EMR EHR Connectivity 2.0

Federation Identity and Single Sign-On – Requirements

December 23, 2019

Document Version & Status: 1.0 – DFC (Draft for Comment)

1. Table of Contents

1. TABLE OF CONTENTS 2

1. INTRODUCTION 3

1.1 RELATED DOCUMENTS AND REFERENCES 3

2. EMR REQUIREMENTS 4

2.1 EMR LOGIN 5

2.2 USER ACCOUNT ASSOCIATION 5

2.3 SESSION MANAGEMENT 7

2.4 ERROR HANDLING 8

2.5 LOGGING AND AUDITING 8

1. INTRODUCTION

The purpose of this document is to provide implementers with the implementation of functional requirements and guidance to integrate an Ontario Health's 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 and References

DOCUMENT NAME	VERSION	PUBLICATION DATE
Example Federated SSO Token.xml	1.0	2017-03-30
Example User Registry Client Token.xml	1.0	2017-03-30
ONE ID Provincial Identity Federation Overview of SAML Configuration (Ontario Health, 2018)[1] https://www.ehealthontario.on.ca/en/standards/view/single-sign-on-patient-context-sharing-standard/	1.49 (1.4)	2017-08-21

[1] Version 1.5 of this document is published but does not apply and should not be referenced.

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 Offering using either their EMR credentials or their IDP credentials.	The EMR Offering MUST present the EMR user with the ability to choose to log in using their EMR credentials or their IDP credentials at the EMR login screen where both options MUST be available. The EMR Offering MUST be able to support a list of potentially more than one IDP. The EMR Offering MUST redirect the EMR user to the respective Federation Identity Broker if the EMR user chooses to log in using their IDP credentials.	M	P
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 an 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

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	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
		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. 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).		
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 a Federation SSO Token (Token 1) issued by the Provincial Federation Identity Broker service for the duration of the Federation SSO session.	The Provincial Federation Identity Broker service will return a Federation SSO Token (Token 1) upon successful authentication of the EMR user.	M	P

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO02.05	The EMR Offering MUST use the UR Client Token (Token 2) to assert an EMR user's identity when accessing provincial EHR solutions and EHR services.	The EMR Offering MUST present the User Registry Client Token (Token 2) each time an EHR service is launched. The EMR Offering MUST use the same UR Client Token (Token 2) when accessing different EHR services within the validity period of the Federation SSO session.	M	P

2.3 Session Management

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO03.01	The EMR Offering MUST notify the EMR user when their security token is about to expire.	The EMR Offering MUST monitor the expiration period of the security token to warn the EMR user to provide an opportunity to complete any work in progress or to re-authenticate.	M	P
SSO03.02	The EMR Offering MUST prompt the EMR user to re-authenticate using their provincial federated identity credentials when the inactivity timeout or period of expiry for the security token has been reached.	The security token returned by the Federation Identity Broker service will timeout after a period of inactivity (e.g., 45 minutes) or expire after a predefined duration (e.g., 8 hours). The inactivity period and the expiration duration may change as defined by the Federation Identity Broker.	M	P
SSO03.03	Logging out of an EMR system 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

2.4 Error Handling

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO04.01	The EMR Offering MUST take appropriate actions for all errors that can occur while communicating with a Federation SSO Identity Broker.	EMR users MUST be notified of any service disruptions that result from errors.	M	P

2.5 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
SSO05.01	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
SS005.02	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. It is recommended to provide access to logs via the EMR user interface.	M	P