

EMR EHR Connectivity

Federation Identity and Single Sign-On – Requirements

May 21, 2021

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



Table of Contents

TABLE OF CONTENTS.....	2
1. INTRODUCTION	3
1.1 RELATED DOCUMENTS, REFERENCES, AND SOURCES.....	3
1.2 VERSION HISTORY	3
1.3 SINGLE SIGN-ON (SSO) AND BINDING.....	4
2. EMR REQUIREMENTS	5
2.1 EMR LOGIN.....	5
2.2 EMR BINDING TO FEDERATED IDENTITY.....	7
2.3 UNDER THE AUTHORITY OF (UAO) VALUES.....	8
2.4 SESSION MANAGEMENT.....	11
2.5 ERROR HANDLING.....	12
2.6 LOGGING AND AUDITING.....	13

1. INTRODUCTION

The purpose of this document is to provide implementers with functional requirements and guidance to integrate Digital Services Identity Federation and Sing Sign-On functionality within an EMR Offering to access provincial Electronic Health Record (EHR) products and services. Single Sign-On is when an EMR user is authenticated with ONE ID, the authentication is used as part of gaining access to ALL EHR assets to which the EMR user is entitled.

1.1 Related Documents, References, and Sources

ID	NAME	VERSION	DATE
1	ONE ID OAuth2/OpenID Specification (Ontario Health Digital Services, 2020) https://ehealthontario.on.ca/en/standards/one-id-openid-connect-specification	1.2	2020-05-20

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2019-12-23	<ul style="list-style-type: none"> a) The initial release including the OAuth2 protocol. b) Added Readme document to identify optionality to implement SSO.
1.1	2020-07-13	<ul style="list-style-type: none"> a) Updated SSO01.02 to log the EMR user into the EMR Offering using SSO. b) Added SSO01.04 to include functional parity between EMR login credentials and SSO login credentials. c) Added SSO01.05 to allow for EHR Service visibility to be configurable. d) Added UAO section into requirements (previously in OAG requirements). e) Added SSO04.02 to allow for UAO error notification. f) Added SSO05.03 for auditing and logging UAO.
2.0	2020-12-09	<ul style="list-style-type: none"> a) Removed example token files from the Specification package. b) Inserted SSO and SSO binding optionality instructions for implementers. c) Updated SSO04.03 to separate requirements around removing exposure to PHI when an EMR user logs out (into SSO04.04). d) Added SSO04.04 to move out PHI-related requirements from SSO04.03 and to include alternative options where an EMR cannot control the display of PHI. e) Re-numbered original SSO04.04, now SSO04.05.
2.1	2021-03-04	<ul style="list-style-type: none"> a) Updated reference to ONE ID OAuth2/OpenID Specification b) New connections to the Health Information Access Layer (HIAL) using the Security Assertion Markup Language (SAML) are no longer accepted. As such, related content and requirements have now been retired. c) Updated SSO01.05 to provide clarity to differentiate access control within and outside of the EMR.
2.1	2021-05-21	EMR Specification released as Draft for Use (DFU).

1.3 Single Sign-On (SSO) and Binding

Functionality related to associating (binding) EMR credentials and Federated IDP credentials in this document is **OPTIONAL** for implementation. Note that proceeding binding functionality requires the implementation of all SSO and SSO binding requirements in full – a partial implementation is not adequate.

The following table identifies the OMD #s of the specific EMR requirements that relate to the binding. Refer to the EMR requirements for implementation guidelines.

OMD #	REQUIREMENT
SSO01.01	The EMR Offering MUST present EMR users with the option to log into the EMR Offering using credentials provisioned by the EMR Offering or their trusted external Identity Provider (IDP) credentials.
SSO01.02	The EMR Offering MUST allow EMR users to log into the EMR Offering using a Federated SSO Identity user account.
SSO01.03	The EMR Offering MUST continue to provide the EMR user with the ability to log in using only credentials provisioned by the EMR Offering.
SSO02.01	The EMR Offering MUST associate an EMR user’s Federated SSO Identity with their EMR user account.
SSO02.02	The EMR Offering MUST provide the ability to disassociate a Federated SSO Identity from an EMR user account.

2. EMR REQUIREMENTS

This section consists of the EMR functional requirements for ID Federation and SSO.

Support:

M = Mandatory. EMR Offerings certified for this specification **MUST** support this requirement.

O = Optional. EMR vendors **MAY** choose to support this requirement in their certified EMR Offering.

Status:

N = New requirement for this EMR Specification.

P = Previous requirement.

U = Updated requirement from the previous EMR Specification version.

R = Retired requirement from previous EMR Specification version.

OMD #:

A unique identifier that identifies each requirement within OntarioMD's EMR Requirements Repository.

CONFORMANCE LANGUAGE:

The following definitions of the conformance verbs are used in this document:

- **SHALL/MUST** – Required/Mandatory
- **SHOULD** – Best Practice/Recommendation
- **MAY** – Acceptable/Permitted

The tables that follow contain column headings named: 1) "Requirement," which generally contains a high-level requirement statement; and 2) "Guidelines," which contains additional instructions or detail about the high-level requirement. The text in both columns is considered requirement statements.

2.1 EMR Login

The following EMR requirements apply to EMR functionality specific to EMR login with federated identity and SSO.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO01.01	The EMR Offering MUST present EMR users with the option to log into the EMR Offering using credentials provisioned by the EMR Offering or their trusted external Identity Provider (IDP) credentials.	<p>The EMR Offering MUST present the EMR user with the ability to choose to log in using credentials provisioned by the EMR Offering (EMR credentials) or trusted external IDP credentials at the EMR login screen where both options MUST be available.</p> <p>The EMR Offering MUST initiate the OAuth2 token workflow the EMR user to the Federated Identity Broker if the EMR user chooses to log in using their trusted external IDP credentials.</p> <p>The EMR Offering MUST ONLY allow an IDP login where the EMR user is already bound to the EMR Offering.</p>	M	P
SSO01.02	The EMR Offering MUST allow EMR users to log into the EMR Offering using a Federated Identity user account.	Once successfully authenticated by a trusted external IDP via the Federated Identity Broker, EMR users MUST be automatically logged into the EMR Offering (i.e., without needing to enter EMR credentials).	M	P
SSO01.03	The EMR Offering MUST continue to provide the EMR user with the ability to log in using only credentials provisioned by the EMR Offering.	If Federated credentials are not needed by the EMR user or the federated service is unavailable, the EMR user MUST still be able to log into their EMR system.	M	P
SSO01.04	The EMR Offering MUST present the EMR user with the same functionality whether logging in with their EMR credentials or their trusted external IDP credentials.	<p>Where an EMR user logs in using trusted external IDP credentials, the EMR Offering MUST NOT limit or remove EMR functionality available to the EMR user.</p> <p>Where an EMR user logs in using their EMR credentials, the EMR Offering MUST NOT limit or remove the ability for an EMR user to initiate launching EHR Services. The EMR user MUST be prompted to log in using their trusted external IDP credentials before being able to gain access to EHR Services.</p> <p>Important: An EMR user logged in with their EMR credentials wishing to launch an EHR Service MUST be prompted to enter their trusted external IDP credentials without logging out of their session.</p>	M	P
SSO01.05	The EMR Offering MUST have functionality to manage EMR user access to EHR services within the EMR Offering.	<p>Access management SHOULD be configurable via a user interface.</p> <p>The ability to configure access to EHR Services within the EMR Offering MUST be restricted to specific (e.g., administrative) users.</p>	O	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		Note: Access management by the EMR Offering provides another level of security, separate from access granted by the owner of an EHR Service.		

2.2 EMR Binding to Federated Identity

The following EMR requirements apply to EMR functionality specific to EMR binding to federated identity.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO02.01	The EMR Offering MUST associate an EMR user’s Federated SSO Identity with their EMR user account.	<p>The EMR Offering MUST bind the Federated SSO Identity with the requesting user’s EMR account, once both credentials have been authenticated. An association MUST be persistent and not required to be re-established after the EMR user logs out of an EMR system.</p> <p>The “Sub” OAuth2 attribute within the ID Token MUST be used to bind the Federated SSO Identity to the respective EMR user account.</p> <p>Binding between a Federated SSO account and an EMR user account MUST not be allowed without first successfully authenticating the user to both accounts.</p> <p>Note: Binding of a Federated SSO Identity with an EMR account allows an EMR user to log into the EMR system using either credential (but only access EHR services if authenticated with using their Federated SSO Identity).</p>	M	P
SSO02.02	The EMR Offering MUST provide the ability to disassociate a Federated SSO Identity from an EMR user account.	<p>The EMR Offering MUST have the functionality to disassociate a Federated SSO Identity with an EMR user account.</p> <p>The ability to disassociate the Federated SSO Identity SHOULD be available through the EMR user interface and does not require assistance from the EMR vendor support staff.</p>	M	P
SSO02.03	The EMR Offering MUST NOT store or cache any EMR user credentials for IDPs.	<p>User credentials, where required, MUST be provided by the EMR user.</p> <p>SSO to the EMR Offering and EHR services only occurs if the EMR user has been successfully authenticated by a Federated Identity Provider via the Federated Identity Broker.</p>	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO02.04	The EMR Offering MUST receive and store the IDP login session information for the duration of the EMR user's login session.	Upon successful authentication of the EMR user, the Provincial Federated Identity Broker service will return IDP login session information for the EMR user. The EMR Offering MUST receive and store the information for the duration of the EMR user's login session.	M	P

2.3 Under the Authority Of (UAO) Values

The following EMR requirements apply to EMR functionality specific to UAO values.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO03.01	The EMR Offering MUST have a configurable functionality to maintain a list of UAO values.	<p>The EMR Offering MUST have an interface to allow an EMR user to manage (e.g., add, modify, delete) UAO values.</p> <p>The EMR Offering MUST restrict authorization to maintain UAO values to specific (e.g., administrative) EMR users.</p> <p>At a minimum the EMR Offering MUST maintain the following information for UAO values:</p> <ul style="list-style-type: none"> a) UAO values b) UAO friendly names <p>Refer to the "Under Authority of (UAO) Management" section of the ONEID OAuth2/OpenID Specification for more details.</p>	M	P
SSO03.02	The EMR Offering MUST allow EMR users to be associated with UAO values.	<p>An EMR user may need to identify which UAO value to send when connecting to an EHR service. The EMR Offering MUST have a means to maintain (e.g., store, provide, update) UAO values for each EMR user registered in the EMR Offering.</p> <p>At a minimum, the EMR Offering MUST:</p>	M	P

		<ul style="list-style-type: none"> a) Be able to support assigning zero, one, or multiple UAO values to each EMR user registered in the EMR Offering b) Be able to add and remove users to the table c) Store the UAO value and attributes (e.g., the type of value, the value itself, and the associated friendly name) <p>Informational: UAO values are provided as part of the OHDS registration process of an EMR user to obtain a federated identity (e.g., ONE ID account).</p>		
SSO03.03	The EMR Offering MUST have the functionality to prompt an EMR user to select a UAO value when logging into the EMR Offering.	<p>Once the EMR user is authenticated, the EMR Offering MUST prompt the EMR user to select a UAO value.</p> <p>Where the EMR user has more than one assigned UAO value, the EMR Offering MUST prompt the EMR user for a selection of all the possible UAO values assigned to them in the EMR Offering.</p> <p>Where the EMR user has only one assigned UAO value, the EMR Offering MUST NOT provide a selection to the EMR user. The EMR Offering MUST continue with the one assigned value as the UAO value (as if the EMR user selected the single option).</p> <p>Where the EMR user no assigned UAO value, the EMR Offering MUST NOT provide a selection to the EMR user. The EMR Offering MUST continue with no assigned UAO value.</p> <p>At a minimum, the EMR Offering MUST display the UAO friendly name to the EMR user.</p> <p>The EMR Offering MAY additionally display the UAO identifier attribute to the EMR user.</p>	M	P
SSO03.04	The EMR Offering MUST use the EMR users assigned or selected UAO value for interactions and requests to the OAG.	<p>Where an EMR user has an assigned or selected a UAO value, the EMR Offering MUST automatically include the UAO value of the EMR user to the OAG when requesting access to an EHR service.</p> <p>Where the EMR user has no assigned or selected UAO value, then it MUST be omitted.</p>	M	P

SSO03.05	<p>The EMR Offering MUST support the functionality for an EMR user to manually change their UAO value within their login session.</p>	<p>Changing UAO values MUST only be available where the EMR user is assigned multiple UAO values.</p> <p>Where the EMR user wishes to change their UAO, the EMR Offering MUST NOT prompt the EMR user to log out of their session.</p> <p>At a minimum, the EMR Offering MUST display the following UAO attributes to the EMR user:</p> <p>Friendly name</p> <p>Informational: An EMR user may work on behalf of multiple HICs, where they need to identify and switch between the HICs when accessing EHR Services. This functionality is pertinent when an EMR user is already connected to an EHR Service as one UAO and needs to switch to a different UAO.</p>	M	P
----------	---	--	---	---

2.4 Session Management

The following EMR requirements apply to EMR functionality session management.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO04.01	The EMR Offering MUST notify the EMR user when the maximum idle timeout period has been reached for their trusted external IDP credentials.	<p>The federated identity broker has a defined maximum idle timeout period. The EMR Offering MUST notify the EMR user when their IDP credentials are about to expire due to a maximum idle timeout period.</p> <p>Where an IDP login session is about to reach a maximum idle time, the EMR Offering MUST provide the EMR user with the opportunity to extend their login session.</p>	M	P
SSO04.02	The EMR Offering MUST prompt the EMR user to re-authenticate using their trusted external IDP credentials when the maximum session period has been reached.	<p>The federated identity broker has a defined maximum session period. The EMR Offering MUST notify the EMR user when their IDP credentials are about to expire due to a maximum session period.</p> <p>Where an IDP login session has reached a maximum session period, the EMR Offering MUST provide the EMR user with the re-authenticate using their IDP credentials.</p> <p>Note: A session period cannot be extended beyond the maximum defined period.</p>	M	P
SSO04.03	The EMR Offering MUST end all active SSO sessions when the EMR user logs out of the EMR Offering.	When an EMR user logs out of the EMR Offering, all active SSO sessions for that EMR user MUST be gracefully ended.	M	P
SSO04.04	The EMR Offering MUST mitigate any potential unauthorized exposure of PHI when the EMR user logs out of the EMR Offering.	<p>When an EMR user logs out of the EMR Offering, the EMR Offering MUST prevent the possible display of, and ability to modify PHI, when the EMR user logs out of the EMR Offering, where possible (e.g., closing of browser windows).</p> <p>Only where it is not possible for the EMR Offering to prevent the potential display of PHI (e.g., on an external browser window), the EMR Offering MUST alternatively notify the EMR user of the potential risk to unauthorized exposure of PHI and instructions to mitigate that risk.</p>	M	P
SSO04.05	The EMR Offering MUST allow the EMR user to log out of their active IDP session	Where an EMR user is logged in with their trusted external IDP credentials without SSO, the EMR Offering MUST provide the EMR user with the option	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	without logging out of the EMR login session.	to remain logged in to the EMR Offering with their EMR credentials without ending the EMR login session.		

2.5 Error Handling

The following EMR requirements apply to EMR functionality specific to error handling with federated identity and SSO.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO05.01	The EMR Offering MUST take appropriate actions for all errors that can occur while communicating with a Federated Identity Broker.	EMR users MUST be notified of any service disruptions that result from errors. The EMR Offering MUST log the errors and notify the EMR user of the error as well as the appropriate next step(s) for the EMR user.	M	P
SSO05.02	The EMR Offering MUST notify the EMR user when a UAO error occurs.	Where an EMR user encounters a UAO error while attempting to connect to an EHR Service, the EMR Offering MUST notify the EMR user of the error. Refer to the “Under Authority of (UAO) Management” section of the ONEID OAuth2/OpenID Specification for more details.	M	P

2.6 Logging and Auditing

EMR systems log different information and interactions. In some instances, PHI may be passed as parameters of the interaction. As a result, precaution should be taken to log only what is necessary, to avoid unintentionally saving and/or providing access to PHI. The following EMR requirements apply to functionality specific to logging and auditing for federated identity and SSO, they are supplementary to the requirements identified in the Primary Care Baseline Specification.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO06.01	The EMR Offering MUST log IDP login attempts to facilitate auditing and troubleshooting.	<p>Successful login attempts MUST be logged. Where possible, failed login attempts MUST also be logged.</p> <p>Additional information MUST be logged, as necessary and available, to facilitate auditing and troubleshooting processes.</p> <p>It is recommended to provide access to logs via the EMR user interface.</p>	M	P
SSO06.02	The EMR Offering MUST be able to log errors generated by a Federated SSO Identity Broker to facilitate troubleshooting.	<p>Any errors received from a Federated SSO Identity Broker MUST be logged by the EMR Offering.</p> <p>At a minimum, the following must be logged:</p> <ul style="list-style-type: none"> a) Action or request attempted by the EMR user b) The EMR user attempting the action or request c) Date and time the action and error occurred <p>It is recommended to provide access to logs via the EMR user interface.</p>	M	P
SSO06.03	The EMR Offering MUST log all transactions associated with UAO assignments.	<p>The EMR Offering MUST be able to keep logs of all transactions for UAO assignments within the EMR Offering.</p> <p>At a minimum it MUST capture:</p> <ul style="list-style-type: none"> a) Which EMR user made changes to any UAO assignments b) Which users were assigned UAO values c) What changes were made to assignment of UAO values d) Date and time when changes were made to assignment of UAO values e) Previous condition of the UAO assignment 	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		<p>Note: Refer to each EHR service specification document for their use of system UAO values.</p>		