Digital Identity Requirements for RFP purpose

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

TECHNICAL REQUIREMENTS

ID	Section	Requirement	Classification
	Identity	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 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 **shall** implement Section **My NS Account**. • Government and/or NS Health employee identity, you **shall** implement either Section **My NS Account** or Section **ICAM**.	Mandatory

	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>
		
		• **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
			Mandatory

	My NS Account	• The proposed digital service **shall**: o 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. o Ensure that all user accounts are prohvided 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. o 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.	Mandatory
	My NS Account	• The proposed digital service **should**: o Leverage the Identity Provider's user identity information to populate any user records. o Provide just-in-time provisioning for new users. o Provide subject resolution / mapping automation to any pre-existing user records. o Participate in Federated Logout for both Relying Party and Identity Provider initiated logouts.	Recommended

	ICAM	1. Credentials **shall not** be stored in the application. No exceptions. 2. Authentication **shall** be through one of the following modalities. a. Integrate with the Microsoft identity platform to authenticate and authorize users – applicable to web apps, mobile apps, native apps, daemon apps, server-side apps, web application programming interfaces (APIs), or apps that call protected web APIs. • Integration, via Azure Active Directory, **shall** leverage industry standard protocols OpenID Connect (OIDC) and OAuth 2.0 for authentication and authorization respectively. Microsoft identity platform documentation available on https://docs.microsoft.com/en-us/azure/active-directory/develop/ can be referred to for specifications around endpoints, tokens and authentication flows. • Integration using Security Assertion Markup Language (SAML) 2.0 is permissible via Azure Active Directory to enable a single sign-on experience for users. Single sign-on and single sign-out SAML profiles for Azure AD explain how SAML assertions, protocols and bindings are used in the identity provider services and can be referred to in the Microsoft identity platform documentation available on https://docs.microsoft.com/en-us/azure/active-directory/develop/. b. Use Kerberos for authentication against Microsoft Active Directory Domain Services on the corporate network. 3. Additional requirements for Azure AD-integrated apps are as follows: c. Leverage the Microsoft Authentication Library (MSAL) for application development. d. Uniform Resource Identifiers (URIs) **shall not** use wildcards. e. URIs need to be secure and encrypted, for example, by using https schemes. f. OAuth2 implicit grant flow **shall not** be used. Use the authorization code flow instead. g. Resource owner password credential flow (ROPC) **shall not** be used. h. Certificate credentials can be used, but password credentials (client secrets) **shall not** be allowed. i. Implement a clean single sign-out experience.	Mandatory

		j. Least privilege permissions model **shall** apply. k. Delegated permissions can be used; application permissions **shall** be allowed only if necessary. l. For web apps, the token cache should be keyed by the account ID. For web APIs, the account should be keyed by the hash of the token used to call the API. MSAL.NET provides custom token cache serialization in the .NET Framework and .NET Core sub-platforms. For security and performance reasons, serialize one cache per user.	
	ICAM	Support the System for Cross-domain Identity Management (SCIM) 2.0 standard to automate provisioning and deprovisioning of users/profiles in the application.	Recommended
	ICAM	Pre-integrate the software-as-a-service (SaaS) application with Azure Active Directory and publish it in the Azure AD marketplace, also known as Azure AD gallery.	Recommended