State of California

Department of Technology

Office of Information Security

Multi-factor Authentication Supplemental

SIMM 5360-D

April 2023

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	April 2023	California Information SecurityOffice	New supplemental document to support the SIMM 5360-C MFA standard.

TABLE OF CONTENTS

Contents

I. Introduction

This document is a supplemental to support the Statewide Information Management Manual (SIMM) 5360-C Multi-Factor Authentication Standard, that contains instructions, workflows, processes, and security controls to ensure compliant and secure authentication for information assets. This document contains frequently asked questions about the multi-factor authentication (MFA) standard and provides hypothetical real-world examples of how an entity would implement MFA based on the processes and workflows defined in the SIMM 5360-C, Federal Information Processing Standard (FIPS) 140, and National Institute of Standards and Technology (NIST) Special Publication (SP) 800-63B.

II. Frequently Asked Questions (FAQs):

Q. Why is an MFA standard needed?

A. A standard for MFA is required to ensure that all implementations of MFA adhere to a common set of rules and best practices that are outlined in FIPS 140 and NIST SP 800-63B. This makes it easier for users to understand how to use MFA, and it ensures that different MFA solutions can work together seamlessly. Additionally, it helps ensure that MFA is implemented securely, as a poorly designed or implemented MFA solution can introduce new vulnerabilities into a system.

Q. Who is responsible for implementing MFA?

A. The responsibility for implementing MFA falls on the organization's IT and/or security team, who are responsible for selecting and implementing the MFA solution that meets the organization's needs and complies with relevant standards and regulations. They are also responsible for providing awareness and educating customers on the importance, installation, and use of their selected solution.

Q. How does the entity ensure the solution adequately protects the authenticator from common exploitation techniques?

A. The entity will ensure its selected and implemented authentication solutions depend on a combination of secret keys that require integrity protection, protection from disclosure, and properly implemented secure random number generators and cryptography.

Q. How does the entity ensure the solution protects the verifier from common exploits and ensure a request for access is from the user bound to the authenticator?

A. The entity will ensure its selected and implemented solution confirms the binding

requires proof-of-possession of ‘what you have,’ evidence that ‘what you know’ and/or ‘what you are’ have been confirmed.

Q. How are communications among components of the authentication solution adequately protected using strong, well-known, and testable cryptographic standards?

A. The entity will ensure its selected and implemented communications require integrity protection, source authentication, and/or encryption to protect authentication evidence from modification or replay.

Q. Does the solution provide support for managing the lifecycle of digital identities and authenticators?

A. Organizations are responsible for the lifecycle management of digital identities. Solutions that support these activities can be more easily managed, and therefore often more securely managed.

Q. If the solution authenticates a user’s request on behalf of a requested service, does the solution securely communicate that authentication to the requested service?

A. Secure integration of an authentication solution into existing mechanisms ensures that the solution does not allow malicious actors to bypass authentication.

Q. Are there approved or established procurement options for MFA solutions?

A. Please consult with your procurement team to visit the Cal eProcure store to review established DGS contracts for MFA vendors.

Q. How do you validate a vendor’s technology against FIPS 140?

A. Vendors are to submit their technology to the NIST Cryptographic Module Validation Program to be federally certified. An entity can determine the FIPS 140 validation level of a vendor product and module(s) by doing a search at https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search/. Non-validated cryptography is viewed by NIST as providing no protection to the information or data.

III. Owners of Information Assets:

Use Case Example 1: Online Email

An Information Asset Owner (IAO) has identified that their department has a business need to provide email access to employees while they are working remote and/or traveling. The executive team specifically requested that the users have the ability to access email without having to use any type of remote access technology and simply only need a secure web browser to gain access to email. The IAO will need to analyze the information asset and apply appropriate authentication controls to ensure risk is mitigated to an acceptable level.

The first task that the IAO will need to accomplish is to classify all data types that the information asset processes, stores, transmits, and visually presents to the user. In this case, the department's email system at the very minimum could contain Social Security numbers and banking information from accounting and potential medical information from Human Resources. After classifying the data, the IAO will go through their FIPS 199 System Categorization process, which they have ranked High as their highest watermark in this specific instance. Afterwards, the IAO will need to identify the correct Authenticator Assurance Level (AAL) of the information asset to appropriately apply secure and mandated authentication controls around the information asset. This will determine if they need to apply MFA or not. After going through the AAL determination workflow, the IAO identified that their information asset is ranked as an AAL3. The IAO will now review the minimum and acceptable required authentication mechanisms and security controls and implement them to the information asset. In this use case, the IAO will enforce a Single-Factor Cryptographic Device (which will be an authenticator app, that has been validated as a FIPS 140 Level 1 verifier or higher, that can be installed on an individual's phone) used in conjunction with a Memorized Secret (which will be the user's username and password). The IAO will additionally ensure that access control lists are implemented to only allow U.S. based logins and that the web browser is utilizing a form of encryption over HTTP for Man-in-the-Middle and replay attack resistance. A two-month retention policy will also be set to archive all emails. The IAO will also enforce authentication tokens to expire every 12 hours, or after 15 minutes of inactivity. This will force users to reauthenticate back into the email system in the event that the user forgets to log out or if their account gets compromised.

Use Case Example 2: Public web site that hosts no Personal Identifiable Information (PII) / Protected Health Information (PHI) / Law Enforcement Sensitive (LES) controlled data

An Information Asset Owner (IAO) has identified that their department has a business need to provide a publicly accessible information website, showcasing a Geographic Information System (GIS) to graphically display public data to customers. In addition, the business requirements do not require authentication for customers to access the information asset. The IAO will need to analyze the information asset and apply appropriate authentication controls to ensure risk is mitigated to an acceptable level.

The first task that the IAO will need to accomplish is to classify all data types that the information asset processes, stores, transmits and visually presents to the user. In this case, the information asset does not contain any personal or health related information, as defined in Civil Code §§ 1798-1798.140. The IAO has also worked through the FIPS 199 System Categorization process and identified that the information asset has ranked Low as its highest watermark. Next, the IAO will assign an Authenticator Assurance Level (AAL), and in this instance, due to information asset only displaying open and public information that requires no authentication to access, the information asset is ranked as an AAL 0 according the AAL determination workflow. AAL0 is intended to define open and public data, requiring no additional mandatory authenticator controls. It is at the discretion of the IAO, and the department, on how they want to secure the information asset based off its FIPS 199 security categorization. The IAO has decided that as a precautionary measure and the FIPS 199 Low security categorization, that at a minimum they will implement web application firewall, allow only U.S. based communication, and utilize a form of encryption over HTTP for Man-in-the-Middle and replay attack resistance.

IV. Authentication Technology Types

Risk Rating	**Authentication Type**	**Vulnerabilities**
Low Risk (Strongest)	Passwordless, Codeless	Malware, Theft
Medium Risk	Code Generator Applications	Malware, Theft, Phishing, Vishing
Medium-High Risk	SMS or E-mail based, Password Manager	Malware, Theft, Phishing, Vishing, Sim-swapping, Account Resets, Account takeovers
High Risk	Quality Passwords	Malware, Phishing, Vishing, Account Resets, Cracking, Password Guessing
Very High Risk – NOT ACCEPTABLE (Weakest)	Unique or Shared Passwords	Malware, Phishing, Vishing, Account Resets, Cracking, Password Guessing, Credential stuffing

- **Passwordless:** A form of authentication that verifies the user's identity without the use of a traditional password and requires two or more authentication factors in the form of biometrics, physical or software one-time code generators, trusted

devices, and/or physical tokens. (e.g. smart card, Fast Identity Online (FIDO) based physical security keys).

- **Codeless:** A form of authentication that requires a quality password and a second factor in the form of an application-based prompt where the user either accepts or denies an authentication attempt. (e.g. mobile push notification)
- **Code Generator Applications:** A form of authentication that requires a quality password and a second factor, in the form of a string of characters, that is generated and accessed through a software-based application. The user would be required to input the string of characters into a log-in prompt for successful authentication. (e.g. mobile authenticator applications)
- **SMS or E-mail based:** A form of authentication that requires a quality password and a second factor, in the form of a string of characters, that is generated and sent via text message (SMS) or e-mail to the user. The user would be required to input the string of characters into a log-in prompt for successful authentication.
- **Password Manager**: A single form of authentication that includes a unique or quality password, and is stored on a securely encrypted application, archive, or software.
- **Quality Passwords**: A single form of authentication where the password is long, random and includes a series of special characters (e.g. passphrases)
- **Unique Passwords**: A single form of authentication where the passwords are not complex, long or random. They may contain personal information about the user; however, the unique password is not shared between different accounts. (e.g. passwords that include social security numbers, pet names, birthdates, are 8 characters long)
- **Shared Passwords**: A form of authentication where a single password is required and is shared between different systems for various accounts.

V. References

State entities shall use the latest version of the following when implementing this standard:

1. NIST Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management: https://pages.nist.gov/800-63-3/sp800-63b.html
2. Federal Information Processing Standards, Standards for Security Categorization of Federal Information and Information Systems (FIPS 199): https://nvlpubs.nist.gov/nistpubs/fips/nist.fips.199.pdf
3. Privacy Related Civil Code §§ 1798-1798.140: https://leginfo.legislature.ca.gov/faces/codes_displayexpandedbranch.xhtml?toc

Code=CIV&division=3.&title=1.8.&part=4.&chapter=1.&article=

4. SIMM 5360-C – Multi-Factor Authentication Standard: TBD