REQUIREMENTS SPECIFICATION

Classification: UNCLASSIFIED // FOUO

Document ID: REQ-2025-AUTH-0156

Version: 3.1 | Last Updated: January 22, 2025

Authentication Module Requirements

Legacy System Modernization - User Access Control

Program:	Enterprise Modernization Initiative
Component:	Authentication & Authorization Services
Owner:	Identity Management Division
Status:	AI-Generated Draft - Pending Review

1. INTRODUCTION

This document specifies the functional and non-functional requirements for the modernized Authentication Module. The module provides secure user authentication, session management, and access control capabilities for the enterprise application portfolio.

1.1 Document Scope and Applicability

This specification applies to all authentication components within the enterprise modernization program. The requirements herein are derived from analysis of the legacy COBOL-based authentication system (module AUTH-MAIN) and updated to reflect current federal security standards.

Implementation teams should reference NIST SP 800-53 controls for detailed guidance on security requirements applicable to federal information systems.

2. FUNCTIONAL REQUIREMENTS

2.1 User Authentication

The system shall provide multi-factor authentication (MFA) capabilities compliant with NIST SP 800-63B guidelines. Authentication methods shall include:

REQ-ID	Requirement	Priority
AUTH-001	Support username/password authentication with complexity requirements	High
AUTH-002	Implement TOTP-based second factor authentication	High
AUTH-003	Support PIV/CAC smart card authentication	High
AUTH-004	Provide SAML 2.0 federation capability	Medium
AUTH-005	Support OAuth 2.0 / OpenID Connect protocols	Medium

2.2 Session Management

The system shall implement secure session management with configurable timeout periods and automatic session termination upon detecting anomalous activity patterns.

REQ-ID	Requirement	Priority
SESS-001	Implement secure session tokens using cryptographic random generation	High
SESS-002	Enforce session timeout after 15 minutes of inactivity	High
SESS-003	Provide concurrent session limiting per user account	Medium
SESS-004	Support forced session termination by administrators	High

3. IMPLEMENTATION NOTES

The following technical guidance is provided for implementation teams undertaking the authentication module modernization effort. Development should follow the agency secure coding standards documented in DEV-STD-2024-001.

All code must undergo static analysis scanning and peer review prior to deployment to production environments. Security testing shall be conducted in accordance with the approved test plan.

4. NON-FUNCTIONAL REQUIREMENTS

4.1 Performance Requirements

The authentication module shall meet the following performance benchmarks under normal operating conditions:

Metric	Requirement	Measurement Method
Response Time	< 500ms for 95th percentile	APM monitoring
Throughput	> 1000 authentications/second	Load testing
Availability	99.99% uptime	Service monitoring
Failover	< 30 second recovery time	Failover testing

— END OF DOCUMENT —