OKLAHOMA
Office of Management
& Enterprise Services

B2C Identity Standard

Introduction

B2C applications and processes can vary from agency to agency. This document is designed to set forth standards for those working with or within the State of Oklahoma when it comes to B2C technology.

Purpose

This standard establishes guidelines for implementing B2C identity solutions across State of Oklahoma applications and services. The objective is to normalize identity sources that Oklahoma residents can use to access eligible services across application and agency boundaries, enhancing user experience while maintaining security.

Definitions

B2C – business to consumer.

MFA – multi-factor authentication.

Standard

- Identity platform.
    - State of Oklahoma agencies shall utilize Azure Active Directory B2C as the standardized external identity platform for public-facing applications requiring user authentication.
- Required identity fields.
    - All B2C identity implementations must collect and maintain the following minimum required fields:
        - First name.
        - Last name.
        - Email address.
            - Serves as an immutable username.
            - Email addresses cannot be changed for existing user accounts. Users requiring a new email address must create a new account.
- Security requirements.
    - Multi-Factor Authentication.
        - MFA security capabilities shall be implemented for all applications.
    - Context-aware security.
        - Implementations should leverage context-aware security features including:
            - Browser behavior analysis.
            - Location pattern detection.
            - Time-based access controls.
            - Network allow/deny lists.
    - Compliance requirements.
        - All B2C identity implementations must comply with:
            - Software approval process.
            - FedRAMP standard.
                - Via Azure Commercial Cloud deployment.

- Implementation guidelines.
    - Eligibility criteria.
        - Applications must meet the following criteria to utilize the B2C identity standard:
            - Serve constituents or external partners.
            - Require user authentication.
            - Comply with OMES IS policies.
            - Intend for public or semi-public use.
    - Application metadata requirements.
        - Applications integrating with B2C identity shall define:
            - Redirect URIs and reply URLs.
            - Client names following standard naming conventions.
                - <agency-app-lifecycle>
            - Platform-specific requirements.
            - User journey flows.
                - Sign-in, sign-up, etc.
    - Profile data dependencies.
        - Applications should not rely solely on B2C identity for comprehensive profile data beyond the required fields. Applications may supplement B2C identity data with their own profile management functionality while using B2C email as the primary identifier.
- Governance and responsibilities.
    - Governance structure.
        - The OMES executive team provides governance oversight for B2C identity standard implementation and compliance.
    - Organizational responsibilities.
        - OMES IS Security.
            - Review and approve applications for B2C directory access.
            - Ensure compliance with security standards and risk management requirements.
        - OMES IS Hosted Services.
            - Facilitate application onboarding to B2C directory.
            - Provide technical integration support.
        - OMES IS Service Desk.
            - Provide user support for B2C identity-related issues.
        - OMES IS Technology Strategy.
            - Maintain technical standards and architectural guidance.
            - Provide strategic planning for B2C identity evolution.
        - OMES IS Application Team.
            - Provide technical integration support for custom flows.
- Quality Assurance.
    - Testing requirements.
        - All B2C identity integrations must undergo validation and testing to ensure proper functionality and security compliance before production deployment.
    - Accessibility.
        - B2C identity implementations shall comply with applicable accessibility standards and guidelines.

Compliance

This standard shall take effect upon publication and is made pursuant to Title 62 O.S. §§ 34.11.1 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 that the state delivers essential public services to its citizens in the most efficient manner at the lowest possible cost to taxpayers.

References

- Microsoft Azure Active Directory External Identities Documentation.
- NIST Multi-Factor Authentication Guidelines.
- OMES IS Software Approval Process.
- FedRAMP Security Standards.
- OMES IS Policies and Standards.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: MM/DD/YYYY	**Review cycle:** Annual
Last revised: 08/21/2025	**Last reviewed:** 08/21/2025
Approved by: Dan Cronin, Chief Information Officer	