1 **Draft NIST Special Publication 800-140E**

2

3 CMVP Approved Authentication 4 Mechanisms:

5 *CMVP Validation Authority Requirements for ISO/IEC*
6 *19790:2012 Annex E and ISO/IEC 24759:2017*

7

8 Kim Schaffer
9

10

11

12

13
14
15

16 I N F O R M A T I O N S E C U R I T Y

17

18

National Institute of
Standards and Technology
U.S. Department of Commerce

Draft NIST Special Publication 800-140E

CMVP Approved Authentication Mechanisms:

CMVP Validation Authority Requirements for ISO/IEC 19790:2012 Annex E and ISO/IEC 24579:2017

Kim Schaffer
Computer Security Division
Information Technology Laboratory

October 2019

U.S. Department of Commerce
Wilbur L. Ross, Jr., Secretary

National Institute of Standards and Technology
Walter Copan, NIST Director and Under Secretary for Standards and Technology

Authority

This publication has been developed by NIST in accordance with its statutory responsibilities under the Federal Information Security Modernization Act (FISMA) of 2014, 44 U.S.C. § 3551 *et seq.*, Public Law (P.L.) 113-283. NIST is responsible for developing information security standards and guidelines, including minimum requirements for federal information systems, but such standards and guidelines shall not apply to national security systems without the express approval of appropriate federal officials exercising policy authority over such systems. This guideline is consistent with the requirements of the Office of Management and Budget (OMB) Circular A-130.

Nothing in this publication should be taken to contradict the standards and guidelines made mandatory and binding on federal agencies by the Secretary of Commerce under statutory authority. Nor should these guidelines be interpreted as altering or superseding the existing authorities of the Secretary of Commerce, Director of the OMB, or any other federal official. This publication may be used by nongovernmental organizations on a voluntary basis and is not subject to copyright in the United States. Attribution would, however, be appreciated by NIST.

National Institute of Standards and Technology Special Publication 800-140E
Natl. Inst. Stand. Technol. Spec. Publ. 800-140E, 18 pages (October 2019)
CODEN: NSPUE2

Certain commercial entities, equipment, or materials may be identified in this document in order to describe an experimental procedure or concept adequately. Such identification is not intended to imply recommendation or endorsement by NIST, nor is it intended to imply that the entities, materials, or equipment are necessarily the best available for the purpose.

There may be references in this publication to other publications currently under development by NIST in accordance with its assigned statutory responsibilities. The information in this publication, including concepts and methodologies, may be used by federal agencies even before the completion of such companion publications. Thus, until each publication is completed, current requirements, guidelines, and procedures, where they exist, remain operative. For planning and transition purposes, federal agencies may wish to closely follow the development of these new publications by NIST.

Organizations are encouraged to review all draft publications during public comment periods and provide feedback to NIST. Many NIST cybersecurity publications, other than the ones noted above, are available at https://csrc.nist.gov/publications.

Public comment period: *October 9, 2019 through December 9, 2019*

National Institute of Standards and Technology
Attn: Computer Security Division, Information Technology Laboratory
100 Bureau Drive (Mail Stop 8930) Gaithersburg, MD 20899-8930
Email: sp800-140-comments@nist.gov

All comments are subject to release under the Freedom of Information Act (FOIA).

Reports on Computer Systems Technology

The Information Technology Laboratory (ITL) at the National Institute of Standards and Technology (NIST) promotes the U.S. economy and public welfare by providing technical leadership for the Nation's measurement and standards infrastructure. ITL develops tests, test methods, reference data, proof of concept implementations, and technical analyses to advance the development and productive use of information technology. ITL's responsibilities include the development of management, administrative, technical, and physical standards and guidelines for the cost-effective security and privacy of other than national security-related information in federal information systems. The Special Publication 800-series reports on ITL's research, guidelines, and outreach efforts in information system security, and its collaborative activities with industry, government, and academic organizations.

Abstract

NIST Special Publication (SP) 800-140E replaces the approved authentication mechanism requirements of ISO/IEC 19790 Annex E. As a validation authority, the Cryptographic Module Validation Program (CMVP) may supersede this Annex in its entirety with its own list of approved authentication mechanisms. This document supersedes ISO/IEC 19790 Annex E and ISO/IEC 24759 paragraph 6.17.

Keywords

authentication; Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC 19790; ISO/IEC 2759; testing requirement; vendor evidence; vendor documentation.

Audience

This document is focused toward the vendors, testing labs, and CMVP for the purpose of addressing issues in cryptographic module testing.

112 **Table of Contents**

134
135

1 Scope

This document specifies the Cryptographic Module Validation Program (CMVP) modifications of the methods to be used by a Cryptographic and Security Testing Laboratory (CSTL) to demonstrate conformance. This document also specifies the modification of methods for evidence that a vendor or testing laboratory provides to demonstrate conformity. The approved sensitive security parameter generation and establishment methods specified in this document supersede those specified in ISO/IEC 19790 Annex E and ISO/IEC 24759 paragraph 6.17.

2 Normative references

This section identifies additional references to the normative references cited in ISO/IEC 19790 and ISO/IEC 24759. For dated references (e.g., ISO/IEC 19790:2012/Cor.1:*2015*(E)), only the edition cited applies. For undated references (e.g., ISO/IEC 19790), the latest edition of the referenced document (including any amendments) applies.

National Institute of Standards and Technology (2019) *Security Requirements for Cryptographic Modules*. (U.S. Department of Commerce, Washington, DC), Federal Information Processing Standards Publication (FIPS) 140-3. https://doi.org/10.6028/NIST.FIPS.140-3

3 Terms and definitions

The following terms and definitions supersede or are in addition to ISO/IEC 19790 and ISO/IEC 24759:

Authenticator: The means used to confirm the identity of a user, processor, or device (e.g., user password or token). Often referred to as a token, this document aligns with much of SP 800-63B and so uses authenticator to reduce confusion.

4 Symbols and abbreviated terms

The following symbols and abbreviated terms supersede or are in addition to ISO/IEC 19790 and ISO/IEC 24759 throughout this document:

CCCS	Canadian Centre for Cyber Security
CMVP	Cryptographic Module Validation Program
CSD	Computer Security Division
CSTL	Cryptographic and Security Testing Laboratory
FIPS	Federal Information Processing Standard
FISMA	Federal Information Security Management/Modernization Act

NIST	National Institute of Standards and Technology
SP 800-XXX	NIST Special Publication 800 series document
TE	Test Evidence
VE	Vendor Evidence

5 Document organization

5.1 General

Section 6 of this document replaces the approved authentication mechanisms requirements of ISO/IEC 19790 Annex E and ISO/IEC 24759 paragraph 6.17. While this document serves a different purpose, much of the authentication is purposely meant to align with SP 800-63B, which is a good informative reference for managing authentication.

5.2 Modifications

Modifications will follow a similar format as in ISO/IEC 24579. For additions to test requirements, new Test Evidence (TEs) or Vendor Evidence (VEs) will be listed by increasing the "sequence_number." Modifications can include a combination of additions using underline and deletions using ~~strikethrough~~. If no changes are required, the paragraph will indicate "No change."

6 CMVP-approved authentication mechanism requirements

6.1 Purpose

This document includes all requirements for CMVP-approved authentication mechanisms. These requirements are in addition to and do not replace authentication requirements specified in ISO/IEC 19790:2012.

6.2 Approved authentication mechanisms

Approved authentication mechanisms include memorized secrets, biometrics, cryptographic software or devices, and multifactor (combining two mechanisms). These mechanisms may be used as indicated in Table 1. Requirements for these mechanisms are provided below.

Table 1 - Authentication mechanism permitted at FIPS 140-3 security levels

FIPS 140-3 Level	Authentication
Level 1	None required—may be implicit. If authentication is used, it should meet the requirements of Level 2 as a minimum.
Level 2	One factor: ● Memorized secret ● Biometric ● Cryptographic software or device
Level 3	One factor: ● Memorized secret ● Biometric ● Cryptographic software or device
Level 4	Two factors: Memorized secret with either: ● Biometric ● Cryptographic software or device or Biometric with: ● Cryptographic software or device

6.3 Memorized secrets

Commonly referred to as a password or, if numeric, a PIN, a memorized secret authenticator 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.

6.3.1 Memorized secret authenticators

Memorized secrets SHALL be at least 8 characters in length if chosen by the operator. Memorized secrets chosen randomly by the module SHALL be at least 6 characters in length and MAY be entirely numeric. If the module disallows a chosen memorized secret based on its appearance on a blacklist of compromised values, the operator SHALL be required to choose a different memorized secret. No other complexity requirements for memorized secrets SHOULD be imposed.

6.3.2 Memorized secret module requirements

Module SHALL require operator-chosen memorized secrets to be at least 8 characters in length. A module SHOULD permit operator-chosen memorized secrets at least 64 characters in length. All printing ASCII [RFC 20] characters, as well as the space character, SHOULD be acceptable in memorized secrets. Unicode [ISO/IEC 10646] characters SHOULD be accepted as well. To make allowances for likely mistyping, a module MAY replace multiple consecutive space

characters with a single space character prior to verification, provided that the result is at least 8 characters in length. Truncation of the secret SHALL NOT be performed. For purposes of the above length requirements, each Unicode code point SHALL be counted as a single character.

If Unicode characters are accepted in memorized secrets, the module SHOULD apply the Normalization Process for Stabilized Strings using either the NFKC or NFKD normalization defined in Section 12.1 of Unicode Standard Annex 15 [UAX 15]. This process is applied before hashing the byte string representing the memorized secret. Operators choosing memorized secrets containing Unicode characters SHOULD be advised that some characters may be represented differently, which can affect their ability to authenticate successfully.

The Module SHALL implement controls to protect against guessing attacks. Unless otherwise specified in the description of a given authenticator, the verifier SHALL limit consecutive failed authentication attempts on a single account to no more than 100.

Additional techniques MAY be used to reduce the likelihood that an attacker will lock the legitimate claimant out as a result of rate limiting. These include:

- Requiring the claimant to complete a CAPTCHA before attempting authentication
- Requiring the claimant to wait following a failed attempt for a period of time that increases as the account approaches its maximum allowance for consecutive failed attempts (e.g., 30 seconds up to an hour)
- Accepting only authentication requests that come from a whitelist of IP addresses from which the subscriber has been successfully authenticated before
- Leveraging other risk-based or adaptive authentication techniques to identify user behavior that falls within or out of typical norms

When the subscriber successfully authenticates, the verifier SHOULD disregard any previous failed attempts for that user from the same IP address.

6.3.3 Memorized secret usability

Aid users to create and change memorized secrets:

- Clearly communicate information on how to create and change memorized secrets.
- Clearly communicate memorized secret requirements as specified in Section 6.3.1.
- Allow at least 64 characters in length to support the use of passphrases. Encourage users to make memorized secrets as lengthy as they want using any characters they like (including spaces), thus aiding memorization.
- Do not impose other composition rules (e.g., mixtures of different character types) on memorized secrets.
- Do not require that memorized secrets be changed arbitrarily (e.g., periodically) unless there is a user request or evidence of authenticator compromise.

Provide clear, meaningful, and actionable feedback when chosen passwords are rejected (e.g., when it appears on a "blacklist" of unacceptable passwords or has been used previously).

6.4 Biometrics

A trusted channel between sensor (or an endpoint containing a sensor that resists sensor replacement) and module SHALL be established, the sensor or endpoint SHALL be established, and the sensor or endpoint SHALL be authenticated prior to capturing the biometric sample from the claimant.

The biometric system SHALL operate with an FMR [ISO/IEC 2382-37] of 1 in 1000 or better. This FMR SHALL be achieved under conditions of a conformant attack (i.e., zero-effort impostor attempt) as defined in ISO/IEC 30107-1.

The biometric system SHOULD implement PAD. Testing of the biometric system to be deployed SHOULD demonstrate at least 90% resistance to presentation attacks for each relevant attack type (i.e., species) where resistance is defined as the number of thwarted presentation attacks divided by the number of trial presentation attacks. Testing of presentation attack resistance SHALL be in accordance with Clause 12 of ISO/IEC 30107-3. The PAD decision MAY be made either locally on the claimant's device or by a central module.

Note: PAD is being considered as a mandatory requirement in future editions.

The biometric system SHALL allow no more than 5 consecutive failed authentication attempts or 10 consecutive failed attempts if PAD is implemented meeting the above requirements. Once that limit has been reached, the biometric authenticator SHALL either:

- Impose a delay of at least 30 seconds before the next attempt, increasing exponentially with each successive attempt (e.g., 1 minute before the following failed attempt, 2 minutes before the second following attempt), or
- Disable the biometric user authentication and offer another factor (e.g., a different biometric modality or a PIN/Passcode if it is not already a required factor) if such an alternative method is already available.

The module SHALL make a determination of sensor and endpoint performance, integrity, and authenticity. Acceptable methods for making this determination include but are not limited to:

- Authentication of the sensor or endpoint
- Certification by an approved accreditation authority
- Runtime interrogation of signed metadata (e.g., attestation)

  Information conveyed MAY include but is not limited to:

  - The provenance (e.g., manufacturer or supplier certification), health, and integrity of the authenticator and endpoint
  - Security features of the authenticator

- Security and performance characteristics of biometric sensor(s)
- Sensor modality
- If this attestation is signed, it SHALL be signed using a digital signature that provides at least the minimum-security strength specified in the latest revision of SP 800-131A (i.e., 112 bits as of the date of this publication).

6.4.1 Biometrics usability considerations

This section provides a high-level overview of general usability considerations for biometrics. A more detailed discussion of biometric usability can be found in *Usability & Biometrics, Ensuring Successful Biometric Systems* NIST Usability.

Although there are other biometric modalities, the following three biometric modalities are more commonly used for authentication: fingerprint, face, and iris.

Typical Usage

- For all modalities, user familiarity and practice with the device improves performance.
- Device affordances (i.e., properties of a device that allow a user to perform an action), feedback, and clear instructions are critical to a user's success with the biometric device. For example, provide clear instructions on the required actions for liveness detection.
- Ideally, users can select the modality they are most comfortable with for their second authentication factor. The user population may be more comfortable and familiar with—and accepting of—some biometric modalities than others.
- User experience with biometrics as an activation factor:
  - Provide clear, meaningful feedback on the number of remaining allowed attempts. For example, for rate-limiting (i.e., throttling), inform users of the time period they have to wait until the next attempt to reduce user confusion and frustration.
- Fingerprint usability considerations:
  - Users have to remember which finger(s) they used for initial enrollment.
  - The amount of moisture on the finger(s) affects the sensor's ability for successful capture.
  - Additional factors influencing fingerprint capture quality include age, gender, and occupation (e.g., users handling chemicals or working extensively with their hands may have degraded friction ridges).
- Face usability considerations:
  - Users have to remember whether they wore any artifacts (e.g., glasses) during enrollment because it affects facial recognition accuracy.
  - Differences in environmental lighting conditions can affect facial recognition accuracy.

317 - Facial expressions affect facial recognition accuracy (e.g., smiling versus neutral
318 expression).
319 - Facial poses affect facial recognition accuracy (e.g., looking down or away from
320 the camera).
321 - Iris usability considerations:
322 - Wearing colored contacts may affect iris recognition accuracy.
323 - Users who have had eye surgery may need to re-enroll post-surgery.
324 - Differences in environmental lighting conditions can affect iris recognition
325 accuracy, especially for certain iris colors.

326 Intermittent Events

327 As biometrics are only permitted as a second factor for multi-factor authentication, usability
328 considerations for intermittent events with the primary factor still apply. Intermittent events with
329 biometrics use include but are not limited to the following, which may affect recognition
330 accuracy:

331 - If users injure their enrolled finger(s), fingerprint recognition may not work. Fingerprint
332 authentication will be difficult for users with degraded fingerprints.
333 - The time elapsed between the time of facial recognition for authentication and the time of
334 the initial enrollment can affect recognition accuracy as a user's face changes naturally
335 over time. A user's weight change may also be a factor.
336 - Iris recognition may not work for people who have had eye surgery unless they re-enroll.
337 - An alternative authentication method must be available and functioning. In cases where
338 biometrics do not work, allow users to use a memorized secret as an alternative second
339 factor.
340 - Provisions for technical assistance:
341 - Clearly communicate information on how and where to acquire technical
342 assistance. For example, provide users information such as a link to an online
343 self-service feature and a phone number for help desk support. Ideally, provide
344 sufficient information to enable users to recover from intermittent events on their
345 own without outside intervention.
346 - Inform users of factors that may affect the sensitivity of the biometric sensor (e.g.,
347 cleanliness of the sensor).

348 ## 6.5 Cryptographic software or device

349 ### 6.5.1 Single-factor cryptographic software

350 A single-factor software cryptographic authenticator is a cryptographic key stored on a disk or
351 some other "soft" media. Authentication is accomplished by proving possession and control of
352 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*.

6.5.1.1 Single-factor cryptographic software authenticator

Single-factor software cryptographic authenticators encapsulate one or more secret keys unique to the authenticator. The key SHALL be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, or TEE, if available). The key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access. Single-factor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.

6.5.1.2 Single-factor cryptographic software module

The requirements for a single-factor cryptographic software module are identical to those for a single-factor cryptographic device module. See 6.5.2.2.

6.5.1.3 Single-factor cryptographic software usability considerations

Usability considerations for typical usage include:

- Give cryptographic keys appropriately descriptive names that are meaningful to users since users have to recognize and recall which cryptographic key to use for which authentication task. This prevents users from having to deal with multiple similarly and ambiguously named cryptographic keys. Selecting from multiple cryptographic keys on smaller mobile devices may be particularly problematic if the names of the cryptographic keys are shortened due to reduced screen size.

6.5.2 Single-factor cryptographic 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*.

6.5.2.1 Single-factor cryptographic device authenticator

Single-factor cryptographic device authenticators encapsulate one or more secret keys unique to the device that SHALL NOT be exportable (i.e., cannot be removed from the device). The authenticator operates by signing a challenge nonce presented through a direct computer interface (e.g., a USB port). Alternatively, the authenticator could be a suitably secure processor integrated with the user endpoint itself (e.g., a hardware TPM). Although cryptographic devices

contain software, they differ from cryptographic software authenticators in that all embedded software is under the control of the issuer, and the entire authenticator is subject to all applicable FIPS 140 requirements at the security level being authenticated.

The secret key and its algorithm SHALL provide at least the minimum-security length specified in the latest revision of SP 800-131A (112 bits as of the date of this publication). The challenge nonce SHALL be at least 64 bits in length. Approved cryptography SHALL be used.

Single-factor cryptographic device authenticators SHOULD require a physical input (e.g., the pressing of a button) in order to operate. This provides defense against unintended operation of the device, which might occur if the endpoint to which it is connected is compromised.

6.5.2.2 Single-factor cryptographic device module interface

Single-factor cryptographic device module interface generates a challenge nonce, sends it to the corresponding authenticator, and uses the authenticator output to verify possession of the device. The authenticator output is highly dependent on the specific cryptographic device and protocol, but it is generally some type of signed message.

The module interface has either symmetric or asymmetric cryptographic keys corresponding to each authenticator. While both types of keys SHALL be protected against modification, symmetric keys SHALL additionally be protected against unauthorized disclosure.

The challenge nonce SHALL be at least 64 bits in length and SHALL either be unique over the authenticator's lifetime or statistically unique (i.e., generated using an approved random bit generator [SP 800-90Ar1]). The verification operation SHALL use approved cryptography.

6.5.3 Multi-factor cryptographic software

A multi-factor software cryptographic authenticator is a cryptographic key stored on a 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 SHALL be activated by either *something you know* or *something you are*.

6.5.3.1 Multi-factor cryptographic software authenticators

Multi-factor software cryptographic authenticators encapsulate one or more secret keys unique to the authenticator and accessible only through the input of an additional factor, either a memorized secret or a biometric. The key SHOULD be stored in suitably secure storage available to the authenticator application (e.g., keychain storage, TPM, TEE). The key SHALL be strongly protected against unauthorized disclosure by the use of access controls that limit access to the key to only those software components on the device requiring access. Multi-factor cryptographic software authenticators SHOULD discourage and SHALL NOT facilitate the cloning of the secret key onto multiple devices.

Each authentication operation using the authenticator SHALL require the input of both factors. Any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of Section 6.3.1 and SHALL be rate-limited as specified in Section 6.3.2. A biometric activation factor SHALL meet the requirements of Section 6.4, including limits on the number of consecutive authentication failures.

The unencrypted key and activation secret or biometric sample—and any biometric data derived from the biometric sample, such as a probe produced through signal processing—SHALL be zeroized immediately after an authentication transaction has taken place.

6.5.3.2 Multi-factor cryptographic software verifiers

The requirements for a multi-factor cryptographic software verifier are identical to those for a single-factor cryptographic device verifier as described in Section 6.5.2.2. Verification of the output from a multi-factor cryptographic software authenticator proves use of the activation factor.

6.5.3.3 Multi-factor cryptographic software usability

In order to authenticate, users prove possession and control of the cryptographic key stored on a disk or some other "soft" media that requires activation. The activation is through the input of a second authentication factor—either a memorized secret or a biometric. Usability considerations for the additional factor apply as well. See Section 6.3.3 for memorized secrets and Section 6.4.1 for biometrics used in multi-factor authenticators.

Usability considerations for typical usage include:

- Give cryptographic keys appropriately descriptive names that are meaningful to users since users have to recognize and recall which cryptographic key to use for which authentication task. This prevents users from having to deal with multiple similarly and ambiguously named cryptographic keys. Selecting from multiple cryptographic keys on smaller mobile devices may be particularly problematic if the names of the cryptographic keys are shortened due to reduced screen size.

6.5.4 Multi-factor cryptographic devices

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 SHALL be activated by either *something you know* or *something you are*.

6.5.4.1 Multi-factor cryptographic device authenticators

Multi-factor cryptographic device authenticators use tamper-resistant hardware to encapsulate one or more secret keys unique to the authenticator and accessible only through the input of an additional factor—either a memorized secret or a biometric. The authenticator operates by signing a challenge nonce presented through a direct computer interface (e.g., a USB port). Alternatively, the authenticator could be a suitably secure processor integrated with the user endpoint itself (e.g., a hardware TPM). Although cryptographic devices contain software, they differ from cryptographic software authenticators in that all embedded software is under the control of the issuer, and the entire authenticator is subject to any applicable FIPS 140 requirements.

The secret key and its algorithm SHALL provide at least the minimum-security length specified in the latest revision of SP 800-131A (112 bits as of the date of this publication). The challenge nonce SHALL be at least 64 bits in length. Approved cryptography SHALL be used.

Each authentication operation using the authenticator SHOULD require the input of the additional factor. Input of the additional factor MAY be accomplished either via direct input on the device or via a hardware connection (e.g., USB, smartcard).

Any memorized secret used by the authenticator for activation SHALL be a randomly chosen numeric value at least 6 decimal digits in length or other memorized secret meeting the requirements of Section 6.3.1 and SHALL be rate-limited as specified in Section 6.3.2. A biometric activation factor SHALL meet the requirements of Section 6.4, including limits on the number of consecutive authentication failures.

The unencrypted key and activation secret or biometric sample—and any biometric data derived from the biometric sample, such as a probe produced through signal processing—SHALL be zeroized immediately after an authentication transaction has taken place.

6.5.4.2 Multi-factor cryptographic device verifiers

The requirements for a multi-factor cryptographic device verifier are identical to those for a single-factor cryptographic device module interface as described in Section 6.5.2.2. Verification of the authenticator output from a multi-factor cryptographic device proves use of the activation factor.

6.5.4.3 Multi-factor cryptographic device usability

Users authenticate by proving possession of the multi-factor cryptographic device and control of the protected cryptographic key. The device is activated by a second authentication factor—either a memorized secret or a biometric. Usability considerations for the additional factor apply as well. See Section 6.3.3 for memorized secrets and Section 6.4.1 for biometrics used in multi-factor authenticators.

Usability considerations for typical usage include:

- Do not require users to keep multi-factor cryptographic devices connected following authentication. Users may forget to disconnect the multi-factor cryptographic device when they are done with it (e.g., forgetting a smartcard in the smartcard reader and walking away from the computer).
    - Users need to be informed regarding whether the multi-factor cryptographic device is required to stay connected or not.
- Give cryptographic keys appropriately descriptive names that are meaningful to users since users have to recognize and recall which cryptographic key to use for which authentication task. This prevents users being faced with multiple similarly and ambiguously named cryptographic keys. Selecting from multiple cryptographic keys on smaller mobile devices (such as smartphones) may be particularly problematic if the names of the cryptographic keys are shortened due to reduced screen size.
- Limited availability of a direct computer interface like a USB port could pose usability difficulties. For example, laptop computers often have a limited number of USB ports, which may force users to unplug other USB peripherals to use the multi-factor cryptographic device.

512 **Document Revisions**

Date	Change

513

514