State of Michigan
Technical Standard

1340.00.020.08 Enterprise Identity and Access Management Services Standard

Issued:	01/12/2022
Revised:	
Reviewed:	01/30/2025
Next Review Date (1 yr):	01/30/2026

Authoritative Policy:	1340.00 Information Technology Information Security Policy
Associated Procedures:	
Distribution:	Statewide

Purpose

This standard provides Enterprise Identity, Credential, and Access Management (ICAM) Services requirements for state of Michigan (SOM) information systems in alignment with the SOM 1340.00.020.01 Access Control Standard and the SOM 1340.00.080.01 Identification and Authentication Standard.

Contact/Owner

Department of Technology, Management and Budget (DTMB)
Center for Shared Solutions (CSS)
Enterprise Identity and Access Management (EIAM)

and

Cybersecurity and Infrastructure Protection (CIP)

and

Department of Technology, Management and Budget (DTMB)
Office of the Chief Technology Officer (OCTO)
Endpoint & User Management (EUM)

Scope

This standard is applicable to all information systems that are part of the Executive Branch Departments, Agencies, Boards or Commissions, and business or vendor partners that manage SOM information technology (IT) Resources including, but not limited to, networks, systems, computers, data, databases, and applications. This standard supersedes all IT security standards that may be in conflict with this standard. If discrepancies exist, this standard stands as the authoritative document.

STANDARD

INTRODUCTION

An Identity Management System refers to information systems and technologies based on approved polices that can be used for enterprise and federated identity management.

Identity Management describes the provisioning and management of individual identities, their authentication, authorization, and roles and privileges within or across system and enterprise boundaries. This reduces the number of access accounts for individuals with the additional goals of increasing security, and productivity and decreasing cost, downtime, and repetitive tasks.

Typical identity management functionality includes but it is not limited to the following:

- User provisioning
- Access control
- Authorization and non-repudiation
- Digital identity management
- Password management

REQUIREMENTS

IT systems and applications requiring authentication or validation of users' credentials for either local or network access to internal or external organizational data and/or IT business and supporting SOM computing and infrastructure systems, are required to use a SOM ICAM Service based on the implementation time frames provided in this standard.

Currently the SOM DTMB provides the following ICAM solutions:

- DTMB Owned and Managed Active Directory (AD) based services
- DTMB MiLogin based services

New IT systems and applications must support and implement ICAM provided by the DTMB enterprise services offerings. Existing IT systems must be updated to support and implement an enterprise ICAM services offerings as part of any significant application updates/architecture changes, application rewrites, or infrastructure revisions as identified as part of the required EASA review process. The use of authorization access controls in addition to those provided by the ICAM service offerings for individuals and/or roles within IT systems and applications is permitted. General public application access authentication services, including non-organizational user access, will be provided using MiLogin services.

COMPLIANCE AND EXCEPTION

If an exception to this standard is necessary, agencies, in conjunction with their DTMB representatives, must comply with the approved DTMB process outlined in SOM 1305.00.02 Technical Policy and Product Exception Standard and SOM

1305.00.02.01 Technical Review Board (TRB) and Executive Technical Review Board (ETRB) Exception Procedure.

Preapproved exception to this standard include:

- MSP Michigan Criminal Justice Information Network (MiCJIN) Single Sign On Solution (NetIQ) is a preapproved exception for Criminal Justice Information Services (CJIS) data only.
- DTMB approved and implemented privileged access tools and multi-factor authentication systems (e.g., Cyberark, Centrify, and SecurID).

REFERENCES

SOM 1305.00.02 Technical Policy and Product Exception Standard

SOM 1305.00.02.01 Technical Review Board (TRB) and Executive Technical Review Board (ETRB) Exception Procedure

SOM 1340.00.020.01 Access Control Standard

SOM 1340.00.080.01 Identification and Authentication Standard

APPROVING AUTHORITY

Michelle Lange, Acting Director Issued: 01/12/2022