OKLAHOMA
Office of Management
& Enterprise Services

Application Authentication Standard

Introduction

Application authentication is the process of verifying user identity to confirm only the right people, services and applications with the right permissions can obtain organizational resources. Single sign-on (SSO) is an application authentication scheme allowing users to log in to multiple sites and services with a single set of credentials. SSO users log in once and can access multiple services without re-entering authentication factors. This helps user productivity by reducing the number of authentication prompts needed to access multiple applications. SSO also provides support for Multi-Factor Authentication to further protect state resources by verifying the identity of the user requesting access.

Purpose

This document outlines the SSO requirements for all applications and services utilized by the State of Oklahoma.

Definitions

- Authentication factors – Categories of evidence a person must present verifying they are who they say they are. The most common are knowledge, possession and inherence (something you know (password), something you have (e.g., mobile phone) and something you are (e.g., fingerprint).
- Life safety system – An interior building element designed to protect and evacuate the building population in emergencies, including fire and tornadoes and less critical events such as power failures.
- MFA – An authentication protocol requiring two different types of authentication (e.g., password, biometrics, authenticator application, etc.).
- SSO – Single sign-on; an authentication method allowing users to log in with a single ID to several related software systems.
- TLS – Transport Layer Security; an authentication and encryption protocol widely implemented in browsers and web servers.

Standard

The State of Oklahoma requires all applications and services with a logon component to adhere to the following guidelines:

- Applications must use a standard State of Oklahoma SSO provider aligned with the type of applications and user audience or an alternative approved by OMES-ISD.
- All applications must use multi-factor authentication using two different authentication factors.
- Applications must use TLS 1.2 or greater to encrypt authentication and application data in transit over the network.
- Applications and systems flagged as life safety or otherwise critical systems must have redundant authentication systems to ensure availability during a crisis.

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.

Revision history

This standard is subject to periodic review to ensure relevancy.

Effective date: 05/23/2025	**Review cycle:** Annual
Last revised: 05/23/2025	**Last reviewed:** 05/23/2025
Approved by: Dan Cronin, Chief Information Officer	