

eHealth Ontario

ONE®ID Provincial Identity Federation

Overview of SAML Configuration

Version: 1.49

Table of Contents

1.0	About This Document	5
1.1	Audience	5
1.2	Reference material.....	5
2.0	Introduction – Identity Federation and SAML	6
2.1	A federated environment.....	6
2.1.1	Federation Role Scenarios.....	7
2.1.2	Identity Federation Solution Component View.....	9
2.2	SAML within a federated environment	10
2.2.1	What is SAML?.....	10
2.2.2	Types of messages.....	10
2.2.3	Assertions	10
3.0	ONE ID Federation Broker	11
3.1	Business Process	11
3.2	ONE ID Federation Broker Functionality	12
3.3	ONE ID Federation Authorization Service.....	13
3.3.1	Roles & Responsibilities	14
3.3.2	Entitlements defined in ONE ID Federation Authorization Service	14
4.0	ONE ID Federated Login Sequences	16
4.1	SP Initiated Login Sequence Diagram	16
4.1.1	SP Initiated Login Steps	17
4.2	Identity Provider Initiated Login Sequence Diagram	18
4.2.1	Identity Provider Initiated Login Steps	19
5.0	SAML Configuration	22
6.0	SAML Authentication Requests	23
6.1	SAML Authentication Request from Delivery Channel	23
6.1.1	SAML Authentication Request Elements.....	23
7.0	SAML Response Assertions	25
7.1	SAML Response from IDP to Federation Broker.....	25
7.1.1	SP Initiated Login.....	25
7.1.2	IDP Initiated Login.....	25
7.1.3	Federation Broker Validation of SAML Response	25

7.2	SAML Response from Federation Broker to Delivery Channel	26
7.2.1	Federation Broker Generation of SAML Response to Delivery Channel.....	26
7.3	Main Elements of SAML Response Assertion	26
8.0	SAML Response Assertion Attribute Statements	34
8.1	Background.....	34
8.2	Identity Attributes	35
8.2.1	DisplayName	35
8.2.2	Email	35
8.2.3	FirstName	36
8.2.4	LastName.....	37
8.2.5	RID	38
8.2.6	UserLoginName.....	40
8.2.7	TelephoneNumber.....	41
8.2.8	StrongAuthenticationRequest	42
8.2.9	PrincipalFedKey.....	43
8.3	Authentication Attributes.....	44
8.3.1	AssertingParty.....	44
8.3.2	AuthenticationLevel.....	45
8.3.3	CredentialManagementSchemeRef	46
8.3.4	IdentityProvider.....	46
8.3.5	IdentityVerificationSchemeRef	47
8.3.6	ProtectedNetwork.....	48
8.4	Delegation Attributes	49
8.4.1	GrantByDelegateMeritOnly	49
8.4.2	OBO	50
8.5	Entitlement Attributes	51
8.5.1	Roles	51
8.5.2	ServiceEntitlements	52
8.5.3	UAO	56
8.6	Patient Context Attributes.....	58
8.6.1	PatientContextID	58
8.6.2	PatientContextIDType	59
8.6.3	PatientContextIDAuthority	60
8.6.4	PatientContextDOB	62
8.6.5	PatientContextGender	62
8.6.6	PatientContextLastName	64
8.6.7	PatientContextFirstName.....	65
8.6.8	ContextSessionID	65

8.7	Clinical Context Attributes	66
8.7.1	ClinicalContextApplicationID	66
8.7.2	ClinicalContextApplication	67
8.7.3	ClinicalContextLocalization	68
8.7.4	ClinicalContextService	69
9.0	Sample Messages	70
9.1	SAML Request Message.....	70
9.2	SAML Response Message	72
10.0	Glossary	77
10.1	General Concepts	77
11.0	Appendix	80
11.1	List of Valid Licensing Authorities	80
11.2	SAML Validation Error Messages	81
11.3	Delivery Channels in the ONE ID Federation	82
11.3.1	Responsibilities	82
11.3.2	Test Areas for Delivery Channels	89
11.4	Point of Service Applications (POSAs) and the ONE ID Federation	98
11.4.1	Responsibilities	98
11.4.2	Test Areas - POSAs	99
11.5	Identity Provider (IDPs) in the ONE ID Federation.....	101
11.5.1	IDP Responsibilities.....	101
11.5.2	Test scenarios for Identity Providers	103

1.0 About This Document

This document contains a general overview of the SAML protocol as set up and used with ONE ID provincial Federation. The documents build upon the generally available SAML specification by detailing the attribute and values necessary for participation in the Federation.

1.1 Audience

The primary audience for this document includes clients of eHealth Ontario with an interest in participating in the ONE ID provincial Federation implementation. The document assumes the reader has a basic working understanding of federated environments and the OASIS SAMLv2 specification in particular. Although not a pre-requisite, a technical background in implementing SAMLv2 for cross-domain single sign-on is recommended.

1.2 Reference material

Assertions and Protocols for the OASIS Security Assertion Markup Language (SAML) 2.0

<http://docs.oasis-open.org/security/saml/v2.0/saml-core-2.0-os.pdf>

Bindings for SAML v2

<http://docs.oasis-open.org/security/saml/v2.0/saml-bindings-2.0-os.pdf>

Profiles for SAML v2

<http://docs.oasis-open.org/security/saml/v2.0/saml-profiles-2.0-os.pdf>

eHealth Ontario Identity Federation – Identity Provider Standard

https://www.ehealthontario.on.ca/images/uploads/support/eHealth_Ontario_Federation_Identity_Provider_Standard_EN.pdf

2.0 Introduction – Identity Federation and SAML

2.1 A federated environment

A ‘federated’ environment allows distinct systems (from different organizations, lines of business, companies) to achieve cross domain (organization) single sign-on (SSO) which allows a user to experience a seamless method for accessing multiple Delivery Channels.

Advantages of using a federated environment:

- The user can use ‘single sign-on’ when accessing a number of Delivery Channels. The user is not required to re-enter credentials when navigating to a Delivery Channel which resides within another organization or security domain.
- Provides a framework for organizations or business partners to share identity information across their respective security domains.
- This enables users from trusted organizations to access provincial and regional Delivery Channels by leveraging their primary login credentials; another set of credentials does not have to be issued.
- Delivery Channels do not need to store organization data and integrate with the Provider Registry (PR) or Provincial Client Registry (PCR) in order to be a member of the Federation.
- Organization mergers will be handled seamlessly.
- The ONE ID Federation Broker provides a centralized process for disabling IDPs and Delivery Channels.
- The ONE ID Federation Broker provides a centralized process for blocking access to users.
- If the ONE ID Federation Authorization Service is used, the authorization details will be populated in the SAML attribute statement. Details include both the Delivery Channel and the organization/person (UAO) that has authorized the user for the Delivery Channel. This allows for ‘just in time’ access to Delivery Channels.
- Patient context details are available in the SAML attribute statement when a user views a patient in a POSA and then, from that POSA, accesses a Delivery Channel. In the future, these attributes will not be included in the SAML attribute statement, but will be managed by a patient context service operated as part of the Federation Broker processing.

Roles within the eHealth Provincial Identity Federation:

- **Principal:** a Principal is a person (a "user"), a corporation, or a system whose identity can be authenticated. For the purpose of this specification a Principal will be used to describe or identify a Health Care Provider Person (also referred to as Clinician or Provider). Principals interact with Identity Providers for user identification purposes.
- **Identity Provider (IDP):** provides credentials to users based on real world identities. They capture and pass verified data required for Federation (e.g., professional designations) and authenticate users when requested by the Federation Broker (operator) at login time. Data is

passed to the Federation Broker via a SAML authentication message (response) generated by the IDP.

- **Federation Broker (Operator):** sets policies, standards and agreements. Provides business processes and technical infrastructure to facilitate Federation operations, e.g., defining standards for each of the federated roles. Processes SAML authentication messages from IDPs, validates applicable data contained within the SAML message, and issues provincially trusted SAML tokens, including authorization information where the Delivery Channel has opted to use the Federation Authorization Service, for itself and, optionally, its Applications.
- **Point Of Service Application (POSA):** A POSA is a launch point to a federated Delivery Channel and so the flow is unidirectional. A HIS is an example of a POSA. A user must use an account from a federated IDP to access the POSA but that access does not go through the Federation Broker. The POSA must contain access point(s) to federated Delivery Channels. A POSA will only send SAML Responses to the Federation Broker in an IDP-initiated flow. These SAML Responses may contain patient context information. It is the responsibility of the POSA to generate valid SAML Responses and some use the Secure Token Service (STS) to do so.
- **Delivery Channel (DC):** A federated DC is a service that provides an entry point to one or more health care Applications/Services, either from a POSA in an IDP-initiated flow or from a login through the DC in an SP-initiated flow. Good examples of Delivery Channels are the regional and provincial portals, i.e. www.eHealthontario.ca, ConnectingOntario and ClinicalConnect. Other examples are Application Providers that support direct access to their services, e.g. CCO and OTN. Delivery Channels don't necessarily store the clinical information or provide the clinical service; they simply provide the interface for the clinical Applications to render their data. A DC sends SAML requests to and processes SAML responses from the Federation Broker and determines access to the DC. Each DC defines the rules by which users are entitled to access it. Some systems are both DCs and POSAs.
- **Application Provider (AP):** provides one or more Applications/Service(s) for consumption by Federation members. Users with credentials from recognized IDPs can access the AP(s) through federated Delivery Channels. It is the Delivery Channel that determines access to the AP. An AP does not have any interaction with the Federation Broker in terms of access as the DC handles that access. An AP may be captured in the Federation Authorization Service, however, if the DC has opted to use that Service. Examples of Applications include OLIS, DI Viewer and SWODIN.

2.1.1 Federation Role Scenarios

Scenario One - Hospital Setting

Overview

Dr. John Doe is a practicing physician for the ACME hospital network. The ACME hospital network meets the provincial standards to become a trusted Identity Provider for the province. ACME Hospital network signs the appropriate agreements with eHealth Ontario and is added to the list of IDPs trusted by the Federation Broker.

Approach

Using his ACME hospital account, Dr John Doe would like to access a regional eHR viewer and the lab service (OLIS portlet) exposed through that viewer.

In the context of Federation roles, each party is defined as follows:

Principal	Identity Provider	Federation Broker	Delivery Channel	Application
Dr John Doe	ACME Health	eHealth Ontario	Regional eHR Viewer	OLIS

Scenario Two – Private Practice

Overview

Dr. Jane Smith is a licensed family practitioner with a small private practice which has opted to deploy a locally managed EMR application. Dr. Jane Smith would like to access the regional eHR viewer for the purpose of obtaining lab results for her patients via the OLIS portlet. Although Dr. Smith is very computer savvy, her local office and EMR implementation do not meet the provincial standards for becoming a trusted Identity Provider. Additionally, Dr. Smith is considering expanding her practice to include additional physicians to satisfy increase patient demand.

Approach

Dr. Jane Smith approaches eHealth Ontario and requests a ONE ID account. After completing the ONE ID registration process Dr. Smith is issued a ONE ID Account. Her new ONE ID account is trusted for accessing all provincially federated Delivery Channels. Also, her new ONE ID account will enable her to create new ONE ID accounts for physicians that join her local practice.

In the context of Federation roles, each party is defined as follows:

Principal	Identity Provider	Federation Broker	Delivery Channel	Application
Dr. Jane Smith	ONE ID	eHealth Ontario	Regional eHR viewer	OLIS

2.1.2 Identity Federation Solution Component View

The purpose of this view is to indicate what are the major components involved in provincial identity Federation solution.

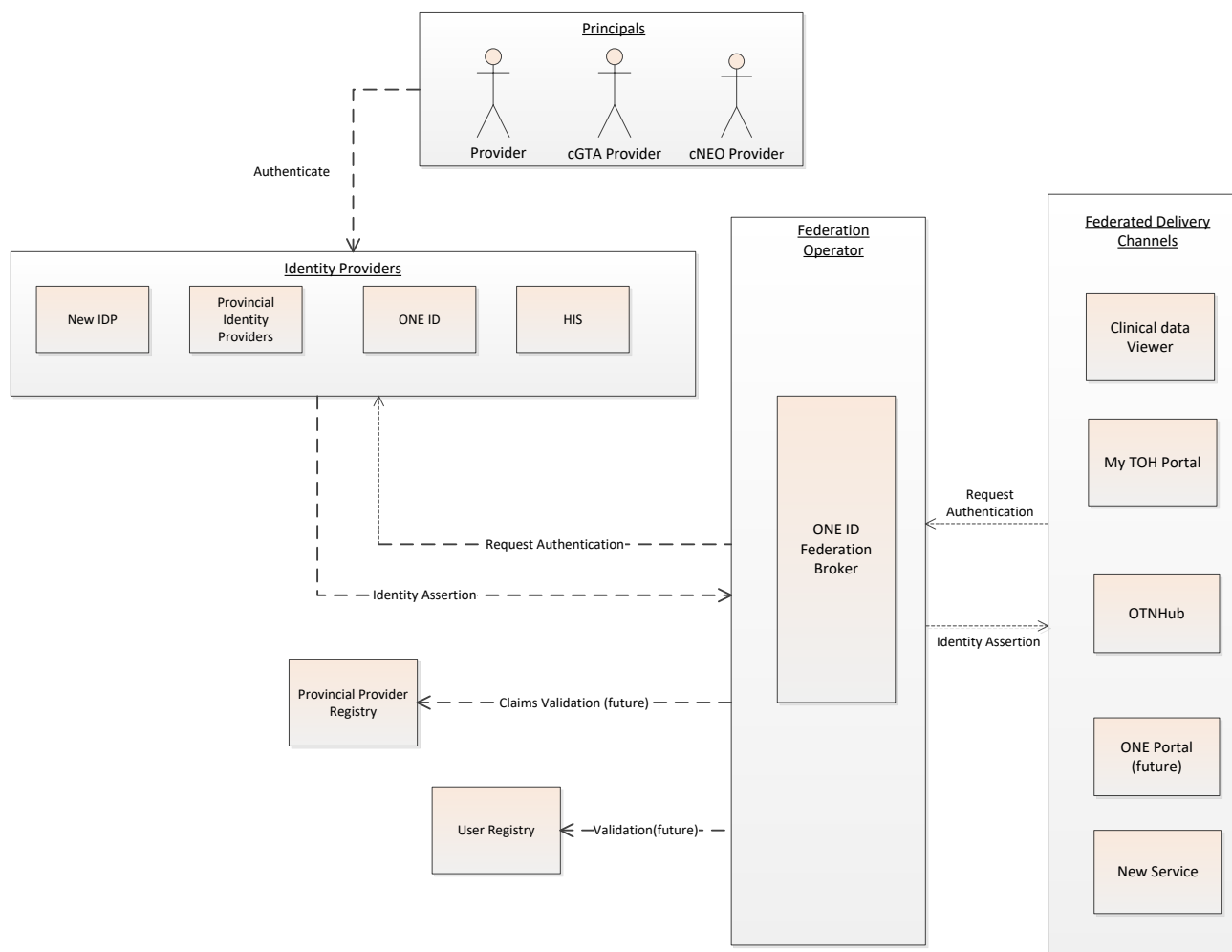


Figure 1: Federation - component view

See 'Roles within the eHealth Provincial Identity Federation' for a definition of roles (Principals, Identity Providers, Federation Broker, Points Of Service, Delivery Channels and Application Providers)

2.2 SAML within a federated environment

2.2.1 What is SAML?

SAML (Security Assertion Markup Language) is a standard format that is used in federated systems for the purpose of exchanging authentication and authorization data. SAML was developed to address the issue of how to achieve cross-domain 'single sign-on'. It is an XML-based open standard that is a product of the OASIS Security Technical Committee.

SAML defines a 'protocol' or framework for requesting and obtaining identity assertions¹. Part of the framework includes 'bindings' which define the standard way that SAML request and response messages are transported across the issuing authorities (i.e. IDP) and relying parties (DC) by providing mappings between SAML messages and standard communication protocols. This enables the exchange of SAML information across different parties in a standard manner.

2.2.2 Types of messages

SAML messages typically exchanged between two parties:

1. **Request:** The requesting party (Delivery Channel) sends a SAML 'request' to the Identity Provider.
2. **Response:** The Identity Provider responds with a SAML 'assertion' contained within a SAML response. The SAML assertion contains information such as whether a subject has been authenticated or not and additional specific information in the form of attributes (the 'attribute statement'). The requesting party uses the information in the assertion to make decisions regarding the subject's access to a resource.

2.2.3 Assertions

There are three basic statements in SAML assertions:

1. **Authentication:** Asserts that the user has proven his/her identity by a particular method at a specific time
2. **Authorization:** States the resources a user can access and under what conditions they can be accessed
3. **Attribute:** Provides details about the user (subject) of the message.

The primary elements that are used within the context of the eHealth Federation are the Authentication and Attribute statements.

¹ A statement of claims made by the trusted Identity Provider regarding the user currently being authentication and about the transaction in general; for example, First Name, Last Name, Login ID, License #)

3.0 ONE ID Federation Broker

The eHealth Ontario ONE ID Federation Broker (FB) functions as a SAML proxy to the Federation. Through the implementation of this provincial proxy, a single Hub/Spoke Federation ecosystem is created. Trust flows between the Federation Broker (Hub) and each of the partner organizations (spokes).

Each partner (spoke) can assume the role of Identity Provider, Delivery Channel, or both. By establishing this single trust relationship with the Federation Broker, participant members can experience all the benefits of the provincial eHealth Federation.

The Federation Broker is capable of interoperating with any IDP or DC that is compliant with the SAMLv2 specification and that also adheres to the specification defined within this document. Although based on the OASIS SAMLv2 specification, additional mandatory attributes are defined in the eHealth specification that the Federation Broker requires in the SAML messages. See section 5.0 'SAML Configuration'.

3.1 Business Process

This diagram illustrates the major steps performed during the establishment of a federated session.

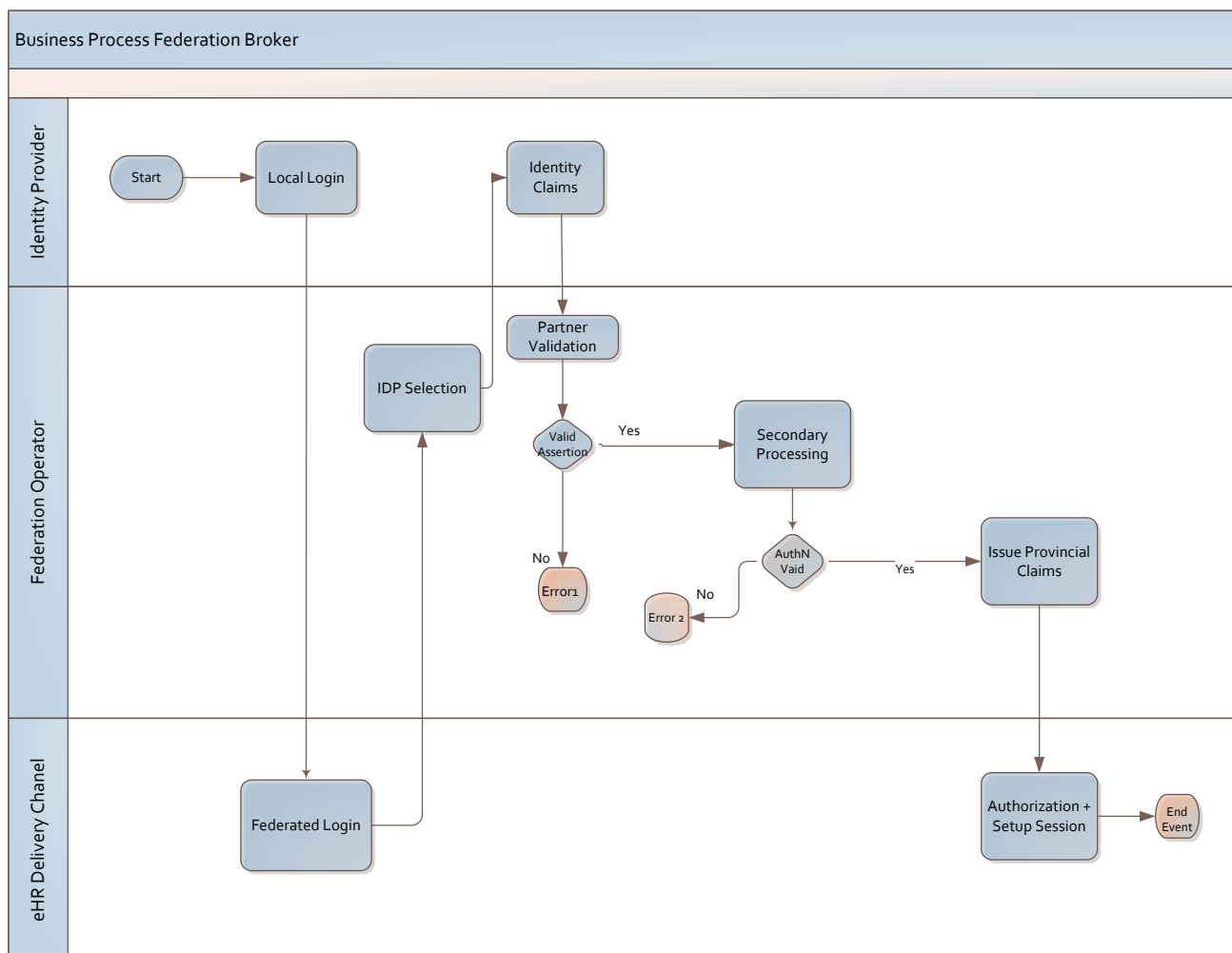


Figure 2: establishment of a federated session through an SP-Initiated flow.

3.2 ONE ID Federation Broker Functionality

Federation Broker Functionality in an SP Initiated Login Sequence

Item	Federation Broker Responsibilities	Reference
FB_SP_1	Onboarding Identity Providers	
FB_SP_2	Accepting SAML Requests and redirected users from the Delivery Channels that are members of the Federation	Section 4.1 ' <i>SP Initiated Login Sequence</i> ', Step 3.
FB_SP_3	Enabling users to select their Identity Provider	Section 4.1 ' <i>SP Initiated Login Sequence</i> ', Step 3.
FB_SP_4	Sending a SAML Request to the selected Identity Provider and redirecting the user to the Identity Provider's login page	Section 4.1 ' <i>SP Initiated Login Sequence</i> ', Step 3. Section 6.1 ' <i>SAML Authentication Request from Delivery Channel</i> '
FB_SP_5	Accepting a SAML Response from the Identity Provider	Section 4.1 ' <i>SP Initiated Login Sequence</i> ', Step 5.
FB_SP_6	Verifying and validating the SAML Response from the IDP. The Federation Broker will fail the login if the SAML Response is invalid	Section 4.1 ' <i>SP Initiated Login Sequence</i> ', Step 5 Section 7.1.3 ' <i>Federation Broker Validation of SAML Response</i> '
FB_SP_7	Adding authorization information to the SAML Response where the Delivery Channel uses the Federation Authorization Service	See section 3.4 ' <i>ONE ID Federated Service Authorization</i> ' Section 7.2.1 ' <i>Federation Broker Generation of SAML Response to Delivery Channels</i> '
FB_SP_8	Sending the SAML Response to the Delivery Channel the user is accessing	Section 4.1 ' <i>SP Login Sequence</i> ', Step 5 Section 7.2.1as above
FB_SP_9	Redirecting the user to the Delivery Channel	Section 4.1 ' <i>SP Initiated Login Sequence</i> ', Step 5 Section 7.2.1as above

Federation Broker Functionality in an IDP Initiated Login Sequence

Item	Federation Broker Responsibilities	Reference
FB_IDP_1	Accepting a SAML Response from the Secure Token Service (STS) of a POSA, for example, an HIS	Section 4.2 ' <i>Identity Provider Initiated Login Sequence</i> ', Step 11
FB_IDP_2	Verifying and validating the SAML Response. The Federation Broker will fail	Section 4.2 ' <i>Identity Provider Initiated Login Sequence</i> ', Step 11

Item	Federation Broker Responsibilities	Reference
	the login if the SAML Response is invalid	Section 7.1.3 ' <i>Federation Broker Validation of SAML Response</i> '
FB_IDP_3	Adding authorization information to the SAML Response where the Delivery Channel uses the Federation Authorization Service	See section 3.4 ' <i>ONE ID Federated Service Authorization</i> ' Section 7.2.1 ' <i>Federation Broker Generation of SAML Response to Delivery Channels</i> '
FB_IDP_4	Sending the SAML Response to the Delivery Channel the user is accessing from the POS	Section 4.2 ' <i>Identity Provider Login Sequence</i> ', Steps 12 and 13 Section 7.2.1as above
FB_IDP_5	Redirecting the user to the Delivery Channel	Section 4.2 ' <i>Identity Provider Initiated Login Sequence</i> ', Step 13 Section 7.2.1as above

3.3 ONE ID Federation Authorization Service

Service authorization is one of the primary responsibilities of the Delivery Channels. Delivery Channels are ultimately accountable for making the final decision regarding the principal's access (or not) to the service requested and may opt to use the Federation Authorization Service for that purpose.

When a principal accesses a Delivery Channel via a federated login, a SAML Response will be posted to the Delivery Channel. The Delivery Channel may use the information in the SAML Response Assertion and attribute statement to determine whether the user gains access to it and, if so, the level of access.

Authorization may be based on identity data, entitlement data (from the Federation Authorization Service repository where the Delivery Channel has opted to use the Federation Authorization Service) or authorization may be role based. The SAML Response will contain both the identity and professional designation data as provided by the IDP and, where applicable, service entitlement data.

3.3.1 Roles & Responsibilities

The figure below illustrates the relationship and responsibilities of each participant.

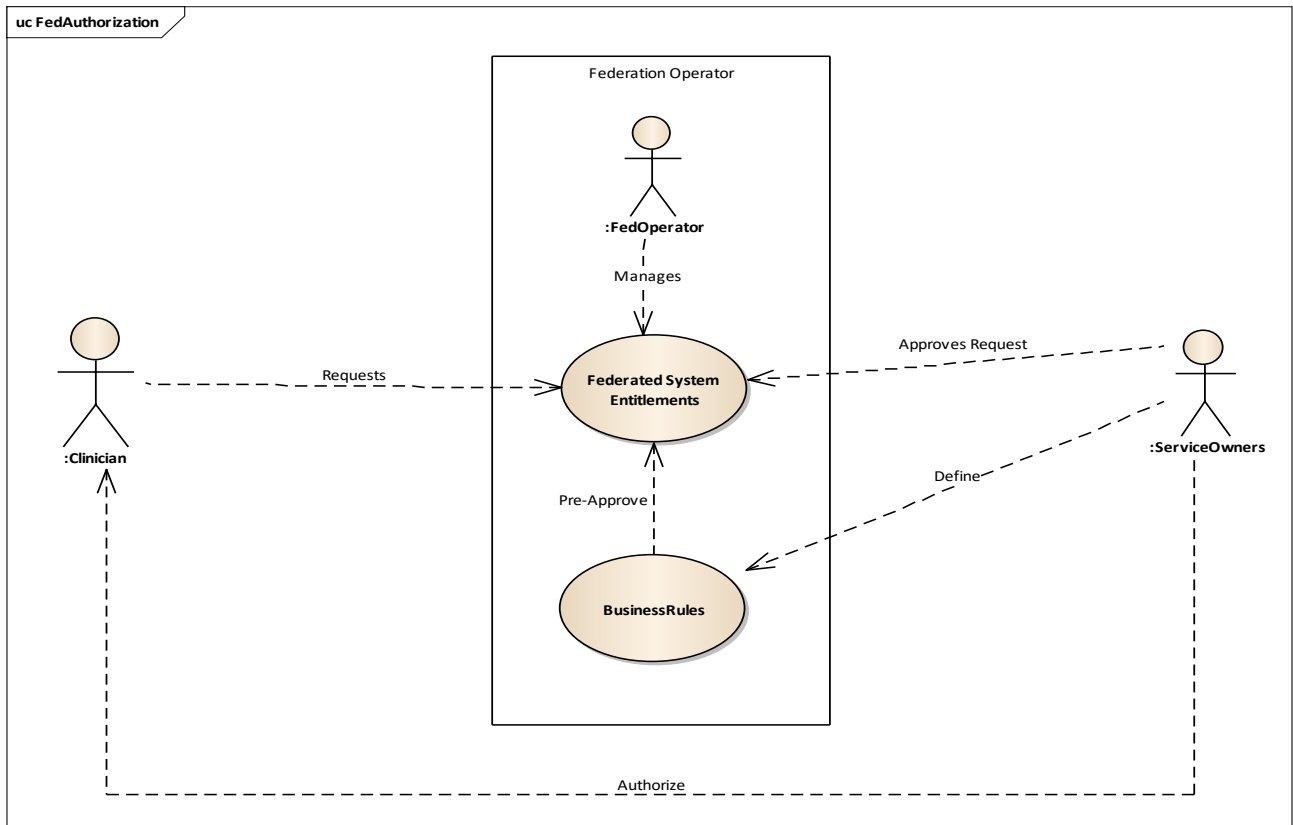


Figure 3 - Authorization Management

Principal (Clinician) – The principal may request access to a particular Delivery Channel.

Federation Broker – The Federation Broker will post a SAML Response to the Delivery Channel. The SAML Response will contain identity and role data as provided by the IDP and service entitlement data from the Federation Authorization Service repository.

Service Owners – The service owner has three key responsibilities:

- Service owners are responsible for defining the specific entitlements related to their Application/Delivery Channel.
- The service owners are responsible for approving (or rejecting) individual Application/Delivery Channel access requests made by clinicians as well as defining the business driven rules (if applicable).
- They are also ultimately responsible for making the final authorization decision when the user attempts to access their Application/Delivery Channel.

3.3.2 Entitlements defined in ONE ID Federation Authorization Service

- If the Delivery Channel uses the ONE ID Federation Authorization service, the Delivery Channel will provide ONE ID with information required to define the user entitlements, such as:
 - Login ID, Service, Delivery Channel, sponsoring organization(s)

- ONE ID will work with the Delivery Channel to establish a process to authorize users for access to it; i.e., grant service entitlements to users or revoke the service entitlements:
 - ONE ID Federation Authorization Web Application (not yet available)
 - Bulk Load of input file
- Entitlement data will be contained in the SAML Response Service Entitlements and UAO attributes and will be extracted by the Delivery Channel at login time to determine if the user is entitled to access it.

Process Flow

The authorization component is incorporated into the overall Federation Broker orchestration. Once the required data validation steps have been completed the Federation Broker will retrieve the user's specific entitlements from the authorization repository. Once the Federation Broker receives the response it will add the authorization data into the outbound, provincially-issued SAML token.

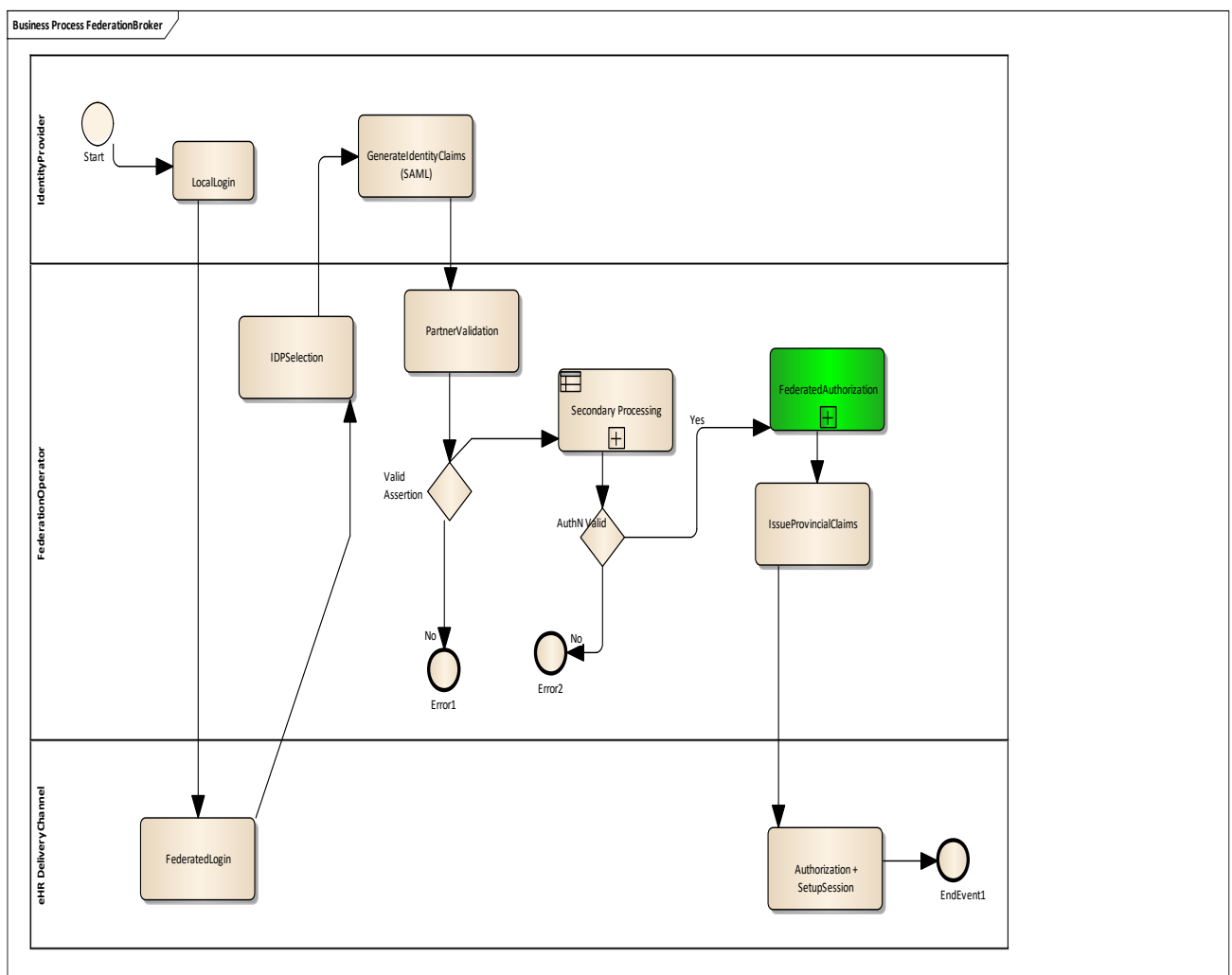


Figure 4 - SSO Business Flow with Authorization

4.0 ONE ID Federated Login Sequences

4.1 SP Initiated Login Sequence Diagram

The following is a sample login flow based on an SP initiated login event using the HTTP Post binding. It does not explicitly include activities that don't directly relate to this interface specification (i.e. creation of an eHealth identity, creation of an audit record).

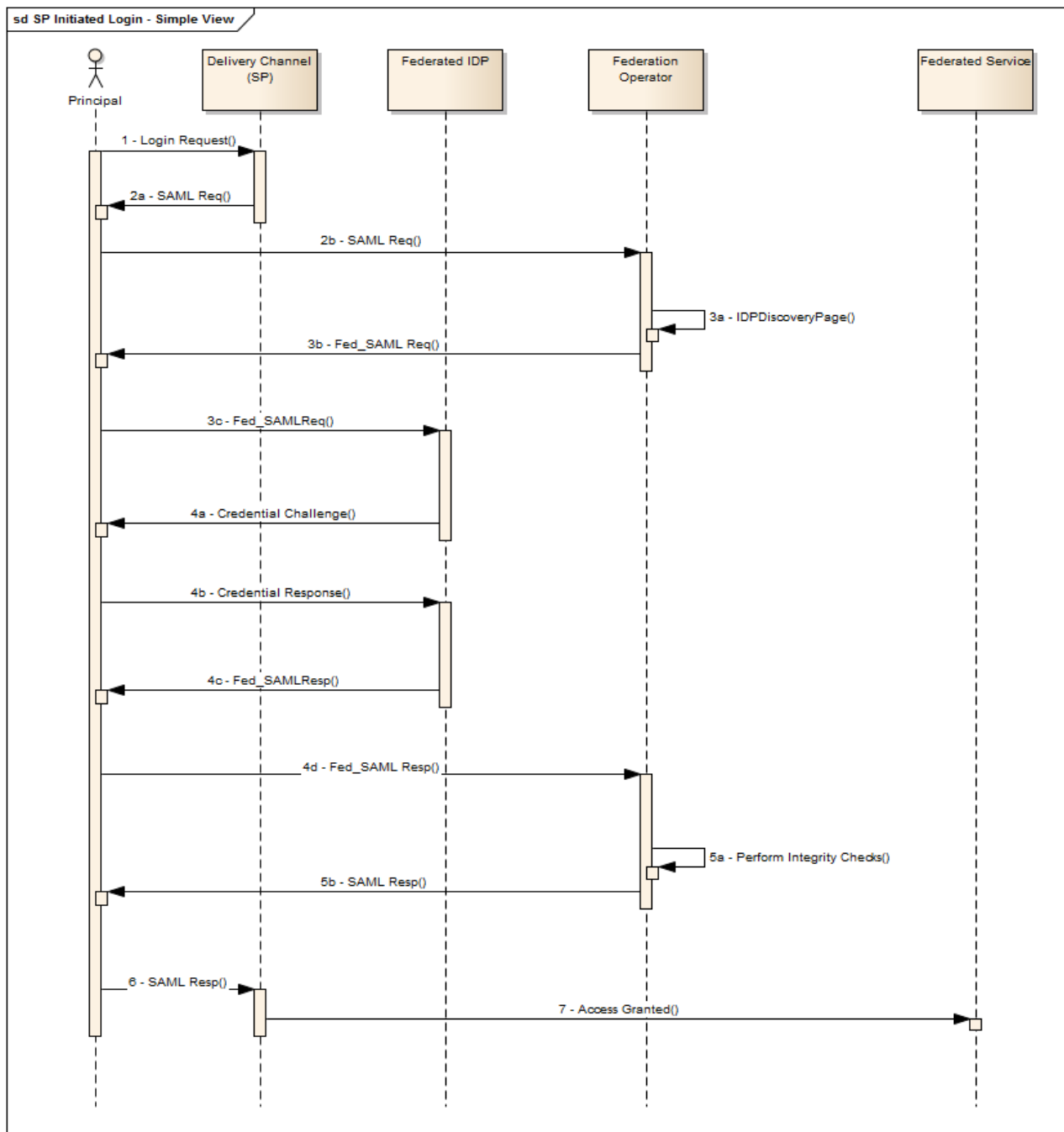


Figure 5: SP-initiated federated login - sequence diagram

4.1.1 SP Initiated Login Steps

Steps	Party	Action
1	Principal – User	The principal (user) requests access to a Delivery Channel in the Federation.
2	Delivery Channel	2a: the Delivery Channel requests an identity assertion. 2b: this request is redirected through the principal's browser to the provincial Federation Broker (Operator).
3	ONE ID Federation	3a: the Federation Broker generates a list of all valid and trusted Federation Identity Providers (IDP Selection). Only valid eHealth federated IDPs will be presented in the list. 3b/3c: the user selects an Identity Provider from the list, and ONE ID Federation sends a SAML Request message to the selected IDP. IDP This is the primary function of the Federation Broker. It acts as the intermediary between the Delivery Channels requesting authentication and the Identity Provider that holds the digital identity. This eliminates the overhead of having individual partners trust and establish connections with one another.
4	IDP	The IDP is responsible for: 4a: challenging the user for credentials (if not previously authenticated) 4b: capturing and evaluating the credentials (such as user name and password) provided by the principal. Second factor Authentication is required. 4c: generating the SAML response token. 4d: once the SAML response token is generated, the principal is redirected to ONE ID Federation Broker (hub) with the IDP-issued SAML token.
5	ONE ID Federation	5a: The Federation Broker processes the response: - Validates the SAML Issuer - Validates the digital signature - Decrypts the SAML assertion contained within the response - Parses and validates attributes contained within the IDP SAML assertion - Performs provincial authentication of claims 5b: issues a signed and encrypted ONE ID Federation SAML response token containing the IDP asserted attributes and, where applicable, authorization information. Carries out data transformation as needed to ensure the response complies with the SAML version that the Delivery Channel is expecting. Forwards the requester back to the initiating Delivery Channel.

Steps	Party	Action
6	Delivery Channel	Based on the information received in the response assertion, the Delivery Channel allows access.
7	Principal	Gains access to the Delivery Channel if authenticated and authorized to use it.

Table 1: federated login – steps

4.2 Identity Provider Initiated Login Sequence Diagram

There is a second scenario for federated login. This scenario will typically occur when a provider is already logged in a POSA (e.g. Hospital Information System) and viewing local organizational applications. This scenario is synonymous with a traditional user login process in which SAML is not required. All the steps required to reach that state are referred to as “precursor events” in the diagram below.

Within the POSAs, e.g. HIS or EMR, links to other federated Delivery Channels can be provided. These links contain redirection instructions to send the user to the local SAML token service (STS). This initial redirection results in the creation of a SAML response token issued by the IDP for the POSA which, in turn, is passed on to the Federation Broker. In essence, the SAML request processes (as illustrated in SP initiated login) are skipped and the process starts with the IDP issued response token.

The following sequence diagram describes the steps required to perform this IDP initiated login. Note that there is a set of precursor events that must happen prior to the IDP initiated login itself.

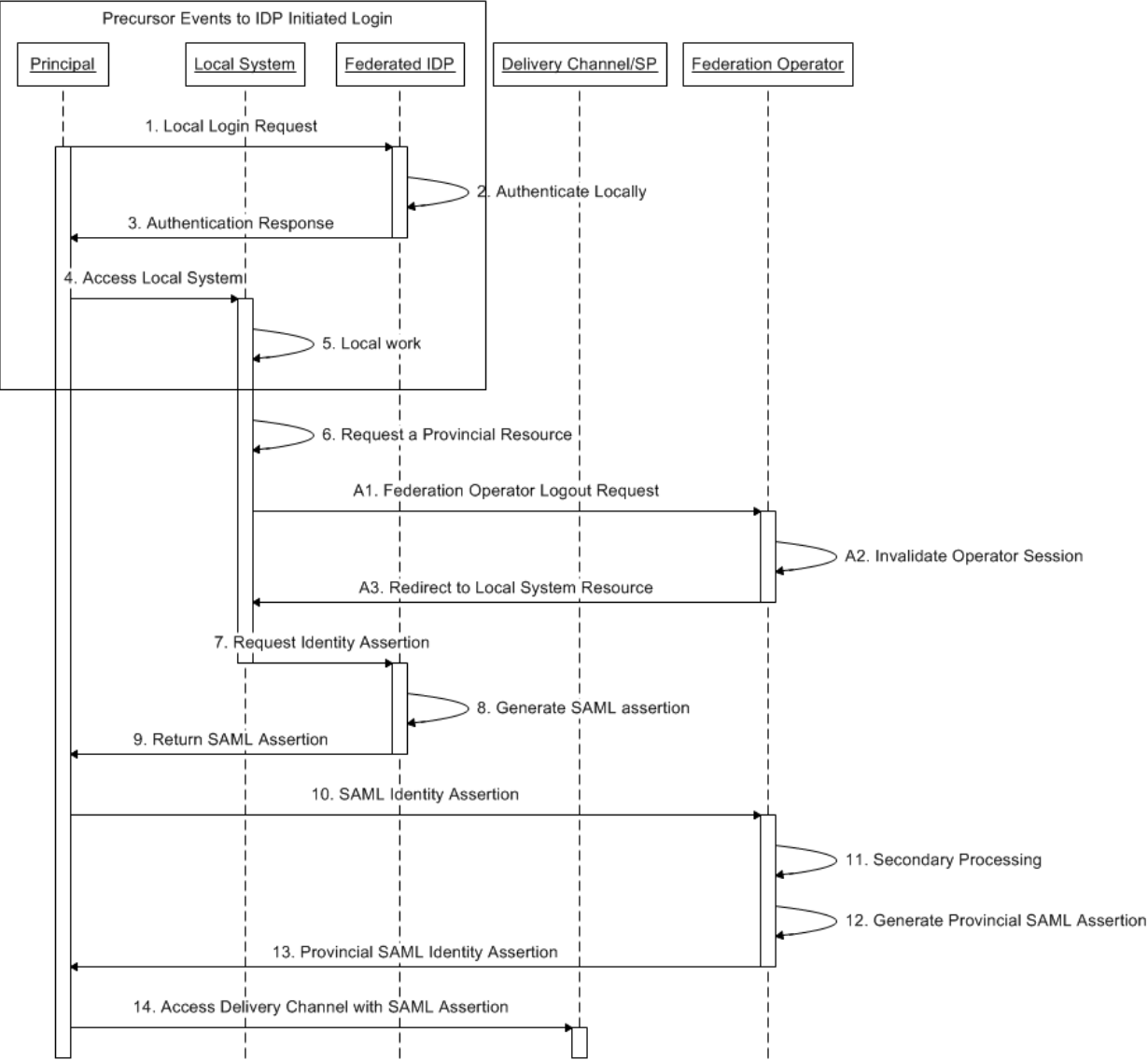


Figure 6 - IDP Initiated Login

4.2.1 Identity Provider Initiated Login Steps

Steps	Party	Action
1	Federated IDP	Precursor step: the user logs in to their POSA through the use of their local Identity Provider. The Identity Provider is a member of the Federation.
2	Federated IDP	Precursor step: the local Identity Provider performs local authentication, no SAML token is generated nor needed.
3	Federated IDP	Precursor step: authentication response returned to the user
4	POSA	Precursor step: the user is granted access to the POSA.

Steps	Party	Action
5	POSA	Precursor step: the user performs work within the POSA.
6	POSA	The user clicks on a link to a Federated Resource.
A1	POSA	The POSA redirects the user to the Federation Broker logout URL with the <code>returnurl</code> and <code>globalslo</code> query string parameters set: <code>https://federationbroker.ehealthontario.ca/fed/user/logout?returnurl=[Local System Return Address]&globalslo=false</code> The <code>returnurl</code> is the URL of the resource in the POSA that the Federation Broker redirects the user back to after invalidating the Federation Broker session (i.e., the resource performing the actions in step 7). The inclusion of the <code>returnurl</code> query string parameter in the URL is optional. The <code>globalslo</code> query string parameter value must be <code>false</code>.
A2	Federation Broker	The Federation Broker invalidates the user's Federation Broker session. Since the query string parameter <code>globalslo</code> was specified as <code>false</code> in step A1, the Federation Broker does a local logout only (by invalidating the Federation Broker session) and does not redirect the request to IDPs to invalidate the IDP session.
A3	Federation Broker	The Federation Broker redirects the user to the URL specified by the <code>returnurl</code> query string parameter from step A1.
7	POSA	Using redirection instructions included in the Federated Resource link, the POSA redirects the user to the local SAML provider to obtain a SAML response message.
8	Federated IDP	The Federated IDP knows that the user is already authenticated and a SAML response message is issued without the need for a new authentication.
9	Federated IDP	The Federated IDP redirects the user to the Federation Broker (Operator) with the SAML response and a reference to the destination Delivery Channel defined in the post data. The destination Delivery Channel is the Entity ID of the DC (provincial resource) that the user requested in step 7, and is specified by the <code>RelayState</code> post parameter in the redirect. ONE ID will provide the Entity IDs of other DCs that the POSA may want to provide "shortcuts" to as these applications become trusted SPs in the Federation.
10	Principal	No action is needed from the user but the redirection goes through the user's browser in order to issue the SAML identity assertion to the Federation Broker

Steps	Party	Action
11	Federation Broker	The Federation Broker processes the response: - Validates the SAML Issuer - Validates the digital signature - Decrypts the SAML assertion contained within the response - Parses and validates attributes contained within the IDP SAML assertion - Performs provincial authentication of claims The user is logged into the Federation Broker and a Federation Broker (single sign on) session will be created for the user.
12	Federation Broker	The Federation Broker issues a Provincial SAML token including, where applicable, authorization information.
13	Federation Broker	The Provincial SAML token is returned to the user together with redirection instructions to the destination Delivery Channel.
14	Principal	The user is redirected to the destination Delivery Channel; the Provincial SAML token is included in this redirection.

Table 3: Identity Provider Initiated Login - steps

5.0 SAML Configuration

The first step in setting up SAML communication between ONE ID and the new federated partner begins with 'metadata'. ONE ID and the Delivery Channel or Identity Provider (depending on the partner role) exchange information about each other via SAML metadata files. Metadata information is needed for configuration to set up cross-domain trust by exchanging partner identifiers, PKI certificates, location of SSO resources, etc.

Metadata contains information such as:

- IDP Identity or Delivery Channel ID
- SAML protocol used
- PKI certificates for encrypting SAML requests and responses and for validating digital signatures. These certificates must be obtained from eHealth Ontario.
- Symmetric key encryption algorithms supported by the provider
- Single sign-in and sign-out information

For a detailed list of information contained within a SAML message please refer to the [OASIS website](#).

Most COTS products will generate this metadata automatically so detailed steps will not be outlined in this document.

The ONE ID Federation broker supports the HTTP Post SAML Profile.

Configuration Item	ONE ID Federation
SAML Binding	• SAML Response – HTTP Post • SAML Request – HTTP Post, HTTP Redirect
SAML Profile	• Web Browser SSO • Identity Provider Selection • SAML attribute profile • <i>Artifact resolution protocol is planned for a later release</i> • <i>Assertion Query/Request Profile is planned for a later release.</i>
Message Encryption	Required. The certificate for this purpose must be obtained from eHealth Ontario.
Message Signing	Required. The certificate for this purpose must be obtained from eHealth Ontario.

Table 2: ONE ID metadata configuration

6.0 SAML Authentication Requests

6.1 SAML Authentication Request from Delivery Channel

SAML Authentication Requests are issued by the Delivery Channel and function as the starting point for the SP Initiated login. The authentication request describes the properties that the resulting SAML assertion needs to have.

In a SP Initiated login sequence, the user will be directed to the ONE ID Federation IDP Selection page. The ONE ID Federation Broker will send a request to the IDP for the user to authenticate. Detailed information on the content structure of SAML request / response messages can be obtained directly from the OASIS website. A high level overview of key information can be found in the following sections.

It should be noted that the intent behind the provincial specification is that the structure and format of request/response message is the same across all Federated partners.

6.1.1 SAML Authentication Request Elements

Element	Nested Elements, fields, details and description		
samlp:AuthnRequest	SAML Authentication request. All elements are within the Authentication request. An authentication request is an explicit request for an assertion from the Identity Provider.		
	xmlns:samlp	n:oasis:names:tc:SAML:2.0:protocol	Protocol used
	Destination	https://healthcare.portal.on.ca/saml/consume-response	Destination of IDPSAML request. This is the value of md:EntityDescriptor/md:IDPSSODescriptor/md:SingleSignOnService/@Location specified in the IDP-issued SAML metadata.
	ForceAuthn	False	A value of 'True' is not currently enforced. This would force re-authentication even if the user has an SSO session at the IDP.
	IssueInstant	2016-01-15T19:13:48.446Z	Time request was issued (UTC).
	Version	2.0	Version of SAML
	saml2:Issuer	Issuer of the SAML request	
	xmlns:saml2	urn:oasis:names:tc:SAML:2.0:assertion	

Element	Nested Elements, fields, details and description		
		Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity
		Issuer value	Example: https://regionalportal.on.ca/fed/idp Entity ID of provider that issued this request
	ds:Signature	Signature Elements	
		xmlns:ds	http://www.w3.org/2000/09/xmldsig#>
		SignedInfo Elements	Signed Info Elements: CanonicalizationMethod SignatureMethod Reference Transforms DigestMethod SignatureValue Keyinfo The request must be signed by the sender and the receiver must verify the digital signature.
	NameID Policy	Specific format of SAML name identifiers that are supported by the IDP.	
		Format	urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified
		AllowCreate	true
	Requested AuthnContext	The Authentication Context for the SAML Request. The user will authenticate via a password in a protected session.	
		Comparison	exact Specify “exact” or omit this attribute
		AuthnContextClassRef	urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport

7.0 SAML Response Assertions

7.1 SAML Response from IDP to Federation Broker

7.1.1 SP Initiated Login

When a user is not already authenticated and attempts to access a Delivery Channel in the Federation, the Delivery Channel requests an identity assertion from the Federation Broker. (See section 6.1. ‘SAML Authentication Request from Delivery Channel’)

- The user is redirected to the ONE ID Federation IDP Selection page to select an IDP. When the user selects an IDP from this page, the ONE ID Federation Broker issues a request to authenticate and redirects the user to the IDP.
- Following user authentication, the Federated IDP generates a SAML Response message and redirects the user with the SAML response to the Federation Broker. See steps 1 to 4 from section 4.1.1 *SP Initiated Login Steps*.
- The Federation Broker performs validation on the SAML response from the IDP. See section 7.2.1 below.

7.1.2 IDP Initiated Login

When a user is already logged into a POSA, a SAML request for authentication is not required. For login steps, see section 4.2.1 ‘Identity Provider Initiated Login Steps’ steps 1 to 7.

- Before generating a SAML Response, the user is directed to the Federation Broker logout URL. The user is redirected back to the POSA after invalidating the Federation Broker session. (See Step A1, A2 and A3 in section 4.2.1)
- The POSA redirects the user to the local SAML provider to obtain a SAML response message. The Federated IDP issues a SAML response message and redirects the user to the Federation Broker.
- Patient context attributes may be included in the SAML response for an IDP Initiated login.
- The Federation Broker performs validation on the SAML response from the IDP. See section 7.2.1 below.

7.1.3 Federation Broker Validation of SAML Response

The Federation Broker performs validation on the SAML response received from the IDP via an SP initiated login sequence or an IDP initiated login sequence. Example validation steps include:

- Validation of the digital signature and issuer. Has the message been sent by a trusted party? Does it include the expected signature key?
- Was the SAML response received within the expected time frame?
- Is the Status of the SAML response success?
- Is the NameID Format acceptable?
- Are all the mandatory attributes in the SAML Assertion attribute statement present? Do the attributes contain data in the expected format, as specified in section 8.0 ‘SAML Response

Assertion Attribute Statements’.

7.2 SAML Response from Federation Broker to Delivery Channel

7.2.1 Federation Broker Generation of SAML Response to Delivery Channel

The Federation Broker generates a SAML response based on the response received from the IDP. The SAML Response is posted to the Delivery Channel. Some of the information included in the response is:

- Destination URL - the DC’s Single Sign On Service location
- Issuer of response - The Federation Broker entity ID
- Digital signature
- Status of the SAML response

Inside the SAML assertion:

- Issuer of the assertion
- Digital signature
- Subject:
 - NameID – The unique, immutable identifier for the user that is not re-used over time for different users
 - NameQualifier – The entity ID of the Federation Broker
 - SPNameQualifier - The Delivery Channel entity ID
- Conditions – the validity period of the response and the audience the response is restricted to
- SAML Authentication Statement – A statement of when and how the user was authenticated
- SAML Attribute Statement – See Section 8.0 ‘*SAML Response Assertion Attribute Statements’*.
 - Attributes are validated and posted as received from the IDP with the following exceptions:
 - ServiceEntitlements and UAO are generated based on recipient of the response and authorization data for the principal.
 - The RID field contains data as passed by the IDP.
 - Attributes may be transformed to conform to the SAML attribute statement version supported by the DC, if it is different from the version supported by the IDP

7.3 Main Elements of SAML Response Assertion

Details on the structure and content of a SAMLv2 response can be found on the OASIS website.

Element	Nested Elements, fields, details and description
samlp:	SAML Authentication Response. All elements are within the SAML response.

Element	Nested Elements, fields, details and description			
Response		xmlns:samlp	urn:oasis:names:tc:SAML:2.0:protocol	Protocol used
		Destination	See S1.Destination in table below.	Destination for SAML response (Federation Broker or Delivery Channel)
		ID	id-ZC8cWz6DuifHvl04uK3j4G2-qw4-	Response ID
		InResponseTo	id-3f18b53b-1104-4af5-8a75-262739a36dbc	ID of original SAML authentication request (if applicable)
		IssueInstant	2012-11-20T18:45:24Z	Time response was issued
		Version	2.0	Version of SAML
	saml2:Issuer	Issuer of the SAML response		
		xmlns:saml2	urn:oasis:names:tc:SAML:2.0:assertion	Version of response assertion
		Format	urn:oasis:names:tc:SAML:2.0:nameid-format:entity	Identifier for IDP that issued the response assertion.
		Issuer value	See S2.Issuer in table below	Entity ID of party that issued the assertion (IDP or Federation Broker)
ds:Signature	Information to determine if the message was issued by a trusted party and has not been tampered with.			
		xmlns:ds	http://www.w3.org/2000/09/xmldsig#>	Structure of the signature
		SignedInfo Elements	Signed Info Elements: CanonicalizationMethod SignatureMethod Reference (includes: Transforms, DigestMethod, Digest Value) SignatureValue Keyinfo	Refer to the OASIS website for details on the structure and content of the signature elements of the SAML response. The sender/issuer must sign the SAML response and the receiver must verify the digital signature.
	Status	Status Code for the SAML Response		

Element	Nested Elements, fields, details and description			
		StatusCode Value	Example: urn:oasis:names:tc:SAML:2.0:status:Success	A code representing whether the user was authenticated successfully or not
	Assertion		Defines the syntax to describe authentication, authorization and attribute information to be carried between systems. Included are schemas and protocols.	
		xmlns:saml	urn:oasis:names:tc:SAML:2.0:assertion	Namespace
		ID	id-DIdfZd1ucsxilJB9Kts6xHKz59U-	Unique ID for the response assertion
		IssueInstant	2012-11-20T18:45:24Z	Time the assertion was issued.
		Version	2.0	Version of assertion
		saml:Issuer	Issuer of the response assertion(format = urn:oasis:names:tc:SAML:2.0:nameid-format:entity). See S3.Issuer in table below	Issuer of the response assertion.
	Signature Elements		Signed Info Elements: CanonicalizationMethod SignatureMethod Reference (includes: Transforms, DigestMethod, Digest Value) SignatureValue Keyinfo	Refer to the OASIS website for details on the structure and content of the signature elements of the SAML assertion. The sender/issuer must sign the SAML assertion and the receiver must verify the digital signature.
	Subject		Subject Elements in Assertion of response	Contains details pertaining to the subject (principal) of the assertion.
			NameID. SubjectConfirmation, SubjectConfirmation Data	NameID Format urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified Method of confirmation (i.e. urn:oasis:names:tc:SAML:2.0:cm:bearer)

Element	Nested Elements, fields, details and description		
			InResponseTo ID of original SAML authentication request, if applicable; e.g.: id-3f18b53b-1104-4af5-8a75-262739a36dbc NotOnOrAfter Timestamp. Subject cannot be confirmed on or after this time; e.g.: 2015-03-25T20:37:52Z Recipient Entity ID of the recipient of assertion See S7.Recipient
		Conditions	Condition Elements in Assertion section of response Contains restrictions describing when the SAML assertion is valid (e.g., not before or after a specific time stamp.) NotBefore Assertion is valid beginning at this time (UTC); e.g., 2015-03-25T20:24:50Z NotOnOrAfter Assertion is not valid as of this time (UTC); e.g., 2015-03-25T20:37:52Z AudienceRestriction, Audience Explicit statement that indicates the entity ID of the party for which the assertion is valid. See S8. Audience
		AuthnStatement	Authentication Statement Elements in Assertion section of response Contains information related to how the user was authenticated. AuthnInstant When the user was authenticated (UTC) SessionIndex Session tracking reference SessionNotOnOrAfter Time (UTC) at which session is invalid; e.g., 2015-03-25T21:28:51Z

Element	Nested Elements, fields, details and description		
		AuthnContext	Authentication context declaration urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport
		Attribute Statements	These are specific attributes related to the user, Identity Provider and asserting party. These attributes are used by the Delivery Channel to determine if the user should gain access to it and any Applications it supports. The information in the attribute statement is used by the DC to determine the authorization of the user and to perform just-in-time local account creation or modification, if needed. The attributes included in the SAML attribute statement are dependent on origin of the SAML Response: • SP Initiated Login: SAML Response posted to Federation Broker • IDP Initiated Login: SAML Response posted to Federation Broker • Federation Broker Provincial SAML Response generated after validating the IDP SAML response. Most attributes are passed on as received by the Federation Broker. See section 8.0 SAML Response Assertion Attribute Statements for details.

SAML Assertion Details

SAML Element	(IDP to Federation Broker or Federation Broker to DC)	Example URL or procedure	Comments
/samlp:Response			
S1.Destination	IDP to Federation Broker	Destination ="https://federationbroker.ehealthontario.ca/federation/sp/authnResponse20"	This is the location of the Federation Broker's assertion consumer service
	Federation Broker to Delivery Channel	Destination ="https://healthcare.portal.on.ca/saml/consumer-response"	This is the location of the DC's assertion consumer service.
/samlp:Response/saml:Issuer			

SAML Element	(IDP to Federation Broker or Federation Broker to DC)	Example URL or procedure	Comments
S2.Issuer	IDP to Federation Broker	https://federation.ehealthontario.ca/fed/idp	The entity ID of the IDP
	Federation Broker to Delivery Channel	https://federationbroker.ehealthontario.ca/fed/idp	The entity ID of the Federation Broker
/samlp:Response/saml:Assertion/saml:Issuer			
S3.Issuer	IDP to Federation Broker	https://federation.ehealthontario.ca/fed/idp	The entity ID of the IDP
	Federation Broker to Delivery Channel	https://federationbroker.ehealthontario.ca/fed/idp	The entity ID of the Federation Broker
• /samlp:response/saml:Assertion/saml:Subject/saml:NameID. NameID is a unique and immutable reference to the principal. It is critical that the NameID value associated with a principal is not (A) changed once assigned, nor (B) reused across different user accounts over time. As an example, a NameID value for an account that has been revoked must not be reused for a new account for a different user. Failure to align with this directive could result in a principal being denied access to or granted inappropriate access to federated systems,. In addition, the behavior of federated systems that use the NameID as the key identifier of users will be unpredictable, e.g. user profiles and other settings may no longer work and users may need to set these up again which can be time consuming. Note that the reference to an ‘unchangeable, unique electronic identity’ within the ‘eHealth Ontario Identity Federation – Identity Provider Standard’ is a reference to the value in the NameID attribute. • If an Identity Provider finds it absolutely necessary to change a NameID previously submitted to the Federation Broker due to exception circumstances, such as a system error or data corruption, then this change must be communicated to the Federation Broker. In addition, the Identity Provider is responsible for immediately updating the user’s authorizations within the Federation Broker if the UserLoginName changes. The Federation Broker will update all appropriate systems and repositories on a ‘best effort’ basis only, noting that some of these systems and repositories may be outside its control. . Due to the overhead associated with changes to NameID and the likely, negative impact on the user’s experience, the objective is to minimize the number of instances when this is required.			

SAML Element	(IDP to Federation Broker or Federation Broker to DC)	Example URL or procedure	Comments
S4.NameID	IDP to Federation Broker	3f7842c1-c4de-4469-b183-a697b8aa5db1	The unique, persistent identifier for this user that was generated by the IDP. This value may or may not be specific for the Federation Broker.
	Federation Broker to Delivery Channel	id-8SYU61PDn--EEUYoDckvua1VBdA-	The unique, persistent identifier for this user that was generated by the Federation Broker. This value is specific for the Delivery Channel as specified by the SPNameQualifier value.
S5.NameQualifier	IDP to Federation Broker	NameQualifier ="https://federation.ehealthontario.ca/fed/idp"	The entity ID of the IDP
	Federation Broker to Delivery Channel	NameQualifier ="https://federationbroker.ehealthontario.ca/fed/idp"	The entity ID of the Federation Broker
S6.SPNameQualifier	IDP to Federation Broker	SPNameQualifier ="https://federationbroker.ehealthontario.ca/fed/sp"	The entity ID of the Federation Broker
	Federation Broker to Delivery Channel	SPNameQualifier ="https://healthcare.portal.on.ca/sso/sp"	The entity ID of the DC.
/samlp:response/saml:Assertion/saml:Subject/saml:SubjectConfirmation/saml:SubjectConfirmationData			
S7.Recipient	IDP to Federation Broker	Recipient ="https://federationbroker.ehealthontario.ca/fed/sp/authnResponse20"	This is the location of the Federation Broker's assertion consumer service
	Federation Broker to Delivery Channel	Recipient ="https://healthcare.portal.on.ca/saml/consume-response"	This is the location of the DC's assertion consumer service

SAML Element	(IDP to Federation Broker or Federation Broker to DC)	Example URL or procedure	Comments
/samlp:response/saml:Assertion/saml:Conditions/saml:AudienceRestriction/saml:Audience			
S8. Audience	IDP to Federation Broker	https://federationbroker.ehealthontario.ca/fed/sp	The entity ID of the Federation Broker.
	Federation Broker to Delivery Channel	https://healthcare.portal.on.ca/sso/sp	The entity ID of the DC.

8.0 SAML Response Assertion Attribute Statements

8.1 Background

The SAML attribute statement is part of the assertion element in a SAML response. This specification defines the eHealth standards for the attributes contained within the SAML attribute statement. Included are both attributes that are standard and optional. Optional attributes:

- Are used to carry additional information that is used to ensure compliance to security & privacy requirements as well as legislative requirements.
- May be used by downstream systems to make entitlement decisions.
- Are currently used to transmit the patient and clinical context to all Federation partners.
 - This patient context is transmitted once per session in a unidirectional manner between the HIS/IDP and the Delivery Channels. It is not a means to convey update, synchronization or notification information back to the originating system.
 - Inclusion of this patient context in the SAML token is a tactical means to fulfill the requirement to pass patient information from a POSA to the regional viewers.

The following information related to the transaction will be conveyed as SAML attribute statements. Unless otherwise specified, values are not case-sensitive.

8.2 Identity Attributes

8.2.1 DisplayName

Attribute Item	Detail
Description	User's display name
Business Value	Allows Delivery Channels to present a consistent name or identifier to the principal in greetings and other messages.
URN	urn:ehealth:names:idm:attribute:DisplayName <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:DisplayName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Cho, Franklin RN</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	Cho, Franklin RN Smith, John
Format	String
Coded Values	No
Mandatory?	No
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker. No validation or transformation is carried out.

8.2.2 Email

Attribute Item	Detail
Description	Email address of the requesting principal

Attribute Item	Detail
Business Value	May be used, in conjunction with other identity attributes, to uniquely identify the principal.
URN Format	urn:ehealth:names:idm:attribute:Email urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:Email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Franklin.Cho@hospital.org</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	Franklin.Cho@hospital.org John.Smith@idp.ca
Format	String
Coded Values	No
Mandatory?	No
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.2.3 FirstName

Attribute Item	Detail
Description	First name of the requesting principal
Business Value	May be used, in conjunction with other identity attributes, to uniquely identify the principal.
URN Format	urn:ehealth:names:idm:attribute:FirstName urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:FirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Franklin</saml:AttributeValue></saml:Attribute>
Sample text value of	Franklin

Attribute Item	Detail
attribute	
Format	String
Coded Values	No
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.2.4 LastName

Attribute Item	Detail
Description	Last name of the requesting principal.
Business Value	May be used, in conjunction with other identity attributes, to uniquely identify the principal.
URN <i>Format</i>	<code>urn:ehealth:names:idm:attribute:LastName</code> <code>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</code>
Sample in message format	<code><saml:Attribute Name="urn:ehealth:names:idm:attribute:LastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Cho</saml:AttributeValue></saml:Attribute></code>
Sample text value of attribute	Cho
Format	String
Coded Values	
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP

Attribute Item	Detail
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.2.5 RID

Attribute Item	Detail
Description	This attribute specifies the Professional Designation (or each Professional Designation if more than one) that the principal has. It can act as a <i>real identity reference</i> and can be resolved to an entry in the Provider Registry where the regulated health college provides a feed.
Business Value	The Professional Designation (or each Professional Designation if the principal has more than one) is a key piece of information about the principal as it enables the Federation Broker to carry out the following activities: • Associate an account to a real world identity that is maintained by a regulated health college • Determine the status of the licence, e.g. active or inactive • Act as a public identifier on transactions inbound to eHealth Ontario assets Future activities may include: • Link different accounts belonging to the same principal • Determine any professions and/or specialties associated to the licence
URN Format	urn:ehealth:names:idm:attribute:rid urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:idm:attribute:rid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string" xmlns:xs="http://www.w3.org/2001/XMLSchema" xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance"> upi:1000000000001:Active</saml:AttributeValue></saml:Attribute></pre>
Sample text value of attribute	IDP Format: upi:1000000000001 UPI:1234566 or CPSO:12345 or URP (Unregulated Provider) Federation Broker format: upi:1000000000001:Active UPI:1234566:Active

Attribute Item	Detail
	or CPSO:12345:Unverified or URP
Format	Identity Provider Format (messages sent from the IDP to the FB) UPI:<value of UPI> or <Licensing authority name>:<licence number> or URP Federation Broker Assertion Format (messages sent from the Federation Broker to the DC) Same format as IDP with :<status> appended to the end UPI:<value of UPI>:<status> or <Licensing authority name>:<licence number>:<status> or URP
Coded Values	If Licensing Authority is used then see list in section 11.1 for valid authorities (e.g. "CPSO"). If there is no licensing authority or UPI, the IDP will pass the value 'URP' (Unregulated provider) Status Code Values; Active Inactive Unverified
Mandatory?	Yes
Multi Value Allowed?	Yes
IDP and/or Federation Broker (FB) Generated	IDP and FB
Federation Broker Processing	• Validate that the RID field is present • Append status to the UPI or Licensing Authority attribute:

Attribute Item	Detail
	○ Active. This means that the licence has been verified against PR and the licence is in good standing. ○ Inactive. This means that the licence has been verified against PR and the licence is not in force. ○ Unverified. This means that either the college the licence pertains to does not yet exist in PR and so the licence cannot be verified or the college does exist in PR but the Federation Broker has not verified the licence • If no regulated college affiliation, pass URP.

8.2.6 UserLoginName

Attribute Item	Detail
Description	The login ID of the user initiating the login request.
Business Value	One of the main identity attributes, that may be used in conjunction with other identity attributes, to uniquely identify the principal.
URN <i>Format</i>	urn:ehealth:names:idm:attribute:UserLoginName urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name=" urn:ehealth:names:idm:attribute:UserLoginName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">JOHN.SMITH@ONEID.ON.CA</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	JOHN.SMITH@ONEID.ON.CA
Format	String
Coded Values	
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.2.7 TelephoneNumber

Attribute Item	Detail
Description	The Telephone number of the user initiating the login request. This attribute may only be used by Identity Providers that have signed the Agreement to enable the Federation Operator to carry out a second factor authentication challenge on their behalf.
Business Value	Contents will be used by the Federation Operator to carry out a second factor authentication challenge on behalf of the Identity Provider. This includes a voice call to the provider or an SMS messages to their mobile device. Longer term it is intended that there will be no restriction on the number of telephone numbers that an Identity Provider can send but initially a maximum of three numbers only will be supported.
URN	urn:ehealth:names:idm:attribute:TelephoneNumber
Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<pre><saml:Attribute Name="TelephoneNumber" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">4167778888</saml:AttributeValue></saml:Attribute></pre>
Sample text value of attribute	4167778888 4164445555:1234
Format	The format of the attribute <i>TelephoneNumber</i> must be specified as nnnnnnnnnn<numeric extension number> where 'nnnnnnnnnn' is exactly 10 digits. The <numeric extension number>, if provided, must contain digits only. Note that the intention to use extension numbers is part of a longer term strategy. They are currently not supported and should not be sent.
Coded Values	N/A
Mandatory?	This attribute is mandatory if strongAuthenticationRequest attribute is set to 'Y' and will be ignored otherwise.
Multi Value Allowed?	Yes Note that initially a maximum of three telephone numbers should be sent in this attribute.
IDP and/or Federation Broker (FB) Generated	IDP – The Federation Operator will not include Telephone number in assertions sent to service providers.

Attribute Item	Detail
Federation Broker Processing	If Telephone number is present, and StrongAuthenticationRequest is set to Y, the operator will invoke an adaptive out of band authentication challenge on behalf of the federated IDP.

8.2.8 StrongAuthenticationRequest

Attribute Item	Detail
Description	This attribute may only be used by Identity Providers that have signed the Agreement that enables them to request the Federation Operator to carry out a second factor authentication challenge on their behalf. The purpose of this attribute is to submit that request to the Federation Operator.
Business Value	The purpose of this attribute is to support the process where the Federation Operator applies strong authentication on behalf of an Identity Provider, thus allowing that Identity Provider to meet the authentication requirements specified in the IDP Agreement. This attribute provides flexibility in that the Identity Provider may not need the Federation Operator to intervene every login for a given user. If the user is onsite then the Identity Provider's authentication may be sufficient but if the user is remote then the Federation Operator may need to apply strong authentication.
URN	urn:ehealth:names:idm:attribute:StrongAuthenticationRequest
Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name=" StrongAuthenticationRequest " NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">Y</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	Y
Format	Y – Yes N - No
Coded Values	Y N
Mandatory?	No

Attribute Item	Detail
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP – The Federation Operator will not include this attribute in assertions sent to service providers.
Federation Broker Processing	If Telephone number is present, and OOB Challenge Indicator is set to Y, the operator will invoke an adaptive out of band authentication challenge on behalf of the federated IDP.

8.2.9 PrincipalFedKey

Attribute Item	Detail
Description	The PrincipalFedKey is a key that can be used to identify a given user. If a user has more than one Federated Account then the same PrincipalFedKey will be associated to each of those accounts, once those accounts have been linked by the Federation Broker.
Business Value	Allows a Delivery Channel to determine who the user (person) is, regardless of the Federated Account used by the user to access the Delivery Channel.
URN	urn:ehealth:names:idm:attribute:PrincipalFedKey urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:PrincipalFedKey " NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">123456abcd</saml:AttributeValue></saml:Attribute>
Format	String
Coded Values	No
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	FB
Federation Broker	This attribute and value is posted in the SAML response generated by the Federation

Attribute Item	Detail
Processing	Broker.

8.3 Authentication Attributes

8.3.1 AssertingParty

Attribute Item	Detail
Description	The originating organization that provided the SAML assertion.
Business Value	This attribute provides information about the organization that submitted the request. This can be used in conjunction with the 'Identity Provider' attribute to determine how the user was authenticated, i.e. what party sent the assertion and what party authenticated the user. The 'Asserting Party' and 'Identity Provider' may be the same.
URN Format	urn:ehealth:names:idm:attribute:AssertingParty urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:AttributeName="urn:ehealth:names:idm:attribute:AssertingParty" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:basic"><saml:AttributeValue xsi:type="xs:string">cn=federation.idpa.,ou=x,dc=y,dc=z</saml:AttributeValue></sa ml:Attribute>
Sample text value of attribute	Cn=IDPA,ou=partners,ou=fed,dc=subscribers,dc=ca cn=federation.idpa,ou=x,dc=y,dc=z http://fedidp.idporg.ca
Format	Distinguished Name URI
Coded Values	
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.3.2 **AuthenticationLevel**

Attribute Item	Detail
Description	The authentication level (based on the eHealth Federation Identity Provider Standards) that the principal was authenticated at.). Note: If the location of the user forms part of the authentication, e.g. the user is on a Protected Network such as a corporate LAN where remote users (off-site) require 2-factor authentication, then the setting of this attribute must include this, i.e. set to AL2. In those cases, setting the ProtectedNetwork attribute to True and this attribute to AL1 only will result in a user being denied access to services containing PI and PHI.
Business Value	This attribute allows a Delivery Channel to determine if a principal should be allowed to view PI and/or PHI or gain access to Applications that contain PI and/or PHI. In order to view PI and PHI, this attribute and the 'IdentityVerificationSchemeRef' attribute (see section 8.3.5) must both be set to a value of AL2 or higher.
URN Format	urn:ehealth:names:idm:attribute:AuthenticationLevel urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	saml:Attribute Name="urn:ehealth:names:idm:attribute:AuthenticationLevel" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:basic"><saml:AttributeValue xsi:type="xs:string">AL2</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	AL2
Format	String
Coded Values	AL1 AL2 AL3
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.3.3 CredentialManagementSchemeRef

Attribute Item	Detail
Description	The eHealth Federation Evaluation Criteria define how eHealth establishes measures of the identity assurance-related aspects of a Federation partner, its identity verification processes, and its credential management processes. This attribute defines eHealth Federation evaluation criteria/level for a Federation partner's credential management.
Business Value	Note: Currently not in use. This is because the management of credentials is covered in the Identity Provider Standard and the organization must meet the required standards in order to join the Federation as an Identity Provider.
URN <i>Format</i>	urn:ehealth:names:idm:attribute:CredentialManagementSchemeRef <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:CredentialManagementSchemeRef" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">AL2</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	AL2
Format	Coded Value for assurance level
Coded Values	AL1 AL2 AL3
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.3.4 IdentityProvider

Attribute Item	Detail
Description	The Federation Partner that authenticated the principal

Attribute Item	Detail
Business Value	This attribute provides information about who authenticated the principal. This attribute can be used in conjunction with the 'Asserting Party' attribute to determine how the principal was authenticated, i.e. what party sent the assertion and what party authenticated the principal. The 'Asserting Party' and 'Identity Provider' may be the same.
URN Format	urn:ehealth:names:idm:attribute:IdentityProvider urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:IdentityProvider" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:basic"><saml:AttributeValue xsi:type="xs:string">http://alicepractice.ca/idp</saml:AttributeValue></saml:Attrib ute>
Sample text value of attribute	Oid:24567.333.111.555.6 Or http://fedidp1.on.ca http://alicepractice.ca/idp
Format	Distinguished Name or OID:<value of OID> (the term "OID" is not case-sensitive) or URI
Coded Values	
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker. Prefix of "OID" or "DN" not validated.

8.3.5 IdentityVerificationSchemeRef

Attribute Item	Detail
Description	The eHealth Federation Evaluation Criteria define how eHealth establishes measures of the identity assurance-related aspects of a Federation partner, its identity

Attribute Item	Detail
	verification processes, and its credential management processes. This attribute contains the eHealth Federation evaluation criteria/level for a Federation partner's verification processes.
Business Value	This attribute allows a Delivery Channel to determine if a principal should be allowed to view PI and/or PHI or gain access to Applications that contain PI and/or PHI. In order to view PI and PHI, this attribute and the 'AuthenticationLevel' attribute (see section 8.3.2) must both be set to a value of AL2 or higher.
URN Format	urn:ehealth:names:idm:attribute:IdentityVerificationSchemeRef urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:IdentityVerificationSchemeRef" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">AL2</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	AL2
Format	Coded Value for assurance level
Coded Values	AL1 AL2 AL3
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Validate that this field is present. This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.3.6 ProtectedNetwork

Attribute Item	Detail
Description	This attribute is used to indicate if the user has been authenticated from a trusted network location (e.g. multi factor VPN, Corporate LAN). This attribute must not be treated as an additional authentication factor. The IDP must take into account whether the user is logging in from a protected network when calculating the AuthenticationLevel value.

Attribute Item	Detail
Business Value	Indicates if the user has been authenticated from a trusted network location.
URN <i>Format</i>	<code>urn:ehealth:names:idm:attribute:ProtectedNetwork</code> <code>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</code>
Sample in message format	<code><saml:Attribute Name="urn:ehealth:names:idm:attribute:ProtectedNetwork"</code> <code>NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-</code> <code>format:basic"><saml:AttributeValue</code> <code>xsi:type="xs:string">true</saml:AttributeValue></saml:Attribute></code>
Sample text value of attribute	True
Format	Coded Value
Coded Values	True False
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	This attribute and value is included ‘as-is’ in the SAML response generated by the Federation Broker.

8.4 Delegation Attributes

Note: Delegation attributes are currently not in use.

8.4.1 **GrantByDelegateMeritOnly**

Attribute Item	Detail
Description	States whether granting of permission is based only on the merits of the delegate. When this attribute is true, the default granting behaviour is altered. Denials based on anti-entitlements are still enforced, but grants are based only on the merits of the delegate. If the transaction is allowed, the Delegator is still used in the audit logs. When true, the following is the meaning 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.”

Attribute Item	Detail
Business Value	Note: Currently not in use
URN <i>Format</i>	urn:ehealth:names:idm:attribute:grantByDelegateMeritOnly <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<saml:Attribute Name="urn:ehealth:names:idm:attribute:grantByDelegateMeritOnly" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:basic"><saml:AttributeValue xsi:type="xs:string">false</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	True False
Format	String
Coded Values	True False (not case sensitive)
Mandatory?	No
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	This attribute and value is included ‘as-is’ in the SAML response generated by the Federation Broker.

8.4.2 OBO

Attribute Item	Detail
Description	The provider on whose behalf the request is being made. The “On Behalf Of” (“OBO”) attribute specifies the provider (typically an individual) on whose behalf the request is being made. An example is an administrative assistant retrieving a patient’s results in preparation for an appointment with a clinician. The “OBO” attribute identifies the clinician by their license (or UPI) number.
Business Value	Note: Currently not in use
URN <i>Format</i>	urn:ehealth:names:idm:attribute:OBO <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>

Attribute Item	Detail
Sample in message format	saml:Attribute Name="urn:ehhealth:names:idm:attribute:OBO" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">cpso:111222222:John Doe</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	CPSO:123445:John Doe
Format	Type:<number>:<Friendly Name>
Coded Values	Type is either UPI or <licensing authority name> - see list in section 11.1.
Mandatory?	No
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Federation Broker sends value as received by IDP (with or without Friendly Name).

8.5 Entitlement Attributes

8.5.1 Roles

Attribute Item	Detail
Description	Role(s) of the requesting provider. These are healthcare roles rather than application roles. Optional data element used to provide additional context information regarding the requesting provider.
Business Value	Note: Currently not in use
URN Format	urn:ehhealth:names:idm:attribute:Roles urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehhealth:names:idm:attribute:Roles" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:basic"><saml:AttributeValue xsi:type="xs:string">Nurse</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	Nurse

Attribute Item	Detail
Format	String
Coded Values	
Mandatory?	No
Multi Value Allowed?	Yes
IDP and/or Federation Broker (FB) Generated	FB
Federation Broker Processing	This attribute and value is included 'as-is' in the SAML response generated by the Federation Broker.

8.5.2 ServiceEntitlements

Attribute Item	Detail
Description	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.
Business Value	If a federated Delivery Channel uses the ONE ID Federation Authorization Service, the value of 'ServiceEntitlements' will provide the following information: • Whether a principal is authorized for a service • The Delivery Channel and Application(s) the principal is authorized for • Whether there are any attributes associated with the Delivery Channel/Application(s) • The legally responsible party sponsoring the user for access to the Delivery Channel/Application(s), in the form of a UPI The Delivery Channel may use this information to determine when the user may access it and under the authority of which organization.
URN Format	urn:ehealth:names:idm:attribute:ServiceEntitlements urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:idm:attribute:ServiceEntitlements" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">OLIS:UPI:1234</saml:AttributeValue></saml:Attribute><saml:A</pre>

Attribute Item	Detail
	<code><Attribute xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.1" Value="ODB:UPI:3333"/></code> <code></saml:Attribute></code> Additional <code><saml:AttributeValue></code> examples: User has access to CVD Delivery Channel only: <pre><saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.1" Value="CVD:UPI:999"/></pre> User has access to CVD Delivery Channel and OLIS: <pre><saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.1" Value="CVD:UPI:999"/> <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.2" Value="OLIS:UPI:999"/></pre> User has access to ClinicalConnect as a ProviderSupport under one organization and has no additional attributes: <pre><saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.1" Value="ClinicalConnect:UPI:999"/> <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.2" Value="ClinicalConnect- ProviderSupport:UPI:999"/></pre> User has access to ClinicalConnect as a ProviderSupport under one organization with CPSO numbers as additional attributes: <pre><saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.1" Value="ClinicalConnect:UPI:999"/> <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.2" Value="ClinicalConnect- ProviderSupport:UPI:999:CPSO:12345;23456"/></pre> User has access to ClinicalConnect as a Provider under two organizations: <pre><saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.1" Value="ClinicalConnect:UPI:999"/> <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.2" Value="ClinicalConnect- Provider:UPI:999"/> <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.3" Value="ClinicalConnect:UPI:888"/> <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.4" Value="ClinicalConnect- Provider:UPI:888"/></pre> User has access to ClinicalConnect as a Provider and Auditor under one organization: <pre><saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.1" Value="ClinicalConnect:UPI:999"/> <saml:AttributeValue xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Name="urn:oid:2.5.6.97.1.2" Value="ClinicalConnect-</pre>

Attribute Item	Detail
	Provider:UPI:999</saml:AttributeValue> <saml:AttributeValue xsi:type="xs:string">ClinicalConnect-Auditor:UPI:999</saml:AttributeValue>
Sample text value of attribute	User has access to CVD Delivery channel only: CVD:UPI:1234 User has access to CVD Delivery channel and OLIS: CVD:UPI:1234 OLIS:UPI:1234 User has access to ClinicalConnect as a ProviderSupport under one organization and has no additional attributes: ClinicalConnect:UPI:999 ClinicalConnect-ProviderSupport:UPI:999 User has access to ClinicalConnect as a ProviderSupport under one organization with CPSO numbers as additional attributes: ClinicalConnect:UPI:999 ClinicalConnect-ProviderSupport:UPI:999:CPSO:12345;23456 User has access to ClinicalConnect as a Provider under two organizations ClinicalConnect:UPI:999 ClinicalConnect-Provider:UPI:999 ClinicalConnect:UPI:888 ClinicalConnect-Provider:UPI:888 User has access to ClinicalConnect as a Provider and Auditor under one organization ClinicalConnect:UPI:999 ClinicalConnect-Provider:UPI:999 ClinicalConnect-Auditor:UPI:999 User has no service entitlements for this Delivery Channel in the Federation Authorization System: Not Authorized
Format	<ServiceName>:<UAO>:<Optional_attributes>

Attribute Item	Detail
	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 - 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 semi colons.
Coded Values	
Mandatory?	No
Multi Value Allowed?	Yes
IDP and/or Federation Broker (FB) Generated	Federation Broker
Federation Broker Processing	- If the user has service entitlements for the Delivery Channel being accessed in the Federation Authorization System, populate the ServiceEntitlements and UAO attribute statements with Delivery Channel, Application and UAO information as contained in the Federation Authorization Service. See format above. - If the organization is associated with an OID as well as a UPI, the OID will be provided in the UAO attribute value, not as part of the ServiceEntitlements attribute value - The service entitlement data populated in the SAML attribute statement

Attribute Item	Detail
	by the Federation Broker will be restricted to the Delivery Channel receiving the SAML assertion

8.5.3 UAO

Attribute Item	Detail
Description	This attribute specifies the legally responsible party for a given transaction. This organization must be a Health Information Custodian (HIC) as defined in PHIPA and defined in the Provider Registry. This attribute will contain an aggregate list of all the legally responsible parties sponsoring the user for access to the Delivery Channel. A default value of 'Not Authorized' will be used whenever the principal has not been approved for Delivery Channel access in the Federation Authorization Service.
Business Value	If a federated Delivery Channel uses the ONE ID Federation Authorization Service, and the principal has access to a service as specified in the Federation Authorization Service, the UAO value will provide information about the legally responsible party authorizing the user to access the Delivery Channel: • The UAO information will be in the format of a UPI and an OID (if available) • The friendly name of the organization/legally responsible party The Delivery Channel may use this information to provide a means for the user to specify which party he/she is acting under the authority of when using the Delivery Channel.
URN Format	urn:ehealth:names:idm:attribute:UAO urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:idm:attribute:UAO" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:basic"><saml:AttributeValue xsi:type="xs:string"> ORGANIZATION:upi:2000000000001:OID:1.1.1.1.1.1.:HospitalA</saml:AttributeVal ue> </saml:Attribute><saml:AttributeValue xsi:type="xs:string">PROVIDER:oid:3333.444.3322.1223:Jane Smith</saml:AttributeValue></saml:Attribute></pre>
Sample text value of attribute	Organization:UPI:1234566:OID:1.1.1.1.1.1.:HospitalA OR Organization:OID:24567.333.111.555.6:HospitalB OR Provider:CPSO:123445:John Doe

Attribute Item	Detail
	OR Provider:UPI:333344445555:Jane Smith OR Not Authorized
Format	The UAO attribute value contains an aggregate list of all UAOs for the user. Each UAO value contains colon-separated string values: <i><Type>:<Identifier Type>:Number:FriendlyName</i> Or <i><Type>:<Identifier Type>:Number:<identifier type>:Number:FriendlyName (if an organization or provider is identified by both a UPI and an OID)</i> Or 'Not Authorized' where • Type is a coded value: 'Organization' or 'Provider' • Identifier type: ○ For Organization – 'UPI' or 'OID' ○ For Provider – 'UPI' or licencing authority • Number: ○ Value for UPI, OID or licence number ○ If type is 'OID' then the number will be generated by eHealth Ontario and formatted according to the 'Object Identifier (OID) Management Policy' (owner: eHealth Standards Program) • Friendly name – Human readable name for the organization or individual that can be presented to the principal in a selection list.
Coded Values	See above.
Mandatory?	Yes
Multi Value Allowed?	Yes
IDP and/or Federation Broker (FB) Generated	FB
Federation Broker validation rules	• If the Delivery Channel being accessed cannot be found in the Federation Authorization System populate the ServiceEntitlements and UAO attribute statements with 'Not Authorized' • If the user is not authorized to access the Delivery Channel, populate the ServiceEntitlements and UAO attribute statements with 'Not Authorized' • If the organization is configured with both UPI and OID, include both

Attribute Item	Detail
	values in the UAO. - The service entitlements and UAO attributes are restricted to Delivery Channel or Application being accessed. - If the IDP sends a value in the UAO attribute, those values are ignored by the Federation Broker.

8.6 Patient Context Attributes

- Patient context attributes may be populated in an IDP Initiated Login Sequence when the user is view a patient from a POSA and clicks on a link to a Federated Delivery Channel.
- Patient context attributes will not be populated in an SP Initiated Login Sequence.

8.6.1 PatientContextID

Attribute Item	Detail
Description	This is the source system patient identifier. It can be either a MRN or JHN number. Will be populated when user is viewing patient record from a Point Of Service. If accessing DC directly then patient context is not available.
Business Value	Used, in conjunction with the other Patient Context attributes, to identify the patient the principal is viewing from the Point Of Service and to find the same patient in the destination Delivery Channel.
URN Format	urn:ehealth:names:patientcontext:attribute:PatientContextID urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">63344387</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	63344387
Format	Alphanumeric (value of either a MRN or JHN per the PatientContextIDType)
Coded Values	
Mandatory?	No. See 'Note' below.

Attribute Item	Detail
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	1. If PatientContextID is specified then PatientContextIDType is mandatory. 2. Value of PatientContextID will be included in the SAML Attribute statement by the Federation Broker as received. Note: If PatientContextID is specified, then the following attributes are also mandatory (PatientContextIDAuthority, PatientContextDOB, PatientContextGender, and PatientContextLastName).

8.6.2 PatientContextIDType

Attribute Item	Detail
Description	This is the source system patient identifier. It can be either MRN (Medical Record Number) or JHN (Jurisdictional Health Number). Will be populated when user is viewing patient record from Point Of Service. If accessing DC directly then patient context is not available.
Business Value	Used, in conjunction with the other Patient Context attributes, to identify the patient the principal is viewing from the Point Of Service and to find the same patient in the destination Delivery Channel.
URN Format	urn:ehealth:names:patientcontext:attribute:PatientContextIDType urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextIDType" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">JHN</saml:AttributeValue></saml:Attribute></pre>
Sample text value of attribute	MRN JHN
Format	MRN JHN
Coded Values	MRN

Attribute Item	Detail
	JHN
Mandatory?	No. Yes if PatientContextID is specified.
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	1. If PatientContextID is specified then PatientContextType is mandatory. 2. Value of PatientContextIDType will be included in the SAML Attribute Statement by the Federation Broker as received. Note: If PatientContextID is specified, then the following attributes are also mandatory (PatientContextIDAuthority, PatientContextDOB, PatientContextGender, and PatientContextLastName).

8.6.3 PatientContextIDAuthority

Attribute Item	Detail
Description	This attribute identifies the source identifier of the system that issued the patient context ID. If the PatientContextID is a MRN #, this value will be set to the OID of the issuing system. If the PatientContextID is a JHN, this value will be set to the health card authority; e.g., "CANON"
Business Value	Used, in conjunction with the other Patient Context attributes, to identify the patient the principal is viewing from the Point Of Service and to find the same patient in the current Delivery Channel.
URN Format	urn:ehealth:names:patientcontext:attribute:PatientContextIDAuthority urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextIDAuthority" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname- format:basic"><saml:AttributeValue xsi:type="xs:string">111.222.333.444.555.7</saml:AttributeValue></saml:Attribute >
Sample text value of attribute	111.222.333.444.555.7 CANON

Attribute Item	Detail
Format	If PatientContextIDType is MRN then specify the OID of the system that issued the PatientContextID value. If PatientContextIDType is JHN then specify the health card authority.
Coded Values	If PatientContextIDType is JHN, the following coded values for jurisdiction health card authorities are acceptable: CANON CANQC CANMB CANSK CANAB CANBC CANNF CANPE CANNB CANYT CANNS CANNT CANNU CAN If PatientContextIDType is MRN, then specify the OID of the system that issued the PatientContextID value See Note below
Mandatory?	No. Yes if PatientContextID is specified.
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	1. Mandatory if PatientContextID is specified. 2. Value of PatientContextIDAuthority will be included in the SAML Attribute Statement by the Federation Broker as received. Note: If PatientContextID is specified, then the following attributes are also mandatory (PatientContextIDAuthority, PatientContextDOB, PatientContextGender, and PatientContextLastName).

8.6.4 **PatientContextDOB**

Attribute Item	Detail
Description	Patient's date of birth.
Business Value	Used, in conjunction with the other Patient Context attributes, to identify the patient the principal is viewing from the Point Of Service and to find the same patient in the destination Delivery Channel.
URN <i>Format</i>	urn:ehealth:names:patientcontext:attribute:PatientContextDOB <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextDOB" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">1951-12-03</saml:AttributeValue> </saml:Attribute>
Sample text value of attribute	1960-01-01
Format	YYYY-MM-DD
Coded Values	
Mandatory?	No, unless PatientContextID is specified. See 'Note' below.
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	1. Mandatory if PatientContextID is specified. 2. Value of PatientContextDOB will be included in the SAML Attribute Statement by the Federation Broker as received. Note: If PatientContextID is specified, then the following attributes are also mandatory (PatientContextIDAuthority, PatientContextDOB, PatientContextGender, and PatientContextLastName).

8.6.5 **PatientContextGender**

Attribute Item	Detail
----------------	--------

Attribute Item	Detail
Description	Patient Gender.
Business Value	Used, in conjunction with the other Patient Context attributes, to identify the patient the principal is viewing from the Point Of Service and to find the same patient in the destination Delivery Channel.
URN <i>Format</i>	urn:ehealth:names:patientcontext:attribute:PatientContextGender <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextGender" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">M</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	M F U
Format	M F U
Coded Values	M for Male F for Female U for Unspecified
Mandatory?	No unless PatientContextID is specified. See 'Note' below.
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	1. Mandatory if PatientContextID is specified. 2. Value of PatientContextDOB will be included in the SAML Attribute Statement by the Federation Broker as received. Note: If PatientContextID is specified, then the following attributes are also mandatory (PatientContextIDAuthority, PatientContextDOB, PatientContextGender, and PatientContextLastName).

8.6.6 PatientContextLastName

Attribute Item	Detail
Description	Patient Last Name
Business Value	Used, in conjunction with the other Patient Context attributes, to identify the patient the principal is viewing from the Point Of Service and to find the same patient in the destination Delivery Channel.
URN <i>Format</i>	<code>urn:ehealth:names:patientcontext:attribute:PatientContextLastName</code> <code>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</code>
Sample in message format	<code><saml:Attribute</code> <code> Name="urn:ehealth:names:patientcontext:attribute:PatientContextLastName"</code> <code> NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"></code> <code> <saml:AttributeValue</code> <code> xsi:type="xs:string">Smith</saml:AttributeValue></saml:Attribute></code>
Sample text value of attribute	Smith
Format	String
Coded Values	
Mandatory?	No unless PatientContextID is specified. See 'Note' below.
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	1. Mandatory if PatientContextID is specified. 2. Value of PatientContextLastName will be posted in the SAML Response by the Federation Broker as received. Note: If PatientContextID is specified, then the following attributes are also mandatory (PatientContextIDAuthority, PatientContextDOB, PatientContextGender, and PatientContextLastName).

8.6.7 PatientContextFirstName

Attribute Item	Detail
Description	Patient first name
Business Value	Used, in conjunction with the other Patient Context attributes, to identify the patient the principal is viewing from the Point Of Service and to find the same patient in the destination Delivery Channel.
URN <i>Format</i>	<code>urn:ehealth:names:patientcontext:attribute:PatientContextFirstName</code> <code>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</code>
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextFirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">John</saml:AttributeValue></saml:Attribute></pre>
Sample text value of attribute	John
Format	String
Coded Values	
Mandatory?	No.
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Value of PatientContextFirstName will be included in the SAML Attribute Statement by the Federation Broker as received.

8.6.8 ContextSessionID

Attribute Item	Detail
Description	This attribute is a unique identifier assigned by the broker to identify a provider and that provider's session. This attribute enables providers and Delivery Channels to set and retrieve patient context information from the Context Management System (CMS). The CMS has been implemented to enable patient context information to be passed outside of SAML Responses. The current implementation with the use of SAML imposes constraints in that new patient context information cannot be injected within the same session.

Attribute Item	Detail
Business Value	Enables bi directional and distributed sharing of patient context. This enables a provider to move between applications without having to re-search for the patient.
URN	urn:ehealth:names:patientcontext:attribute:ContextSessionID
Format	urn:oasis:names:tc:SAML:2.0:attrname-format:basic
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:ContextSessionID" 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></pre>
Sample text value of attribute	3455-3334-4467-54637-3457
Format	String
Coded Values	No
Mandatory?	Yes
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	Federation Broker
Federation Broker Processing	The federation broker will generate this unique identifier on behalf of the provider and; • Add this identifier to the CMS. • Pass this identifier to each service provider the provider logs into. Service providers that consume the CMS can use the identifier to set and retrieve patient context information on behalf of a provider.

8.7 Clinical Context Attributes

8.7.1 ClinicalContextApplicationID

Attribute Item	Detail
Description	Identifier for the calling system, based on its pre-assigned OID
Business Value	Note: Currently not in use
URN Format	urn:ehealth:names:clinicalcontext:attribute:ClinicalContextApplicationID urn:oasis:names:tc:SAML:2.0:attrname-format:basic

Attribute Item	Detail
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextApplicationID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"><saml:AttributeValue xsi:type="xs:string">1.3.6.1.4.1.12201.999.101.1</saml:AttributeValue></saml:Attribute></pre>
Sample text value of attribute	1.3.6.1.4.1.12201.999.101.1
Format	String (OID value)
Coded Values	
Mandatory?	No
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Value of ClinicalContextApplicationID will be included in the SAML Attribute Statement by the Federation Broker as received.

8.7.2 ClinicalContextApplication

Attribute Item	Detail
Description	This is a plain text/English description of the software package used to generate the request message.
Business Value	Note: Currently not in use
URN <i>Format</i>	urn:ehealth:names:clinicalcontext:attribute:ClinicalContextApplication <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<pre><saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextApplication" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">Testing Medical Record Software</saml:AttributeValue></saml:Attribute></pre>
Sample text value of attribute	Testing Medical Record Software

Attribute Item	Detail
Format	String
Coded Values	
Mandatory?	No
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Value of ClinicalContextApplication will be included in the SAML Attribute Statement by the Federation Broker as received.

8.7.3 ClinicalContextLocalization

Attribute Item	Detail
Description	Language Preference
Business Value	Note: Currently not in use
URN <i>Format</i>	urn:ehealth:names:clinicalcontext:attribute:ClinicalContextLocalization <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextLocalization" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">Fr-CA</saml:AttributeValue> </saml:Attribute>
Sample text value of attribute	En-CA
Format	String
Coded Values	En-CA Fr-CA En-US
Mandatory?	No
Multi Value Allowed?	No

Attribute Item	Detail
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Value of ClinicalContextLocalization will be included in the SAML Attribute Statement by the Federation Broker as received.

8.7.4 ClinicalContextService

Attribute Item	Detail
Description	This is an identifier that provides additional context related to the information being requested, e.g. patient visit.
Business Value	Note: Currently not in use
URN <i>Format</i>	urn:ehealth:names:clinicalcontext:attribute:ClinicalContextService <i>urn:oasis:names:tc:SAML:2.0:attrname-format:basic</i>
Sample in message format	<saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextService" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic"> <saml:AttributeValue xsi:type="xs:string">Lab</saml:AttributeValue></saml:Attribute>
Sample text value of attribute	Lab
Format	String
Coded Values	
Mandatory?	No
Multi Value Allowed?	No
IDP and/or Federation Broker (FB) Generated	IDP
Federation Broker Processing	Value of ClinicalContextService will be included in the SAML Attribute Statement by the Federation Broker as received.

9.0 Sample Messages

9.1 SAML Request Message

The following is an example of a SAML request message.

```
<samlp:AuthnRequest xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://federationbroker.ehealthontario.ca/fed/idp/samlv2o" ID="id--tqGstormp2vq5aClhWcUdS1w5c-"
IsPassive="false" IssueInstant="2016-03-11T21:44:23Z" ProtocolBinding="urn:oasis:names:tc:SAML:2.0:bindings:HTTP-POST" Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity"></saml:Issuer>
    <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
      <dsig:SignedInfo>
        <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#"/>
        <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
        <dsig:Reference URI="#id--tqGstormp2vq5aClhWcUdS1w5c-">
          <dsig:Transforms>
            <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature"/>
            <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
          </dsig:Transforms>
          <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
          <dsig:DigestValue>0rZlI7AhQ9J/FNwYECUaj4uxzuk=</dsig:DigestValue>
        </dsig:Reference>
      </dsig:SignedInfo>
      <dsig:SignatureValue>nqXq8Rh5EqEwHFZVoDV+WJC1+d4Fzt1Gy61k+akvonNAuVTahxfkjK4TxGuX9WpEcjvlzJo2aSLb1NC3LG1cFv6AjLoMGbxtpSDsYOlsyboLKsVx1YRciqFVEgr9rWtDLapVn48tLEhyiAO
ouUuhkF+K+MXbHwoP+sWKGvhlE=</dsig:SignatureValue>
    <dsig:KeyInfo>
      <dsig:X509Data>
        <dsig:X509Certificate>MIIGCTCCBPGgAwIBAgIERvoJOjanBgkqhkiG9w0BAQUFADCBzETMBEGCGmSJomT8ixkArkWA3NzaDEbMBkGCgmSJomT8ixkArkWC3N1YnNjcmlhZXJzMURUeWYwYDVMQLEwxTU0ggU2VydmliZXMxEtAPBgNVBAsTCFNIY3VyaXRSMQwwCgYDVQQLEwNQSO0kxQzBBBgNVBAMTOiNTYXJOIFN5c3RlbXBMcGZm9yIEhlYWx0aCBBDZ2VuY3kgUm9vdCBDZDJXOaWZpY2F0ZSBBDXRob3JpdHkwHhcNMTAxMTA4MjE1NDMwWhcNMtUxMTA4MjlyNDMwWjCBkzETMBEGCGmSJomT8ixkArkWA3NzaDEbMBkGCgmSJomT8ixkArkWC3N1YnNjcmlhZXJzMURUeWYwYDVMQLEwxTU0ggU2VydmliZXMxDDAKBgNVBAsTA09JRjERMAGAA1UECxMIU2VydmljZXMxZjAlBgNVBAMTHnNzaG9pZjFhMDAwMS5laGVhbHRob250YXJpbjpy5jYTCBznANBgkqhkiG9w0BAQEFAAOBJQAawgYkCgYEAtkuXXYwrhTukllW8lf91LrFZBDct9SHkZ0qpaZF40Bzu7VYPye8MpJsk+m8U2dluUbw0B7OSixT/mdy6FdKan0dpdUlxiYuhclwxcLonu+ek288DqtI5AhDCah/d1YITBoeCuLAOWMM1QujmZP87ZrfJof8QlzPkOhhoOqgtzokCAwEAaOCAskwgGLFMASGA1UdDwQEAwIfFoDarBgNVHRAEJD AigA8yMDEwMTEwODIxNTQzMfQgBDzlMtMQWNTEwMDIYNDMwWjJARBgIghkgBhvChCAQEABAMCBaAwKQYJIYIZIAyb4QgECBBwWGmh0dHBzOi8vU0lURV9OQU1FL2NkYS1jZ2kvMEgGCWGSAGG+EIBAwQ7FjljbGlbnRJ2Z2kuZXhlp2FjdGlvb3JjaGVva1Jldm9jYXRpb24mJkNSTD1bj1DUkwXJnNlcmllbD0wggGZBGZBNVHR8EggGQMIIbJDCByqCBx6CBxBwTCBvjETMBEGCGmSJomT8ixkArkWA3NzaDEbMBkGCgmSJomT8ixkArkWC3N1YnNjcmlhZXJzMURUeWYwYDVMQLEwxTU0ggU2VydmliZXMxEtAPBgNVBAsTCFNIY3VyaXRSMQwwCgYDVQQLEwNQSO0kxQzBBBgNVBAMTOiNTYXJOIFN5c3RlbXBMcGZm9yIEhlYWx0aCBBDZ2VuY3kgUm9vdCBDZDJXOaWZpY2F0ZSBBDXRob3JpdHkwDTALBgNVBAMTBENSTDDEwbgbygbgmbgaGbGsNsZGFwOi8vY3JsLnNzaGEuY2EvY249U21hcnQUMzNm9y1TwSGVhbHRoJTlwQWdlbmN5JTIwUm9vdCUyMENlcnpZmljYXRlJTlwQXV0aG9yYXRS5G91PVBLS5xdvT1TZWN1cmI0eSxdvT1TU0glMIjBTZXJ2aWNlcyxkYz1zdWJzY3JpYmVycyxkYz1zc2g/Y2VydGlmaWNhdGVSZXZvY2F0aW9uTGZldAFBgNVHSMEGDAwGt6nBpn6X8UEayh4Pvc5gLQ9IHQBjAdBgNVHQ4EFgQUijK5HBVj4o/4HWjzmfx9kOyVMzYEWcQYDVROTBAlwADAZBgkqhkiG9n0HQQAEDDAKgRWNY4xAwiDqDANBgkqhkiG9w0BAQUFAAOCAQEAkdw29wnZv0UoB4Yj6dpdXkblLu/PfGyC+HpOGLZjgLEoUCun5W05qt+jRvCEp3snb1ASnfZStNNfzv70mzsFjshtmd/UCE7smaklj/tfxRFkhWzkWoREat36SHQSQSWE66Y1jp567/A+4uD8brlrlooAshewKoQU8DGkuZWp/TPCIHdhETmW+sQmZ/ngUCAXW2gdgKHYZca21i+3fa6tNLcW87MCHKfJvcH/p7HTeHqeMaGYBPBarPad0SyMO+1DPKFf/xGTZVKVI62XE304P5TPs+jSp6hLQHRS759E/XrHmPICZ5MP6X+5250+T0vh8Zuw69kH+CetUrS73A0IQ==</dsig:X509Certificate>
      </dsig:X509Data>
    </dsig:KeyInfo>
  </saml:Issuer>
</samlp:AuthnRequest>
```

```
</dsig:KeyInfo>
</dsig:Signature>
<samlp:NameIDPolicy AllowCreate="true" Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified"/>
<samlp:RequestedAuthnContext>
  <saml:AuthnContextClassRef xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion"> urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
</samlp:RequestedAuthnContext>
</samlp:AuthnRequest>
```

9.2 SAML Response Message

The following is an example of a SAML response message.

Note: /samlp:Response[@InResponseTo] is only present if the SAML response is sent in response to a SAML request. The value of InResponseTo must match the corresponding /samlp:AuthnRequest[@ID] value.

```
<samlp:Response xmlns:saml="urn:oasis:names:tc:SAML:2.0:protocol" Destination="https://federation.ehealthontario.ca/fed/sp/authnResponse20" ID="id-pEcdB4-sq-FoH4hWDMuzQwG26V4-"
InResponseTo="id-SQYEQ96Gss0914WLUY26J5nDbq8-" IssueInstant="2016-05-22T19:29:54Z" Version="2.0">
  <saml:Issuer xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" Format="urn:oasis:names:tc:SAML:2.0:nameid-format:unspecified">https://federation.ehealthontario.ca/fed/idp</saml:Issuer>
  <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
    <dsig:SignedInfo>
      <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <dsig:Reference URI="#id-pEcdB4-sq-FoH4hWDMuzQwG26V4-">
        <dsig:Transforms>
          <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </dsig:Transforms>
        <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <dsig:DigestValue>8vIlVH9/RI/CepKXvzjwFDM1UqU=</dsig:DigestValue>
      </dsig:Reference>
    </dsig:SignedInfo>
    <dsig:SignatureValue>Jhiyq50fh1Keqf/uef1yvHjHOwl4s+vvQOfil/051SnVuvNRxPHiQed6Cby5FBdUm9a+MCNHZ9iPp6TOXQbTrWKzTOzkFefNTc/LBAFWmnQFiNFAgsCphQRoH5kTD3KDKphHj/GYdPRU8zhPk
XP9DYEtGmd44Q4buXaa60RIf0g=</dsig:SignatureValue>
    <dsig:KeyInfo>
      <dsig:X509Data>
        <dsig:X509Certificate>MIIGCTCCBPGgAwIBAgIERvoJOjANBgkqhkiG9w0BAQUFADCBzETMBEGCgmSJomT8ixkArkWA3NzaDEbMBkGCgmSJomT8ixkArkWC3N1YnNjcmlhZlZlMRUwEwYDVQQLEwxtU0ggU2
VydmljZXMxETAPBgNVBAsTCFNIY3VyaXR5MQwwCgYDVQQLLEwNQS0kxQzBBBgNVBAMTOiNtYXJ0IFN5c3RlbXMgZm9yIUhYwX0aCBBDZ2VvY3kgUm9vdCBDZDJ0aWZpY2F0ZSBBDXRob3JpdHkwHhcNMTA4MjE1N
DMwWWhcNMTUxMTA4MjlyNDMwWjCBKzETMBEGCgmSJomT8ixkArkWA3NzaDEbMBkGCgmSJomT8ixkArkWC3N1YnNjcmlhZlZlMRUwEwYDVQQLLEwxtU0ggU2VydmljZXMxETAPBgNVBAsTCFNIY3VyaXR5MQwwCgYDVQQLLEwNQS0kxQzBBBgNVBAMTOiNtYXJ0IFN5c3RlbXMgZm9yIUhYwX0aCBBDZ2VvY3kgUm9vdCBDZDJ0aWZpY2F0ZSBBDXRob3JpdHkwDTALBg
NVBAMTBENSTDEwgbygbmggBaGgbNsZGFwOi8vY3J5LnNzaGEuY2EvY249U21hcnQlMjBtEXNOZWV1ZTlwZm9yYjIwSGVhbHROJTIwQWdlbmN5JTlwUm9vdCUyMENicnRpZmlyYXRlJTIwQXV0aG9yaXR5LSG91PVBLSXsvdT
1TZWN1cm0eSxvdT1TU0glMjBtZXJ2aWVhZm9wY3JpYmVycyYz1zd2g/Y2VydGlmaWVhdGV5ZSZvY2F0aW9uTGZzdDAfBgNVHSMEGDAAWgBT6nBpn6X8UEayh4PvC5gLU9lHQBJAdBgNVHQ4EFgQUJk5HBVj4o/
4HWJmzfx9kOyVMzYEWcQYDVROTBAlwADAZBgkqhkiG9w0HQQAEDDAKGwRWNY4AwIdQdANBgkqhkiG9w0BAQUFAAOCAQEAKdw29wnZv0UoB4bYj6dpzXKjBLu/PfGyC+HpOGLZjgLEoUCun5W05qt+jRvCEp3snb1AS
nfzStNNfZv70mzsFjshtmd/UCe7smakJk/tfxRFkHwzKWOrEAT36SHQQSWE66Y1jpS67/A+4uKD8brllooAshewKoQU8DGkuZwp/TPCIHdhETmW+sQmZ/ngUCAXW2gdgKHYZcA21i+3fA6tNLcW87MCHkfJvcH/p7HTeHqeM
aGYBpBARPad05yMO+1DPKff/xGtVZKVI62XE304PSTp+jSp6hLQIHR7S9E/XrHmPICZ5Mp6X+5250+T0vH8Zuw69kh+jCetUrS73AOIQ=</dsig:X509Certificate>
      </dsig:X509Data>
    </dsig:KeyInfo>
  </dsig:Signature>
</samlp:Response>
```

```
<samlp:Status>
  <samlp:StatusCode Value="urn:oasis:names:tc:SAML:2.0:status:Success"/>
</samlp:Status>
<saml:Assertion xmlns:saml="urn:oasis:names:tc:SAML:2.0:assertion" ID="id-iqG5nJDr1AmZoKHB27VAMn4-vzA-" IssueInstant="2016-05-22T19:29:54Z" Version="2.0">
  <saml:Issuer Format="urn:oasis:names:tc:SAML:2.0:nameid-format:entity">https://federation.ehealthontario.ca/fed/idp</saml:Issuer>
  <dsig:Signature xmlns:dsig="http://www.w3.org/2000/09/xmldsig#">
    <dsig:SignedInfo>
      <dsig:CanonicalizationMethod Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
      <dsig:SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1" />
      <dsig:Reference URI="#id-iqG5nJDr1AmZoKHB27VAMn4-vzA-">
        <dsig:Transforms>
          <dsig:Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signature" />
          <dsig:Transform Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
        </dsig:Transforms>
        <dsig:DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1" />
        <dsig:DigestValue>yKkEZSwJnH4N6SCnHr0R2nce+bE=</dsig:DigestValue>
      </dsig:Reference>
    </dsig:SignedInfo>

    <dsig:SignatureValue>WsZX7kSJ4VP6fxYx41rUcoNCxDNWXAQOez+Q3RIMdYmMdcj5LSLb9Deazv7ih/LjrlR5JnfLJ8mdrXxEQk4wH7F2jNHAFFJeZkKf1j//x1cpK8RDExVdz4rKqi73BgILK2IrN/lurYyU0qgpaiErl3Yh/ODbyO9+dL8AMkf=</dsig:SignatureValue>
    <dsig:KeyInfo>
      <dsig:X509Data>

        <dsig:X509Certificate>MIIGCTCCBPGGAWiBAGlERvoJOjANBgkqhkiG9w0BAQUFADCBzETMBEGCgmSjomT8ixkArkWA3NzaDEbMBkGCgmSjomT8ixkArkWc3N1YnNjcmlhZlZjMRUwEwYDVQQLEwxtU0ggU2VydmljZXMxETAPBgNVBAsTCFNIY3VyaXR5MQwwCgYDVQQLEwNQS0kxQzBBBgNVBAMTOiNTYXJ0IFN5c3RlbXMGZm9yIEhlYWx0aCBBZ2VuY3kgUm9vdCBDZXJ0aWZpY2F0ZSBBDXRob3JpdHkwHhcNMTA4MTA4MTA0MjYyZDlmZjYXRpb24mJkNSTD1jb1JDUkwXJnNlcmlihbD0wggGZBgNVHR8EggGQMIIlBjDCByqCBx6CBxKSbWTCBvjETMBEGCgmSjomT8ixkArkWA3NzaDEbMBkGCgmSjomT8ixkArkWc3N1YnNjcmlhZlZjMRUwEwYDVQQLEwxtU0ggU2VydmljZXMxETAPBgNVBAsTCFNIY3VyaXR5MQwwCgYDVQQLEwNQS0kxQzBBBgNVBAMTOiNTYXJ0IFN5c3RlbXMGZm9yIEhlYWx0aCBBZ2VuY3kgUm9vdCBDZXJ0aWZpY2F0ZSBBDXRob3JpdHkwDTALBgNVBAMTBENSTDEwgbgmbggbaGgbNsZGFwOi8vY3JSLnNzaGEuY2EvY249U21hcnQlMjBtEXNOZW1zJTlwZm9yJTIwSGVhbHROJTIwQWdlbmN5JTlwUm9vdCUyMENlcncpZm9yYXR5XSR5LGR1PVBLSSxvdT1TZWN1cmI0eSxvdT1TU0glMjBTZjZjZWJzY3JpYmVycyYz1zc2g/Y2VydGlnYWVhbnR5ZGVzZXZvY2F0aW9uTGlzdDAfBgNVHSMEGDAGwBT6nBpn6X8UEayh4PvC5gLLQ9IHQBjAdBgNVHQ4EFgQUJk5HBVj4o/4HWJmzfx9koYVMzYEWcQYDVR0TBAIwADAZBgkqhkiG9w0HQQAEDDAKGwRWNY4AwIdQDANBgkqhkiG9w0BAQUFAAOCAQEAKdw29wnZv0UoB4byJ6dpzXKjBLu/PfGyC+HpOGLZjgLEoUCun5W05qt+jRvCEp3snb1ASnfzStNNfZv70mzsFjshtmd/UCE7smakJk/tfxRfKHwzKWOrEAt36SHQQSWE66Y1jpS67/A+4uKD8brllooAshewKoQU8DGkuZwp/TPCIhDhETmW+sQmZ/ngUCAXW2gdgKHYZcA21i+3fA6tNLcW87MCHkfJvcH/p7HTeHqeMaGYBpBARPad0SyMO+1DPKf/xGtVZKVI62XE304P5TPs+jSp6hLQlHR7S9E/XrHmPICZ5Mp6X+5250+T0vH8Zuw69Kh+jCetUrS73AOIQ=;</dsig:X509Certificate>
      </dsig:X509Data>
    </dsig:KeyInfo>
  </dsig:Signature>
</saml:Subject>
  <saml:NameID Format="urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified">5439584390fc589459</saml:NameID>
  <saml:SubjectConfirmation Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
    <saml:SubjectConfirmationData InResponseTo="id-SQYEQ96Gss0914WLUY26JSnDbq8-" NotOnOrAfter="2016-05-22T19:34:54Z"
Recipient="https://federationbroker.ehealthontario.ca/fed/sp/authnResponse20"/>
  </saml:SubjectConfirmation>
</saml:Subject>
<saml:Conditions NotBefore="2016-05-22T19:29:54Z" NotOnOrAfter="2016-05-22T19:34:54Z">
  <saml:AudienceRestriction>
```

```

        <saml:Audience>https://federationbroker.ehealthontario.ca/fed/sp</saml:Audience>
    </saml:AudienceRestriction>
</saml:Conditions>
<saml:AuthnStatement AuthnInstant="2014-06-22T19:29:54Z" SessionIndex="id--4nhV3tKVoLRfEU3ZalWrP-BFak-" SessionNotOnOrAfter="2014-06-22T20:29:54Z">
    <saml:AuthnContext>
        <saml:AuthnContextClassRef>urn:oasis:names:tc:SAML:2.0:ac:classes:PasswordProtectedTransport</saml:AuthnContextClassRef>
    </saml:AuthnContext>
</saml:AuthnStatement>
<saml:AttributeStatement xmlns:x500="urn:oasis:names:tc:SAML:2.0:profiles:attribute:X500" xmlns:xs="http://www.w3.org/2001/XMLSchema"
xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:IdentityVerificationSchemeRef" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">AL2</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:IdentityProvider" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">OID:1.3.6.1.4.1.12201.1</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextApplicationID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">111.222.444.5</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextLastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">Smith</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:ProtectedNetwork" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">false</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:FirstName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">Tom</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:grantByDelegateMeritOnly" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">false</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextLocalization" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">En-CA</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:UAO" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">Organization:UPI:3424243324;OID:1.3.6.1.4.1.12201:HospitalA</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">Provider:UPI:5443535435435:John Doe</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:ServiceEntitlements" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">OLIS:UPI: 3424243324</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">CVD:UPI: 3424243324</saml:AttributeValue>
        <saml:AttributeValue xsi:type="xs:string">CVD:UPI: 5443535435435</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:idm:attribute:PrincipalFedKey" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">123456abcd</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextIDType" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
        <saml:AttributeValue xsi:type="xs:string">MRN</saml:AttributeValue>
    </saml:Attribute>

```

```

<saml:Attribute Name="urn:ehealth:names:idm:attribute:CredentialManagementSchemeRef" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">AL2</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:DisplayName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">Smith, Tom</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:Roles" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">Nurse</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextGender" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">M</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:AssertingParty" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">federation.ehealthontario.ca</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:UserLoginName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">TOM.SMITH@ONEID.ON.CA</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:LastName" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">Smith</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:rid" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">COTO:2234567</saml:AttributeValue>
  <saml:AttributeValue xsi:type="xs:string">CPSO:1234567</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextService" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">LAB</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:Email" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">tom.smith@gmail.com</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextID" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">12314132421</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:OBO" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">CPSO:123445</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:idm:attribute:AuthenticationLevel" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">AL2</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:clinicalcontext:attribute:ClinicalContextApplication" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">Meditech</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextDOB" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">1970-01-01</saml:AttributeValue>
</saml:Attribute>
<saml:Attribute Name="urn:ehealth:names:patientcontext:attribute:PatientContextIDAAuthority" NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-format:basic">
  <saml:AttributeValue xsi:type="xs:string">1122.3344.5555.6</saml:AttributeValue>
</saml:Attribute>

```

```
        </saml:AttributeStatement>
    </saml:Assertion>
</samlp:Response>
```

10.0 Glossary

10.1 General Concepts

Term	Definition
AL1, AL2, AL3	Assurance Level 1, 2, and 3, respectively
Artifact Resolution Protocol	Some browsers may limit the number of URL characters they can handle. The SAML Browser Artifact profile accommodates this by transmitting data using a compact reference to an assertion, called an artifact, instead of sending the full assertion. The recipient of the artifact then uses an artifact resolution protocol to obtain the full assertion referred to by the artifact. In SAML 2.0, the HTTP Artifact Binding provides a framework for the embedding and transport of artifacts under real-world communication protocols. Note that the SAML Browser Artifact profile is not currently implemented in the Federation Broker.
Asserting Party	The party that issues the SAML Token. In most cases this will be the Identity Provider.
Binding	Binding are sets of conventions for invoking code. They are identified by a URL. In the context of this document, the 'binding' elements are defined by SAML 2.0. SAML 2.0 provides a framework for embedding and transporting SAML protocol messages. Bindings define the standard way that SAML request and response messages are transported between the issuing authorities and relying parties by providing mappings between SAML messages and standard communication protocols. For example, one defined transport mechanism for SAML requests and responses over HTTP is Simple Object Access Protocol (SOAP). This enables the exchange of SAML information across several Web services in a standard manner. Other common types of binding elements in this document are: HTTP Post, HTTP Redirect
CR	Client Registry: repository for the Identity and Personal Characteristics data of all people who have received health services in Ontario. It also includes all Ontario residents covered by OHIP.
Delivery Channel	A Delivery Channel is an organization with a portal that may be accessed as a service or may provide access to Applications provided by service owners. The eHealth Ontario Portal is a Delivery Channel as users can access Applications through https://www.ehealthontario.ca/ . Cancer Care Ontario (CCO) and Ontario Telemedicine Network (OTN) are Delivery Channels as they host portals that provide access to their own Application. The Ottawa Hospital (TOH) Portal is a Delivery Channel as it hosts eHealth Ontario portlets such as the OLIS Practice Lab

Term	Definition
	Results Viewer and Client Selector. Each Delivery Channel must sign a Portal Services Agreement. There will be an onboarding process for Delivery Channels to establish the trust relationship between the Delivery Channel and the Federation Broker.
Federated Service	This is a Delivery Channel (e.g. a portal) or Application (e.g. a portlet) that can be accessed by any Registrant who is enrolled for that Federated Service and who has an account with an IDP that is a member of Federation. An Application will only be accessible through a Delivery Channel that is also a member of Federation.
HIS	Hospital Information System
HTTP Redirect	A type of response whereby a Web Server provides to a client browser instructions to access a new URL upon receipt of that response.
HTTP Post	A type of request supported by SAML 2.0 binding conventions. See the definition of "binding" above. For example, this type of request might be sent when a user is completing a web form. The SAML Browser POST profile sends a full assertion from an Identity Provider to a Delivery Channel without the use of an artifact. The Federation Software sends the assertion to the user's browser as a hidden variable in the HTML form, and the browser then posts the assertion to the destination site.
Identity Federation	Identity Federation is the linking of two or more accounts a principal may hold with one or more Identity Providers or Delivery Channels within a given circle of trust.
Identity Provider	An Identity Provider is responsible for managing, authenticating, and asserting a set of identities within a given circle of trust. IDPs provide accounts to users that may be used to access Delivery Channels through POSAs such as HISes or Applications available through Delivery Channels.
Name Identifier Profiles	Name Identifier Profiles define how providers communicate with each other when one of the providers wishes to update the name identifier assigned to one of their common users. These profiles allow a Delivery Channel or Identity Provider to specify (or register) a <i>name identifier</i> for a principal. Peer providers, for their part, must use this name identifier when communicating with other providers about the principal.
POSA	Point of Service Application. A launch point to a Delivery Channel. The source of patient context. Examples of POSAs are hospital information systems and electronic medical record systems.
PR	Provider Registry: repository containing an enumeration of all Health Care Organisations and Providers (Identity, Personal Characteristics and Professional Roles) and the associations between them

Term	Definition
Principal	A Principal is a person (a "user"), a corporation, or a system entity whose identity can be authenticated. For the purpose of this specification a Principal will be used to describe or identify a Health Care Provider Person.
SAML	Security Assertions Markup Language (SAML), a standard developed by OASIS, provides a means for exchanging security information between online business partners. In a typical exchange of SAML messages between two parties, one party acts as a Relying Party (Delivery Channel) while the other acts as an Asserting Party.
SAML Profile	A profile describes how SAML assertions are embedded into and extracted out of standard frameworks and protocols. Web browser profiles for single sign-on and SOAP profiles for securing SOAP payloads are some of the available profiles.
Service	Applications that can be accessed through Delivery Channels.
Service Owner	These are organizations that manage Delivery Channels/Applications and make these available to healthcare professionals in Ontario. eHealth Ontario is an example of a Service Owner, providing Applications such as DPV and OLIS. Other Service Owners include CCO, OTN and UHN.
Service Provider	A service provider provides services or goods to a Principal while relying on an Identity Provider to authenticate the Principal's identity. A service provider is also referred to as a Relying Party (SAML) or a destination domain. From the domain perspective, a service provider contains the resource that users from source domains wish to access. A Delivery Channel is a Service Provider and may be either the end point or may provide access to more than one Application.
SOAP	SOAP (Simple Object Access Protocol) is a set of conventions for invoking code using XML and HTTP. It is identified by a URL.
SSO Protocol	Single Sign-On of multiple related but independent software systems. A user logs in once and gains access to all the systems without being prompted to log in multiple times.

11.0 Appendix

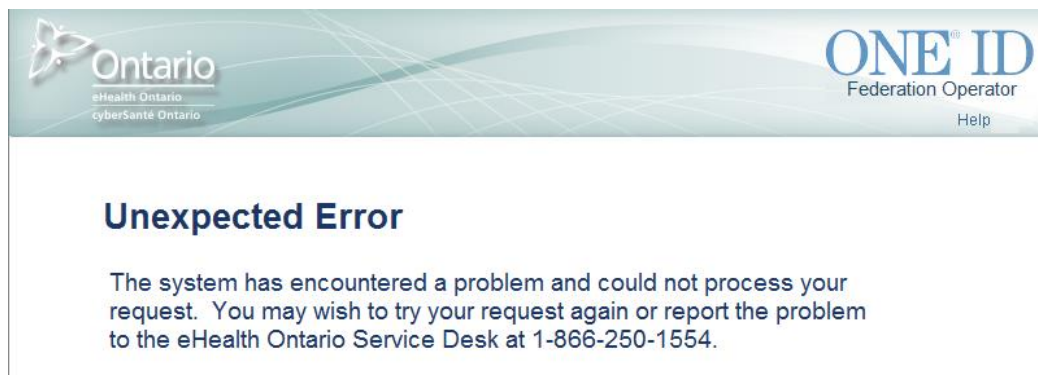
11.1 List of Valid Licensing Authorities

Licensing codes used to identify the authority indicated when specifying values for the UAO, RID, and OBO attributes of the SAML attribute statement.

Code (MOH)	Description
BDDT-N	Board of Regents, Board of Directors of Drugless Therapy-Naturopathy
CASLP	College of Audiologists and Speech-Language Pathologists of Ontario
CDHO	College of Dental Hygienists of Ontario
CDEO	College of Denturists of Ontario
CDIO	College of Dietitians of Ontario
CDTO	College of Dental Technologists of Ontario
CMLTO	College of Medical Laboratory Technologists of Ontario
CMO	College of Midwives of Ontario
CMRTO	College of Radiation Technologists of Ontario
CMTO	College of Massage Therapist of Ontario
CNO	College of Nurses of Ontario
CCDO	College of Chiropodists of Ontario
COTO	College of Occupational Therapists of Ontario
CRTO	College of Respiratory Therapists in Ontario
CTCMPAO	College of Traditional Chinese Medicine Practitioners and Acupuncturists of Ontario.
OCPh	Ontario College of Pharmacists
OCSWSSW	Ontario College of Social Workers and Social Service Workers
RCDSO	Royal College of Dental Surgeons of Ontario
TCCHO	Transitional Council of the College of Homeopaths of Ontario
TCCKO	Transitional Council for the College of Kinesiologists of Ontario
TCCPO	Transitional Council of the College of Psychotherapists of Ontario
CPYO	College of Psychologists of Ontario
CPSO	College of Physicians and Surgeons of Ontario
CPHO	College of Physiotherapists of Ontario
CONO	College of Opticians of Ontario
CCO	College of Chiropractors of Ontario
COPO	College of Optometrists of Ontario

11.2 SAML Validation Error Messages

The following error message is displayed by the Federation Broker to the user if the SAML Response from the Identity Provider fails the standard validation check, or if the SAML request from the DC fails validation:



The following error message is displayed by the Federation Broker to the user if any of the attributes or attribute values in the attribute statement of the SAML Response from the Identity Provider fails validation:

Access to this service cannot be granted as the organization that issued your account, i.e. provided you with your username and password, has sent the following information incorrectly:

- *[attribute name]*

Please contact your organization for assistance and provide them with the information above.

11.3 Delivery Channels in the ONE ID Federation

A Delivery Channel is an organization with a portal that may be accessed as a service in itself or provide access to Applications provided by service owners.

11.3.1 Responsibilities

Item	Function	Details	Reference
SP_1	Sign Agreement	The Delivery Channel Services Agreement/Schedule must be signed.	
SP_2	Determine the IDPs of the Delivery Channel's user base Note: The DC cannot specify which particular IDPs will be allowed to assert the identities of users accessing it. All IDPs in the Federation may be used.	Determine which organizations the users of the Delivery Channel will be from: • Work with eHealth to define IDPs for DC • If IDPs are not part of the Federation, eHealth will follow onboarding procedures to add IDP and set up as a Federated IDP • If organizations are not IDPs, work with eHealth to use the ONE ID IDP	
SP_3	Define Authorization rules	The service owners of Delivery Channels are responsible for determining who may access them: • Define business rules to approve or reject an individual's request to access a DC • Define what entitlements are required for their DC • Based on those entitlements and how and where they are defined, requests to access the DCs may be permitted or denied. • Decide, in conjunction with ONE ID and based on the DC's requirements and Federation Broker integration requirements, if the DC will use the ONE ID Federation Authorization service; if so, the entitlements for a user will be included in the attribute statement of the SAML Response. The DC must take the values specified for the ServiceEntitlements and UAO attributes into account when deciding whether the user is authorized to access the DC or not.	See section 3.3 '<i>ONE ID Federation Authorization Service</i>' See section 8.5 '<i>Entitlement Attributes</i>'

Item	Function	Details	Reference
		- Ensure local consent management rules are followed when displaying patient data to the user - Note: This is dependent on how patient consent has been implemented with the Delivery Channel. - Some Delivery Channels may have 'Terms of Use' which specify criteria that must be met by the user (principal) before patient data may be accessed.	
SP_4	Complete SAML Configuration	Set up the trust relationship between the Delivery Channel and ONE ID: - This begins with exchanging 'metadata' which contains information that is needed to set up cross-domain trust - Information exchanged in the metadata include the SAML protocol, entity ID and signing and encryption PKI certificates - This must be performed in each environment, for example, development, QA, pre-production, production and post-production (partner)	See section 5.0 'SAML Configuration'
SP_5	Update SAML Version	Stay within n-1 versions of the most current eHealth Ontario SAML Specification. Each new eHealth Ontario SAML Specification will be valid for a minimum of at least 6 months.	
SP_6	Provide Access Point	Provide an access point that can be used by users to navigate directly to the Delivery Channel. The portal may also be the service or the user may access Applications from within the portal	See step 1 in section 4.1.1 'SP Initiated Login Steps' See step 6 in section 4.2.1 'IDP Initiated Login Steps'
SP_7	Send SAML Request in an SP initiated process	The DC must generate a SAML Request when the access point is requested by the user. - When a user requests this access point, this resource will issue a SAML request and redirect the user to the Federation Broker single sign on service location. The SAML request will be included as post data in this user redirection. - From the user's point of view, the user will be redirected to the Federation Broker IDP selection page. The user will then select an IDP and authenticate with that IDP.	See section 6.0 'SAML Authentication Requests' See step 2 in section 4.1.1 'SP Initiated Login Steps'
SP_8	Receive SAML Response from Federation Broker (FB)	The Delivery Channel will provide an assertion consumer service that will accept a SAML Response generated by the ONE ID Federation Broker. The SAML response will be included as post data in the user request to the assertion consumer service. The Delivery Channel is to validate elements based on current eHealth Ontario SAML Specification version Steps include validation of:	See section 7.2 'SAML Response from Federation Broker to Delivery'

Item	Function	Details	Reference
		• Issuer • Digital signature • Time frame of response • Unique name identification (NameID) • Status Code • Attributes and values: Validate that the attributes contain valid values according to the current version of the eHealth Ontario SAML specification.	<i>Channel'</i> See section 7.3 'Main Elements of SAML Response Assertion' See section 8.0 'SAML Response Assertion Attribute Statements' See step 6 and 7 in section 4.1.1 'SP Initiated Login Steps' See step 14 in section 4.2.1 'Identity Provider Initiated Login Steps'
SP_9	Session Management	Logout: DCs must provide two options for logout. The first is a 'local logout': • When a user logs out from the DC then the DC invalidates the user's local session. The user is not be logged out of the Federation Broker session. • If the user logs into the DC again, the user does not need to log in again if the Federation Broker session has not timed out. The second is a 'global logout': • When a user logs out from the DC then the DC invalidates the user's local session. The DC then redirects the user to the URL https://federationbroker.ehealthontario.ca/fed/user/logout?globalslo=false to invalidate the Federation Broker's user session. Note that an applicable 'returnurl' can be specified by the DC. • If the user logs into the DC again, the user does not need to log in again if the IDP SSO session has not timed out.	

Item	Function	Details	Reference
		Note: There is a provincial review of the logout functionality currently underway which is likely to result in changes to the logout process. This document will be updated to reflect those changes once the review has completed. That new logout functionality may require DCs to provide a Single Logout Service in case the Federation Broker needs to log users out from all DCs that have been opened in the session. Timeout: • If the Federation Broker session times out, but the DC session is still active, the user may continue to use the DC • If the DC session times out and the Federation Broker session is still active, the user will not need to actively log in again to access the DC • If both the DC and Federation Broker session time out, but the IDP session is still active, the user will be required to complete the Federation Broker IDP selection page and choose the same IDP in order to access the DC again • If the DC session, Federation Broker session and IDP session all time out, the user will need to log in again (i.e., choose the IDP on the Federation Broker IDP selection page and authenticate with the IDP) • If the Delivery Channel receives the SAML response after the SAML request timeout, the user will need to log in again. The SAML Response will be considered to be invalid. Bookmarks: • If the user bookmarks a page or resource that is part of the login flow and that is not the access point described in SP_4 and SP_5, the DC will redirect the user to an error page if the user attempts to go directly to the bookmarked page/resource • If the user bookmarks a page or resource that should only be accessible to a fully authenticated user, the DC should redirect the user to the start of the login process (possibly the access point described in SP_4 and SP_5) if the user has not authenticated and attempts to go directly to the bookmarked page/resource Outages: • If DC is not available due to an outage, the user should see a user-friendly, meaningful error message when the user attempts to access the DC Audit: • DCs to capture all user transactions: ○ Functions ○ Time and Date ○ Data accessed • DCs will log the following for audit and troubleshooting	

Item	Function	Details	Reference
		purposes: ○ SAML requests sent to the Federation Broker ○ SAML responses received from the Federation Broker (including the decrypted assertion) ○ Any errors encountered in the generating of the SAML request and the parsing, decryption, validation, processing, etc. of the SAML response with sufficient detail to allow determination of the cause of the error • Audit and log data will be retained for the period specified in the Delivery Channel Services Agreement/Schedule.	
SP_10	Support Single Sign-On	Single Sign On to multiple DCs: • Applies to an integration in which users are expected to access more than one Delivery Channel by logging in only once: ○ Delivery Channel A → Delivery Channel B → Delivery Channel C ○ Delivery Channel C → Delivery Channel B ○ Delivery Channel C → Delivery Channel A ○ Etc. Provide links to facilitate the access of users from their Delivery Channel to other Delivery Channels.	
SP_11	Implement Just-In-Time Account Provisioning	It is expected that most DCs will implement the following just-in-time provisioning functionality that will be executed upon receipt of a SAML response from the Federation Broker, and once the SAML response has been successfully parsed, decrypted and validated: 1. Determine if a SAML assertion has been received for the same NameID previously: • If yes, go to step 2 • If no, go to step 3 2. If the DC stores a copy of the user data contained in the SAML attribute statement, update the user data if needed (just-in-time update) and go to step 4 3. If the DC stores a copy of the user data contained in the SAML attribute statement, create a user record (just-in-time creation) and go to step 4 • The DC may choose to link the Federated user (as identified by the NameID) to a local user at this time; e.g., by requiring the user to log in with his/her local credentials, by using the Identity attributes identified (such as those included in §8.2) to identify the local user, etc. 4. Log the user in, create the DC session, and redirect the user to the appropriate page/resource. The functionality described above may be customized to meet the	See section 8.2 'Identity Attributes'

Item	Function	Details	Reference
		specific needs of the DC and the specific integration requirements with the Federation Broker.	
SP_12	Define use of authentication attributes to access PI/PHI data	The Delivery Channel will define criteria to access PI/PHI as one or more of the following. - Asserting Party is as expected. - Authentication Level = AL2 or higher AND IdentityVerificationSchemeRef = AL2 or higher	See section 8.3 'Authentication Attributes'
SP_13	Define use of Delegation attributes (Optional)	The DC will define whether users may delegate access and authorization to other users. If so, the DC will grant access upon login based on the following delegation-related attributes in the SAML attribute statement: - If the value of GrantByDelegateMeritOnly is true, this means that the user (delegate) needs to be authorized for access to the DC and authorization of the delegator is not sufficient to determine that the user is authorized for access. They may act as a delegate to another, but they need access to the DC in their own right. - If OBO is specified, the user is granted access to be the delegate of the person that is specified by the value of the OBO attribute. (Note: currently this is a single value attribute.) • Note: The delegation attributes 'GrantByDelegateMeritOnly' and 'OBO' are currently not in use.	
SP_14	Determine user authorization based on values in the SAML attribute statement	There are three attributes which may contain entitlements attributes: Role, Service Entitlements and UAO. Values will only be specified for the Service Entitlements and UAO attributes if the DC elects to use the Federation Authorization Service. If the DC elects to handle authorization through its own processes/functions then the SAML response is used solely to identify the user and confirm the user has been authenticated. Roles: - Entitlement based on the role(s) of the requesting provider. (This attribute has not yet been used by existing ONE ID Federation implementations) Service Entitlements: - Access to Delivery Channels and Applications. Includes Organizations (or persons) that authorized each access. Where needed by a DC, additional attributes may also be included. UAO: - Organization(s) legally responsible for a given	See section 8.5 'Entitlements Attributes'

Item	Function	Details	Reference
		transaction. May contain values for more than one organization Notes: - Entitlement data may be provided for both the DC and Applications within the DC, e.g. portlets. - It may be a combination where access to the Delivery Channel is contained in the entitlements section of the SAML Response, but entitlement information is not available for Applications available from within the Delivery Channel, such as local services. - Delivery Channels may choose not to use the ONE ID Federation Authorization Service as part of their authorization process. In those cases, the ServiceEntitlements and UAO attribute values will be specified as 'Not Authorized' and these values should be ignored by the DC. - If the DC chooses to use the ONE ID Federation Authorization Service as part of their authorization process, the DC must take into account the values specified for the ServiceEntitlements and UAO attributes to decide whether the user is authorized to access the Delivery Channel. - The DC must display an appropriate message and deny access if the user is deemed not to be authorized to access it, whether the DC uses the Federation Authorization Service or not. If the UAO entitlement attribute is being used by the Delivery Channel and user is authorized under multiple organizations/individuals (HICs), the portal must provide a UAO selector so the user can select the applicable organization/individual. Note that the 'UAO' attribute contains the names of the organizations, as known to users, for this purpose. The UAO must be selected for the DC whether the DC uses the Federation Authorization Service or not.	
SP_15	Extract Patient Context Information (if specified in the SAML attribute statement) and determine use in DC to display patient data.	Patient context information is valid only from IDP initiated requests. - Distinguish between SP Initiated and IDP Initiated Request. - If there is a matching SAML Request the flow is SP initiated - If the SAML Response Token contains an 'InResponseTo' attribute the flow is SP initiated - If the SAML Response Token contains patient context information, the DC will use this information to perform a search for the patient and display the patient record if a matching patient is found. If a matching patient is not found, the DC should not display an error to the user, and instead should allow the user to manually search for a patient. - If the login flow is IDP initiated and the SAML Response Token does not contain patient context information, then the Delivery Channel must ensure a patient is not displayed and to allow the user to initiate a patient search.	See section 8.6 'Patient Context Attributes' See section 8.7 'Clinical Context Attributes'

Item	Function	Details	Reference
SP_16	Do not capture or store credential information	The DC must not capture or store the credential information pertaining to Federated Accounts. In this context, credential information means password and second factor authentication challenge data. The DC can only store data that is returned in the SAML Response from the Federation Broker.	
SP_17	If the DC uses HIAL Services, authenticate users prior to using those Services	If a user (hands on keyboard) is involved in the submission of the electronic message using HIAL Services then the DC must ensure that that user has been redirected to the Federation Broker within the user's DC session and prior to the use of HIAL Services for that electronic message. If HIAL Services rejects the electronic message as the user needs to be authenticated then the DC must redirect the user to the Federation Broker for that purpose, prior to resubmitting the electronic message using HIAL Services.	
SP_18	If the DC uses HIAL Services, populate the User Registry SAML Assertion correctly	The DC must populate attributes in the User Registry SAML Assertion from the attributes in the SAML Response from the Federation Broker. The DC must use local data to populate an attribute in the User Registry SAML Assertion ONLY if the required data is not available in the SAML Response from the Federation Broker. Notes: A token mapping document will be included in projects that onboard DCs. If a DC receives an attribute 'AuthenticationToken' from the Federation Broker then the 'AuthenticationToken' attribute must be included in the User Registry SAML Assertion.	
SP_19	Provide links to other Delivery Channels (optional)	The addition of links to other Delivery Channels will provide more convenience for users within single sign-on, particularly when there is a business relationship between Delivery Channels. The links do not need to support the transfer of patient information.	

11.3.2 Test Areas for Delivery Channels

SAML Request

Item	Functional Area	Prerequisites	Scenario
SP_5.1	SAML Request	User attempts to access the Delivery Channel	User goes to the DC's access point (see SP_4 and SP_5). The DC generates a SAML Request and redirects the user to the Federation Broker's single sign on service location with the SAML request contained in the post data of the HTTP request The DC validates the following elements in the SAML Request:

			• AuthnRequest • Issuer • NameIDPolicy • RequestedAuthnContext • The DC is responsible to ensure the values for the elements and attributes are properly set
--	--	--	--

SAML Response

3	Functional Area	Prerequisites	Scenario
SP_1.1	IDP Authentication	SP Initiated Request. User clicks on DC access point (see SP_5.1) which posts a SAML Request to the Federation Broker.	User authenticates with their IDP: • From the IDP selection page, select an IDP • Authenticate with the IDP Upon successful authentication, the FB returns a SAML Response to the DC.
SP_6.1	SAML Response Elements	Status code in SAML Response is not 'Success'	If StatusCode of the SAML Response is not 'Success' then DC to block user from accessing it and display appropriate message to the user; i.e., /saml:Response/saml:Status/saml:StatusCode/@Value is not "urn:oasis:names:tc:SAML:2.0:status:Success" Example scenarios where the StatusCode is not 'Success': 1. DC to send an unsigned SAML request to the Federation Broker or a request with an invalid signature 2. eHealth to manually disallow the HTTP Post binding for the DC and the DC attempts to post the SAML request to the Federation Broker
SP_7.1	User Identification - NameID	NameID User can log into multiple DCs with same account.	DC should use the NameID attribute to identify users. The NameID will contain the same value each time a given user logs in. • If a user uses their account for multiple DCs (e.g. Clinical Connect, HPG, eShift) then the same NameID is used each time a user logs into a specific DC • At first log in, the DC may use other identity attributes such as UserLoginName. The NameID is generated upon first login and can be used to identify the user on subsequent logins.
SP_8.1	SAML Identity attributes	SP or IDP Initiated Request with Response. Validate identity attributes conform to	The identity attributes are populated according to the eHealth Ontario SAML Specification. • Mandatory fields are populated • Data is in correct format

3	Functional Area	Prerequisites	Scenario
		eHealth Ontario SAML Specification	The identity attributes are: • DisplayName • Email • FirstName • LastName • RID • UserLoginName • PrincipalFedKey Test with both IDP-initiated logins and SP-initiated logins.
SP_9.1	SAML Authentication Attributes	SP or IDP Initiated Request with Response. Validate authentication attributes conform to eHealth Ontario SAML Specification	The authentication attributes are populated according to the eHealth Ontario SAML Specification. • Mandatory fields are populated • Data is in correct format The authentication attributes are: • Asserting Party • AuthenticationLevel • CredentialManagementSchemeRef • IdentityProvider • IdentityVerificationSchemeRef Protected Network Test with both IDP-initiated logins and SP-initiated logins.
SP_9.2	SAML Authentication attributes	SP or IDP Initiated Request with Response. Validate authentication attributes.	Validate that the user is able to access PI/PHI data within the DC based on the DC rules for the attribute values and the actual values passed for the user. The DC will define criteria to access PI/PHI based on values in the following authentication attributes: • Authentication Level = AL2 or higher • IdentityVerificationSchemeRef = AL2 or higher If the authentication values meet the criteria defined by the DC then the user may access PI/PHI in the DC. If at least one of 'Authentication Level' and 'IdentityVerificationSchemeRef' = AL1 then the SP must not allow access to PI/PHI.
SP_10.1	SAML Delegation Attributes	SP or IDP Initiated Request with Response. Validate delegation attributes conform to	The authentication attributes are populated according to the eHealth Ontario SAML Specification and are accepted by the Federation Broker.

3	Functional Area	Prerequisites	Scenario
		eHealth Ontario SAML Specification	- Delegation attributes are optional - Data is in correct format The delegation attributes are: - GrantByDelegateMeritOnly - OBO Test with both IDP-initiated logins and SP-initiated logins. Note: Delegation attributes are currently not in use.
SP_10.2	SAML Delegation attributes	SP or IDP Initiated Request with Response. Validate delegation attributes.	Grant access to the DC based on delegation type attributes. - DC to define whether delegation is valid - If valid, DC to define whether GrantByDelegateMeritOnly and/or OBO attributes are used If populated, test that the attributes are populated according to the eHealth Ontario SAML Specification Note: Delegation attributes are currently not in use.
SP_11.1	SAML Entitlements attributes	SP or IDP Initiated Request with Response. Validate Entitlements attributes conform to eHealth Ontario SAML Specification	The Entitlements attributes (ServiceEntitlements, UAO and or Roles) are generated according to the eHealth Ontario SAML Specification by the Federation Broker. - If ONE ID Federation Authorization System is used then the ServiceEntitlements and UAO attributes to be populated in correct format. - Validate format with Entitlements scenarios below. - If user is not in the ONE ID Federation Authorization System or the user is in it but not authorized for the Delivery Channel, both ServiceEntitlements and UAO contain 'Not Authorized' - If Roles attribute is used instead of ServiceEntitlements and UAO, ensure format is correct. Test with both IDP-initiated logins and SP-initiated logins. Note: The roles attribute is currently not in use.
SP_11.2	SAML Entitlements	SP or IDP Initiated Request with Response.	The user will gain access to the DC based on child elements of the ServiceEntitlements attribute

3	Functional Area	Prerequisites	Scenario
	attributes	DC uses Federation Authorization Services ServiceEntitlements is populated with one Delivery Channel and organization, UAO is populated with one organization	element: - The ServiceEntitlements attribute element contains one attribute value element: [service_a]:UPI:[upi_x] - The UAO attribute element contains one attribute value element with UPI only or UPI and OID
SP_11.3	SAML Entitlements attributes	SP or IDP Initiated Request with Response. DC uses Federation Authorization Services ServiceEntitlements and UAO attributes are populated with 'Not Authorized'	The user will not gain access to the DC based on value for in the ServiceEntitlements attribute: - Contains 'Not Authorized' - UAO also contains 'Not Authorized'
SP_11.4	SAML Entitlements attributes	SP or IDP Initiated Request with Response. DC uses Federation Authorization Services User has access to a Delivery Channel and an Application within that Delivery Channel under the authority of one organization.	The user will gain access the Delivery Channel and from within the Delivery Channel the user may access a service. - The ServiceEntitlements attribute element contains two attribute value elements: [dc]:UPI:[upi_x] [service]:UPI:[upi_x] - The UAO attribute element contains one attribute value element with UPI only or UPI and OID
SP_11.5	SAML Entitlements attributes	SP or IDP Initiated Request with Response. DC uses Federation Authorization Services User has access to two services under one organization, e.g. two Delivery Channels or a Delivery Channel and an Application available on that Delivery Channel	The user will gain access to service 1 or service 2, depending on which service was accessed, or if one of the services is a Delivery Channel, then the user will gain access to the Delivery Channel and also the Application (test above). - The ServiceEntitlements attribute element contains three attribute value elements: [service_a]:UPI:[upi_x] [service_b]:UPI:[upi_x] [dc]:UPI:[upi_x] - The UAO attribute element contains one attribute value element with UPI only or UPI and OID
SP_11.6	SAML Entitlements attributes	SP or IDP Initiated Request with Response. DC uses Federation	The user will need to select organization or provider that the user is accessing the DC under the authority of. After selection the user will gain

3	Functional Area	Prerequisites	Scenario
		Authorization Services User has access to one Delivery Channel under two organizations.	access to the DC. The Delivery Channel will need to provide a method to select the organization. - The ServiceEntitlements attribute element contains three attribute value elements: [service_a]:UPI:[upi_x] [service_a]:UPI:[upi_y] [dc]:UPI:[upi_x] [dc]:UPI:[upi_y] - The UAO attribute element contains two attribute value elements, one corresponding to each organization. The attribute value elements will contain UPI only, or UPI and OID - The Delivery Channel will use the UAO information to present the names of the organizations to the user.
SP_11.7	SAML Entitlements attributes	SP or IDP Initiated Request with Response. DC does not use Federation Authorization Services	The DC will use their own system to determine whether a user is authorized to access their service. - ServiceEntitlements is specified as 'Not Authorized' - UAO is specified as 'Not Authorized'
SP_11.8	SAML Entitlements attributes	SP or IDP initiated request with response. DC uses roles to determine access.	Note: Roles attribute is currently not used by existing implementations.
SP_12.1	SAML Patient Context Attributes	No patient context attributes populated, IDP Initiated login sequence	When users access the Delivery Channel, there is no pre-set/default patient context. The IDP initiated response may contain patient context data; however, if not included then no specific patient record should be displayed.
SP_12.2	SAML Patient Context Attributes	No patient context attributes populated, SP Initiated login sequence	When users access the Delivery Channel, there is no pre-set/default patient context. SP initiated responses are not expected to have patient context data.
SP_12.3	SAML Patient Context attributes	SP Initiated login sequence	When users access the Delivery Channel, no specific patient record is displayed SP initiated responses will not have patient context data.
SP_12.4	SAML Patient Context attributes	Patient context attributes populated, IDP Initiated login sequence,	In an IDP-initiated login from POSA to Delivery Channel X with patient context data specified in the SAML attribute statement, the patient can be

3	Functional Area	Prerequisites	Scenario
		Matching patient record in DC	found in Delivery Channel X. Matching patient is displayed when the user accesses the DC. • Patient context data is valid in IDP flow • Matching patient data is found
SP_12.5	SAML Patient Context attributes	Patient context attributes populated, IDP Initiated login sequence, No match for patient record in DC	In an IDP-initiated login from POSA to Delivery Channel X with patient context data specified in the SAML attribute statement, the patient is not found in Delivery Channel X. Patient is not displayed in DC • Patient context data is valid in IDP flow • No matching patient data is found
SP_12.6	SAML Patient Context attributes	Patient context attributes populated, IDP Initiated login sequence, Multiple searches in POSA	Go to the DC two times with different patient contexts. The expected patient is displayed in the DC with a new search in the POSA 1. Logon to POSA with IDP A and search for patient A. Access Delivery Channel X from POSA (first IDP-initiated login). Record for Patient A is displayed in Delivery Channel X 2. Return to POSA and search for patient B. Access Delivery Channel X from POSA (second IDP-initiated login). Record for Patient B is displayed in Delivery Channel X.
SP_12.7	SAML Patient Context attributes	Patient context data populated. DC access from two different browsers IDP Initiated login sequence	If DC is accessed from two different browser sessions. Correct patient record is displayed in each session 1. User logs on to IDP A and opens POSA A from tab A in browser. User searches for a patient X. 2. User logs on to IDP A and opens POSA A from tab B in browser. User searches from patient Y. 3. From tab A, user clicks on link to DC. User should be redirected to the DC via an IDP initiated SAML response. The DC invalidates any existing DC session and creates a new DC session. The user accesses the DC and sees Patient X. 4. From Tab B, user clicks on link to DC. User should be redirected to the DC via an IDP initiated SAML response. The DC invalidates any existing DC session and creates a new DC session. The user accesses the DC and sees Patient Y. 5. If the user goes back to tab A, the patient

3	Functional Area	Prerequisites	Scenario
			context should remain as Patient X.
SP_12.8	SAML patient context attributes	Patient context data populated. DC access from two different computers IDP Initiated login sequence	If DC is accessed from two different browser sessions. Correct patient record is displayed from each session 1. User logs on to IDP A and opens POSA A from computer A. User searches for a patient X. 2. User logs on to IDP A and opens POSA A from computer B. User searches from patient Y. 3. From Computer A, user clicks on link to DC. User should be redirected to the DC via an IDP initiated SAML response. The DC invalidates any existing DC session and creates a new DC session. The user accesses the DC and sees Patient X. 4. From Computer B, user clicks on link to DC. User should be redirected to the DC via an IDP initiated SAML response. The DC invalidates any existing DC session and creates a new DC session. The user accesses the DC and sees Patient Y.
SP_2.1	SAML Patient Context attributes – Consent management	Patient context attributes populated, IDP Initiated login sequence, Matching patient record in DC	In an IDP flow from POSA to Delivery Channel X with patient context data populated in SAML, the patient can be found in Delivery Channel X. There are various test cases needed to cover the different consent directives that may be requested by patients.

Session Management

Item	Functional Area	Prerequisites	Scenario
SP_7.1	Session Management – Logout	User has logged into the DC. The DC session and the Federation Broker session are active.	The user logs out of the DC (local logout). The Federation Broker session remains active.
SP_7.2	Session Management – Logout	User has logged out of the DC but the Federation Broker session remains active.	The user accesses the link to log into the DC after having logged out of the DC session. The user accesses the DC without having to log in (authenticate) again.
SP_7.3	Session Management – Logout	User has logged into the DC. The DC session and the Federation Broker session are active.	The user logs out of the DC and redirects the user to the Federation Broker's logout URL (global logout). The user is then redirected to the return URL specified by the DC. The Federation Broker session is ended.
SP_7.4	Session Management –	User has logged out of both the DC and the	The user accesses the link to log into the DC after having logged out of the DC session.

Item	Functional Area	Prerequisites	Scenario
	Logout	Federation Broker.	The user is presented with the 'IDP Selection' screen and selects their Identity Provider. The user re-authenticates if the IDP session is expired otherwise the user accesses the DC without having to log in (authenticate) again.
SP_7.5	Session Management – Logout	User has logged into the DC but then closes the browser.	The user accesses the link to log into the DC after having closed the browser. Depending on the browser, browser version, browser settings, IDP authentication, if the user chooses to access the DC again, the user may or may not be required to choose the IDP and authenticate again with the IDP.
SP_7.6	Session Management – Timeout	The Federation Broker session has timed out. The DC session remains active.	The Federation Broker session times out while the user is actively using the DC. The user may continue to use the Delivery Channel.
SP_7.7	Session Management – Time Out	The Federation Broker session, the DC session and the IDP session have timed out.	The DC session, Federation Broker session and IDP session have timed out and the user attempts to access the DC. The user will need to log in (authenticate) again.
SP_7.8	Session Management – Timeout	The request time out settings will need to be adjusted to perform this test.	The user accesses the DC and has logged in but receives a SAML response after the SAML request timeout limit The user will need to log in again.
SP_7.9	Session management – Bookmarks	A URL that is part of the log in flow has been bookmarked.	The user accesses bookmark to a URL that is part of the login flow. The DC will display an error message to the user, and the DC will redirect the user to the access point to log in.
SP_7.10	Session management - Bookmarks	A URL that can only be viewed after authentication has been bookmarked.	The user accesses a bookmark to a URL that cannot only be viewed if the user has not authenticated. The user will be redirected to the beginning of the login process (access point) if they have not authenticated.
SP_7.11	Session Management – Outage	The DC is not available.	The DC is experiencing an outage when the user logs in. The user will see a meaningful error message.
SP_7.12	Session Management – Audit	The DC is auditing all transactions	Details of a user's transactions are requested. The SAML requests sent to the Federation Broker and the decrypted SAML responses that are sent from the Federation Broker are logged and available upon request. DCs should also maintain

Item	Functional Area	Prerequisites	Scenario
			sufficient logging information to support troubleshooting.
SP_7.13	Session Management – SSO with multiple partners	An implementation that allows the user to authenticate once and access more than one DC with a single Token	In an implementation in which two or more Delivery Channels may be accessed with single sign on, the user logs on and is able to access the other Delivery Channels without having to authenticate again. For example: • User logs on to Delivery Channel A • The user accesses Delivery Channel B • From Delivery Channel B the user accesses Delivery Channel C. • The single sign on (Federation Broker) session remains valid. The user does not have to log on again.

11.4 Point of Service Applications (POSAs) and the ONE ID Federation

A point of service application is a type of service that is a launch point to a Federated Delivery Channel. POSAs are the sources of patient context. IDP initiated login sequences begin with a launch from a POSA.

11.4.1 Responsibilities

Item	Function	Details	Reference
POSA_1	Use Federated IDP for accounts	The Identity Provider that provides the accounts used by users to access the POSA follows the onboarding process to become a member of the Federation. This involves reviewing and meeting the Identity Provider Standard	
POSA_2	Provide Link from POSA to Federated Delivery Channel	The POSA must display an access point (i.e., link) to each Delivery Channel that the POS expects users to access and “synchronize” patient context with, i.e. requires patient context and SSO.	See section 4.2 ‘Identify Provider Initiated Login Sequence Diagram’ Step 6.
POSA_3	Send Logout request to FB	The POSA must send a logout request to the Federation Broker when the user clicks on the link to the Delivery Channel portal. The POSA redirects the user to the Federation Broker logout URL. The Federation Broker invalidates the user’s single sign on session. If the <code>returnurl</code> query string parameter is specified in the redirect URL, the Federation Broker will redirect the user back to the location specified by the value of <code>returnurl</code>.	See section 4.2 ‘Identify Provider Initiated Login Sequence Diagram’ Steps A1, A2 and A3

Item	Function	Details	Reference
POSA_4	Generate a SAML Response	Once the POSA has redirected the user to the Federation Broker logout URL to invalidate any existing Federation Broker session, the POSA will redirect the user to the local SAML token service to obtain a SAML token. - The SAML token service generates a SAML response. If a patient context is available, patient context data is added to the SAML attribute statement - The SAML response to be compliant with current eHealth Ontario SAML Specification - The SAML token service will redirect the user to the Federation Broker and include the SAML token generated as post data. The 'RelayState' post parameter must be specified as the Entity ID of the destination DC in the redirect request to the Federation Broker.	See section 4.2 'Identify Provider Initiated Login Sequence Diagram' Steps 7 and 8 See section 7.1.2 'IDP Initiated Login'
POSA_5	User accesses the target Delivery Channel as provided by the POSA in the service link url.	The user accesses the destination URL as provided by the POSA. Steps: - Federation Broker accepts response and performs secondary processing on the SAML response received from the POSA - If the SAML response is valid, the user is directed to the destination URL as provided by the link from the POSA. If patient context information was provided, the user will view the patient in the target Delivery Channel.	See section 4.2 'Identity Provider Login Sequence Diagram' steps 8 through 13' (not POSA responsibilities) and step 14 (POSA) See section 7.1.2 'IDP Initiated Login'
POSA_6	POSA must address access SAML errors posted by Federation Broker as a result of invalid SAML attributes.	The POSA must address SAML Errors identified by Federation Broker. Steps: - Federation Broker accepts response and performs secondary processing on the SAML response received from the POSA - Errors are identified and the Federation Broker denies access and issues an error message (see section 11.2) to the user explaining why access cannot be provided, along with the names of the invalid attributes. The error message advises users to contact the Help Desk of the POSA - The POSA must handle the above error scenario when contacted by users as a result of the message presented by the FB.	See section 4.2.1 'Identity Provider Login Sequence Diagram' steps 8 through 13' (not POSA responsibilities) and step 14 (POSA) See section 7.1.2 'IDP Initiated Login'

11.4.2 Test Areas - POSAs

Item	Functional Area	Prerequisites	Scenario
POSA_1.1	Local login	A Federated IDP is used by user to access POSA	The user logs into their POSA with an account issued by a Federated IDP. For example, log into an HIS where the hospital is a Federated IDP.
POSA_2.1 POSA_3.1 POSA_4.1 POSA_5.1	Access a Federated Delivery Channel	A link is available to a Federated Delivery Channel. (POSA_2 from section 11.4.1) The link directs user to the Federation Broker logout URL and optionally provides a return URL to the POSA (POSA_3 from section 11.4.1) The redirection instructions direct user to local SAML token service.(POSA_4 from section 11.4.1) The redirect contains the SAML response and a reference to the target Delivery Channel as post data. (POSA_5 from section 11.4.1)	The user accesses a patient in the POSA and then accesses a link to a Federated Delivery Channel. The Federation Broker session is invalidated (confirm with Federation Broker logs) The local STS issues a valid SAML Response with patient context. The user accesses the patient (if a matching patient found) in the Federated Delivery Channel.
POSA_2.1 POSA_3.1 POSA_4.1 POSA_5.2	Access a Federated Delivery Channel	A link is available to a Federated Delivery Channel. (POSA_2 from section 11.4.1) The link directs user to the Federation Broker logout URL and optionally provides a return URL to the POSA (POSA_3 from section 11.4.1) The redirection instructions direct user to local SAML token service. (POSA_4 from section 11.4.1) The redirect contains the SAML response and a reference to the target service as post data. (POSA_5 from section	The user accesses POSA and then accesses a link to a Federated Delivery Channel. The user has no patient context in the POSA at this point. The Federation Broker session is invalidated (confirm with Federation Broker logs) The local STS issues a valid SAML Response without patient context. The user accesses the Federated Delivery Channel.

Item	Functional Area	Prerequisites	Scenario
		11.4.1)	
POSA_6.1	Errors accessing a Federated Delivery Channel	A link is available to a Federated Delivery Channel. The link directs user to the Federation Broker logout URL and provides a return URL to the POSA The redirection instructions direct user to local SAML provider (for example STS). The link contains the target Delivery Channel.	The user accesses a link to a Federated Delivery Channel. The POSA displays an error message as the SAML Response was not successful. The following steps occur in the background: • The Federation Broker session is invalidated (can be confirmed via Federation Broker logs) • The POSA generates a SAML. The SAML is posted through the IDP to the FB. • Federation Broker will fail access and present an error message to the user. •

11.5 Identity Provider (IDPs) in the ONE ID Federation

An IDP in a ONE ID environment is an organization that provides accounts to health professionals and other users that can be used to access Applications through Delivery Channels. The IDP is responsible for managing, authenticating and asserting the identity of users accessing federated Delivery Channels, and must become a member of the ONE ID Federation.

11.5.1 IDP Responsibilities

Item	Function	Details	Reference
IDP_1	Provide accounts for users	The Identity Provider is responsible for ascertaining real world identities for individuals and for providing credentials to link digital and real world identities • IDPs capture and store identification data such as name, date of birth and professional designation	
IDP_2	Join the ONE ID Federation	The Identity Provider for the accounts used to access ONE ID Federation Delivery Channels must follow the onboarding process to become a member of the Federation. • This involves reviewing and meeting the Identity Provider Standard. • The IDP will be available for selection on the ONE ID Federation IDP Selection page. The user must select the IDP to authenticate with in SP-initiated logins where the user does not already have an	

Item	Function	Details	Reference
		active Federation Broker session.	
IDP_3	Implement SAML Token Service (STS)	The Identity Provider must implement a SAML Token Service to handle all operations for SAML requests and responses. This includes implementing an assertion consumer service endpoint and a single sign on service endpoint.	
IDP_4	STS Integration	The Identity Provider must integrate the STS with its existing credential store and session management system.	
IDP_5	Immutable NameID	The Identity Provider must ensure that the NameID is immutable, unique for any given user and not used again over time for different users.	
IDP_6	Logout Capabilities	The Identity Provider may need to provide logout capabilities to invalidate the user's IDP session; i.e., a single sign out service.	
IDP_7	Current eHealth Ontario SAML specification	The Identity Provider must stay within n-1 versions of the most current eHealth Ontario SAML Specification.	
IDP_8	Test "Delivery Channel"	The Identity Provider may create a test "Delivery Channel" to facilitate development and testing.	
IDP_9	IDP Initiated Login Sequence - Redirect user to the Federation Broker	The IDP will redirect the user to Federation Broker with SAML Response as generated by the POSA (e.g. STS) - The user logs on first to their POSA. The IDP will challenge the user for credentials to log onto the POSA and perform local authentication - The POSA or STS then redirects the user to Federation Broker logout URL to invalidate the Federation Broker session - Target Delivery Channel is specified in the second redirect to the Federation Broker as RelayState post parameter, which must be set to the Entity ID of the Delivery Channel. - The assertion must be signed and encrypted - the response must be signed - The Response may contain patient context data - The Response will correctly set the 'Authentication_Level' and 'IdentityVerificationSchemeRef' attributes.	See section 4.2.1 'Identity Provider Login Sequence' steps 8 and 9. See section 7.1.2 'SAML Response from IDP to Federation Broker, IDP Initiated Login' See section 8.0 'SAML Response Assertion Attribute Statements'
IDP_10	SP Initiated Login Sequence – Select IDP for login	The Identity Provider for the accounts used to access ONE ID Federation Delivery Channels will be available from the ONE ID Federation IDP Selection page - This page is displayed if the user has not already authenticated - Once the user selects the IDP, the ONE ID	See section 4.1.1 'SP Initiated Login Sequence' step 3

Item	Function	Details	Reference
		Federation Broker sends an authentication request to the IDP single sign on service	
IDP_11	SP Initiated Login Sequence - Response to Federation Request – Authenticate user	The IDP to validate the SAML Request and authenticate the user. The IDP is responsible for: • Determining if request from ONE ID is valid • Challenging the user for credentials if not previously authenticated • Evaluating the credentials (such as user name and password) submitted by the user. • Authenticating the user at AL2.	See section 4.1.1 'SP Initiated Login Sequence' step 4.
IDP_12	SP Initiated Login Sequence - Response to Federation Request – Generate SAML Response token	The IDP to generate SAML response after authentication: • The SAML response token to be compliant with current eHealth Ontario SAML Specification • Any patient context that may exist in the user's session with the IDP must be omitted from the SAML response that the IDP generates and issues to the user in response to a SP-initiated login • Redirect user to the ONE ID Federation Broker with the IDP issued SAML Token.	See section 4.1.1 'SP Initiated Login Sequence' step 4. See section 7.1.1 'SAML Response from IDP to Federation Broker, SP Initiated Login' See section 8.0 'SAML Response Assertion Attribute Statements'
IDP_14	Session Management	Timeout: • The idle session time is enforced • The IDP maximum session time is enforced • If the SAML request had timed out during the user log in, display an appropriate error message to the user. Bookmarks: • Accessing a bookmarked URL that is part of the IDP login flow: the user will be redirected to an appropriate error page Outages: • If IDP is not available due to an outage, the user should see a meaningful error message Audit: • IDPs to log authentication activities	

11.5.2 Test scenarios for Identity Providers

Item	Functional Area	Prerequisites	Scenario
IDP_4.1	IDP Initiated Login Sequence, Broker logout, With patient context	User is logged on to their POSA (e.g. an HIS) and viewing a patient. A link is available to a Federated Delivery Channel. The IDP redirects user to the Federation Broker logout URL and provides a return URL to the POSA. The redirection instructions direct user to local SAML token service The redirect of the user to the Federation Broker contains the SAML response and a reference to the target Delivery Channel as post data.	The STS redirects the user to the FB with the SAML Response it generates as part of the request. The response contains patient context data: 1. Validate that the user is logged out of the Federation Broker (use Federation logs to determine) 2. The IDP redirects the user to Federation Broker with SAML Response as generated by the POSA (e.g. STS). 3. The user is directed to the Federation resource using the relay state parameter from the link. 4. The user accesses the patient (if a matching patient found) in the Federated Delivery Channel.
IDP_4.2	IDP Initiated Login Sequence, Broker logout, With no patient context	User is logged on to their POSA (i.e. an HIS) and not viewing a patient. A link is available to a Federated Delivery Channel. The link directs user to the Federation Broker logout URL and provides a return URL to the POSA. The redirection instructions direct user to local SAML token service. The link contains the target Delivery Channel (relay state)	The IDP sends a SAML Response from the POSA provider (e.g. STS) to the FB. The response does not contain patient context data: 1. Validate that the user is logged out of the Federation Broker (use Federation logs to determine) 2. The IDP redirects the user to Federation Broker with SAML Response as generated by the POSA (e.g. STS): 3. The user is directed to the Federation resource using the relay state parameter from the link. 4. The user accesses the Federated Delivery Channel.
IDP_5.1	SP Initiated Login sequence, ONE ID Federation Selection page	User goes to the DC access point. User has not authenticated.	The IDP should be available on the ONE ID Federation IDP Selection page with the correct name, i.e. the name that users will recognize and understand. • The IDP Selection page is displayed after the user clicks a link to the Delivery Channel if the user is not already

			authenticated When the user selects an IDP from the page, the ONE ID Federation Broker sends a SAML request to the IDP
IDP_6.1	SP Initiated Login Sequence, Authentication, Request	User goes to the DC access point. User has not authenticated. User has selected an IDP	The user to select the IDP from the IDP Selection page. The IDP to validate the ONE ID SAML Request sent to the IDP after selection: - Valid issuer - Digitally signed - Received within an appropriate validity period
IDP_6.2	SP Initiated Login Sequence, Authentication, SAML Response Access Service	User goes to the DC access point. User selects IDP User authenticates successfully SAML Response generated User accesses Delivery Channel.	The user clicks the link to a DC, selects an IDP and authenticates successfully - ONE ID sends request to IDP - The IDP challenges the user for credentials - The IDP evaluates the credentials and determines if 2nd factor authentication is required - User authenticates successfully - The IDP generates a valid SAML response token and directs user to the Federation Broker. The following should be tested: - All attributes sent to the Broker are valid. - Mandatory fields are populated with permissible values - Patient context fields are not populated - See section 8.0 SAML Response Assertion statement Note that the FB will check this response once it is received from the IDP.
IDP_6.3	SP Initiated Login sequence, Authentication	User goes to the DC access point User selects IDP User has already authenticated with the IDP and has an active IDP session	The user clicks the link to a DC. The user has already authenticated IDP responds with SAML Response The user needs to choose the IDP on the IDP Selection page.
IDP_6.4	SP Initiated Login Sequence, Authentication	User goes to the DC access point. User selects IDP. User has not authenticated and does not have active sessions with the IDP, the	The user clicks the link to a DC and selects an IDP but fails to authenticate successfully. The IDP to handle errors. User does not gain access to the Delivery Channel. The following are examples failed authentication: - Incorrect credentials - Unsuccessful second factor authentication

		Federation Broker and the SP	- User did not accept IDP terms of usage - Account is locked
IDP_6.5	SP Initiated Login Sequence, 2 nd Authentication	User goes to the DC access point. The DC requires 2nd factor authentication. User selects IDP User has not authenticated and does not have active sessions with the IDP, the Federation Broker and the DC	The user clicks link to a DC and selects an IDP - The user is challenged for username and password - The user is challenged with 2nd factor authentication - The user is successfully authenticated - The IDP generates a SAML response token with 'Authentication Level' at AL2 - The user gains access to the Delivery Channel.
IDP_6.6	SP Initiated Login Sequence, Account at AL1 Identity Verification (if supported by IDP)	User goes to the DC access point. User selects IDP User has not authenticated and does not have active sessions with the IDP, the Federation Broker and the DC	The user clicks link to a DC and selects an IDP - The user is challenged for username and password - The user is challenged with 2nd factor authentication - The user is successfully authenticated - The IDP generates a SAML response token with 'Authentication Level' at AL2 and 'Identity Verification Scheme Ref' at AL1.
IDP_6.8	SP Initiated Login Sequence, 2 nd Authentication	User goes to the DC access point. The DC requires 2nd factor authentication. User selects IDP	The user clicks link to a DC and selects an IDP - The user is challenged for their credentials - The user is NOT challenged with 2nd factor authentication - The IDP generates a SAML response token with 'Authentication Level' at AL1
IDP_7.2	SP Initiated or IDP initiated Login Sequence, SAML Response NameID scenario	The user logs into the Federation Broker.	The IDP generates a SAML Response in either an SP or IDP initiated login sequence. The response contains a username, IDP and NameID. The IDP-issued NameID for a given user will never change; i.e., it is unique and persistent for a given user account and will not be used again over time for different users.
IDP_8.1	SP Initiated Login Sequence, Authentication, IDP is down for maintenance or is experiencing an unexpected outage	Link to DC from portal. User selects IDP	The user clicks the link to a DC and selects an IDP but IDP is unavailable The IDP to display error message. User does not gain access to Delivery Channel.

IDP_8.2	SP Initiated, Authentication, Session management Request time out	Link to DC from portal. User selects IDP	The user clicks the link to a DC and selects an IDP. The user waits to complete the authentication steps. The ONE ID Request to authenticate has timed out. - The user authenticates successfully. - The IDP sets the Status of the SAML Response to 'RequestDenied' as a result of the time out. - User does not gain access to the Delivery Channel.
SP_8.3	Session Management – Time Out	IDP or SP login sequence. The user has accessed a Delivery Channel. The IDP idle time limit has been reached.	The user has authenticated and is accessing a Delivery Channel but the IDP idle session time limit has been reached The user will need to log in (authenticate) again.
SP_8.4	Session Management – Time Out	IDP or SP login sequence The user has accessed a Delivery Channel. The IDP maximum session time limit has been reached.	The DC session, IDP session and IDP session have timed out and the user accessed the DC. The user will need to log in (authenticate) again.
SP_8.5	Session Management-Bookmark	SP Login Sequence The user bookmarked a URL that is part of the login sequence	The user accesses a bookmark that is part of the login sequence. The user will be redirected to the beginning of the login sequence.
SP_8.6	Session management – Audit	IDP or SP Login Sequence Request to authenticate from ONE ID	The user completes a request to authenticate. The SAML requests received by the IDP from the Federation Broker and the SAML responses that are generated by the IDP and sent to the Federation Broker are logged and available upon request. IDPs should also maintain sufficient logging information to support troubleshooting, e.g., why attribute values were specified as they were in the SAML response.
SP_8.6	Session management – Revoke	SP Login Sequence Account revoked while user is logged on.	The user has authenticated and is accessing a Delivery Channel but the user's account has been revoked while the user is logged on and the DC, FB and IDP sessions have been invalidated or timed out. Login will fail on next authentication request at the IDP

Copyright Notice

Copyright © 2018, eHealth Ontario

All rights reserved

No part of this document may be reproduced in any form, including photocopying or transmission electronically to any computer, without prior written consent of eHealth Ontario. The information contained in this document is proprietary to eHealth Ontario and may not be used or disclosed except as expressly authorized in writing by eHealth Ontario.

Trademarks

Other product names mentioned in this document may be trademarks or registered trademarks of their respective companies and are hereby acknowledged.