SAML, or Security Assertion Markup Language, also lets you log in to multiple sites using a [single sign-on, or SSO](https://fusionauth.io/blog/2022/09/08/how-sso-works). It delivers assertions in XML that give information to authenticate users. Assertions can also include [attributes or authorization decisions](https://www.varonis.com/blog/what-is-saml/).

*SAML is primarily an authentication system, while OAuth is an authorization system*. [*Authentication*](https://fusionauth.io/articles/authentication/common-authentication-implementation-risks) is about confirming the user’s identity. [*Authorization*](https://fusionauth.io/docs/get-started/core-concepts/authentication-authorization#overview) is about deciding what services they can access.

References:

**SAML vs. OAuth - Understand Differences and Benefits -** [**https://fusionauth.io/articles/oauth/saml-vs-oauth**](https://fusionauth.io/articles/oauth/saml-vs-oauth)

Yes, SAML (Security Assertion Markup Language) can play a role in this integration as an alternative or complement to OAuth 2.0 and OpenID Connect (OIDC) for federated authentication and Single Sign-On (SSO). Here's how SAML could be integrated into your solution, along with considerations for its use.

**Understanding SAML**

* **SAML Overview**: SAML is an XML-based framework for exchanging authentication and authorization data between parties, specifically between an **Identity Provider (IdP)** and a **Service Provider (SP)**.
* **Purpose**: It enables SSO by allowing users to authenticate with one identity provider and access multiple service providers without the need for separate logins.
* **Key Components**:
  + **SAML Assertions**: XML documents that contain authentication statements, attribute statements, and authorization decision statements.
  + **SAML Protocols**: Define how SAML requests and responses are communicated.
  + **Bindings**: Specify how SAML protocols map onto standard messaging or communication protocols (e.g., HTTP POST, HTTP Redirect).

**Potential Role of SAML in Your Integration**

Given your requirements:

* **BC Services Card** acts as the central identity provider in British Columbia.
* **Health Gateway** relies on BC Services Card for authentication and does not have its own authorization server.
* **VPP Patient Portal** needs to securely receive user information (e.g., PHN, birthdate) and authentication tokens from Health Gateway.

SAML can be used to facilitate secure authentication and attribute sharing between Health Gateway and your VPP Patient Portal.

**How SAML Integration Would Work**

**1. SAML Authentication Flow**

* **Step 1**: **User Authentication at Health Gateway**
  + The user logs into Health Gateway using BC Services Card authentication (which may already be using SAML).
* **Step 2**: **Initiate SAML SSO to VPP Patient Portal**
  + When the user clicks the link to access the VPP Patient Portal, Health Gateway acts as an **Identity Provider (IdP)** and initiates a SAML SSO process.
  + Health Gateway generates a SAML **Response** containing assertions about the user's identity and attributes.
* **Step 3**: **SAML Response to VPP Patient Portal**
  + The SAML Response is sent to the VPP Patient Portal (the **Service Provider (SP)**) via the user's browser, typically using an HTTP POST binding.
* **Step 4**: **VPP Patient Portal Validates SAML Response**
  + The Portal verifies the SAML Response, ensuring it is properly signed and from a trusted IdP.
  + Extracts user attributes (e.g., PHN, birthdate) from the SAML assertions.
* **Step 5**: **User Session Established**
  + The Portal creates a session for the user based on the verified information.
  + The user can now access their health records securely.

**2. Establish Trust Between Health Gateway and VPP Patient Portal**

* **Metadata Exchange**: Both parties exchange SAML metadata files containing entity IDs, endpoints, and public keys.
* **Certificates**: Use X.509 certificates to sign and encrypt SAML assertions, ensuring message integrity and confidentiality.

**3. Handling User Attributes**

* **Attribute Statements**: SAML allows the inclusion of user attributes in the assertion, facilitating the transfer of necessary user information.
* **Attribute Mapping**: Map the received attributes to your application's user model for proper session management and access control.

**Advantages of Using SAML**

* **Single Sign-On (SSO)**: Provides a seamless authentication experience across multiple services.
* **Security**: Strong security features with signed and encrypted assertions.
* **Interoperability**: Widely supported standard, facilitating integration with systems that also support SAML.

**Considerations and Challenges**

**1. Compatibility**

* **BC Services Card Support**: Confirm whether BC Services Card supports SAML for third-party integrations.
* **Health Gateway as IdP**: Verify if Health Gateway can act as a SAML Identity Provider to issue assertions to your Portal.

**2. Implementation Complexity**

* **Configuration**: Setting up SAML involves configuring metadata, certificates, and endpoints accurately.
* **Error Handling**: SAML messages are XML-based, and debugging can be more complex compared to JSON-based tokens in OAuth 2.0/OIDC.

**3. User Experience**

* **Redirection Flows**: SAML SSO involves browser redirects which need to be managed to maintain a seamless user experience.

**4. Token Refresh Mechanism**

* **Session Management**: SAML does not inherently support token refresh like OAuth 2.0's refresh tokens.
* **Session Duration**: Sessions are typically maintained via application sessions or cookies, which may require re-authentication upon expiration.

**Alternative Approach: Using OAuth 2.0 and OpenID Connect (OIDC)**

Given your existing setup and requirements, OAuth 2.0 with OpenID Connect may be more suitable:

* **BC Services Card Support**: Likely supports OAuth 2.0/OIDC, which are modern standards for authentication and authorization.
* **Token Handling**: OAuth 2.0 provides access tokens and refresh tokens, allowing for session continuation without re-authentication.
* **User Attributes**: OIDC includes an ID token (JWT) that carries user identity claims.
* **Simpler Implementation**: OAuth 2.0/OIDC are often considered easier to implement, especially with RESTful APIs and JSON-based tokens.

**Recommendations**

**1. Verify Protocol Support**

* **Contact BC Services Card and Health Gateway**: Determine whether they support SAML for third-party integration or if they recommend OAuth 2.0/OIDC.

**2. Assess Feasibility**

* **Technical Resources**: Consider your team's familiarity with SAML versus OAuth 2.0/OIDC.
* **Maintenance Overhead**: Evaluate the long-term maintenance implications of using SAML.

**3. Security and Compliance**

* **Regulatory Requirements**: Ensure that whichever protocol you choose complies with data protection regulations and industry standards.
* **Security Features**: Both protocols offer robust security when implemented correctly.

**4. User Experience**

* **Seamless Flow**: Aim for the solution that provides the smoothest experience for users, with minimal redirects and prompts.

**Conclusion**

While SAML can technically be used in this integration, OAuth 2.0 with OpenID Connect is likely a better fit given:

* **Existing Infrastructure**: If BC Services Card and Health Gateway primarily use OAuth 2.0/OIDC, integrating with these protocols would be more straightforward.
* **Token Management**: OAuth 2.0 provides mechanisms for token refresh, aligning with your requirement to refresh tokens within the Portal.
* **Ease of Integration**: OAuth 2.0/OIDC are widely supported with numerous libraries and community support, potentially reducing development time.

**Next Steps**

1. **Consult Documentation**: Review technical documentation from BC Services Card and Health Gateway regarding supported authentication protocols.
2. **Prototype Testing**: Develop a small proof of concept using SAML to test compatibility and assess complexity.
3. **Decision Making**: Based on findings, decide whether to proceed with SAML or continue with OAuth 2.0/OIDC.
4. **Implementation Planning**: Plan the integration accordingly, ensuring all security considerations are addressed.

**Additional Resources**

* **SAML Standards**: OASIS SAML Specifications
* **OpenID Connect**: OpenID Connect Documentation
* **SAML vs. OAuth 2.0**: Understanding the differences can help in making an informed decision.