**Digital Identity**

To provide and manage digital service delivery, many government programs require the ability to validate a person’s identity. The Department of Service Nova Scotia and Internal Services (SNS-IS) offers several Identity Providers to allow for both provincial employee and citizen identity validation.

The successful proponent shall integrate their digital service with one of the following Identity Providers.

If your digital service / application uses:

* Any citizen identity, you must implement #1.
* Government and NS Health employee identity, you must implement #1 or #2.
* Either Government or NS Health employee identity, the preferred order is #1, #2, #3, #4.

1. **Nova Scotia ID (NSiD)**

The digital service must be capable of using one of the following authentication protocols supported by NSiD:

* **Security Assertion Markup Language 2.0 (SAML 2.0)**
  + Must adhere to the current specifications of the Cyber Authentication Technology Solutions (CATS) SAML 2.0 Deployment Profile (<https://canada-ca.github.io/CATS-STAE/> )
  + Required profile/binding combinations supported by the NS Login Service:
    - For Single Sign On (SSO)
      * SingleSignOnService (HTTP-Redirect)
      * AssertionConsumerService (HTTP-Redirect)
    - For Single Logout (SLO)
      * SingleLogoutService (HTTP-Redirect or HTTP-Redirect/SOAP)
    - Profile Update and Service Revocation
      * ChangeNotifyService (SOAP)
      * ManageNameIDService (SOAP)
  + Additional Required Elements:
    - <md:Extensions><md:UIInfo><mdui:DisplayName>
* **Open ID Connect (OIDC) 1.0**
  + Must adhere to the current specifications of the International Government (iGov) Assurance Profile for Open ID Connect (<https://openid.net/wg/igov/> )
  + Grant Types Supported: Authorization Code only
  + Response Types Supported: Code only
    - Public Client Authorization:
      * PKCE with a S256 code challenge required
      * Application Type: Native only
    - Confidential Client Authorization:
      * Token Endpoint Authorization: private\_key\_jwt only
      * Application Type: Web only

1. **Azure Active Directory (AAD)**

Documentation on AAD integration requirements can be found here:

<https://docs.microsoft.com/en-ca/azure/active-directory/develop/v2-overview>

1. **Kerberos via Active Directory Domain Services (****AD** **DS)**

For employees supported by Shared Services and only on the Provincial Data Network (PDN).

1. **Active Directory Federation Services (AD FS)**

The requirements for Government / NS Health AD FS integration are as follows:

Must be able to integrate with AD FS 4.0 using one of the following protocols:

* SAML 2.0
* WS-Federation
* WS-Trust

Consideration will be made for integration with Government / NS Health AD DS leveraging LDAPS on a case-by-case basis if the digital service is not able to integrate with NSiD, AAD, Kerberos or AD FS. The user base of the service should be taken into consideration as the Government of Nova Scotia and NS Health maintain separate AD DS / AD FS environments.

**Additional Identity Requirements**

* The proposed digital service **shall**:
  + Be responsible for maintaining valid digital certificates and metadata (Relying Party/Identity Provider) as required. For NSiD integrations requiring digital certificates for signing or encryption, the certificates shall be issued by the Province of Nova Scotia.
  + Ensure that all user accounts are provided with a persistent unique identifier. For NSiD integrations, a persistent unique identifier provided by NSiD and associated with an authenticated user shall be stored and should be leveraged for user identification in the proposed solution.
  + Be responsible for user/group authorization to the resources of the service. Basic group-based access control / group-based attributes may be provided by the Identity Provider.
* The proposed digital service **should**:
  + Leverage the Identity Provider’s user identity information to populate any user records.
  + Provide just-in-time provisioning for new users.
  + Provide subject resolution / mapping automation to any pre-existing user records.