EMR EHR Connectivity 2.0

Federation Identity and Single Sign-On – Business View

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. BUSINESS VIEW 4

2.1 BUSINESS DRIVERS 4
2.2 FEDERATION IDENTITY 4
2.3 SINGLE SIGN-ON 5
2.4 BUSINESS CONTEXT 5
2.5 USER STORIES 6
2.5.1 Accessing EHR Services without SSO 6
2.5.2 SSO – Initial Credential Binding from the EMR Login Screen 6
2.5.3 SSO – Initial Credential Binding from an EHR Service Request 7
2.5.4 SSO to EMR Offering and EHR Services 7

3. SYSTEM VIEW 8

3.1 SYSTEM OVERVIEW 8
3.2 FEDERATION LOGIN 9
3.2.1 Federation Login Request 9
3.2.2 Federation Login Response - Federation SSO Token (Token 1) 10
3.3 USER REGISTRY CLIENT TOKEN IN EHR SERVICE REQUESTS 13

4. APPENDIX A: MAPPING OF SAML ASSERTION ELEMENTS FOR TOKEN 1 AND 2 20

5. APPENDIX B: WORKFLOW FOR EMR USERS WITH MULTIPLE RIDS 29

1. INTRODUCTION

Integrating EMR Offerings with support for identity federation and single sign-on (SSO) functionality allows for seamless access to EHR products and services by allowing the EMR user to have a single user account to access different systems. Simplifying access with a single user account reduces the need for clinicians to manage multiple user accounts to access different systems, promoting greater adoption and use of EHR products and services that provide clinicians with greater access to information and the ability to coordinate with other care providers.

1.1 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. BUSINESS VIEW

2.1 Business Drivers

Clinicians can provide enhanced patient care with improved access to information and the ability to coordinate patient care. Integrating EMR Offerings with provincial EHR products and services makes it easier for clinicians to access, helping clinicians achieve this goal.

The provincial ONE Access Provider Gateway (Provincial Gateway) is the primary means for a point-of-service system (such as an EMR) to access provincial EHR products and services, that comprise the provincial EHR.

EMR Offerings connect to the Provincial Gateway regardless of which EHR products or services they intend to consume. Implementers need requirements that describe how to authenticate EMR users and connect to the Provincial Gateway. Once authenticated, EMR users can access the EHR products and services that they are authorized to use. This document focuses on user authentication using a federated identity, such as Ontario Health's ONE ID, to access EHR products and services. Implementers may opt to integrate ONE ID for SSO functionality into their EMR Offering's authentication service to also integrate seamless access from logging into the EMR Offering to access EHR products and services.

2.2 Federation Identity

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 shown to be a barrier to the adoption of new technologies. A federation identity links the user's credentials to enable the user to authenticate to the multiple EHR products and services using a single assigned credential, such as an Ontario Health's ONE ID account. Without having to maintain a separate username and password for each EHR product or service. Integrating federation identity within an EMR Offering enables the EMR user to access different EHR products with the same federated credentials.

2.3 Single Sign-On

Ontario Health provides the ability for implementers, who opt to integrate SSO capabilities within their EMR Offerings using the ONE ID Federation service, to leverage a user's Ontario Health ONE ID account to be used to also log into the EMR Offering. This allows for an even more seamless interaction to log into their EMR Offering and access EHR products and services from within the EMR Offering without having to re-enter multiple credentials.

2.4 Business Context

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

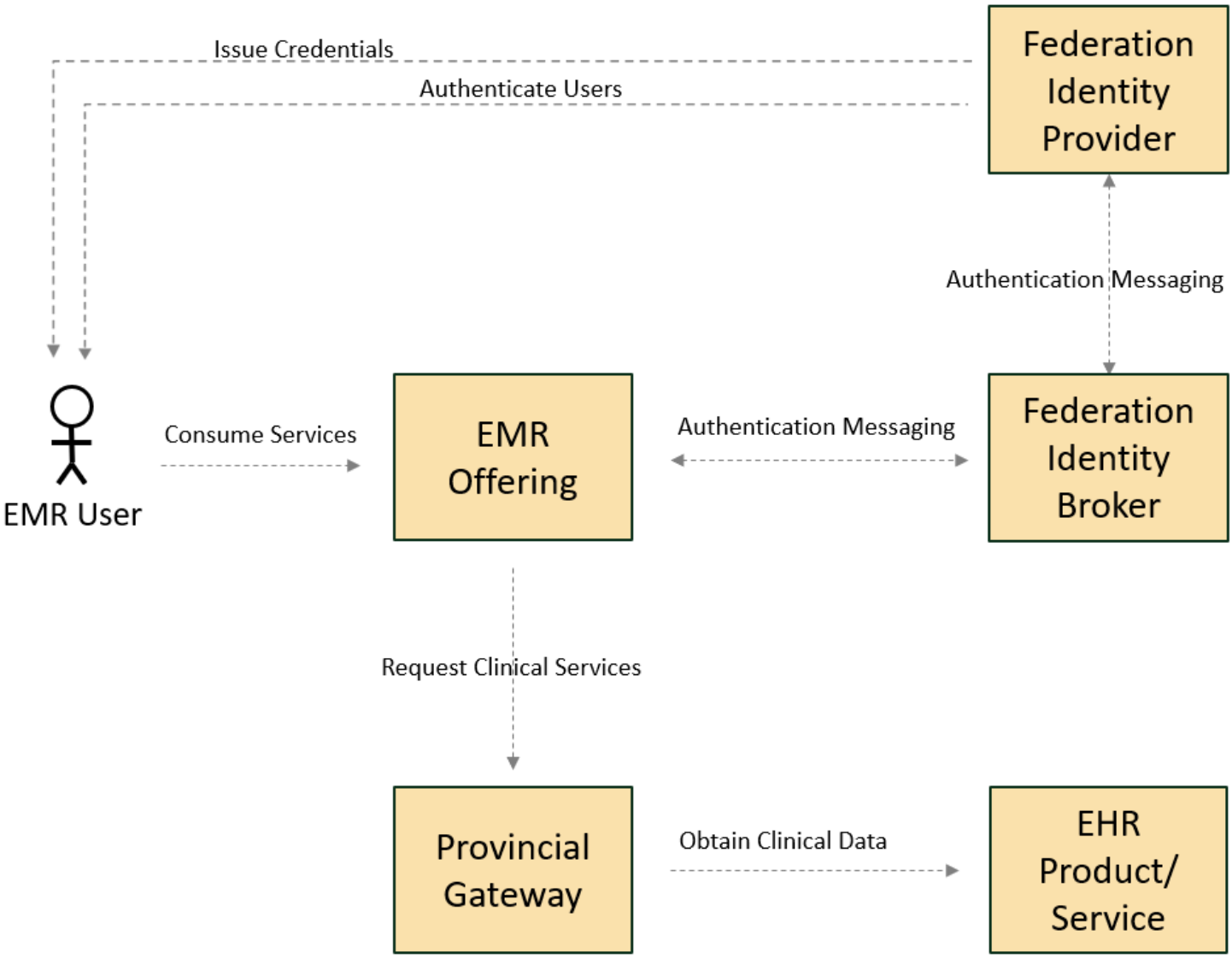

Figure 1 - Business Context Diagram

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

STAKEHOLDER ROLE	DESCRIPTION
EMR user	Sometimes called a "principal" in Ontario Health specifications, they use an EMR Offering to access EHR products and services. Examples include a clinician, physician, nurse, or delegate.
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 / Line of Business (LOB)	Manage the business service to grant and authorize EMR users' access to a given EHR product or service, and provide applications that provide EHR products or services.

2.5 User Stories

2.5.1 Accessing EHR Services without SSO

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

2.5.2 SSO – 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 federation IDP credentials.
- The physician selects the federation IDP and is redirected to the Federation Identity Broker where she is prompted to select her IDP from a list of approved federation IDPs. Upon selection, she is redirected to the selected federation 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 federation 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.

2.5.3 SSO – 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 federation IDP credentials.
- The physician enters her EMR credentials and is authenticated.
- The physician is using her EMR Offering to view a patient record and decides she would like to access an EHR service (e.g., Request a consult, access the ConnectingOntario Portal, etc.)
- When the physician attempts to access the EHR service, the EMR Offering informs her that she needs to be authenticated using credentials from a federation IDP.
- The EMR Offering redirects the physician to the Federation Identity Broker where she is prompted to select her federation IDP from a list of approved federation IDPs. Upon selection, she is redirected to the selected federation 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 federation 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.

2.5.4 SSO 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 federation IDP credentials.
- The physician selects the federation IDP and is redirected to the Federation Identity Broker where she is prompted to select her federation IDP from a list of approved federation IDPs. Upon selection, she is redirected to the selected federation IDP's login page.
- After the physician is successfully authenticated by the federation 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 federation IDP credentials, access the EMR application, and EHR products and services
2. **Federation ID Broker:** Orchestrates authentication of EMR users with federation IDPs
3. Federated Identity Provider: Authenticates EMR users
4. **Provincial Gateway:** 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.

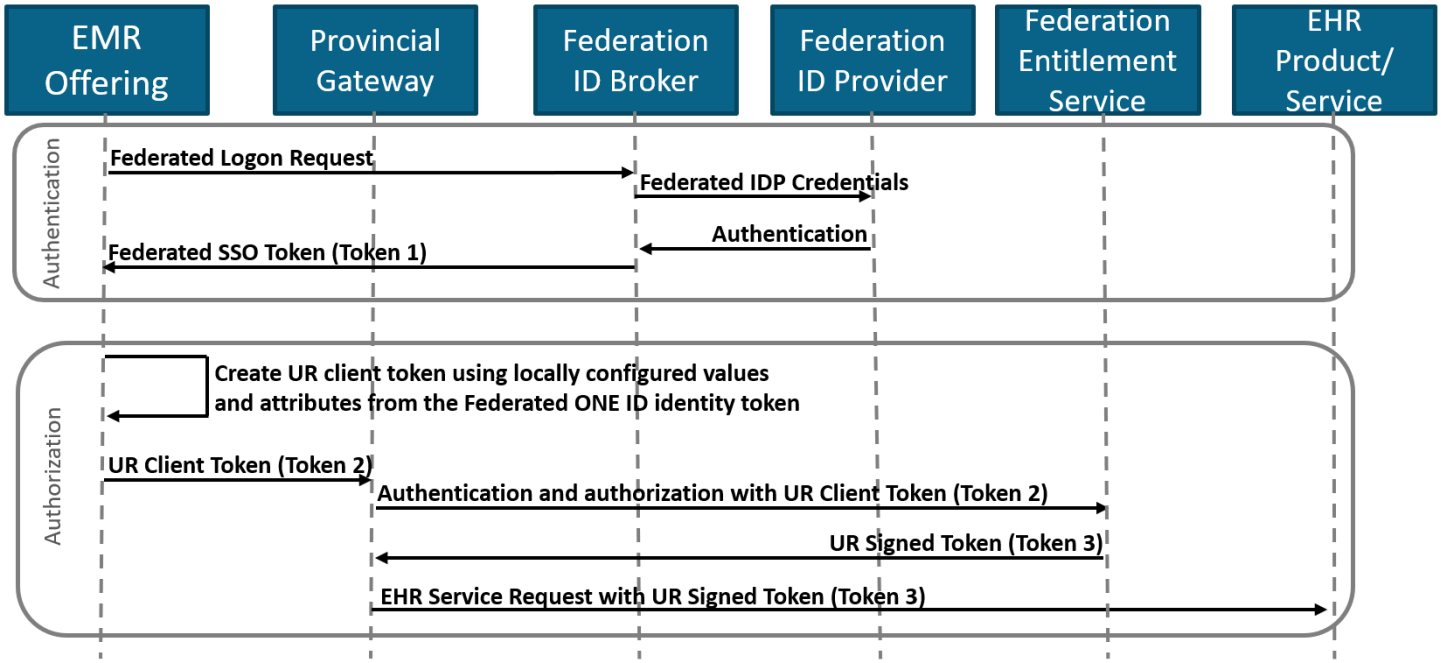

Figure 2 - Transaction Patterns

There are two potential triggers for a federation login request:

1. **EMR Offering Login** – The EMR user selects a federation IDP at the EMR Offering login screen and enters their credentials.
2. **EHR Service Login** – 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.

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 Gateway.

3.2 Federation Login

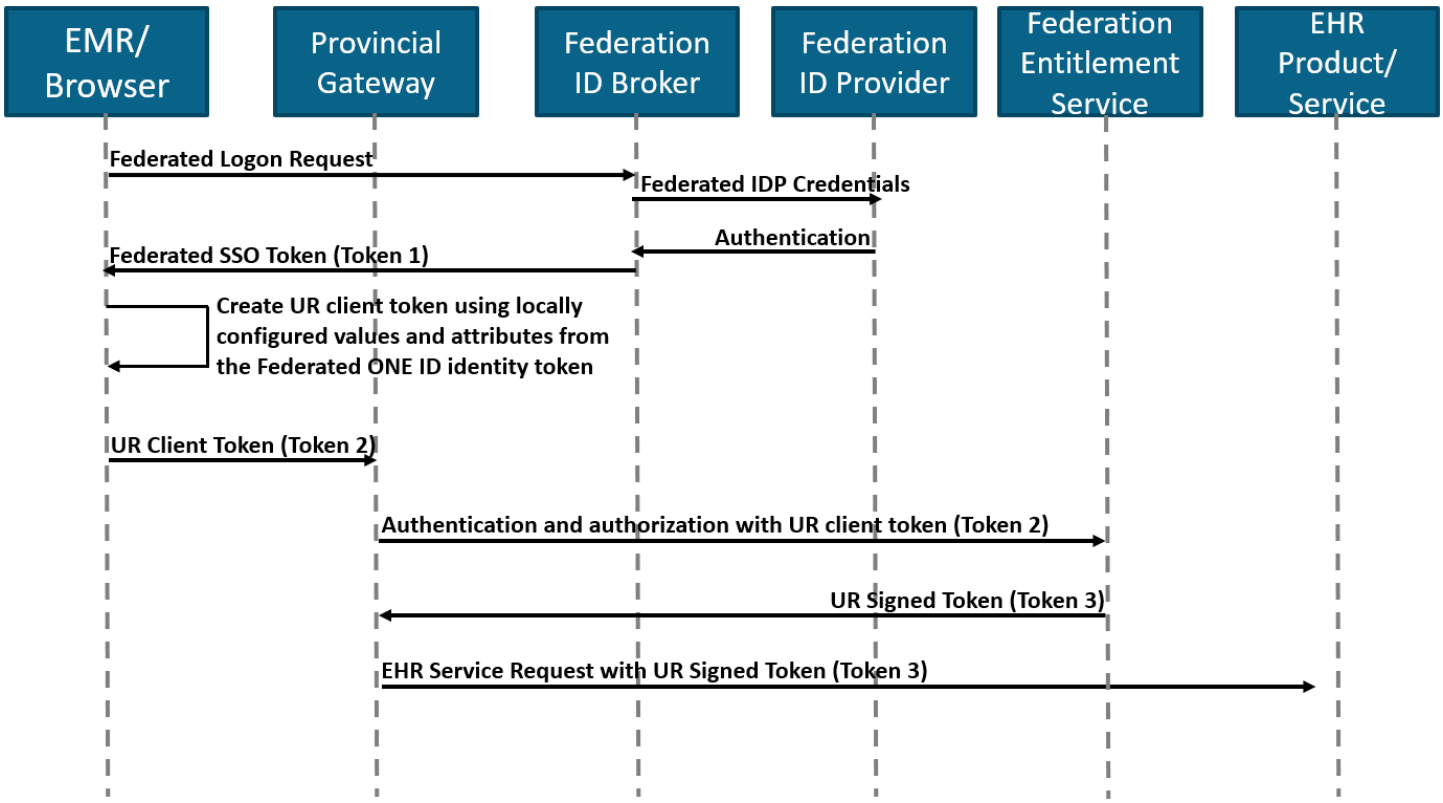

Figure 3 - Federation Login Request

3.2.1 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 a federation IDP (e.g., either at the EMR Offering's login screen or after selecting an EHR product or service from within the EMR Offering).

3.2.2 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.
/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 a federation IDP's verification processes.
CredentialManagementSchemeRef	The eHealth Federation evaluation criteria/level for a federation IDP's credential management processes.
IdentityProvider	The federation 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

SAML ASSERTION ELEMENT/ATTRIBUTE	FEDERATION SSO TOKEN (TOKEN 1) CONCEPTS
	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
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

SAML ASSERTION ELEMENT/ATTRIBUTE	FEDERATION SSO TOKEN (TOKEN 1) CONCEPTS
	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. 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.

3.3 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 Gateway in requests for EHR services. The data in Token 2 is used by the Provincial Gateway 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.

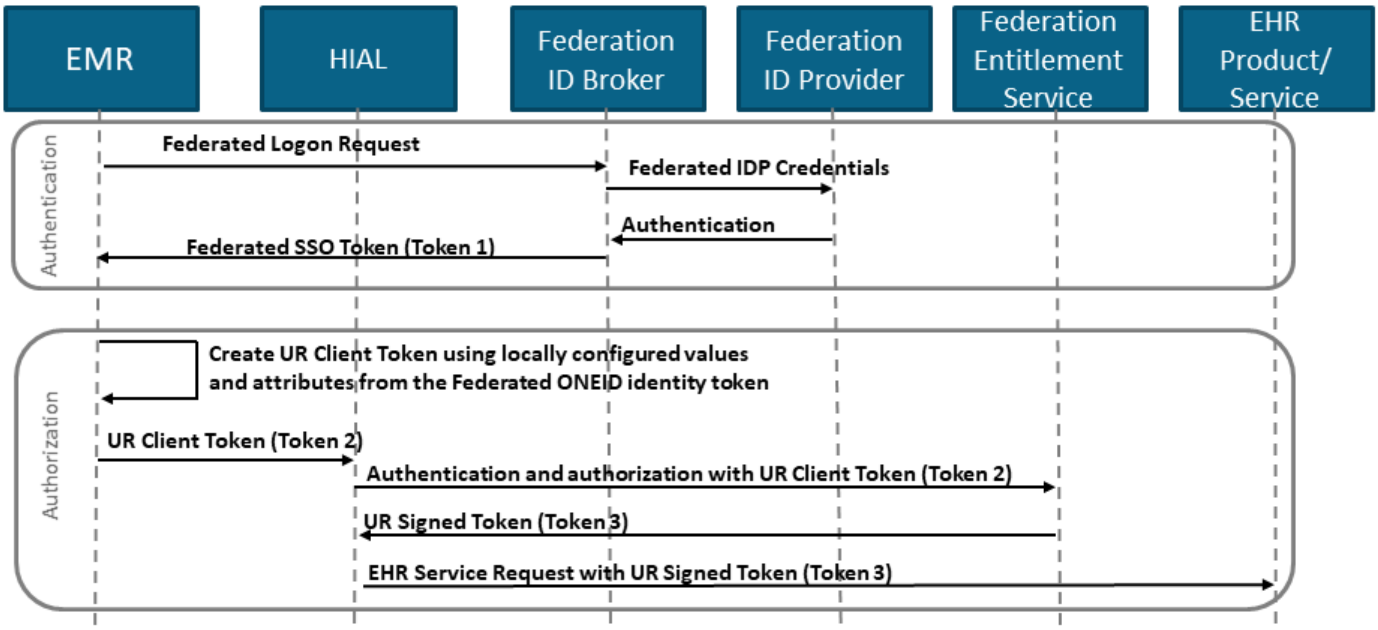

Figure 4 - Transaction Patterns

The information in the Federation SSO Token (Token 1) is subsequently used by the EMR Offering to 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	EMR Offering

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
	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. 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 federation 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 a federation IDP, its identity verification processes, and it's 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 the 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)
UAOIdentityVerificationSchemeRef	[Authn Statement]/Identification/Extension/UAOIdentityVerificationSchemeRef	Federation SSO Token (Token 1)

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
	Specify the value received for the Authentication Level attribute in Federation SSO Token (Token 1).	
IdentityProvider	[Authn Statement]/AuthnMethod/Extension/IdentityProvider/AuthenticatingAuthority The federation IDP that authenticated the user. Federation IDP Identifiers are part of the 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/Authenticating Authority The federation IDP that is connected to Ontario Health 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 Ontario Health 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 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 a federation 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

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
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. 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)
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	Obtained during the EMR onboarding and configured during an EMR install; may require the EMR user

SAML ASSERTION ELEMENT OR ATTRIBUTE	USER REGISTRY CLIENT TOKEN (TOKEN 2) CONCEPTS	DATA ELEMENT SOURCE IN TOKEN 2
	(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 that 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>	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 affects 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
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.

4. APPENDIX A: MAPPING OF SAML ASSERTION ELEMENTS FOR TOKEN 1 AND 2

SAML Assertion Element	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
/Issuer	Entity ID of the Federation Broker	PKI certificate Distinguished Name (DN) used by the partner for signing SAML Token	EMR Offering

		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"	
/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 use a validity period of 30 seconds for SAML Token 2.	EMR Offering
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 a federation IDP's verification processes.	[Authn Statement]/Identification/Extension /IdentityManagementSchemeRef Optional - The eHealth Federation Evaluation Criteria defines how Ontario Health establishes measures of the identity assurance related aspects of a federation 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 a federation IDP's credential management process.	[Authn Statement]/Identification/Extension /CredentialManagementSchemeRef Optional - Derived using the eHealth Federation Evaluation Criteria. Indicates the strength of the 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 Specify the value received for the Authentication Level attribute in Federation SSO Token (Token 1)	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 federation IDP that authenticated the EMR user.	[Authn Statement]/AuthnMethod/Extension/ IdentityProvider/AuthenticatingAuthority The federation IDP that authenticated the user. Federation IDP identifiers are part of the 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 federation IDP that is connected to Ontario Health 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 Ontario Health configured in the EMR
/AuthnStatement/AuthnContext/ AuthnContextClassRef	Authentication context of EMR user Value= urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport	[Authn Statement]/AuthnMethod/Principal AuthenticationMechanism/Extension/PrimaryFactor Specify "password"	EMR/ Delivery Channel
ProtectedNetwork	Indication if the user has been authenticated from a trusted network location	[Authn Statement]/AuthnMethod/Principal AuthenticationMechanism/Extension/ProtectedNetwork	EMR/ Delivery Channel

		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 a federation 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 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)
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. 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	No direct equivalent in Federation SSO Token (Token 2)	

	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: • 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	No direct equivalent in Federation SSO Token (Token 2)	

	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.		
UAO	The party that is legally responsible for this transaction. This organization MUST be a Health Information Custodian (HIC) as 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).	[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 that 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 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	[Attribute tatement]/grantByDelegateMeritOnly	Defined as configured in the EMR, False by

	delegate.This value will always be specified as "false".	Mandatory - The value affects how the 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.	default; for future use
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	It 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)

5. 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 as follows to determine the RID to supply in the User Registry Client Token (Token 2).

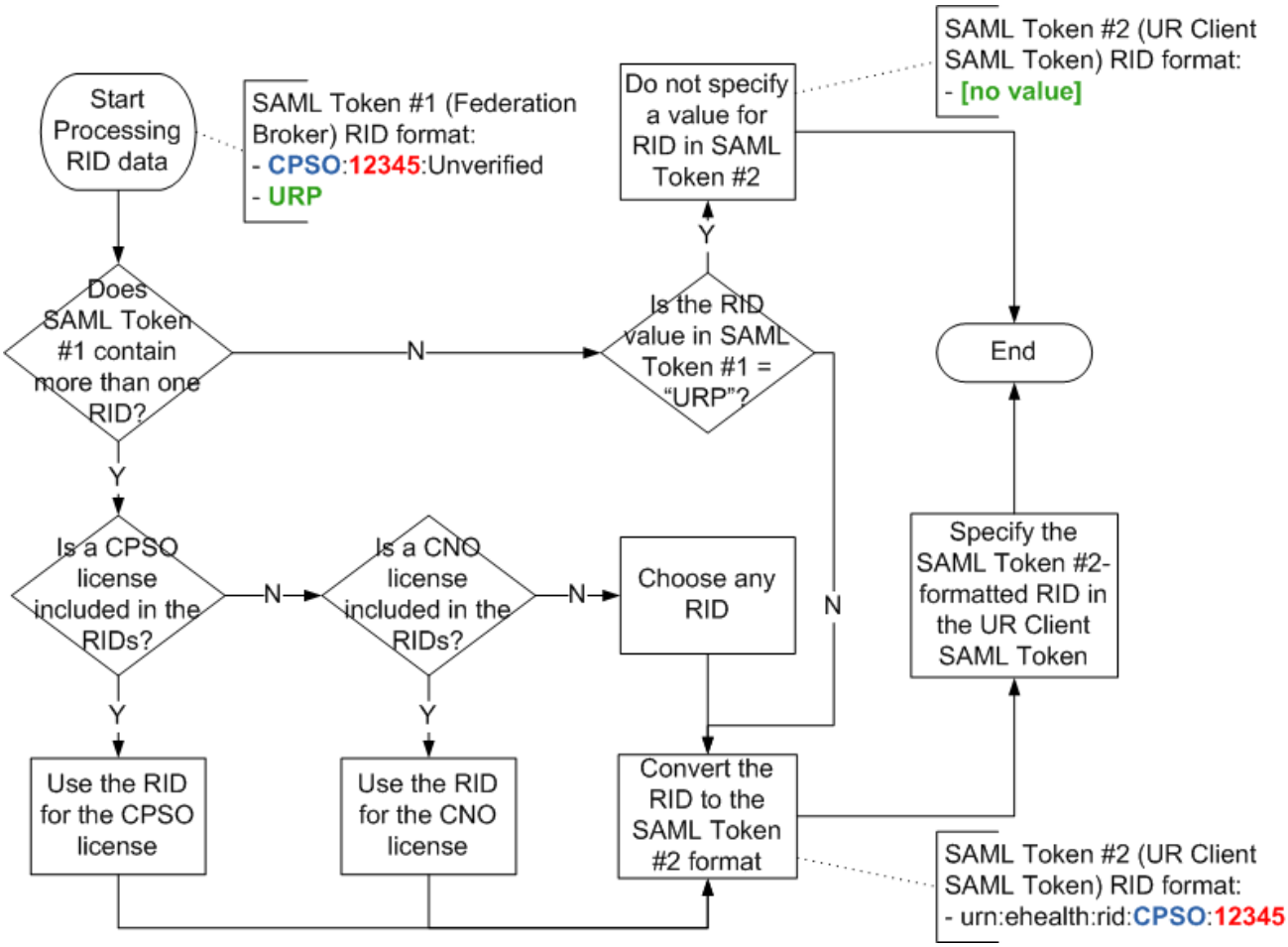

Figure 5 - RID Decision Tree