 OAuth2 Protocol

There are conceptually four systems involved in providing EMR users access to EHR products and services:

1. **EMR Offering:** Used by EMR users to access the Authentication Server and in turn to authenticate their federated IDP credentials and, access the EMR application and EHR services.
2. **Authentication Server:** Accepts token requests and issues authentication tokens once a user is authenticated.
   Federated Identity Provider/ONE ID: Authenticates EMR users' federated IDP credentials for secure access to Provincial EHR Services.
3. **Line of Business (LOB)**: Any EHR Service or Viewlet that provides the EMR user with access to clinically relevant information for the provision of care.

3.4.2 Federated IDP vs. Local EMR Credential Workflows

The following diagram depicts the role of each of these systems and the transactions they support for login with Federated IDP to connect to EHR services. The EMR user logs into the EMR with ONE ID credentials. Note this diagram does not depict UAO picker functionality.

Figure 3 – Federated Transaction Patterns

The following diagram depicts the role of each of these systems and the transactions they support with local EMR credentials to connect to EHR services. The user initially connects via local EMR credentials, then ONE ID to access EHR services. Note this diagram does not depict UAO picker functionality.

Figure 4 – Local EMR Login Transaction Patterns

4. APPENDIX A: GLOSSARY OF KEY TERMS AND DEFINITIONS

4.1 Acronyms and Abbreviations

This table identifies definitions for terms used within or that are relevant to this document.

ACRONYM	DEFINITION
EMR	Electronic Medical Record
LOB	Line of Business (EHR product or service)
HIC	Health Information Custodian
OHDS	Ontario Health Digital Services (formerly eHealth Ontario)
SSO	Single Sign-On
UAO	Under the Authority of
URI	Uniform Resource Identifier