NIST Special Publication 800-140E

CMVP Approved Authentication Mechanisms:

CMVP Validation Authority Requirements for ISO/IEC 19790:2012 Annex E and ISO/IEC 24759 Section 6.17

Kim Schaffer

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140E

INFORMATION SECURITY

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

NIST Special Publication 800-140E

CMVP Approved Authentication Mechanisms:

CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17

Kim Schaffer
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140E

March 2020

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, 9 pages (March 2020)
CODEN: NSPUE2

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-140E

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.

Comments on this publication may be submitted to:

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 and ISO/IEC 24759 paragraph 6.17. As a validation authority, the Cryptographic Module Validation Program (CMVP) may supersede ISO/IEC 19790 Annex E and ISO/IEC 24759 paragraph 6.17 in its entirety with its own list of approved authentication mechanisms.

Keywords

authentication; Cryptographic Module Validation Program; CMVP; FIPS 140 testing; FIPS 140; ISO/IEC 19790; ISO/IEC 24759; testing requirement; vendor evidence; vendor documentation.

Audience

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

Table of Contents

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 the normative references cited as ISO/IEC 19790 and ISO/IEC 24759. The specific editions to be used are ISO/IEC 19790:2012 and ISO/IEC 24759:2017. Please note that the version 19790:2012 referenced here includes the corrections made in 2015.

> 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:

> *Rate Limiting:* Used to control the rate of requests sent or received by a network interface and is used to prevent automated attacks.
>
> *Authenticator*: The means used to confirm the identity of a user, processor, or device (e.g., user password or token). Sometimes defined as *something you know*, *something you have* or *something you are*. Referred to as a token in earlier versions of SP 800-63 and in ISO/IEC 19790 and ISO/IEC 24759.

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
FMR	False Match Rate. The proportion of zero-effort impostor attempt samples falsely declared to match the compared non-self template
NIST	National Institute of Standards and Technology
PAD	Presentation Attack Detection. An automated determination of a presentation attack
SP 800-XXX	NIST Special Publication 800 series document

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 an informative reference for module authentication.

5.2 Modifications

Modifications will follow a similar format as in ISO/IEC 24579. 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 for operators. Some of these mechanisms may be employed to establish module provided protected communication services; however, these must meet the cryptographic strength requirements of SP 800-140C and SP 800-140D. These requirements supplement the authentication requirements specified in ISO/IEC 19790.

6.2 Approved authentication mechanisms

While there are currently no approved authentication mechanisms, allowed authentication mechanisms may be used as indicated in Table 1. Except at level 1, operator authentication acceptance is required to be performed by the module or by the Operating Environment as defined in ISO/IEC 19790.

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	Memorized secret or Level 3 authentication mechanism
Level 3	• Memorized Secret; • Look-Up Secret; • Out-of-Band; • Single-Factor One Time Password (OTP) Device; • Multi-Factor OTP Device; • Single-Factor Crypto Software; • Single-Factor Crypto Device; • Multi-Factor Crypto Software; • Multi-Factor Crypto Device
Level 4	• Multi-Factor Crypto Software; • Multi-Factor Crypto Device

Vendors should use SP 800-63B as a framework for authentication requirements and should provide justification whenever SP 800-63B requirements cannot be met. Testers should review and affirm the vendor documentation.

Normative SP 800-63B sections include

- Section 5, Detailed requirements specific to each type of authenticator;
- Section 6, Lifecycle management;
- Section 7, Session Management;

Informative information to be assessed for each authenticator includes:

- Section 8, Threats and Security Considerations; and
- Section 10, Usability Considerations.

Document Revisions

Date	Change