**Digital Identity**

To provide and manage digital service delivery, many government programs require the ability to validate a person’s identity through the digital channel. The Department of Internal Services offers the Nova Scotia Login System (NSLS) which provides individuals with the ability to manage their credential and identity information online and access government services and information in an easy and secure manner.

New users will register their account in NSLS before being granted access to the digital service to complete a transaction. Additional program related information may be collected by the digital service, if required. Existing NSLS users can use their NSLS account to log in to the new digital service.

The successful proponent must (M) integrate their digital service with one of the following standards.

If your digital service / application uses:

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

1. **The Nova Scotia Login System (NSLS)**

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

* **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. **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)**

Consideration will be made for integration with Government / NS Health AD FS on a case by case basis if the digital service is not able to integrate with the NSLS or use Kerberos. The users of the service should be taken into consideration as the Government of Nova Scotia and NS Health maintain separate AD FS environments.

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

**Additional Requirements**

* The proposed digital service must ensure that all user accounts are provided with a persistent unique identifier. The unique identifier can be the identifier provided by the NSLS or it can be generated by the digital service and mapped to the NSLS identifier.
* The digital service should leverage the user's identity information managed in NSLS and use applicable identity attributes to pre-populate applications and requests.
* The proponent should have the capability to support users with program related inquiries.