EMR EHR Connectivity 2.1

Federation Identity and Single Sign-On – Requirements

July 13, 2020
Document Version & Status: 1.1 – DFC (Draft for Comment)

Table of Contents

TABLE OF CONTENTS **2**

1. INTRODUCTION **3**

1.1 Related Documents, References and Sources 3
1.2 Version History 3

2. EMR REQUIREMENTS **4**

2.1 EMR Login 4
2.2 User Account Association 6
2.3 Under the Authority Of (UAO) Values 8
2.4 Session Management 11
2.5 Error Handling 12
2.6 Logging and Auditing 12

1. INTRODUCTION

The purpose of this document is to provide implementers with the implementation of functional requirements and guidance to integrate an
Digital Services Identity Federation and Sing Sign-On (SSO) functionality within an EMR Offering to access provincial Electronic Health Record (EHR) products and services.

1.1 Related Documents, References and Sources

ID	DOCUMENT NAME	VERSION	PUBLICATION DATE
1	Example Federated SSO Token.xml	1.0	2017-03-30
2	Example User Registry Client Token.xml	1.0	2017-03-30
3	ONE ID Provincial Identity Federation Overview of SAML Configuration (Ontario Health Digital Services, 2018) https://www.ehealthontario.on.ca/en/standards/view/single-sign-on-patient-context-sharing-standard/	1.4 (1.49)	2018-08-21
4	ONE ID OAuth2/OpenID Specification (Ontario Health Digital Services, 2020) https://www.ehealthontario.on.ca/en/standards/view/one-id-openid-connect-specification	1.0	2020-01-09

1.2 Version History

VERSION	REVISION DATE	REVISION NOTES
1.0	2019-12-23	a) The initial release that includes OAuth2 protocol b) Added Readme document to identify optionality to implement SSO
1.1	2020-07-13	a) Updated SSO01.02 to log the EMR user into the EMR Offering using SSO b) Added SSO01.04 to include functional parity with 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. 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

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO01.01	The EMR Offering MUST present EMR users with the option to log into the EMR	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)	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
	Offering using credentials provisioned by the EMR Offering or their trusted external IDP credentials.	or a trusted external IDP credentials at the EMR login screen where both options MUST be available. The EMR Offering MUST initiate the OAuth2 token workflow the EMR user to the Federation Identity Broker if the EMR user chooses to log in using their trusted external IDP credentials. The EMR Offering MUST ONLY allow an IDP login where the EMR user is already bound to the EMR Offering.		
SSO01.02	The EMR Offering MUST allow EMR users to log into the EMR Offering using a Federation SSO Identity user account.	Once successfully authenticated by a trusted external IDP via the Federation 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 SSO Federation credentials are not needed by the EMR user or the federation 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.	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. 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. **Important**: An EMR user logged in with their EMR credentials wishing to launch an EHR Service MUST be prompted to enter in their trusted external IDP credentials without logging out of their session.	M	U
SSO01.05	The EMR Offering MUST have a configurable option to allow the EMR user access to EHR services	EMR user access to EHR Services SHOULD be configurable within the EMR Offering. The ability to configure access to EHR Services within the EMR Offering MUST be restricted to specific (e.g., administrative) user(s).	O	U

2.2 User Account Association

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO02.01	The EMR Offering MUST associate an EMR user's Federation SSO Identity with their EMR user account.	The EMR Offering MUST bind the Federation 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. The "PrincipalFedKey" SAML assertion attribute/element value MUST be used to bind the Federation SSO Identity to the respective EMR user account. The "Sub" OAuth2 attribute within the ID Token MUST be used to bind the Federation SSO Identity to the respective EMR user account. Binding between a Federation SSO account and an EMR user account MUST not be allowed without first successfully authenticating the user to both accounts. **Note**: Binding of a Federation 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).	M	U
SSO02.02	The EMR Offering MUST provide the ability to disassociate a Federation SSO Identity from an EMR user account.	The EMR Offering MUST have the functionality to disassociate a Federation SSO Identity with an EMR user account. The ability to disassociate the Federation SSO Identity SHOULD be available through the EMR user interface and not require assistance from the EMR vendor support staff.	M	P
SSO02.03	The EMR Offering MUST NOT store or cache any EMR user credentials for IDPs.	User credentials, where required, MUST be provided by the EMR user. SSO to the EMR Offering and EHR services only occurs if the EMR user has been successfully authenticated by a Federation Identity Provider via the Federation Identity Broker.	M	P
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 Federation 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	U

2.3 Under the Authority Of (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.	The EMR Offering MUST have an interface to allow an EMR user to manage (e.g., add, modify, delete) UAO values. The EMR Offering MUST restrict authorization to maintain UAO values to specific (e.g., administrative) EMR users. At a minimum the EMR Offering MUST maintain the following information for UAO values: a) UAO values b) UAO friendly names Refer to the "Under Authority of (UAO) Management" section of the ONEID OAuth2/OpenID Specification for more details.	M	P
SSO03.02	The EMR Offering MUST allow EMR users to be associated with UAO values.	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. At a minimum, the EMR Offering MUST: 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) **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).	M	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.	Once the EMR user is authenticated, the EMR Offering MUST prompt the EMR user to select a UAO value. 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. 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). 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. At a minimum, the EMR Offering MUST display the following UAO friendly name to the EMR user. The EMR Offering MAY additionally display the UAO identifier attribute to the EMR user.	M	U
SSO03.04	The EMR Offering MUST use the EMR users assigned or selected UAO value for interactions and requests to the OAG.	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. Where the EMR user has no assigned or selected UAO value, then it MUST be omitted.	M	P
SSO03.05	The EMR Offering MUST support the functionality for an EMR user to manually change their UAO value within their login session.	Changing UAO values MUST only be available where the EMR user is assigned multiple UAO values. Where the EMR user wishes to change their UAO, the EMR Offering MUST NOT prompt the EMR user to log out of their session. At a minimum, the EMR Offering MUST display the following UAO attributes to the EMR user:	M	P

		Friendly name **Informational**: An EMR user may work on behalf of multiple HICs, where they need to identify and switch between the HICs when access 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.		

2.4 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.	The federation 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. 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.	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.	The federation 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. 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. **Note**: A session period cannot be extended beyond the maximum defined period.	M	P
SSO04.03	Logging out of an EMR Offering MUST terminate all active SSO sessions.	When an EMR user logs out of the EMR Offering, all active SSO sessions for that EMR user MUST be terminated. Any related access to PHI (e.g., ability to view or modify PHI from a browser or modal window) MUST be inaccessible once logged out.	M	P
SSO04.04	The EMR Offering MUST allow the EMR user to log out of their active IDP session without logging out of the EMR login 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 to remain logged in to the EMR Offering with their EMR credentials without ending the EMR login session.	M	P

2.5 Error Handling

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 Federation 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	U
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.

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO06.01	The EMR Offering MUST log IDP login attempts to facilitate auditing and troubleshooting.	Successful login attempts MUST be logged. Where possible, failed login attempts MUST also be logged. Additional information MUST be logged, as necessary and available, to facilitate auditing and troubleshooting processes. It is recommended to provide access to logs via the EMR user interface.	M	P
SS006.02	The EMR Offering MUST be able to log errors generated by a Federation SSO Identity Broker to facilitate troubleshooting.	Any errors received from a Federation SSO Identity Broker MUST be logged by the EMR Offering. t a minimum the following must be logged: 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	M	U

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		It is recommended to provide access to logs via the EMR user interface.		
SSO06.03	The EMR Offering MUST log all transactions associated with UAO assignments.	The EMR Offering MUST be able to keep logs of all transactions for UAO assignments within the EMR Offering. At a minimum it MUST capture: 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 **Note**: Refer to each EHR service specification document for their use of system UAO values.	M	P