State of California

Department of Technology

Office of Information Security

Multi-Factor Authentication Standard

SIMM 5360-C

May 2023

REVISION HISTORY

REVISION	DATE OF RELEASE	OWNER	SUMMARY OF CHANGES
Initial Release	May 2023	California Information Security Office	New Standard in support of SAM Section 5360, Identity and Access Management

TABLE OF CONTENTS

Contents

I. INTRODUCTION

To ensure compliance with State Information Management Manual (SIMM) 5305-A and the development of a mature information security and risk management program, Multi-Factor Authentication (MFA) is a required technology for identity assurance. MFA can help securely authenticate an individual for access to a state information asset.

MFA protects against a multitude of threats including but not limited to:

- Compromised password – A password can be used by anybody who gets their hands on it. If a user writes down their password on a pad of paper, for example, that password can be stolen to gain access to an account.
- Social Engineering – The psychological manipulation of people into performing actions or divulging confidential information.
- Key Logging – A program designed to record which keys are pressed on a computer keyboard used to obtain passwords or encryption keys and thus bypass other security measures.
- Phishing – A digital form of social engineering that uses authentic-looking, but fraudulently forged emails, to request information from users or direct them to a fake Web site that requests information.
- Brute-Force Attack – An attack method using multiple numeric/alphanumeric passwords and trying all possible combinations to find a match.

The National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-63B defines Authenticator Assurance Levels (AAL), which refers to the authentication process and how additional factors may impact risk mitigation, provides standard definitions, and assigns assurance levels for various authentication solutions to assist in the selection of an MFA solution.

II. MINIMUM MULTIFACTOR AUTHENTICATION REQUIREMENTS

A. IDENTIFY

Any publicly accessible information asset that stores, processes, transmits or visually presents confidential, sensitive, or personal information (as defined in Civil Code sections 1798-1798.140) is subjected to this standard. This standard is designed to align with and support the California Information Practices Act of 1977 and Cal-Secure.

Based on the criticality, and the potential negative impact a compromised information asset could have, one of four AALs shall be assigned for each publicly accessible information asset. The AAL will determine the security controls needed for proper compliance, and to ensure that risk is mitigated to the most acceptable level.

The AALs are as follows:

AAL0: Information assets that only display open and public information that requires no authentication to access.

AAL1: Provides some assurance that the member of the public or employee (User) controls an authenticator bound to the subscriber's account. AAL1 requires either Single-Factor or Multi-Factor Authentication using a wide range of available authentication technologies. Successful authentication requires that the User prove possession and control of the authenticator through a secure authentication protocol.

AAL2: Provides high confidence that the User controls authenticator(s) bound to the subscriber's account. Proof of possession and control of two distinct authentication factors is required through secure authentication protocol(s). Approved cryptographic techniques are required at AAL2 and above.

AAL3: Provides very high confidence that the User controls authenticator(s) bound to the subscriber's account. Authentication at AAL3 is based on proof of possession of a key through a cryptographic protocol. AAL3 authentication MUST use a hardware-based authenticator and an authenticator that provides verifier impersonation resistance; the same device MAY fulfill both these requirements. To authenticate at AAL3, Users MUST prove possession and control of two distinct authentication factors through secure authentication protocol(s).

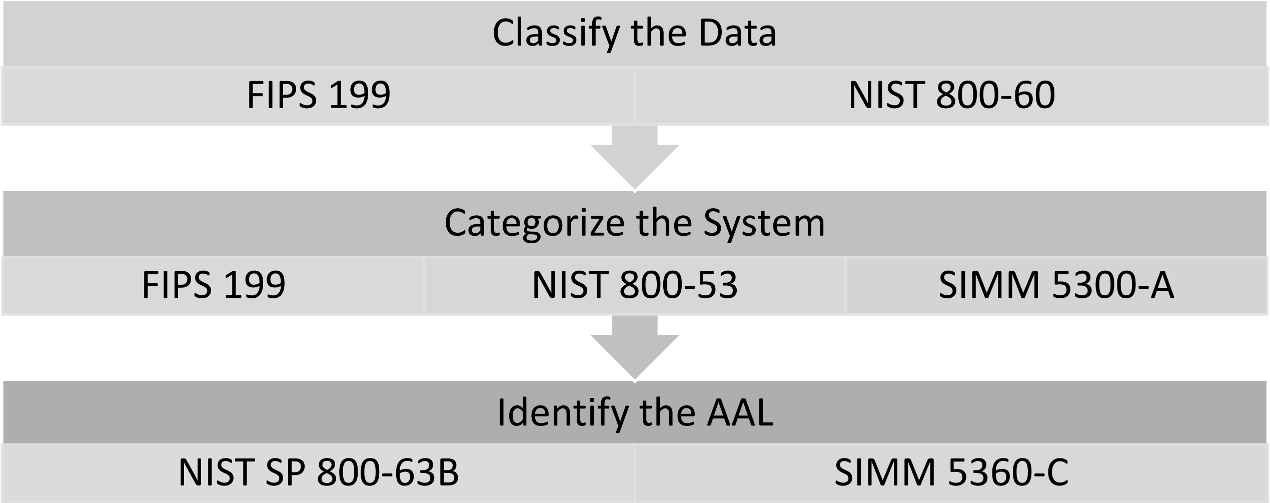
Before assignment of an AAL, the data of the information asset must be classified, and the information asset must be categorized in accordance with the SIMM 5305-A Information Security Program Management Standard. This classification will help determine the appropriate AAL while contextualizing the identities accessing the information asset.

The defined identities are categorized into two groups: state enterprise identity and public member identity.

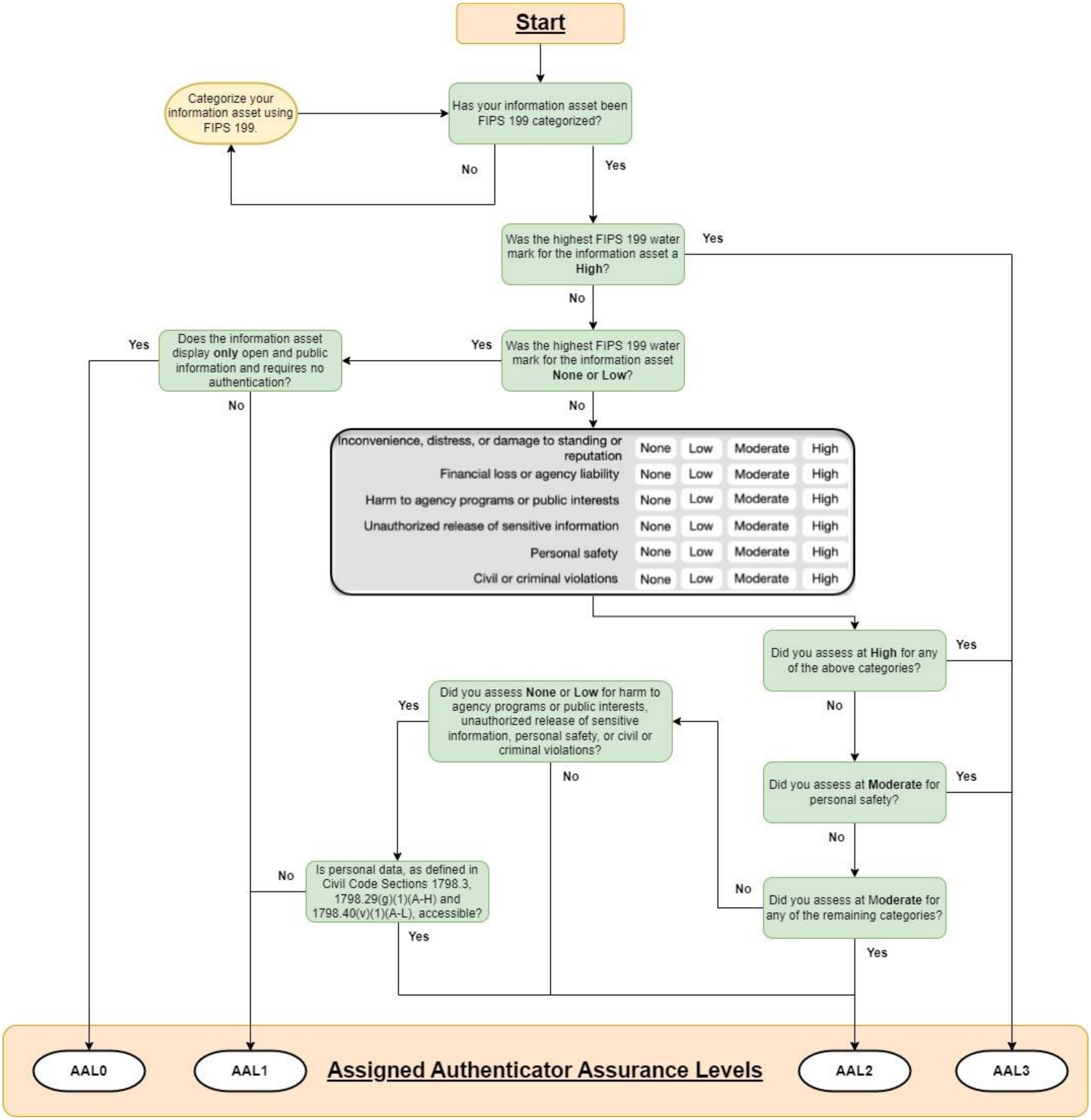
- State enterprise identity, or simply enterprise identity, refers to the unique representation of an employee, a contractor, an enterprise user, a mission or business partner, a device, or a technology that a state entity manages to achieve its mission and business objectives.

- Public member identity refers to the unique representation of an individual that a state entity interacts with, but does not directly manage, to achieve its mission and business objectives.

The following diagram illustrates the actionable items that must be performed before the assignment of an AAL:



The appropriate authenticator requirements to an information asset, are to be assigned after the AAL has been determined. The following flow diagram illustrates the AAL determination process.


Start
Has your information asset been FIPS 199 categorized?
No
Categorize your information asset using FIPS 199.
Yes
Was the highest FIPS 199 water mark for the information asset a **High**?
Yes
No
Was the highest FIPS 199 water mark for the information asset **None or Low**?
Yes
Does the information asset display **only** open and public information and requires no authentication?
Yes
No
No
Did you assess at **High** for any of the above categories?
Yes
No
Did you assess at **Moderate** for personal safety?
Yes
No
Did you assess at **Moderate** for any of the remaining categories?
No
Yes
Did you assess **None** or **Low** for harm to agency programs or public interests, unauthorized release of sensitive information, personal safety, or civil or criminal violations?
Yes
No
Is personal data, as defined in Civil Code Sections 1798.3, 1798.29(g)(1)(A-H) and 1798.40(v)(1)(A-L), accessible?
No
Yes
Assigned Authenticator Assurance Levels
AAL0
AAL1
AAL2
AAL3

Inconvenience, distress, or damage to standing or reputation	None	Low	Moderate	High
Financial loss or agency liability	None	Low	Moderate	High
Harm to agency programs or public interests	None	Low	Moderate	High
Unauthorized release of sensitive information	None	Low	Moderate	High
Personal safety	None	Low	Moderate	High
Civil or criminal violations	None	Low	Moderate	High

B. PROTECT

Refer to SIMM 5300-A State-Defined Security Parameters, the NIST SP 800-53, and the Federal Information Processing Standards (FIPS) 199 publications to cross-reference the minimum standard necessary when assigning AALs and security controls for information assets. State entities shall validate vendor solutions and modules to meet the minimum requirements outlined in this standard. The table below identifies the AAL of an information asset and its minimum assigned Security Categorization. The categorization and classification of information assets shall be used in the determination of an asset's needed level of protection. If the information asset's level of protection is not clear, the state entity is to protect the asset to the categorization level of "Moderate" as defined by FIPS 199 and AAL 2 as defined by NIST SP 800-63B. The assigned AAL of an information asset cannot be lower than its associated FIPS 199 categorization.

(SIMM-5300-A State-Defined Security Parameters can be found on AgencyNet or requested through security@state.ca.gov.)

Minimum Assigned Security Categorization (FIPS 199)

Security Categorization (FIPS 199)	**Low**	**Moderate**	**High**
	↓	↓	↓
Authenticator Assurance Level (NIST SP 800-63B)	AAL 0 or AAL 1	AAL 2	AAL 3

The tables below identify the permitted authenticator types for each AAL to ensure that an authenticator solution is validated to resist foreseeable threats and reduces risk to the most acceptable level while ensuring statutory, legal, and state compliance. Each entity shall implement the following mechanisms at a minimum for the assigned AAL of their publicly accessible information assets:

Requirement	**Authenticator Assurance Level 0 (AAL0)**
Example	The loss of the confidentiality, integrity, or availability of the information asset(s) would have minimal to no impact on organizational operations, organizational assets, or individuals. Any adverse effects would cause minimal to no degradation in the effectiveness and efficiency of primary functions and capabilities, little or no financial loss, and/or results in no harm to individuals.

AAL0 is intended to apply to open and public data, requires no additional authenticator controls, and allows the entity discretion on how to secure the information asset based on its FIPS 199 security categorization.

Requirement	**Authenticator Assurance Level 1 (AAL1)**
Example	The loss of the confidentiality, integrity, or availability of the information asset(s) would have limited adverse effects on organizational operations, organizational assets, or individuals. Any adverse effects would cause limited, yet notable degradation in the effectiveness and efficiency of primary functions and capabilities, minor financial loss, and/or results in minor harm to individuals, not including loss of life or bodily injury.
Permitted Authenticator Types	**Choose one of these:** • Memorized Secret • Look-Up Secret • Out-of-Band Devices • Single-Factor One-Time Password (OTP) Device • Multi-Factor OTP Device • Single-Factor Cryptographic Software • Single-Factor Cryptographic Device • Multi-Factor Cryptographic Software • Multi-Factor Cryptographic Device
FIPS 140 Validation	Level 1 (Government agency verifiers)
Security Controls	SP 800-53 Low Baseline (or equivalent)
Reauthentication	30 days
Replay Resistance	Not Required
Verifier – Compromise Resistance	Not Required
Verifier – Impersonation Resistance	Not Required

Authentication Intent	Not Required
MitM Resistance	Required
Records Retention Policy	Record retention is required and MUST align with State Administrative Manual (SAM) 1600 Records Management Program (RMP).
Privacy Controls	Required

Requirement	**Authenticator Assurance Level 2 (AAL2)**
Example	The loss of the confidentiality, integrity, or availability of the information asset(s) would have serious adverse effects on organizational operations, organizational assets, or individuals. Any adverse effects would cause significant degradation in the effectiveness and efficiency of mission-critical capabilities (although primary functions can still be performed), significant financial loss, and/or results in significant harm to individuals, not including loss of life or bodily injury.
Permitted Authenticator Types	Multi-Factor OTP Device Multi-Factor Cryptographic Software Multi-Factor Cryptographic Device Memorized Secret **plus**: Look-Up Secret Out-of-Band Device Single-Factor OTP Device Single-Factor Cryptographic Software Single-Factor Cryptographic Device
FIPS 140 Validation	Level 1 (Government agency authenticators and verifiers)
Security Controls	SP 800-53 Moderate Baseline (or equivalent)
Reauthentication	Requires reauthentication after 30 minutes of inactivity; however, may only require MFA authentication once within a 12-hour period.
Replay Resistance	Required
Verifier – Compromise Resistance	Not Required

Verifier – Impersonation Resistance	Not Required
Authentication Intent	Recommended
MitM Resistance	Required
Records Retention Policy	Record retention is required and MUST align with SAM 1600 RMP.
Privacy Controls	Required

Requirement	**Authenticator Assurance Level 3 (AAL3)**
Example	The loss of the confidentiality, integrity, or availability of the information asset(s) would have severe or catastrophic adverse effects on organizational operations, organizational assets, or individuals. Any adverse effects would cause severe degradation in or loss of mission-critical functions so they cannot be performed, major financial loss and/or statutory fines, and/or would pose severe risk to public safety including loss of life or injury.
Permitted Authenticator Types	Multi-Factor Cryptographic Device Single-Factor Cryptographic Device used in conjunction with Memorized Secret Multi-Factor OTP device (software or hardware) used in conjunction with a Single-Factor Cryptographic Device Multi-Factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software Single-Factor OTP device (hardware only) used in conjunction with a Multi-Factor Cryptographic Software Authenticator Single-Factor OTP device (hardware only) used in conjunction with a Single-Factor Cryptographic Software Authenticator and a Memorized Secret.
FIPS 140 Validation	Level 2 overall (MULTI-FACTOR authenticators) Level 1 overall (verifiers and SINGLE-FACTOR Crypto Devices) Level 3 physical security (all authenticators)
Security Controls	SP 800-53 High Baseline (or equivalent)
Reauthentication	Requires re-authentication after 15 minutes of inactivity or a 12-hour period. Reauthentication MUST require MFA.
Replay Resistance	Required

Verifier – Compromise Resistance	Required
Verifier – Impersonation Resistance	Required
Authentication Intent	Required
MitM Resistance	Required
Records Retention Policy	Record retention is required and MUST align with SAM 1600 RMP.
Privacy Controls	Required

Refer to https://pages.nist.gov/800-63-3/sp800-63b.html for further implementation guidelines.

Considerations: Note that all Multi-Factor Authentication protocols do not provide the same level of protection. The most significant vulnerability in MFA is how the MFA codes are created, handled, and sent to the users. Attempt to avoid codes that require manual input by the user to authenticate. Rather have your department aim for codeless (e.g., push-notifications or number matching through a mobile authenticator application) or passwordless (e.g., physical token, third-party identity provider) MFA technologies to implement or further mature the current program.

Please refer to SIMM 5360-D for more examples of authentication technology types and their risks associated with them.

C. DETECT

Detect - There are no additional **Detect** capabilities required by this standard.

D. RESPOND

Respond - There are no additional **Respond** capabilities required by this standard.

E. RECOVER

Recover - There are no additional **Recover** capabilities required by this standard.

III. Exceptions

Exceptions: Any exceptions must be documented, based on a compelling business case to be determined by the state entity. All risks identified and accepted via an authorized exception/policy variance are approved by the business/program owner, entity head, Information Security Officer (ISO), and Chief Information Officer (CIO). If the entity reports to an Agency, approval is needed by the Agency Information Security Officer (AISO) and Agency Information Officer (AIO) as well.

IV. Definitions

Controlled Unclassified Information (CUI) - CUI is government created or owned information that requires safeguarding or dissemination controls consistent with applicable laws, regulations and government wide policies. CUI is not classified information. It is not corporate intellectual property unless created for or included in requirements related to a government contract.

Look-Up Secret - A look-up secret authenticator is a physical or electronic record that stores a set of secrets shared between the User and the credential service provider. The User uses the authenticator to look up the appropriate secret(s) needed to respond to a prompt from the verifier. For example, the verifier may ask a User to provide a specific subset of the numeric or character strings printed on a card in table format. A common application of look-up secrets is the use of "recovery keys" stored by the subscriber for use in the event another authenticator is lost or malfunctions. A lookup secret is something you have.

Memorized Secret - Memorized Secret authenticator — commonly referred to as a password or, if numeric, a Personal Identification Number (PIN) — is a secret value intended to be chosen and memorized by the user. Memorized secrets need to be of sufficient complexity and secrecy that it would be impractical for an attacker to guess or otherwise discover the correct secret value. A memorized secret is something you know.

MULTI-FACTOR Authentication - A second, third or fourth form of authentication, not limited, but usually in the form of “something you have” or “something you are” that is used in conjunction with a first form of authentication that is typically a PIN or passcode in the form of “something you know”. This allows that in the event if one form of authentication has been compromised, an unauthorized user still has at least one more barrier to breach before successfully exploiting a target system.

MULTI-FACTOR Crypto Device - A Multi-Factor cryptographic device is a hardware device that performs cryptographic operations using one or more protected cryptographic keys and requires activation through a second authentication factor. Authentication is accomplished by proving possession of the device and control of the key. The authenticator output is provided by direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. The Multi-Factor cryptographic device is something you have, and it MUST be activated by either something you know or something you are.

MULTI-FACTOR Crypto Software - A Multi-Factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media that requires activation through a second factor of authentication. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The Multi-Factor software cryptographic authenticator is something you have, and it MUST be activated by either something you know or something you are.

MULTI-FACTOR OTP Device – A Multi-Factor OTP device generates OTPs for use in authentication after activation through an additional authentication factor. This includes hardware devices and software-based OTP generators installed on devices such as mobile phones. The second factor of authentication may be achieved through some kind of integral entry pad, an integral biometric (e.g., fingerprint) reader, or a direct computer interface (e.g., USB port). The OTP is displayed on the device and manually input for transmission to the verifier. For example, an OTP device may display 6 characters at a time, thereby proving possession and control of the device. The Multi-Factor OTP device is something you have, and it MUST be activated by either something you know or something you are.

Out-of-Band - The out-of-band device SHOULD be uniquely addressable and communication over the secondary channel MUST be encrypted. Methods that do not prove possession of a specific device, such as voice-over-IP (VOIP) or email, MUST NOT be used for out-of-band authentication.

SINGLE-FACTOR Crypto Software - Single-Factor software cryptographic authenticator is a cryptographic key stored on disk or some other "soft" media. Authentication is accomplished by proving possession and control of the key. The authenticator output is highly dependent on the specific cryptographic protocol, but it is generally some type of signed message. The Single-Factor software cryptographic authenticator is something you have.

SINGLE-FACTOR Crypto Device - A Single-Factor cryptographic device is a hardware device that performs cryptographic operations using protected cryptographic key(s) and provides the authenticator output via direct connection to the user endpoint. The device uses embedded symmetric or asymmetric cryptographic keys and does not require activation through a second factor of authentication. Authentication is accomplished by proving possession of the device via the authentication protocol. The authenticator output is provided by direct connection to the user endpoint and is highly dependent on the specific cryptographic device and protocol, but it is typically some type of signed message. A Single-Factor cryptographic device is something you have.

SINGLE-FACTOR OTP Device - A Single-Factor OTP device generates OTPs. This category includes hardware devices and software-based OTP generators installed on devices such as mobile phones. These devices have an embedded secret that is used as the seed for generation of OTPs and does not require activation through a second factor. The OTP is displayed on the device and manually input for transmission to the verifier, thereby proving possession and control of the device. An OTP device may, for example, display 6 characters at a time. A Single-Factor OTP device is something you have.

V. References

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

1. NIST Special Publication 800-53 Security and Privacy Controls for Information Systems and Organizations: https://csrc.nist.gov/Projects/risk-management/

2. NIST Special Publication 800-63B, Digital Identity Guidelines Authentication and Lifecycle Management: https://pages.nist.gov/800-63-3/sp800-63b.html

3. NIST Special Publication 800-63B Authenticator Assurance Levels: https://pages.nist.gov/800-63-3-Implementation-Resources/63B/AAL/

4. NIST Definition of Controlled Unclassified Information: https://csrc.nist.gov/glossary/term/controlled_unclassified_information/

5. 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

6. Statewide Information Management Manual (SIMM) 5300 policies: https://cdt.ca.gov/policy/simm/#SIMM

7. Information Security Program Management Standard SIMM 5305-A: https://cdt.ca.gov/wp-content/uploads/2018/01/SIMM-5305_A_2018-0108.pdf

8. Multi-Factor Authentication Supplemental SIMM 5360-D: TBD

9. Cloud Computing policy SIMM 4983.1:

https://www.dgs.ca.gov/Resources/SAM/TOC/4900/4983-1/

10. State Administrative Manual (SAM) 1600 Records Management Program (RMP) https://www.dgs.ca.gov/Resources/SAM/TOC/1600/

11. Cryptographic Module Validation Program: https://csrc.nist.gov/projects/cryptographic-module-validation-program/

12. Cryptographic Module Validation Program Search: https://csrc.nist.gov/Projects/cryptographic-module-validation-program/validated-modules/Search/

13. HIPAA Information that is Protected: https://www.hhs.gov/hipaa/for-professionals/privacy/index.html

14. Personal Information that is Protected under Civil Code 1798.3: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.3

15. Personal Information that is Protected under Civil Code 1798.29: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.29

16. Personal Information that is Protected under Civil Code 1798.140: https://leginfo.legislature.ca.gov/faces/codes_displaySection.xhtml?lawCode=CIV&sectionNum=1798.140.

17. California Consumer Privacy Act (CCPA): https://oag.ca.gov/privacy/ccpa/

18. State of California Independent Security Assessment Criteria: *Please reach out to the California State Military Department for a copy of the reference.*

VI. QUESTIONS

Please reference the SIMM 5360-D – MFA Supplemental for FAQs, examples and additional information regarding MFA. Questions regarding the implementation of this standard may be sent to:

California Department of Technology
Office of Information Security
Security@state.ca.gov