EMR EHR Connectivity 1.1

Single Sign-On

April 1, 2019

Document Version & Status: 1.1 – Final

Table of Contents

1. INTRODUCTION

The purpose of this document is to provide EMR vendors with the implementation guidance and functional requirements to implement the Federation Single Sign-On (SSO) described in eHealth Ontario's ONE®ID Provincial Identity Federation Overview of SAML Configuration Standard (eHealth Ontario, 2017) to integrate Federation SSO functionality within EMR Offerings to access provincial Electronic Health Record (EHR) products and services.

This document is organized into the following sections:

1) **Business View**: Describes the business context and benefits of connecting EMR Offerings to provincial EHR products and services using Federation SSO; provides a high-level overview of the primary stakeholders and systems involved in helping EMR users access EHR products and services from their EMR Offering.
2) **System View**: Provides an overview of the systems involved in accessing EHR products and services.
   Data View: Specifies the Security Assertion Markup Language (SAML) elements and attributes that EMR Offerings need to support for the identification of EMR users and authorization of their access to EHR products and services.
   EMR Offering Functional Requirements: Describes the functional requirements that EMR Offerings must support to enable Federation SSO for EMR users.

1.1 Related Documents and References

DOCUMENT NAME	VERSION	PUBLICATION DATE
ONE®ID Provincial Identity Federation Overview of SAML Configuration (eHealth Ontario, 2017) https://www.ehealthontario.on.ca/en/standards/view/single-sign-on-patient-context-sharing-standard/	1.5	2017-01-02
Example Federated SSO Token.xml	1.0	2017-03-30
Example User Registry Client Token.xml	1.0	2017-03-30

2. BUSINESS VIEW

2.1 Business Drivers

Clinicians can provide enhanced patient care with improved access to information and the ability to coordinate with other care providers. Integrating EMR Offerings with provincial EHR products and services is one of the ways to help clinicians achieve this goal.

The provincial Health Information Access Layer (HIAL) is a component of the provincial EHR that acts as the gateway between point-of-service systems (such as an EMR) and an EHR service provider, that comprise the provincial EHR. The provincial HIAL will be the primary means of accessing provincial EHR products and services. Over time, the list of EHR products and services and their value to clinicians is projected to grow.

EMR Offerings must connect to the provincial HIAL regardless of which EHR product(s) or service(s) they intend to consume. EMR vendors need specifications that describe how to authenticate EMR users and make a connection to the provincial HIAL. Once authenticated, EMR users can access the EHR product(s) and service(s) that they are authorized to use. This document focuses on authentication.

2.1.1 Single Sign-On

Anyone accessing provincial EHR products or services must be authenticated (to be certain the person is who they say they are) and authorized (to ensure they have appropriate access to the EHR product or service). Authentication requires a person to provide one or more information to identify themselves, such as something that 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 been shown to be a barrier to the adoption of new technologies. eHealth Ontario provides the ability for EMR vendors to integrate SSO capabilities within their EMR Offerings using a federated service which allows a person to log into their EMR Offering and seamlessly access EHR products and services from within the EMR Offering without having to re-enter multiple credentials.

Note: eHealth Ontario does not permit EMR Offerings to store or cache passwords from Federation Identity Providers (IDPs). This means that if a person logs in to the EMR Offering using their non-Federation EMR credentials they will still need to enter their IDP credentials if they attempt to access an EHR product or service.

2.2 Stakeholders

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 “principals” in eHealth Ontario specifications, they use EMR Offerings to access EHR products and services. Examples include clinicians, physicians, nurses, or their delegates.
Federation Identity Provider (IDP)	Provides the business services to assign credentials to healthcare providers and provide the identity management applications that authenticate credentials.
EHR Application / Service Providers	Manage the business service to grant and authorize EMR user access to a given EHR product or service and provide applications that provide EHR product or service.

2.3 Business Context

The following diagram conceptually depicts how EMR users interact with an EMR Offering to access EHR products and services.

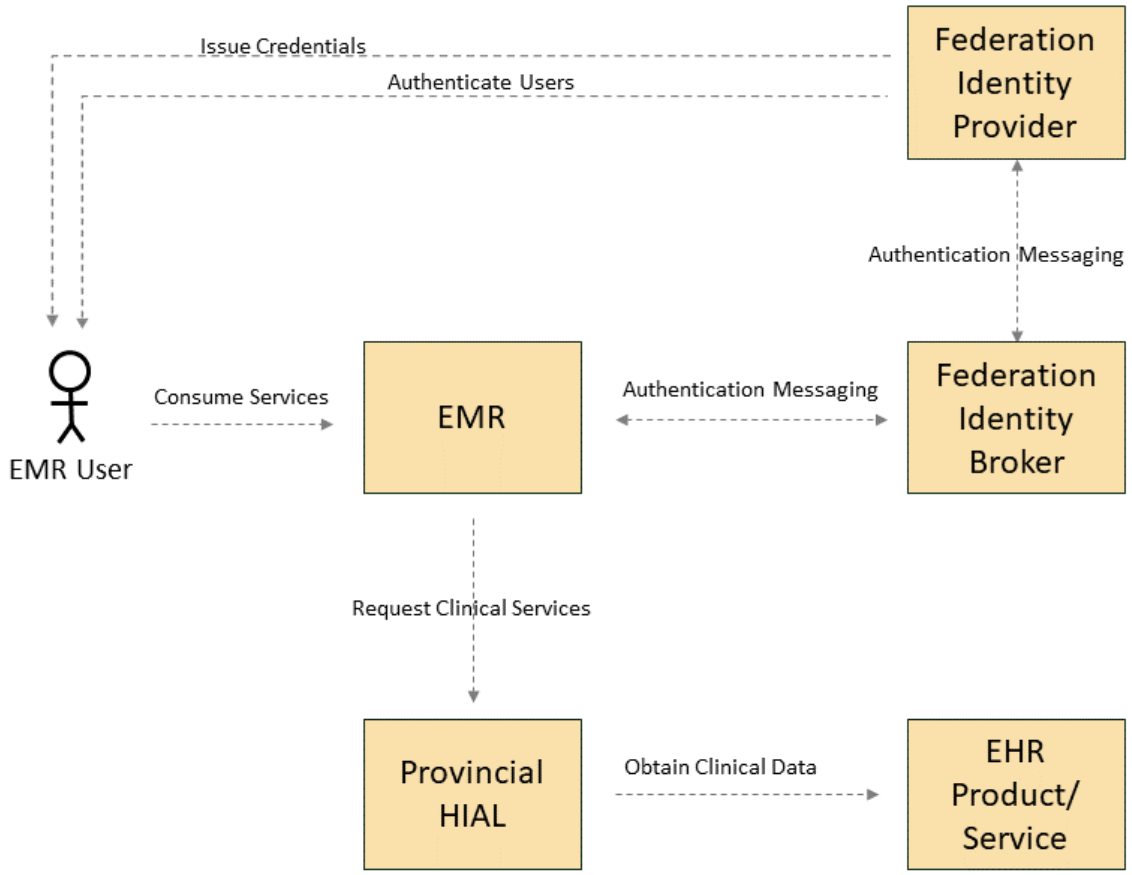

Figure 1 - Business Context Diagram

2.4 User Stories

2.4.1 Single Sign-On – Initial Credential Binding from the EMR Login Screen

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

2.4.2 Single Sign-On – Initial Credential Binding from an EHR Service Request

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

2.4.3 Single Sign-On to EMR Offering and EHR Services

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

3. SYSTEM VIEW

3.1 System Overview

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

1. **EMR Offering:** Used by EMR users to access the Federation Identity Broker and in turn authenticate their IDP credentials, access the EMR application, and EHR products and services.
2. **Federation Identity Broker:** Orchestrates authentication of EMR users with IDPs.
3. Federated Identity Provider: Authenticates EMR users.
4. **HIAL:** Orchestrates connections between EMR Offerings and the applications that provide EHR services.
5. **EHR Product/Service**: The system or application that provides the EHR product or service.

The following diagram depicts the role of each of these systems and the transactions they support to enable SSO in order to connect to EHR products and services.

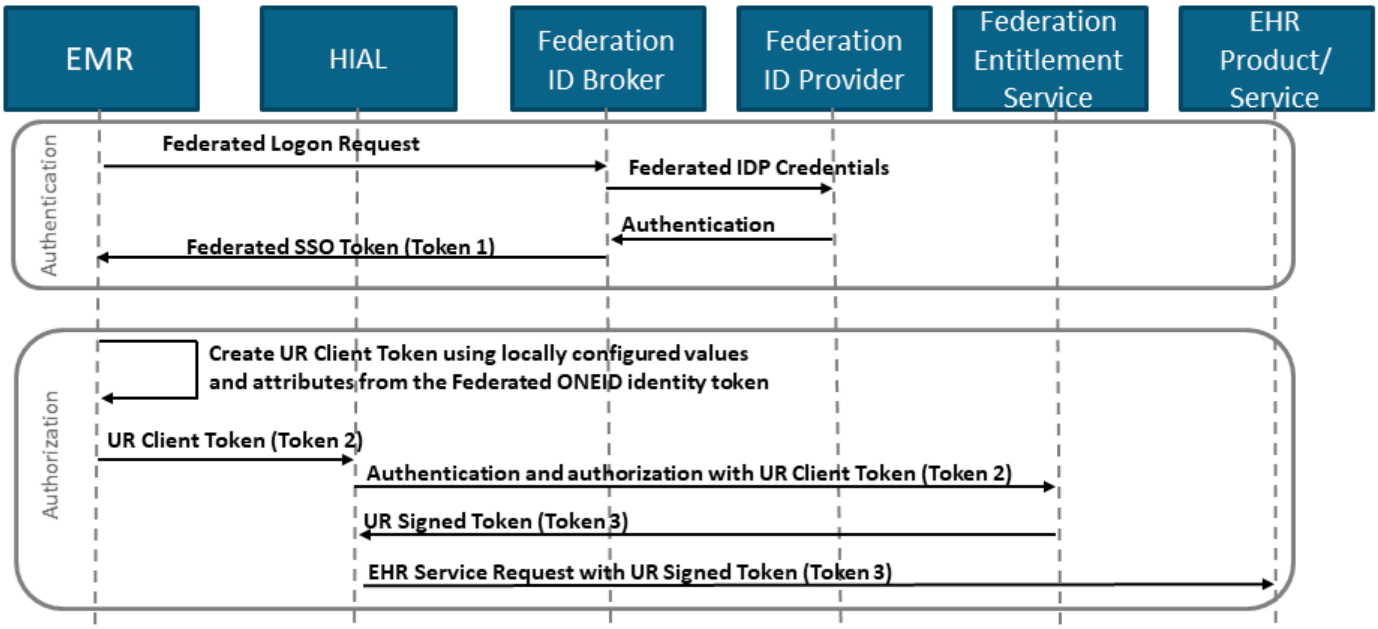

Figure 2 - Transaction Patterns

There are two potential triggers for a federation login request:

1) The EMR user selects an IDP at the EMR Offering login screen and enters their credentials.
2) The EMR user has logged into the EMR Offering using their EMR credentials and attempts to access an EHR product or service and the EMR does not have a valid Federation SSO session.

In both scenarios, the EMR Offering MUST check for a valid User Registry (UR) Client Token (Token 2) first before making the Federation Login Request.

4. DATA VIEW

The following section specifies the authentication interaction patterns and the use of SAML tokens to express authentication information. This section contains guidance on the purpose of specific SAML assertion elements/attributes, and how to populate them when interacting with the provincial HIAL.

4.1 Federation Login

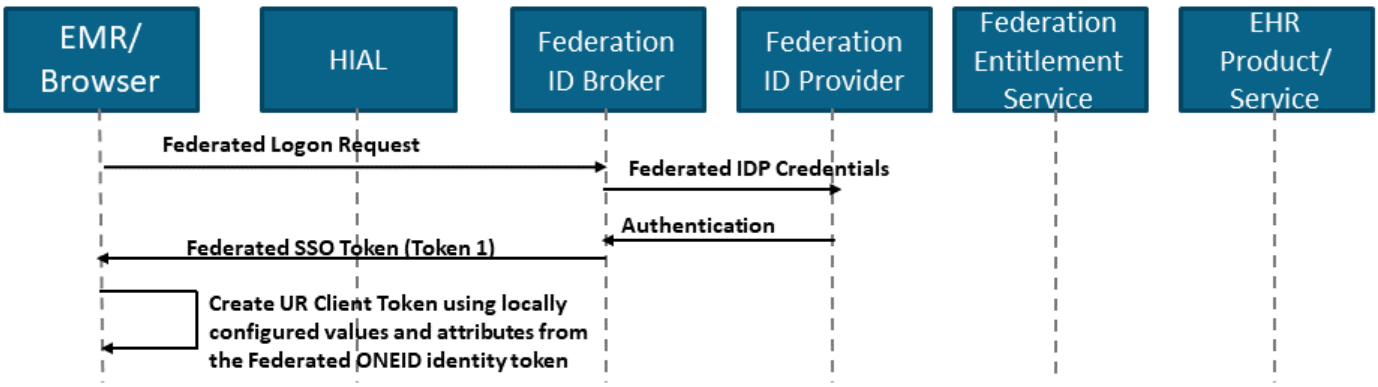

Figure 3 - Federation Login Request

4.1.1 Federation Login Request

A request to the Federation ID Broker is triggered after an EMR user has been prompted to log in using credentials from an IDP (e.g., either at the EMR Offering's login screen or after selecting an EHR product or service from within the EMR Offering).

4.1.2 Federation Login Response - Federation SSO Token (Token 1)

Once the EMR user is authenticated, the Federation ID Broker creates a SAML token called the Federation Single Sign-On (SSO) Token (Token 1) and returns it to the EMR Offering. Token 1 contains the information in the table below.

SAML ASSERTION ELEMENT/ATTRIBUTE	FEDERATION SSO TOKEN (TOKEN 1) CONCEPTS
/Signature	A digital signature of the SAML response. See https://www.w3.org/TR/xmldsig-core/ for more information on all child elements of /Signature, as well as validation of the digital signature. The Federation ID Broker's public key, supplied in the PKI certificate in "/Signature/KeyInfo/X509Data/X509Certificate" is used to verify the digital signature.

SAML ASSERTION ELEMENT/ATTRIBUTE	FEDERATION SSO TOKEN (TOKEN 1) CONCEPTS
/Issuer	Entity ID of the Federation ID Broker
/Subject/NameID	A unique identifier generated by the Federation ID Broker. Example: id-8SYU62PDn--EEUYoDckvua1UBdL-
/Subject/NameID[@Format]	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
/Subject/NameID[@NameQualifier]	Entity ID of the Federation ID Broker or IDP issuer
/Subject/SubjectConfirmation[@Method]	Used to verify the message came from a system entity that is associated with the subject of the assertion, within the context of a particular profile. The Federation ID Broker will specify: urn:oasis:names:tc:SAML:2.0:cm:bearer
/Conditions[@NotBefore] and /Conditions[@NotOnOrAfter]	These two values indicate the SAML assertion validity period. This period is set to five minutes to allow for user interaction and redirection.
AuthenticationLevel	The authentication level (based on eHealth Federation Standards) at which the EMR user was authenticated.
IdentityVerificationSchemeRef	The eHealth Federation evaluation criteria/level for an IDP's verification processes.
CredentialManagementSchemeRef	The eHealth Federation evaluation criteria/level for an IDP's credential management processes.
IdentityProvider	The IDP that authenticated the EMR user.
AssertingParty	The originating organization. The organization providing the asserted values. For example, the ONE®ID Identity Provider value is: federation.ehealthontario.ca
/AuthnStatement/AuthnContext/AuthnContextClassRef	Authentication context of EMR user Value=urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
Compensating Factor	No direct equivalent in Federation SSO Token (Token 1); value is determined by the EMR based on other values in Federation SSO Token (Token 1).
FirstName	[Attribute Statement]/firstName First name of requesting EMR user

SAML ASSERTION ELEMENT/ATTRIBUTE	FEDERATION SSO TOKEN (TOKEN 1) CONCEPTS
LastName	[Attribute Statement]/lastName Last name of requesting EMR user
Rid	Real Identity References – identifiers that can be resolved to an entry in the Provincial Provider Registry. This attribute is mandatory with the coded value used to identify unregulated providers.
ServiceEntitlements	Federated Delivery Channels/Applications that the user has been authorized for and the organization(s)/provider person(s) that authorized each Delivery Channel/Application. A default value of “Not Authorized” will be used whenever the principal has not been approved for Delivery Channel/Application access in the Federation Authorization Service. Format: <ServiceName>:<UAO>:<Optional_attributes:eff>:<YYYY-MM-DD> ServiceName = Delivery Channel, Application or ‘Not Authorized’ For some Applications, a Delivery Channel alone is valid as the Delivery Channel is also an Application. For other Applications, a Delivery Channel is required along with specific Applications. For those Applications, a minimum of two ServiceEntitlement attributes are required (one for the Delivery Channel and a second for the Application accessed from the Delivery Channel) UAO: Each ServiceName must be associated with a UAO Format of UAO is <Identifier Type>:<Number> where “Type” is a UPI The OID type of identifier is not valid in the ServiceEntitlements attribute as a UAO type. If the Delivery Channel requires additional information about the organization, the UAO attribute may be used to find other identifiers (i.e. OID) for the organization Optional Attributes:

SAML ASSERTION ELEMENT/ATTRIBUTE	FEDERATION SSO TOKEN (TOKEN 1) CONCEPTS
	If Delivery Channels require additional detail, the Federation Authorization Service may be configured to capture additional attributes The ServiceEntitlements attribute has been extended to allow for additional attributes The additional attributes will be denoted with a label, specific to the Delivery Channel, followed by a colon and then the alphanumeric value for the attribute. For multi-valued attributes, the values are denoted by a list of alphanumeric characters separated by semicolons. Effective To Date: The date until which a user is authorized to access the service.
PatientContextSessionID	This attribute is a unique identifier assigned by the Federation ID Broker during the user login process. This attribute enables providers and delivery channels to set and retrieve patient context information on behalf of the provider. Example Format: <saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextSessionID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">3455-3334-4467-54637-3457</saml:AttributeValue></saml:Attribute>

Please see Sample Token 1.xml for an example of the XML expression of a SAML token.

4.2 User Registry Client Token in EHR Service Requests

The User Registry (UR) Client Token (Token 2) is sent from the EMR Offering to the provincial HIAL in requests for EHR services. The data in Token 2 is used by the provincial HIAL and ONE®ID to authenticate the EMR system, EMR user and authorize their request for access to an EHR product or service.

The following section describes how to create Token 2. Specifying how to request an EHR product or service from an EMR Offering is out of scope for this specification and expected to be described in specific EHR product or service implementation guides.

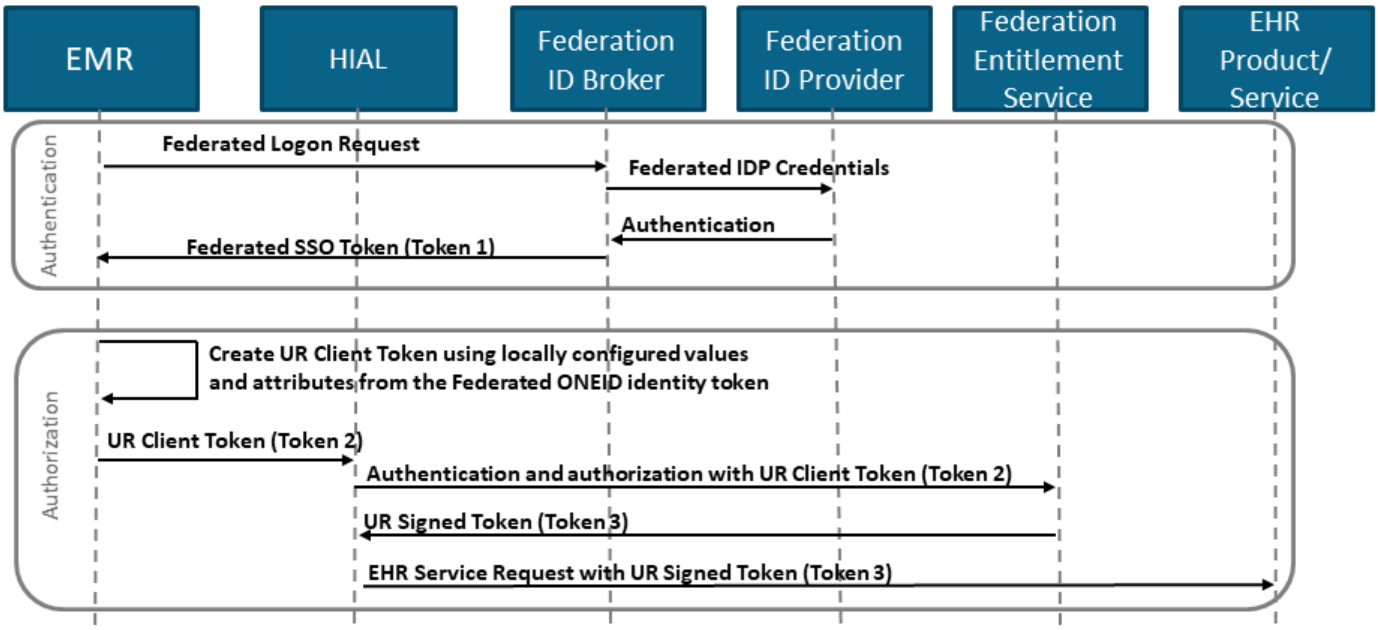

Figure 4 - Transaction Patterns

The information in the Federation SSO Token (Token 1) is subsequently used by the EMR Offering to a create the User Registry Client Token (Token 2) that is sent by the EMR in requests for access to EHR products or services. The table below describes the important SAML assertion elements or attributes used in the User Registry Client Token (Token 2) and where the EMR Offering sources the data from.

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
/Signature	A digital signature of SAML Token 2. Briefly, the digital signature is created by the EMR Offering as follows for SAML Token 2: Apply the following transformation algorithms to SAML Token 2: Enveloped Signature Transforms Exclusive XML Canonicalization with no namespaces specified in the InclusiveNamespaces Prefix List (the InclusiveNamespaces element may be omitted)	EMR Offering

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
	Note: these transformation algorithms MUST be specified in the Transforms and CanonicalizationMethod elements for the receiver to apply the same transformation algorithms to the message. Calculate the digest value by applying the SHA2 digest method and base64 encode the resultant value. Encrypt the digest value using the RSA-SHA2 encryption algorithm and the EMR/delivery channel's private key and base64 encode the resultant value to generate the signature value. See https://www.w3.org/TR/xmldsig-core/ for detailed information on all child elements of /Signature, as well as more details on the generation of the digital signature, and https://www.w3.org/TR/xml-exc-c14n/ and https://www.w3.org/TR/xml-c14n/ for more information on XML canonicalization.	
/Issuer	PKI certificate Distinguished Name (DN) used by the partner for signing SAML Token 2. The value MUST conform to https://www.ldap.com/ldap-dns-and-rdns, with whitespace following each comma in the DN and no whitespace preceding nor following each equal sign; e.g., "CN=HealthCareApp1, OU=Applications, OU=eHealthUsers, OU=Subscribers, DC=subscribers, DC=ssh"	EMR Offering
/Subject/NameID	Specify the NameID value received in Federation SSO Token (Token 1)	Federation SSO Token (Token 1)
/Subject/NameID[@Format]	Specify: urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified	Federation SSO Token (Token 1)
/Subject/NameID[@NameQualifier]	Specify the NameQualifier value received in Federation SSO Token (Token 1)	Federation SSO Token (Token 1)
/Subject/SubjectConfirmation[@Method]	Specify: urn:oasis:names:tc:SAML:2.0:cm:sender-vouches	EMR Offering
/Conditions[@NotBefore] and	These two values indicate the SAML assertion validity period.	EMR Offering

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
/Conditions[@NotOnOrAfter]	This period MUST not be greater than one minute, although the maximum validity period may be set to a larger value for convenience during development and testing. Many IDPs use a validity period of 30 seconds for SAML Token 2.	
AuthenticationLevel	See DelegationManagementSchemeRef and UAOIdentityVerificationSchemeRef attributes.	N/A
IdentityVerificationSchemeRef	[Authn Statement]/Identification/Extension/IdentityManagementSchemeRef Optional - The eHealth Federation Evaluation Criteria (FEC) defines how eHealth Ontario establishes measures of the identity assurance related aspects of an IDP, its identity verification processes, and its credential management processes. The eHealth Identity Assurance Framework describes how the FEC is represented in technical terms. Specify the value received in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
CredentialManagementSchemeRef	[Authn Statement]/Identification/Extension/CredentialManagementSchemeRef Optional - Derived using the eHealth Federation Evaluation Criteria. Indicates the strength of credential management process for the identified user. This attribute follows the same scheme reference mechanism as “Identity Verification”. Specify the value received in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
DelegationManagementSchemeRef	[Authn Statement]/Identification/Extension/DelegationManagementSchemeRef Specify the value received for the Authentication Level attribute in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
UAOIdentityVerificationSchemeRef	[Authn Statement]/Identification/Extension/UAOIdentityVerificationSchemeRef Specify the value received for the Authentication Level attribute in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
IdentityProvider	[Authn Statement]/AuthnMethod/Extension/IdentityProvider/AuthenticatingAuthority The IDP that authenticated the user. IDP Identifiers are part of Authentication Context. Although the specification indicates that this value is a Uniform Resource Identifier (URI), please specify the corresponding value received from the Federation Broker regardless of whether it is a URI or not.	Federation SSO Token (Token 1)
AssertingParty	[Authn Statement]/AuthnMethod/Extension/AssertingParty/AuthenticatingAuthority The IDP that is connected to eHealth and is submitting transactions. These will be a DN of the PKI certificate that is used to sign SAML Token 2. The value MUST conform to https://www.ldap.com/ldap-dns-and-rdns, with whitespace following each comma in the DN and no whitespace preceding nor following each equal sign; e.g., “CN=HealthCareApp1, OU=Applications, OU=eHealthUsers, OU=Subscribers, DC=subscribers, DC=ssh”	A static value assigned to the EMR by eHealth Ontario, configured in the EMR Offering
/AuthnStatement/AuthnContext/AuthnContextClassRef	[Authn Statement]/AuthnMethod/PrincipalAuthenticationMechanism/Extension/PrimaryFactor Specify "password"	EMR/Delivery Channel
ProtectedNetwork	[Authn Statement]/AuthnMethod/PrincipalAuthenticationMechanism/Extension/ProtectedNetwork	EMR/Delivery Channel

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
	Protected Access Point (Optional) - The goal of the “Protected Access Point” attribute is to reduce the need for traditional two-factor authentication in situations where users are authenticating from a trusted network location such as a Hospital that is an IDP, which acts as a de facto second factor. Most community-based clinics are not considered trusted networks and the type attribute for this element will be set to "false".	
Compensating Factor	[Authn Statement]/AuthnMethod/PrincipalAuthenticationMechanism /Extension/CompensatingFactor Additional authentication method. If the IdentityProvider attribute value="ONE ID" and AuthnContextClassRef="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport", then specify "urn:ehealth:names:idm:compensatingFactor:extendedSessionToken"; otherwise, do not specify a value for this attribute.	Federation SSO Token (Token 1)
FirstName	[Attribute Statement]/FirstName First name of requesting EMR user Specify the value received for this attribute in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
LastName	[Attribute Statement]/LastName Last name of the requesting EMR user Specify the value received for this attribute in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
Rid	[Attribute Statement]/Rid Real Identity (RID) Binding - This attribute specifies an identifier for the subject (EMR user) in terms of an identifier that can be resolved to an entry in the Provincial Provider Registry.	Federation SSO Token (Token 1)

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
	Use the value received in Federation SSO Token (Token 1) to determine the value to specify here. It is rare but theoretically possible that an EMR user has more than one RID. Please see APPENDIX B for more information.	
UAO	[Attribute Statement]/uao This attribute specifies the responsible party for a given transaction. In most situations, the responsible party will be the Health Information Custodian (HIC) (i.e., the primary care practice or organization) to which the EMR user is accountable. The attribute value needs to represent a unique identifier which can be mapped to an entry in the Provider Registry. The unique identifiers need to conform to one of the acceptable formats. Specify the Universal Provider Identifier (UPI) corresponding to the Health Information Custodian that is the responsible party for this transaction in this format: urn:ehealth:rid:upi:<UPI number>	Obtained during the EMR onboarding and configured during an EMR install; may require EMR user to select if EMR may submit requests for multiple HICs.
uaoType	[Attribute Statement]/uaoType The content is the word "person" or "org". Mandatory (if UAO or GrantByDelegateMeritOnly are present). This attribute specifies the type of provider in the UAO attribute. The UAO can be a provider person or a provider organization.	Configured during EMR install; obtained during the EMR onboarding
GrantByDelegateMeritOnly	[Attribute Statement]/GrantByDelegateMeritOnly Mandatory - The value effects how the User Registry Policy Decision Point (UR PDP) performs authorization for individuals marked as a delegate. This attribute (when true) means the following to the Delegator: “Do not take my entitlements into account when granting access to my delegate. Should you grant access, I accept responsibility for the transaction”. Specify "false" for the value of this attribute.	Defined as configured in the EMR, False by default; for future use

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
Subject Locality	[Assertion]/AuthnStatement/SubjectLocality This attribute specifies the technical location (IP address) of the user.	EMR workstation/ device IP, inserted by the EMR
AuthenticationToken	[Attribute Statement]/AuthenticationToken Specify the value received in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
PrincipalFedKey	[Attribute Statement]/PrincipalFedKey Specify the value received in Federation SSO Token (Token 1). A value that uniquely identifies a given user and is also used to bind a user's Federation SSO identity to their EMR user account.	Federation SSO Token (Token 1)

Please see Sample Token 2.xml for an example of the XML expression of the SAML token.

5. EMR REQUIREMENTS

This section consists of the EMR functional requirements for Single Sign-On.

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 #:
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.

5.1 EMR Login

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

5.2 User Account Association

OMD #	REQUIREMENT	GUIDELINES	M/O	STATUS
SSO02.01	The EMR Offering MUST associate a 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. A 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 from 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	N
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 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	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
	Identity Broker service for the duration of the Federation SSO session.			
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 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

5.3 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 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	N

5.4 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	U

5.5 Logging and Auditing

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	U
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	N

6. APPENDIX A: MAPPING OF SAML ASSERTION ELEMENTS/ATTRIBUTES FOR TOKEN 1 AND 2

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
/Signature	A digital signature of the SAML response. See https://www.w3.org/TR/xmldsig-core/ for more information on all child elements of /Signature, as well as validation of the digital signature. The Federation Broker's public key, supplied in the PKI certificate in /Signature/KeyInfo/X509Data/X509Certificate, is used to verify the digital signature.	A digital signature of SAML Token 2. Briefly, the digital signature is created by the EMR/delivery channel as follows for SAML Token 2: 1. Apply the following transformation algorithms to SAML Token 2: a. Enveloped Signature Transforms b. Exclusive XML Canonicalization with no namespaces specified in the InclusiveNamespaces Prefix List (the InclusiveNamespaces element may be omitted) **Note**: these transformation algorithms MUST be specified in the Transforms and CanonicalizationMethod elements for the receiver to apply the same transformation algorithms to the message. 2. Calculate the digest value by applying the SHA2 digest method and base64 encode the resultant value 3. Encrypt the digest value using the RSA-SHA2 encryption algorithm and the EMR/delivery channel's private key and base64 encode the resultant value to generate the signature value See https://www.w3.org/TR/xmldsig-core/ for detailed information on all child elements of /Signature, as well as more details on the generation of the digital signature, and http://www.w3.org/TR/xml-exc-c14n/ and https://www.w3.org/TR/xml-c14n for more information on XML canonicalization.	EMR Offering

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
/Issuer	Entity ID of the Federation Broker	PKI certificate Distinguished Name (DN) used by the partner for signing SAML Token 2. The value MUST conform to https://www.ldap.com/ldap-dns-and-rdns, with whitespace following each comma in the DN and no whitespace preceding nor following each equal sign; e.g., "CN=HealthCareApp1, OU=Applications, OU=eHealthUsers, OU=Subscribers, DC=subscribers, DC=ssh"	EMR Offering
/Subject/NameID	A unique identifier generated by the Federation Broker. Example: id-8SYU62PDn--EEUYoDckvua1UBdL-	Specify the NameID value received in Federation SSO Token (Token 1)	Federation SSO Token (Token 1)
/Subject/NameID[@Format]	urn:oasis:names:tc:SAML:1.1:nameid-format:persistent	Specify: urn:oasis:names:tc:SAML:1.0:nameid-format:unspecified	Federation SSO Token (Token 1)
/Subject/NameID[@NameQualifier]	Entity ID of the Federation Broker or IDP issuer	Specify the NameQualifier value received in Federation SSO Token (Token 1)	Federation SSO Token (Token 1)
/Subject/SubjectConfirmation[@Method]	Used to verify the message came from a system entity that is associated with the subject of the assertion, within the context of a particular profile. The Federation ID Broker will specify: urn:oasis:names:tc:SAML:2.0:cm:bearer	Specify: urn:oasis:names:tc:SAML:2.0:cm:sender-vouches	EMR Offering
/Conditions[@NotBefore] and /Conditions[@NotOnOrAfter]	These two values indicate the SAML assertion validity period. This period is set to five minutes to allow for user redirection to the Assertion Consumer Service.	These two values indicate the SAML assertion validity period. This period MUST not be greater than one minute, although the maximum validity period may be set to a larger value for convenience during development and testing. Many partners	EMR Offering

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
		use a validity period of 30 seconds for SAML Token 2.	
AuthenticationLevel	The authentication level (based on eHealth Federation Standards) at which the EMR user was authenticated.	See DelegationManagementSchemeRef and UAOIdentityVerificationSchemeRef attributes.	N/A
IdentityVerificationSchemeRef	The eHealth Federation evaluation criteria/level for an IDP's verification processes.	[Authn Statement]/Identification/Extension /IdentityManagementSchemeRef Optional - The eHealth Federation Evaluation Criteria defines how eHealth establishes measures of the identity assurance related aspects of an IDP, its identity verification processes, and its credential management processes. The eHealth Identity Assurance Framework describes how the FEC is represented in technical terms. Specify the value received in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
CredentialManagementSchemeRef	The eHealth Federation evaluation criteria/level for an IDP's credential management processes.	[Authn Statement]/Identification/Extension /CredentialManagementSchemeRef Optional - Derived using the eHealth Federation Evaluation Criteria. Indicates the strength of credential management process for the identified user. This attribute follows the same scheme reference mechanism as "Identity Verification". Specify the value received in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
DelegationManagementSchemeRef - No equivalent		[Authn Statement]/Identification/Extension / DelegationManagementSchemeRef	Federation SSO Token (Token 1)

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
		Specify the value received for the Authentication Level attribute in Federation SSO Token (Token 1)	
UAOIdentityVerificationSchemeRef - No equivalent		[Authn Statement]/Identification/Extension /UAOIdentityVerificationSchemeRef Specify the value received for the Authentication Level attribute in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
IdentityProvider	The IDP that authenticated the EMR user.	[Authn Statement]/AuthnMethod/Extension/ IdentityProvider/AuthenticatingAuthority The IDP that authenticated the user. IDP Identifiers are part of Authentication Context. Although the specification indicates that this value is a URI, please specify the corresponding value received from the Federation Broker regardless of whether it is a URI or not.	Federation SSO Token (Token 1)
AssertingParty	The originating organization – The organization providing the asserted values. For example, the ONE®ID Identity Provider value is: federation.ehealthontario.ca	[Authn Statement]/AuthnMethod/Extension/ AssertingParty/AuthenticatingAuthority The IDP that is connected to eHealth and is submitting transactions. These will be a DN of the PKI certificate that is used to sign SAML Token 2. The value MUST conform to https://www.ldap.com/ldap-dns-and-rdns, with whitespace following each comma in the DN and no whitespace preceding nor following each equal sign; e.g., "CN=HealthCareApp1, OU=Applications, OU=eHealthUsers, OU=Subscribers, DC=subscribers, DC=ssh"	A static value assigned to the EMR by eHealth Ontario configured in the EMR

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
/AuthnStatement/AuthnContext/AuthnContextClassRef	Authentication context of EMR user Value= urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	[Authn Statement]/AuthnMethod/PrincipalAuthenticationMechanism/Extension/PrimaryFactor Specify "password"	EMR/ Delivery Channel
ProtectedNetwork	Indication if the user has been authenticated from a trusted network location	[Authn Statement]/AuthnMethod/PrincipalAuthenticationMechanism/Extension/ProtectedNetwork The goal of the “Protected Access Point” attribute is to reduce the need for traditional two-factor authentication in situations where users are authenticating from a trusted network location such as a Hospital that is an IDP, which acts as a de facto second factor. Most community-based clinics are not considered trusted networks and the type attribute for this element will be set to "false".	EMR/ Delivery Channel
Compensating Factor No direct equivalent in Federation SSO Token (Token 1); value is determined by the EMR based on other values in Federation SSO Token (Token 1)		[Authn Statement]/AuthnMethod/PrincipalAuthenticationMechanism/Extension/CompensatingFactor Additional authentication method. If the IdentityProvider attribute value="ONE ID" and AuthnContextClassRef="urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport", specify "urn:ehealth:names:idm:compensatingFactor:extendedSessionToken"; otherwise, do not specify a value for this attribute.	Federation SSO Token (Token 1)

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
FirstName	[Attribute Statement]/firstName First name of requesting EMR user	[Attribute Statement]/firstName First name of requesting EMR user Specify the value received for this attribute in Federation SSO Token (Token 1)	Federation SSO Token (Token 1)
LastName	[Attribute Statement]/lastName Last name of requesting EMR user	[Attribute Statement]/lastName Last name of the requesting EMR user Specify the value received for this attribute in Federation SSO Token (Token 1)	Federation SSO Token (Token 1)
Rid	Real Identity References – identifiers that can be resolved to an entry in the Provincial Provider Registry. This attribute is mandatory with the coded value used to identify unregulated providers.	[Attribute Statement]/Rid Real Identity (RID) Binding - This attribute specifies an identifier for the subject (EMR user) in terms of an identifier that can be resolved to an entry in the Provincial Provider Registry. Use the value received in Federation SSO Token (Token 1) to determine the value to specify here. It is rare but theoretically possible that an EMR user has more than one RID. Please see APPENDIX B for more information.	Federation SSO Token (Token 1)
ServiceEntitlements	Federated Delivery Channels/Applications that the user has been authorized for and the organization(s)/provider person(s) that authorized each Delivery Channel/Application.	No direct equivalent in Federation SSO Token (Token 2)	

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
	A default value of “Not Authorized” will be used whenever the principal has not been approved for Delivery Channel/Application access in the Federation Authorization Service. Format: <ServiceName>:<UAO>:<Optional_attributes:eff>:<YYYY-MM-DD> ServiceName = Delivery Channel, Application or ‘Not Authorized’ • For some Applications, a Delivery Channel alone is valid as the Delivery Channel is also an Application. • For other Applications, a Delivery Channel is required along with specific Applications. For those Applications, a minimum of two ServiceEntitlement attributes are required (one for the Delivery Channel and a second for the Application accessed from the Delivery Channel) UAO: • Each ServiceName must be associated with a UAO Format of UAO is <Identifier Type>:<Number> where “Type” is a UPI • The OID type of identifier is not valid in the ServiceEntitlements attribute as a UAO type. • If the Delivery Channel requires additional information about the organization, the UAO attribute may		

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
	be used to find other identifiers (i.e. OID) for the organization Optional Attributes: • If Delivery Channels require additional detail, the Federation Authorization Service may be configured to capture additional attributes • The ServiceEntitlements attribute has been extended to allow for additional attributes • The additional attributes will be denoted with a label, specific to the Delivery Channel, followed by a colon and then the alphanumeric value for the attribute. For multi-valued attributes, the values are denoted by a list of alphanumeric characters separated by semicolons. Effective To Date: The date until which a user is authorized to access the service.		
PatientContextSessionID	This attribute is a unique identifier assigned by the Federation ID Broker during the user login process. This attribute enables providers and delivery channels to set and retrieve patient context information on behalf of the provider.	No direct equivalent in Federation SSO Token (Token 2)	
UAO	The party that is legally responsible for this transaction. This organization MUST be a Health Information Custodian (HIC) as	[Attribute Statement]/uao	Obtained during the EMR onboarding and

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
	defined in PHIPA and defined in the Provider Registry. A default value of Not Authorized will be added to the message whenever the EMR user has not been approved for service access.The value "Not Authorized" will be specified in Federation SSO Token (Token 1).	This attribute specifies the responsible party for a given transaction. In most situations, the responsible party will be the Health Information Custodian (HIC) (i.e., the primary care practice or organization) to which the EMR user is accountable. The attribute value needs to represent a unique identifier which can be mapped to an entry in the Provider Registry. The unique identifiers need to conform to one of the acceptable formats. Specify the Universal Provider Identifier (UPI) corresponding to the Health Information Custodian that is the responsible party for this transaction in this format: urn:ehealth:rid:upi:<UPI number>	Configured during EMR install; may require the EMR user to select if EMR may submit requests for multiple HICs
uaoType - No equivalent in Federation SSO Token (Token 1) and is specified by the EMR/Delivery Channel		[Attribute Statement]/uaoType The content is the word "person" or "org". Mandatory (if UAO or GrantByDelegateMeritOnly are present). This attribute specifies the type of provider in the UAO attribute. The UAO can be a provider person or a provider organization.	Configured during EMR install; obtained during the EMR user onboarding
GrantByDelegate MeritOnly	States whether granting of permission is to be based only on the merits of the delegate.This value will always be specified as "false".	[Attribute tatement]/grantByDelegateMeritOnly Mandatory - The value effects how the UR PDP performs authorization for individuals marked as a delegate. This attribute (when true) means the following to the Delegator:	Defined as configured in the EMR, False by default; for future use

SAML Assertion Element/Attribute	Federation SSO Token (TOKEN 1)	UR Client Token (TOKEN 2)	Data Element Source in Token 2
		"Do not take my entitlements into account when granting access to my delegate. Should you grant access, I accept responsibility for the transaction." Specify "false" for the value of this attribute.	
Subject Locality - No equivalent in SAML token#1 and is specified by the EMR/Delivery Channel		[Assertion]/AuthnStatement/SubjectLocality This attribute specifies the technical location (IP address) of the user.	EMR workstation/device IP, inserted by the EMR
AuthenticationToken	Contains data about the EMR user's identity, the time that the EMR user created his/her SSO session with the Federation Broker and the Delivery Channel the user logged into. This attribute includes a digital signature issued by the Federation Broker.	[Attribute Statement]/AuthenticationToken Specify the value received in Federation SSO Token (Token 1).	Federation SSO Token (Token 1)
PrincipalFedKey	The unique, persistent identifier for the EMR user issued by the Federation Broker	[Attribute Statement]/PrincipalFedKey Specify the value received in Federation SSO Token (Token 1). A value that uniquely identifies a given user and is also used to bind a user's Federation SSO identity to their EMR user account.	Federation SSO Token (Token 1)

7. APPENDIX B: WORKFLOW FOR EMR USERS WITH MULTIPLE RIDS

The RID value specified in User Registry Client Token (Token 2) is determined from the RID value received in Federation SSO Token (Token 1). While extremely rare, it is possible for an EMR user to have more than one RID returned in the Federation SSO Token (Token 1). If multiple RIDs are provided the EMR Offering SHOULD use the logic described in **Error! Reference source not found.** to determine the RID to supply in the User Registry Client Token (Token 2).

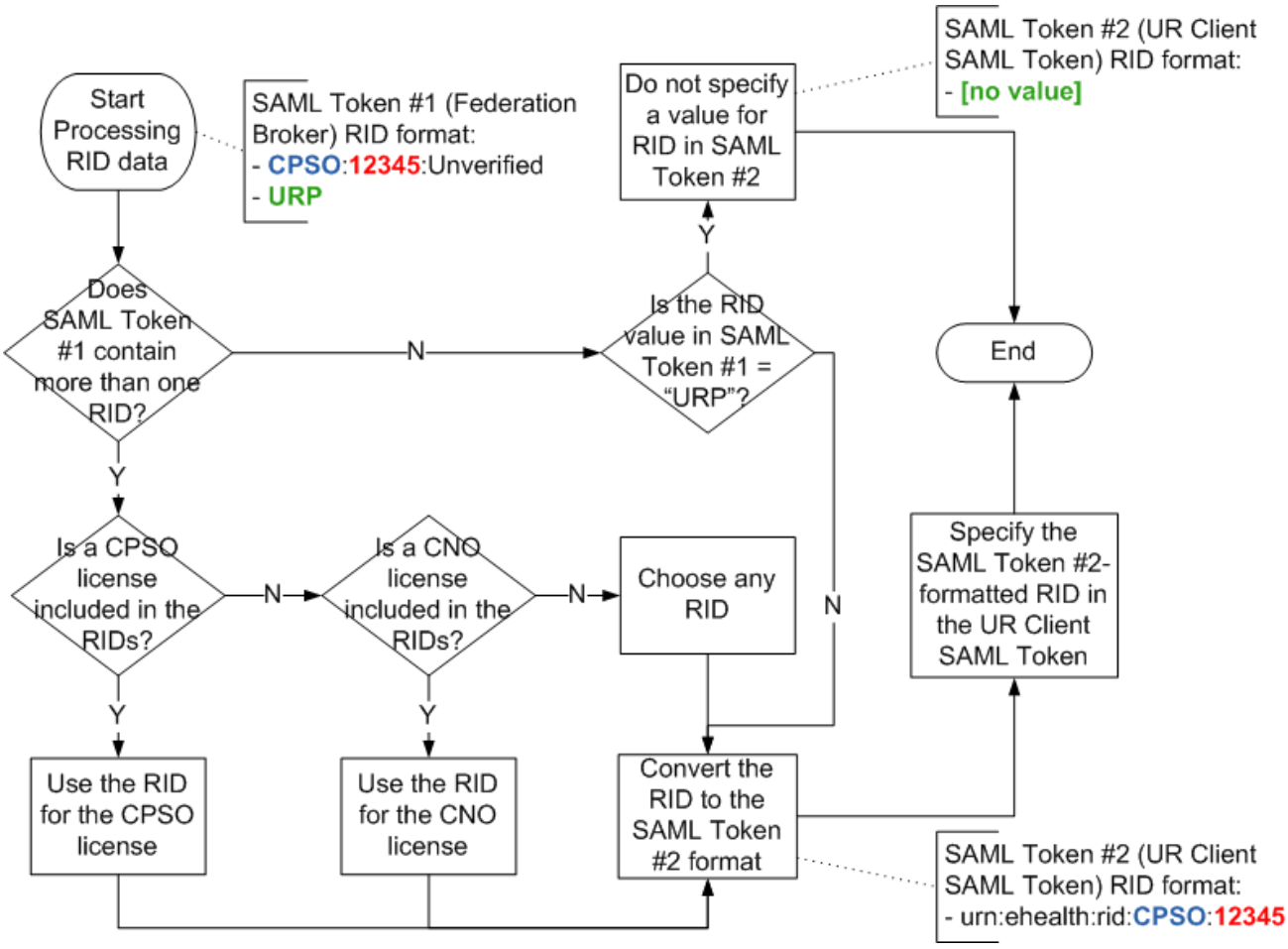

Figure 5 - RID Decision Tree