Digital Public Facing Identity Standard

Introduction
This standard normalizes and enhances the security posture of customer facing identity
source(s). The people of Oklahoma can use portable identities to access eligible services
across application and agency boundaries. Implementation will make it easier for constituents of
the State of Oklahoma to interact with State offices, agencies and programs, allow for seamless
constituent support and enhance the security posture of public facing applications.

Purpose
Agencies implementing new customer facing solutions requiring user accounts are responsible
to plan, architect, design, implement or manage new applications utilizing B2C identity. This
document addresses the requirements, security and constraints for B2C identity deployment by
the State of Oklahoma agencies and partners.

Definitions
Application Registration – The web, mobile or SPA application registration enables the
application to sign in with Azure AD B2C. The application registration process generates
an application ID, also known as a client ID, which uniquely identifies an application.

B2C – Business to consumer, referring to agencies rendering services to customers who are
direct consumers.

Context Aware - An implementation of a security analytics engine that returns a risk score
based on multiple factors. The SAE is configurable to weigh the who, what, when, where and
why of access requests according to the organization’s needs, user populations, threats,
practices, applications and infrastructure. The engine returns scores to enforcement points (i.e.
access management software, firewalls and encryption technologies) can allow or deny access
or require step-up two-factor authentication before allowing access, a concept called adaptive
authentication.

IAM – Identity and access management.

MFA – An authentication system that requires more than one distinct authentication factor for
successful authentication. Multifactor authentication can be performed using a multifactor
authenticator or by a combination of authenticators that provide different factors. The three
authentication factors are something you know, something you have and something you are.

Standard
- Implementing parties must use Microsoft’s Azure Active Directory External Identities for
  public facing web and mobile application IAM. The product selected is based on:
  - MFA.
  - Context aware.
  - Operational insight.
  - Scalability.
- Modularity.
- Standardized protocols.
- Supportability.
- Cost.

- Application registrations shall collect only the following claims: given name, surname and email address. When a registered application needs to collect other information, that information should be collected and stored elsewhere.
- Applications may use OpenIDConnect, SAML 2, and OAuth 2 protocols for authentication and authorization.
- Onboarding of new production applications must follow provisioning processes set forth by Oklahoma Cyber Command, hosted technology teams.

**Compliance**
This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ and 34.12 and Title 62 O.S. § 35.8. OMES IS may amend and publish the amended standards policies and standards at any time. Compliance is expected with all published policies and standards, and any published amendments thereof. Employees found in violation of this standard may be subject to disciplinary action, up to and including termination.

**Rationale**
To coordinate and require central approval of state agency information technology purchases and projects to enable the chief information officer to assess the needs and capabilities of state agencies as well as streamline and consolidate systems to ensure the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

**References**
- Microsoft.
- NIST.
- One Identity.

**Revision history**
This standard is subject to periodic review to ensure relevancy.

<table>
<thead>
<tr>
<th>Effective date: 01/18/2022</th>
<th>Review cycle: Quarterly</th>
</tr>
</thead>
<tbody>
<tr>
<td>Last revised: 05/05/2022</td>
<td>Last reviewed: 05/05/2022</td>
</tr>
</tbody>
</table>

Approved by: Jerry Moore, Chief Information Officer