Withdrawn Draft

Warning Notice

The attached draft document has been withdrawn, and is provided solely for historical purposes. It has been superseded by the document identified below.

Withdrawal Date	March 20, 2020
Original Release Date	October 9, 2019

Superseding Document

Status	Final
Series/Number	NIST Special Publication 800-140E
Title	CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17
Publication Date	March 2020
DOI	https://doi.org/10.6028/NIST.SP.800-140E
CSRC URL	https://csrc.nist.gov/publications/detail/sp/800-140e/final
Additional Information	FIPS 140-3 Transition Effort
	https://csrc.nist.gov/projects/fips-140-3-transition-effort/fips-140-3-docs

1

2

Draft NIST Special Publication 800-140E

3

CMVP Approved Authentication Mechanisms:

4

5
6

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

7

8
9

Kim Schaffer

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

NIST

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

20

CMVP Approved Authentication Mechanisms:

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

25

Kim Schaffer
Computer Security Division
Information Technology Laboratory

October 2019

49 **Authority**

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

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

66

80

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

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

87   **Reports on Computer Systems Technology**

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

98   **Abstract**

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

104   **Keywords**

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

107

108   **Audience**

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

111

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

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

5   Document organization

5.1   General

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

5.2   Modifications

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

6   CMVP-approved authentication mechanism requirements

6.1   Purpose

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

6.2   Approved authentication mechanisms

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

192 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

193

6.3 Memorized secrets

195 Commonly referred to as a password or, if numeric, a PIN, a memorized secret authenticator is a
196 secret value intended to be chosen and memorized by the user. Memorized secrets need to be of
197 sufficient complexity and secrecy that it would be impractical for an attacker to guess or
198 otherwise discover the correct secret value. A memorized secret is something you know.

6.3.1 Memorized secret authenticators

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

6.3.2 Memorized secret module requirements

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

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

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

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

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

226   ● Requiring the claimant to complete a CAPTCHA before attempting authentication

227   ● Requiring the claimant to wait following a failed attempt for a period of time that
228   increases as the account approaches its maximum allowance for consecutive failed
229   attempts (e.g., 30 seconds up to an hour)

230   ● Accepting only authentication requests that come from a whitelist of IP addresses from
231   which the subscriber has been successfully authenticated before

232   ● Leveraging other risk-based or adaptive authentication techniques to identify user
233   behavior that falls within or out of typical norms

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

236 **6.3.3   Memorized secret usability**

237 Aid users to create and change memorized secrets:

238   ● Clearly communicate information on how to create and change memorized secrets.

239   ● Clearly communicate memorized secret requirements as specified in Section 6.3.1.

240   ● Allow at least 64 characters in length to support the use of passphrases. Encourage users
241   to make memorized secrets as lengthy as they want using any characters they like
242   (including spaces), thus aiding memorization.

243   ● Do not impose other composition rules (e.g., mixtures of different character types) on
244   memorized secrets.

245   ● Do not require that memorized secrets be changed arbitrarily (e.g., periodically) unless
246   there is a user request or evidence of authenticator compromise.

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

249 **6.4 Biometrics**

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

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

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

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

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

267 ● Impose a delay of at least 30 seconds before the next attempt, increasing exponentially
268 with each successive attempt (e.g., 1 minute before the following failed attempt, 2
269 minutes before the second following attempt), or

270 ● Disable the biometric user authentication and offer another factor (e.g., a different
271 biometric modality or a PIN/Passcode if it is not already a required factor) if such an
272 alternative method is already available.

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

275 ● Authentication of the sensor or endpoint

276 ● Certification by an approved accreditation authority

277 ● Runtime interrogation of signed metadata (e.g., attestation)

278 Information conveyed MAY include but is not limited to:

279 ○ The provenance (e.g., manufacturer or supplier certification), health, and integrity
280 of the authenticator and endpoint

281 ○ Security features of the authenticator

282 ○ Security and performance characteristics of biometric sensor(s)

283 ○ Sensor modality

284 ○ If this attestation is signed, it SHALL be signed using a digital signature that
285 provides at least the minimum-security strength specified in the latest revision of
286 SP 800-131A (i.e., 112 bits as of the date of this publication).

287 **6.4.1 Biometrics usability considerations**

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

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

293 Typical Usage

294 ● For all modalities, user familiarity and practice with the device improves performance.

295 ● Device affordances (i.e., properties of a device that allow a user to perform an action),
296 feedback, and clear instructions are critical to a user's success with the biometric device.
297 For example, provide clear instructions on the required actions for liveness detection.

298 ● Ideally, users can select the modality they are most comfortable with for their second
299 authentication factor. The user population may be more comfortable and familiar with—
300 and accepting of—some biometric modalities than others.

301 ● User experience with biometrics as an activation factor:

302 ○ Provide clear, meaningful feedback on the number of remaining allowed attempts.
303 For example, for rate-limiting (i.e., throttling), inform users of the time period
304 they have to wait until the next attempt to reduce user confusion and frustration.

305 ● Fingerprint usability considerations:

306 ○ Users have to remember which finger(s) they used for initial enrollment.

307 ○ The amount of moisture on the finger(s) affects the sensor's ability for successful
308 capture.

309 ○ Additional factors influencing fingerprint capture quality include age, gender, and
310 occupation (e.g., users handling chemicals or working extensively with their
311 hands may have degraded friction ridges).

312 ● Face usability considerations:

313 ○ Users have to remember whether they wore any artifacts (e.g., glasses) during
314 enrollment because it affects facial recognition accuracy.

315 ○ Differences in environmental lighting conditions can affect facial recognition
316 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

353 it is generally some type of signed message. The single-factor software cryptographic
354 authenticator is *something you have*.

6.5.1.1 Single-factor cryptographic software authenticator

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

6.5.1.2 Single-factor cryptographic software module

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

6.5.1.3 Single-factor cryptographic software usability considerations

367 Usability considerations for typical usage include:

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

6.5.2 Single-factor cryptographic device

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

6.5.2.1 Single-factor cryptographic device authenticator

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

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

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

395 Single-factor cryptographic device authenticators SHOULD require a physical input (e.g., the
396 pressing of a button) in order to operate. This provides defense against unintended operation of
397 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

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

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

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

6.5.3   Multi-factor cryptographic software

410 A multi-factor software cryptographic authenticator is a cryptographic key stored on a disk or
411 some other "soft" media that requires activation through a second factor of authentication.
412 Authentication is accomplished by proving possession and control of the key. The authenticator
413 output is highly dependent on the specific cryptographic protocol, but it is generally some type of
414 signed message. The multi-factor software cryptographic authenticator is *something you have*,
415 and it SHALL be activated by either *something you know* or *something you are*.

6.5.3.1   Multi-factor cryptographic software authenticators

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

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

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

434   ### *6.5.3.2   Multi-factor cryptographic software verifiers*

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

439   ### *6.5.3.3   Multi-factor cryptographic software usability*

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

445   Usability considerations for typical usage include:

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

452   ### 6.5.4   Multi-factor cryptographic devices

453   A multi-factor cryptographic device is a hardware device that performs cryptographic operations
454   using one or more protected cryptographic keys and requires activation through a second
455   authentication factor. Authentication is accomplished by proving possession of the device and
456   control of the key. The authenticator output is provided by direct connection to the user endpoint
457   and is highly dependent on the specific cryptographic device and protocol, but it is typically
458   some type of signed message. The multi-factor cryptographic device is *something you have*, and
459   it SHALL be activated by either *something you know* or *something you are*.

460   ### 6.5.4.1   Multi-factor cryptographic device authenticators

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

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

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

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

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

484   ### 6.5.4.2   Multi-factor cryptographic device verifiers

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

489   ### 6.5.4.3   Multi-factor cryptographic device usability

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

495   Usability considerations for typical usage include:

496   ● Do not require users to keep multi-factor cryptographic devices connected following
497   authentication. Users may forget to disconnect the multi-factor cryptographic device
498   when they are done with it (e.g., forgetting a smartcard in the smartcard reader and
499   walking away from the computer).

500   ○ Users need to be informed regarding whether the multi-factor cryptographic
501   device is required to stay connected or not.

502   ● Give cryptographic keys appropriately descriptive names that are meaningful to users
503   since users have to recognize and recall which cryptographic key to use for which
504   authentication task. This prevents users being faced with multiple similarly and
505   ambiguously named cryptographic keys. Selecting from multiple cryptographic keys on
506   smaller mobile devices (such as smartphones) may be particularly problematic if the
507   names of the cryptographic keys are shortened due to reduced screen size.

508   ● Limited availability of a direct computer interface like a USB port could pose usability
509   difficulties. For example, laptop computers often have a limited number of USB ports,
510   which may force users to unplug other USB peripherals to use the multi-factor
511   cryptographic device.

512 **Document Revisions**

Date	Change

513

514