Digital Authentication Requirements for RFP Purposes

For any question, please reach out to the Digital Trust and Credentials Program/team by using the email address: NSIdentity@novascotia.ca

ID	Section	Requirement	Importance Level
1	My NS Account	To provide and manage digital service delivery, many government programs require the ability to validate a person's identity. The Department of Cyber Security and Digital Solutions (CSDS) offers a number of Identity Providers to allow for both provincial employee (Health/Gov) and citizen identity validation. The successful proponent **shall** integrate their digital service with one of the following Identity Providers. If your digital service / application serves only citizens **OR** both provincial employees (Health/Gov) and the citizens • you **shall** implement Section **My NS Account**. If your digital service / application serves only provincial employees (Health/Gov) • you shall follow the **Identity and Access Management** requirements.	CRITICAL
2	My NS Account	The digital service **shall** be capable of using one of the following authentication protocols supported by **My NS Account**: • **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 My NS Account: ▪ 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>	CRITICAL

ID	Section	Requirement	Importance Level
		• **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	
3	My NS Account	• The proposed digital service **shall**: ○ Be responsible for maintaining valid digital certificates and metadata (Relying Party/Identity Provider) as required. For My NS Account integrations requiring digital certificates for signing or encryption, the certificates shall be issued by the Digital Identity and Trust team. ○ Ensure that all user accounts are provided with a persistent unique identifier. For My NS Account integrations, a persistent unique identifier provided by My NS Account 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.	CRITICAL
4	My NS Account	• 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. ○ Participate in Federated Logout for both Relying Party and Identity Provider initiated logouts.	HIGH