NIST Handbook 150-17

NVLAP Cryptographic and Security Testing

Bradley Moore
Beverly Trapnell
James Fox
Carolyn French

This publication is available free of charge from:
https://doi.org/10.6028/NIST.HB.150-17-2021

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

NIST Handbook 150-17

NVLAP Cryptographic and Security Testing

Bradley Moore
National Voluntary Laboratory Accreditation Program
Standards Coordination Office
Laboratory Programs

Beverly Trapnell
James Fox
Security Test, Validation and Measurement Group
Information Technology Laboratory

Carolyn French
Canadian Centre for Cyber Security (CCCS)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.HB.150-17-2021

June 2021

U.S. Department of Commerce
Gina M. Raimondo, Secretary

National Institute of Standards and Technology
James K. Olthoff, Performing the Non-Exclusive Functions and Duties of the Under Secretary of Commerce for Standards and Technology & Director, National Institute of Standards and Technology

National Institute of Standards and Technology Handbook 150-17
Natl. Inst. Stand. Technol. Handbook 150-17, 89 pages (June 2021)

This publication is available free of charge from:
https://doi.org/10.6028/NIST.HB.150-17-2021

NVLAP AND THE NVLAP LOGO

Contents

Acknowledgments

The authors wish to thank the many colleagues who provided numerous reviews and contributions to the revision of this document. NIST Handbook 150-17 has been the work of many contributors, most notably the technical staff of the NIST Cryptographic Module Validation Program (CMVP), the Cryptographic Algorithm Validation Program (CAVP), the Personal Identification Validation Program (NPIVP), the General Services Administration FIPS 201 Validation Program (GSA EP), the Security Content Automation Protocol Validation Program (SCAP), and the Department of Homeland Security, Transportation Security Administration (TSA), the Transportation Worker Identification Credential (TWIC) program.

The following authors of earlier editions of the handbook provided a foundation without which the present edition is inconceivable: Jeffrey Horlick, Annabelle Lee, and Lisa Carnahan (2000 edition); Michaela Iorga and Carroll Brickenkamp (Pi Group) (2008 edition); Dana Leaman (2013 edition).

Special thanks are extended to the NIST Editorial Review Board readers, past and present, for their thorough, thoughtful content reviews and valuable comments, who include, most recently, Amy Phelps, Christopher Celi, Lisa Carnahan, Allen Roginsky, Hildegard Ferraiolo, and Dragos Prisaca. It is the authors' opinion that these inputs have improved the overall quality and usefulness of the publication.

Foreword

The National Institute of Standards and Technology (NIST) Handbook 150 publication series sets forth the procedures, requirements, and guidance for the accreditation of testing and calibration laboratories by the National Voluntary Laboratory Accreditation Program (NVLAP). The series comprises the following publications:

- NIST Handbook 150, *NVLAP Procedures and General Requirements*, which contains the general procedures and requirements under which NVLAP operates as an unbiased third-party accreditation body;

- NIST Handbook 150-xx program-specific handbooks, which supplement NIST Handbook 150 by providing additional requirements, guidance, and interpretive information applicable to specific NVLAP laboratory accreditation programs (LAPs).

The program-specific handbooks are not stand-alone documents, but rather are companion documents to NIST Handbook 150 and ISO/IEC 17025. They tailor the general criteria found in ISO/IEC 17025 and NIST Handbook 150 to the specific tests, calibrations, or types of tests or calibrations covered by a LAP.

NIST Handbook 150-17, *NVLAP Cryptographic and Security Testing,* presents technical requirements and guidance for the accreditation of laboratories under the NVLAP Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP). The handbook is intended for use by accreditedlaboratories, assessor(s) conducting onsite assessments, laboratories seeking accreditation, laboratory accreditation systems, users of laboratory services, and others needing information on the requirements for accreditation under this program. All statements in this handbook are supplemental to and do not contradict ISO/IEC 17025 and NIST Handbook 150. If ambiguity unintentionally arises, the ISO/IEC 17025 and NIST Handbook 150 requirements take precedence.

The June 2021 edition of NIST Handbook 150-17 includes a consolidation of the Cryptographic Modules test methods (17/CM), revisions for alignment with FIPS 140-3, and other minor updates to existing testing programs included in this handbook. The requirements of ISO/IEC 17025, NIST Handbook 150, and NIST Handbook 150-17 combine to produce the criteria for accreditation in the NVLAP Cryptographic and Security Testing LAP. In the previous April 2020 edition, the numbering had been updated to reflect that used by ISO/IEC 17025:2017, *General requirements for the competence of testing and calibration laboratories* (hereafter referred to as ISO/IEC 17025).

The June 2021 edition of NIST Handbook 150-17 supersedes and replaces the April 2020 edition.

This handbook is also available on the NVLAP website: https://www.nist.gov/nvlap and through the NIST Research Library at https://doi.org/10.6028/NIST.HB.150-17-2021.

Questions or comments concerning this handbook should be submitted to: NVLAP, National Institute of Standards and Technology, 100 Bureau Drive, Stop 2140, Gaithersburg, MD 20899-2140; phone: (301) 975-4016; fax: (301) 926-2884; e-mail: nvlap@nist.gov.

Introduction

NIST Handbook 150-17 augments ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*, and NIST Handbook 150, *NVLAP Procedures and General Requirements*, by gathering the technical requirements of the Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP) for conformance testing of Federal Information Processing Standards (FIPS)-approved and NIST-recommended security functions (e.g., cryptographic algorithms, security components, and protocols), and of cryptographic and security modules. Technical requirements of this handbook identify NVLAP criteria applicable to accreditation for conformance testing under the CST LAP.

Any laboratory (including commercial; manufacturer; university; federal, state, or local government; foreign or domestic) that performs any of the test methods covered by the CST LAP may apply for NVLAP accreditation unless prohibited by other programmatic requirements specific to the validation authority. Accreditation will be granted to a laboratory that complies with the criteria for accreditation. Accreditation does not imply a guarantee of laboratory performance. It is a finding of laboratory competence and proficiency in conducting testing.

Testing services covered: Testing services include conformance testing of FIPS-approved and NIST-recommended security functions, of cryptographic and security modules, including module interfaces (and their interoperability), and of security policy compliance. For more information, see the CST LAP's website: https://www.nist.gov/nvlap/nvlap-cst-lap.cfm.

Types of security functions covered: A security function is a part, a subset of parts, or the whole set of the Implementation-Under-Test (IUT) or System-Under-Test (SUT) that must be relied upon for enforcing a closely related set of cryptographic procedures or security rules as defined in the specified standard and/or security policy. A security function can be a single cryptographic algorithm or a set of cryptographic algorithms, procedures or modes of operations that operate together to produce the output. Examples of security functions covered by the CST LAP are FIPS-approved and NIST-recommended cryptographic algorithms, security components, and protocols, as found in the applicable version of FIPS 140 Annexes, Personal Identity Verification (PIV) modules, identity and privilege credential management modules, automated vulnerabilities management modules, security policy compliance evaluation modules, and modules used in protecting sensitive information within computer and telecommunication systems.

Types of cryptographic modules covered: A cryptographic module is defined as a set of hardware, software, and/or firmware that implements FIPS-approved and/or NIST-recommended security functions that are contained within a defined cryptographic module boundary. The types of cryptographic modules covered by the CST LAP are modules used in security systems protecting sensitive information within computer and telecommunication systems. These modules include, but are not limited to, hardware components or hardware modules, software programs or software modules, computer firmware or hybrid modules, or any combination thereof. For all cryptographic modules, the interfaces specified in each module specification are within the boundaries of the cryptographic module, and therefore are covered by the CST LAP.

Types of cryptographic algorithms covered: A cryptographic algorithm is a well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output. A cryptographic algorithm can be a subset of a security function. The types of cryptographic algorithms covered by the CST LAP are either:

- specified in a FIPS-approved standard or NIST recommendation; or

- adopted in a FIPS-approved standard or NIST recommendation and specified either in an appendix of the FIPS-approved standard or recommendation or in a document referenced by the FIPS-approved standard or recommendation; or
- specified in the list of FIPS-approved and/or NIST-recommended security functions.

Types of security modules covered: The types of security modules covered by the CST LAP are automated vulnerabilities management modules, security policy compliance evaluation modules, and modules used in protecting sensitive information within computer and telecommunication systems. For all security modules, the interfaces specified in each module specification are within the boundaries of the security module, and therefore are covered by the CST LAP.

1 General information

1.1 Scope

1.1.1 This handbook specifies the technical requirements and provides guidance for the accreditation of laboratories under the NVLAP CST LAP. It supplements the NVLAP procedures and general requirements found in NIST Handbook 150 and ISO/IEC 17025, by tailoring the general criteria found in NIST Handbook 150 and ISO/IEC 17025 to the specific types of tests covered by the CST LAP.

1.1.2 This handbook is intended for use by all accredited CST laboratories, assessor(s) conducting onsite assessments, laboratories seeking accreditation, other laboratory accreditation systems, users of laboratory services, and others needing information on the requirements for accreditation under theCST LAP.

1.2 Organization of handbook

1.2.1 The numbering and titles of the first eight clauses of this handbook are patterned after NIST Handbook 150, *NVLAP Procedures and General Requirements*, and ISO/IEC 17025 *General requirements for the competence of testing and calibration laboratories* to allow easy cross-reference. The primary subclauses in clauses 4 through 8 (e.g., 4.1, 4.2) are also numbered and titled to correspond with those of ISO/IEC 17025:2017, even when there are no additional requirements.

1.2.2 In addition, the handbook contains information in the annexes that supplements the text. Annex A (informative) lists the available types of tests offered by the CST LAP, and provides additional information and links to the CST LAP, NVLAP and NIST websites where the most current information and resources are located. Annexes B through G (normative) list additional requirements specific to the type of tests in terms of personnel competence, managerial and technical requirements, specific tools, management system, and other documentation. Annex H (informative) provides a list of additional acronyms.

1.2.3 The procedures and general requirements of ISO/IEC 17025, NIST Handbook 150, and specific requirements in this handbook are combined to produce the criteria for accreditation under the CST LAP.

1.3 Program description

1.3.1 The CST LAP was established by NVLAP to accredit laboratories that perform cryptographic algorithm testing, cryptographic module validation conformance testing, and SCAP Conformance Testing. Originally named Cryptographic Module Testing (CMT), the LAP expanded in 2006 and 2007 to offer additional security types of tests. At that time, the program name was changed to Cryptographic and Security Testing (CST). However, references on the web and in older documents from this LAP utilizing the obsolete nomenclature may still exist.

1.3.2 The Cryptographic Algorithm Validation Program (CAVP) is a validation program developed by NIST/Information Technology Laboratory (NIST/ITL) and administered jointly by NIST/ITL and the Canadian Centre for Cyber Security (CCCS) for the validation of all FIPS-approved and NIST-recommended security functions. For every FIPS-approved and NIST-recommended security function, NIST/ITL develops a validation test suite for testing the correctness of a security function's implementation. Security function implementations that are successfully validated can claim conformance to the appropriate security function standard. All algorithm-specific test suites are bundled into the CAVP's Automated

Cryptographic Validation Testing System (ACVTS) validation testing tool. Access to the CAVP's ACVTS validation testing tool is provided by NIST/ITL to those laboratories obtaining accreditation in the NVLAP CST LAP.

1.3.3 The Cryptographic Module Validation Program (CMVP**)** is a validation program developed by NIST/ITL and administered jointly by NIST/ITL and the CCCS. The requirements for this program are derived by NIST/ITL from FIPS 140, *Security Requirements for Cryptographic Modules* or successors. The testing requirements are specified in the Derived Test Requirements (DTR) for FIPS 140, *Security Requirements for Cryptographic Modules* or successors. Cryptographic modules validated by the CMVP are accepted for use in Canada and by the U.S. Government for the protection of sensitive, unclassified information. NIST and CCCS have developed an Implementation Guidance for FIPS 140 or successors and the CMVP document for cryptographic module vendors and testing laboratories. This is intended to provide clarifications of the testing process, FIPS 140 or successors, and the FIPS 140 DTR or successors.

1.3.4 The NIST Personal Identity Verification Program (NPIVP) is a program developed to validate Personal Identity Verification (PIV) components required by FIPS 201. In response to the Homeland Security Presidential Directive (HSPD) 12 of August 2004, the NIST ITL initiated a new program for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. FIPS 201, Personal Identity Verification of Federal Employees and Contractors, was developed to satisfy the requirements of HSPD 12, approved by the Secretary of Commerce, and issued on February 25, 2005. NVLAP accredits NPIVP laboratories to test PIV Card Application and PIV Middleware implementations for conformance to NIST SP 800-73, Interfaces for Personal Identity Verification, which is normatively referenced from FIPS 201. The PIV objectives to validating PIV components by NPIVP are:

- to validate the conformance of two PIV components, PIV Middleware and PIV Card Application, with the specifications in NIST SP 800-73-4 or successors; and
- to provide assurance that the set of PIV Middleware and PIV Card Applications that have been validated by NPIVP are interoperable.

More information on the PIV test methods and the NPIVP validation program can be found at https://csrc.nist.gov/groups/SNS/piv/npivp/index.html.

1.3.5 The GSA FIPS 201 Evaluation Program (GSA EP) was established to evaluate and approve products and services as compliant with specified FIPS 201 requirements and ensure product interoperability (see https://fips201ep.cio.gov/). In 2007 the U.S. General Services Administration (GSA) requested that NVLAP add the test methods defined in the GSA FIPS 201 Evaluation Program (GSA EP) to the CST LAP, building upon NPIVP test methods for which laboratories had already attained accreditation. The GSA EP directly supports the acquisition process for implementing HSPD 12 by listing products that meet FIPS 201 and are interoperable with each other. The GSA EP requires NVLAP accreditation of the set of test methods referred to as GSA Precursor (GSAP) as a prerequisite for all laboratories seeking to become a GSA FIPS 201 Testing Laboratory.

As a prerequisite for all laboratories seeking to become a GSA FIPS 201 Testing Laboratory, the GSA EP requires NVLAP accreditation for the test methods listed as GSAP in this handbook.

1.3.6 The Security Content Automation Protocol (SCAP) Validation Program was created by NIST/ITL in response to the Office of Management and Budget (OMB) Memorandum M-07-18 of July 31, 2007, which required the use of SCAP-validated tools for assessing compliance with the Federal Desktop Core Configuration (FDCC) as a part of FISMA continuous monitoring. The SCAP Validation Program tests the ability of products to use the features and functionality available through SCAP and its components. To

meet the needs defined in the Memorandums M-07-11, M-07-18, and M-08-22, NVLAP established the accreditation of SCAP conformance testing laboratories in December 2007.

SCAP enables automated vulnerability management, measurement, and policy compliance evaluation; enumerates vulnerabilities, misconfigurations, platforms, and scoring; and provides machine-readable security configuration checklists. SCAP is a suite of specifications for expressing and manipulating security data in standardized ways. Adoption of SCAP facilitates an organization's automation of continuous monitoring, vulnerability management, and security policy compliance evaluation reporting. The SCAP Validation Program requires NVLAP accreditation for the test methods listed as SCAP in this handbook. For additional information regarding SCAP see the program website: https://scap.nist.gov.

1.3.7 The Department of Homeland Security Identity and Privilege Credential Management (DHSIPCM) Validation Program was created in 2009 when the Department of Homeland Security (DHS) requested NIST to assist with the establishment of an administrative process for developing and managing an unified Qualified Products List (QPL) for its Identity and Privilege Credential Management (DHSIPCM) systems. Because of this effort, NVLAP added DHSIPCM testing to the LAP for the independent laboratories interested in conformance testing of DHS's identity and privilege credential management systems. The DHSIPCM testing provides program-specific test methods while building upon PIV test methods for which laboratories have already attained accreditation. The DHSIPCM testing directly supports the DHS' Identity and Privilege Credential Management program (i.e., Transportation Worker Identification Credential [TWIC]) and requires NVLAP accreditation to the full set of the test methods referred herein as DHSIPCM test methods for all laboratories seeking to become a DHSIPCM testing laboratory.

For additional information regarding DHSIPCM, see the program website: https://www.tsa.gov/twic.

1.3.8 Information regarding the most current additions, enhancements and extensions to the CST LAP types of tests at the time of this publication can be found in the annex associated with the specific test methods.

1.3.9 NVLAP reserves the right to expand the CST LAP and offer to interested laboratories additional types of tests not listed in this handbook. Laboratories are advised to review the CST LAP's website for the most current information (see https://www.nist.gov/nvlap/nvlap-cst-lap.cfm).

1.3.10 All of the cryptographic and security testing performed under any of the CST LAP programs (e.g., CMVP, CAVP) are handled by test facilities that are accredited as CST laboratories by NVLAP as described in this handbook and as described on the laboratory's published scope of accreditation. A laboratory's scope of accreditation will be published to the NVLAP website (see https://www-s.nist.gov/niws/index.cfm?event=directory.results).

1.3.11 Figure 1 provides a generic overview of the accreditation process and the relationship between:

- the accreditation authority (NVLAP);
- the applicant laboratory; and
- the validation program (e.g., CAVP, CMVP, NPIVP, GSAP, DHSIPCM, and SCAP) as customer and technical requirements provider.

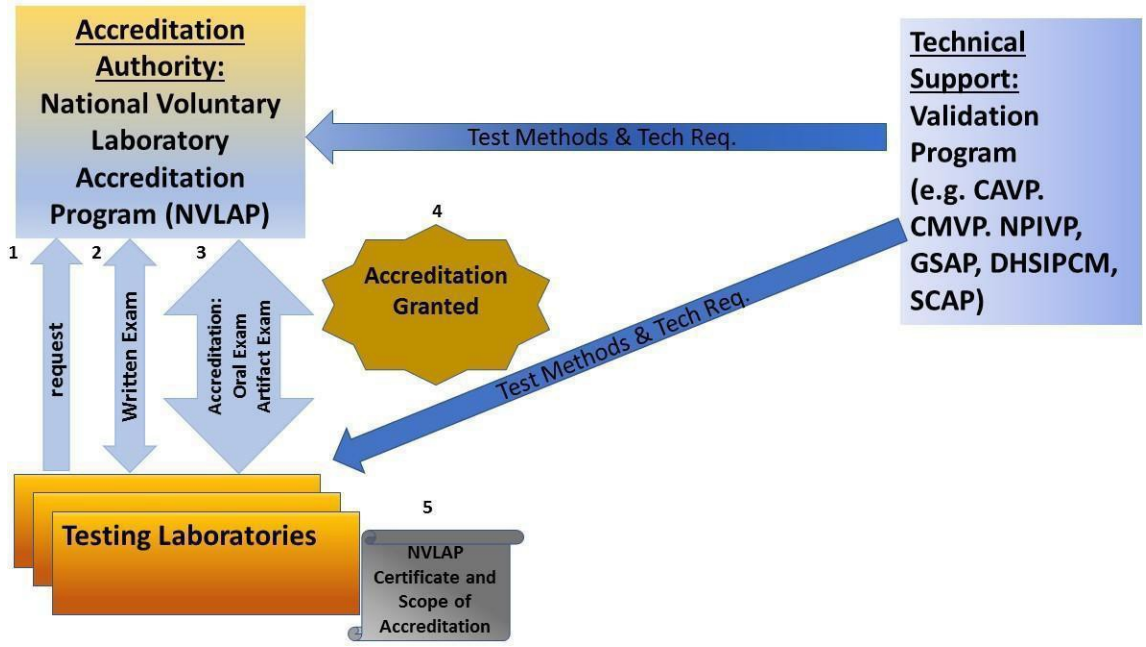

Figure 1. Accreditation process.

For a complete summary on the validation process, see the informative diagram in Annex A.

1.4 References

The following documents are referenced in this handbook. For dated references, only the edition cited shall apply. For undated references, the most current edition of the referenced document (including any amendments) shall apply within one year of publication or within the time limit specified by regulations or other requirement documents.

1.4.1 NVLAP publications

— NIST Handbook 150, *NVLAP Procedures and General Requirements*
(see https://nvlpubs.nist.gov/nistpubs/hb/2020/NIST.HB.150-2020.pdf)

1.4.2 FIPS publications

FIPS publications are issued by NIST after approval by the Secretary of Commerce pursuant to Section 5131 of the Information Technology Reform Act of 1996 (Public Law 104-106) and the Federal Information Security Modernization Act of 2015 (Public Law 107-347). For FIPS references specific to types of tests and/or test methods, see the annex associated with the specific test methods.

1.4.3 ISO/IEC publications

In addition to the ISO/IEC references listed in NIST Handbook 150, ISO/IEC references specific to types of tests and/or test methods are listed in the annex associated with the specific test methods.

— ISO/IEC 17043, *Conformity assessment – General requirements for proficiency testing.*

1.4.4 NIST Special Publications (SP)

NIST Special Publications (SP) in the 800 series present documents of general interest to the computer security community. The SP 800 series was established in 1990 to provide a separate identity forinformation technology security publications. The SP 800 series reports on ITL's research, guidelines, andoutreach efforts in computer security, and its collaborative activities with industry, government and academic organizations. NIST SP relevant to this program can be downloaded from the NIST Computer Security Resource Center (CSRC) (https://csrc.nist.gov/publications/sp800). For NIST/ITL references specific to the types of tests and/or test methods, see the annex associated with the specific test methods.

The CST LAP website (https://www.nist.gov/nvlap/nvlap-cst-lap.cfm) also provides a complete list of links to validation program sites. The references listed on the website supersede the information provided herein unless otherwise specified.

1.4.5 Other NIST publications and tools

See the associated annexes for test-specific descriptions of the Cryptographic and Security Testing tools relevant to the desired type of test.

1.5 Terms and definitions

For the purposes of this handbook, the relevant terms and definitions given in NIST Handbook 150 apply unless a term is redefined in this handbook. The definitions provided in this handbook are specific to the CST LAP, and when applicable, they supersede the definitions given in NIST Handbook 150. For a list of all acronyms, see Annex H. Additional test-specific terms and definitions are provided in the annexes specific to the testing. Test-specific terms, defined in other technical publications referenced in this document, supersede the definitions given in this handbook.

1.5.1
abstract test case
The specification of a test case that is independent of any implementation language.

1.5.2
accessibility
The assurance of continuous operation, continuous service, or data availability of the referred entity.

1.5.3
approved
FIPS-approved and/or NIST-recommended.

1.5.4
approved security function
A security function (e.g., cryptographic algorithm, cryptographic key management technique, or authentication technique) that is either (a) specified in an Approved standard, (b) adopted in an Approved standard and specified either in an appendix of the Approved standard or in a document referenced by the Approved standard, or (c) specified in the list of Approved security functions.

1.5.5
assertion
The statement or claim about the IUT that must be true for a cryptographic or security requirement from the governing standard to be met by the IUT. A cryptographic or security requirement may be expressed as one or more assertions.

1.5.6
authentication
Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.

1.5.7
availability
Ensuring timely and reliable access to and use of information.

1.5.8
confidentiality
The property that information is not disclosed to unauthorized individuals, entities, or processes.

1.5.9
configuration management
The management of security features and assurance through control of changes made to hardware, software, firmware, documentation, tests, test tools, and test documentation through the life cycle of the system.

1.5.10
conformance
The state of an implementation satisfying the requirements and specifications of a specific standard as tested by a test suite or an approved test method.

1.5.11
conformance testing
The testing of an implementation against the requirements specified in one or more standards.

1.5.12
cryptographic algorithm
A well-defined computational procedure that takes variable inputs, which may include cryptographic keys, and produces an output. A cryptographic algorithm can be a subset of a security function.

1.5.13
cryptographic boundary
An explicitly defined continuous perimeter that establishes the physical bounds of a cryptographic module and contains all the hardware, software, and/or firmware components of a cryptographic module.

1.5.14
cryptographic key
A parameter used in conjunction with a cryptographic algorithm that determines operations such as: transformation of plain text data into cipher text data, transformation of cipher data into plaintext data, computation of a digital signature, verification of a digital signature, computation of the authentication code from data or shared secret exchange protocol.

1.5.15
cryptographic module
The set of hardware, software, and/or firmware that implements approved security functions (including cryptographic algorithms and key generation) and is contained within the cryptographic boundary.

1.5.16
Derived Test Requirements (DTR)
Description of the methods that will be used by accredited laboratories to test whether the IUT or SUT conforms to the requirements of the specified standards and the requirements for vendor information that must be provided as supplementary evidence to demonstrate conformance to the program-specific standard requirements.

1.5.17
GSA Evaluation Program (GSA EP)
The GSA FIPS 201 Evaluation Program administered by GSA. For more information, see the validation program website: https://fips201ep.cio.gov/.

1.5.18
Implementation Guidance (IG)
A set of documents published during the lifetime of the given standard that provides additional clarification, testing guidance, and interpretations of the given standard. (IGs cannot change or add requirements to the given standard.)

1.5.19
Implementation-Under-Test (IUT)
The entity (e.g., the algorithm or the cryptographic or security module under test) defined within a cryptographic boundary that is the subject of the conformance testing and validation under the elected program.

1.5.20
Independent Tester
Person that performs testing without supervision.

1.5.21
information assurance
The practice of protecting and defending information and information systems by ensuring confidentiality, integrity, and availability.

1.5.22
integrity
The property that data has not been modified or deleted in an unauthorized and undetected manner.

1.5.23
key personnel
The members of the staff who can perform a conformance testing task and who cannot be replaced by any other existing laboratory staff member due to a lack of experience, knowledge, or credentials.

1.5.24
security
The assurance that a system will maintain an acceptable level of information confidentiality, integrity, and availability.

1.5.25
security functions
A part, a subset of parts, or the whole set of the SUT that is relied upon for enforcing a closely related set of cryptographic procedures or security rules as defined in the specified standard and/or security policy. A security function can be a single cryptographic algorithm or a set of algorithms, protocols, procedures, or modes of operations that operate together to produce the output.

1.5.26
security requirements
Functionality and design controls which, when implemented in a system, facilitate information assurance.

1.5.27
survivability
The quantified ability of an entity to continue to operate or to survive during and after a natural or man-made disturbance, at a minimum acceptable level or post-disturbance functionality, and the maximum acceptable outage duration.

1.5.28
System-Under-Test (SUT)
The entity (e.g., the algorithm, the cryptographic or security module under test) that is the subject of the conformance testing and validation under the elected program.

1.5.29
test method
The definitive procedure that produces a test result. The test result can be generated by one test or by a test suite and can be qualitative (yes/no), categorical, or quantitative (a measured value). The test result can be a personal observation or the output of a test tool.

1.5.30
traceability
Interpreted in the CST LAP to mean that the conformance testing tool is traceable back to the underlying requirements of the provided normative standards.

1.5.31
validation
The administrative act by the governing Validation Program (e.g., CMVP, CAVP, NPIVP, etc.) of determining conformance of an implementation to specified standards and requirements (e.g., applicable version of FIPS 140, FIPS 201-2 or successor) based on the review and acceptance of the test results from the accredited laboratories.

1.5.32
Version Control System (VCS)
The management of multiple revisions of the same unit of information (revision control system).

1.6 Program documentation

1.6.1 General

This handbook details the CST program-specific requirements and technical procedures, while detailing and expanding portions of NIST Handbook 150 for CST LAP use. Both the NIST Handbook 150 checklist and the NIST Handbook 150-17 checklist are used in conducting assessments in the CST LAP. Assessor

use of the NVLAP checklists ensures that each laboratory receives an assessment consistent with that received by other laboratories. Checklists assist the assessor(s) in documenting the assessment to the NVLAP requirements found in NIST Handbook 150 and in this handbook. Checklists contain definitive statements or questions about all aspects of the NVLAP criteria for accreditation, and form part of the On-Site Assessment Report (see NIST Handbook 150). The most current version of each checklist is available upon request or on the NVLAP website: https://www.nist.gov/nvlap.

1.6.2 NVLAP General Criteria Checklist

All NVLAP programs use the NVLAP General Criteria Checklist (formerly called the NIST Handbook 150 Checklist), which contains the requirements published in ISO/IEC 17025 and NIST Handbook 150. The checklist items are numbered to correspond to clauses 4 through 8 of ISO/IEC 17025:2017 and Annexes A, B, and E of NIST Handbook 150. The current version of the checklist is available from the NVLAP upon request. Evidence of laboratory ownership of ISO/IEC 17025 is required prior to NVLAP providing a copy of the NVLAP General Criteria Checklist.

1.6.3 NIST Handbook 150-17 Checklist

1.6.3.1 The NIST Handbook 150-17 Checklist (also referred to as the CST program-specific checklist) addresses the requirements specific to cryptographic and security testing given in NIST Handbook 150-17. The checklist contains the requirements provided in this handbook, including testing requirements and additional details and notes for the assessor(s) (e.g., the names of the key personnel), with an emphasis on observing and performing tests, testing accuracy, instrumentation, calibration, personnel competency, and test reporting. The current version of the checklist is available from the CST LAP website: https://www.nist.gov/nvlap/nvlap-cst-lap.cfm.

1.6.3.2 The CST program-specific checklist applies only to cryptographic and security testing.

1.6.4 Scope of accreditation and test method selection

1.6.4.1 The CST LAP offers a set of test methods for accreditation. Depending on the breadth of its testing capabilities, the applicant laboratory may select test(s) from the list of offered test methods. Some of the test methods have additional prerequisites, which are identified in the test-specific annex(es).

1.6.4.2 The scope of accreditation is determined by the selection of the available test methods by a laboratory seeking accreditation as part of the NVLAP application process. For additional information regarding the methods available for selection, refer to Annex A of this handbook.

1.6.5 CST Template for Oral Quizzing

The assessor(s) use(s) the CST Template for Oral Quizzing to document the information gathered during the oral quizzing. The template captures the questions asked, the personnel participating in the quiz, and any assessor(s) comments regarding the responses provided by the laboratory personnel.

1.6.6 NVLAP Lab Bulletins

NVLAP Lab Bulletins are issued to laboratories and assessors, when needed, to clarify program-specific requirements and to provide information about the most current program additions and/or changes. Lab Bulletins providing additions or changes to the current program may supersede the requirements of the current published handbook until the additions or changes are published in a revision of the handbook.

1.6.7 Other publications

Some of the tests and associated test methods reference additional documentation that can be found in the annex associated with the specific test methods and/or on the CST LAP website. The types of tests are available on the NVLAP website: https://www.nist.gov/nvlap/nvlap-cst-lap.cfm.

2 LAP establishment, development and implementation

2.1 Bases for establishment

There are no requirements additional to those set forth in NIST Handbook 150.

2.2 Development of technical requirements

2.2.1 All technical requirements identified in this handbook are derived from ISO/IEC 17025, and tailored to the associated test methods for this LAP.

2.2.2 Additional interpretations and clarifications on laboratory organization and conflicts of interest may be provided in the implementation guidance issued by each validation program. If any discrepancy in the provided information regarding the accreditation process and/or conflict of interest arises, NVLAP's guidance supersedes any other program-specific documentation.

2.3 Announcing the establishment of a LAP

There are no requirements additional to those set forth in NIST Handbook 150.

2.4 Adding to or modifying a LAP

Upon identifying the need for additional cryptographic and/or security tests or test types, NVLAP reserves the right to add or modify the CST LAP either by adding new subsidiary programs or new test methods to existing programs or modifying the existing test methods. All changes will be published in a timely manner in a NVLAP Lab Bulletin and will be reflected on the NVLAP website: https://www.nist.gov/nvlap.

2.5 Termination of a LAP

There are no requirements additional to those set forth in NIST Handbook 150.

3 Accreditation process

A laboratory interested in accreditation for any of the types of tests offered under the CST LAP shall review and become familiar with all the requirements listed in ISO/IEC 17025, NIST Handbook 150, and in this handbook, review the CST LAP website at https://www.nist.gov/nvlap/nvlap-cst-lap.cfm, and contact NVLAP for the most current updates on the requirements and application process.

3.1 Application for accreditation

The accreditation process starts with the submission of the laboratory's application and fees payment.

3.2 Management system evaluation

3.2.1 The management system documentation provided to NVLAP during the application for accreditation process will be reviewed by a NVLAP assessor(s) prior to the onsite assessment. The management system documentation shall be capable of demonstrating the ability to produce consistent and repeatable test results.

3.2.2 For some of the test methods, the test tools are available for download upon request from NVLAP and/or registration with the validation authority to obtain the credentials to download and decrypt the tools. Other methods require the assessor(s) to determine whether the laboratory is ready to be trained to use the test tools before receiving them at its initial onsite evaluation. In other cases, the test tools will be provided to the laboratory during the onsite visit or provided to the laboratory after accreditation has been granted. When available, the laboratory shall register, download, and install the test tool before the NVLAP assessor(s) arrive(s). The laboratory will be responsible for demonstrating, if required, competence to prepare and use these tools. This demonstration will include: loading, configuring, and running the tools; preparing the test reports; and performing updates if necessary. A complete test report produced by the laboratory using these tools should be available for discussion as instructed, either during or after the onsite visit. Distribution and confidentiality of test tools may have specific validation authority restrictions.

3.3 Onsite assessments

Once the application is deemed complete, the process continues with steps a) through c) represented below. Upon completion of any corrective action response(s) to any nonconformities found during the onsite assessment and/or proficiency exam, the process ends with NVLAP's final decision regarding the laboratory's accreditation.

a) *Proficiency exam* – For initial accreditation, once the assessor(s) determines that the management system meets the requirements, a proficiency exam will then be administered to the applicant laboratory depending upon the intended scopes of accreditation. This exam evaluates the laboratory personnel's technical expertise and knowledge of the standards and test methods applicable to the scope of accreditation for which the laboratory is applying. The laboratory/individual shall obtain a score of 75% or greater for correct responses for the accreditation process to continue and the onsite visit to be scheduled. The technical expert(s) from the associated technical program administers this exam as defined by the scope. This exam is conducted prior to the onsite assessment visit.

b) *Onsite visit and proficiency* – For all applicants, the onsite assessment is scheduled once it is determined that the management system meets the necessary requirements found in ISO/IEC 17025, NIST Handbook 150, and NIST Handbook 150-17, and if applicable, the initial exam is passed. The onsite visit is scheduled at a mutually agreed-upon date. The laboratory personnel may be quizzed during the assessment, and team dynamics observed for proficiency and technical expertise. Staff member interaction and knowledge distribution among team members are key factors that will be monitored by the assessor(s). The laboratory staff shall provide 75% or greater correct responses for the accreditation process to continue. During the onsite assessment, the laboratory shall also demonstrate that the required set of tools is available, and the testing environment is adequate for testing (e.g., space, ventilation, security, test chambers, and test benches).

c) *Proficiency artifact* – A proficiency artifact is provided to the applicant laboratory (at the end of the initial onsite assessment or shortly thereafter) for the applicable scopes. The proficiency artifact is designed to evaluate the laboratory's understanding of and competence to apply the CST conformance testing methodology specific to the scope of accreditation for which the laboratory is applying. For applicable scopes, the laboratory shall successfully complete the proficiency artifact exam as evaluated by the technical expert assessor(s).

3.3.1 Conduct of onsite assessment

3.3.1.1 It is important to note that the laboratory cannot be granted accreditation until:

a) The laboratory has completed and passed the proficiency exam as applicable (normally conducted before the initial onsite assessment);

b) The laboratory has passed the proficiency quiz as applicable [3.3a] (normally conducted during the onsite assessment) and the laboratory staff has demonstrated an understanding of and competence to apply the Cryptographic and Security Testing conformance testing methodology as evaluated by the results of the proficiency quiz;

c) The laboratory has completed and passed the proficiency artifact exam as applicable [3.3c];

d) The laboratory has exercised the management system and has produced appropriate records of all management system activities; and

e) The laboratory has demonstrated for the selected test(s) that the required set of tools and test methods are available, and the testing environment is adequate (e.g., space, ventilation, security, separation, storage, test chambers and test benches).

3.3.1.2 The length of time for the onsite assessment is dependent upon the applicant's scope of accreditation. Typically, the onsite assessment will occur over two to three days and typically will be performed by two or more NVLAP assessors. Observations and findings identified by the assessor(s) during the assessment are held in the strictest confidence.

3.3.1.3 In some cases, the onsite assessment may involve the laboratory site and a separate test site for the proficiency testing. If the separate test site for the proficiency demonstration is within a short commuting distance from the main laboratory site, the demonstration will have to be scheduled at a date and time mutually agreed-upon between the assessor(s) and laboratory management and will be included as part of the onsite assessment. If the geographic distance to the separate test site requires significant travel, then this is deemed by NVLAP to be a separate laboratory that must be separately accredited with a specific and separate onsite assessment.

3.3.1.4 The assessor(s) will use, in addition to the NVLAP General Criteria Checklist, based on ISO/IEC 17025 and NIST Handbook 150, the CST program-specific checklist, which is derived from the technical requirements contained in this handbook. Even though the CST checklist is derived dynamically from the elected scope of accreditation and corresponding test methods, the derivation is done such that the composed checklist ensures that the assessment is complete, and that each assessor covers the same items at laboratories with an equivalent chosen scope of accreditation.

3.3.1.5 Assessor(s) are encouraged to use good engineering judgement whenever the need arises (e.g., new updated requirements are available on the CST LAP's website), to delve more deeply into technical issues.

3.3.1.6 The agenda for a typical onsite assessment is given below.

a) *Opening meeting*: During the onsite visit, the assessor(s) conduct(s) an entry briefing with laboratory management and supervisory personnel to explain the purpose of the onsite and to discuss the schedule for the assessment activities. Information provided by the laboratory on the accreditation application form may be discussed during this meeting. At the discretion of the laboratory manager, other staff may attend this meeting.

b) *Staff interviews, discussions, proficiency quizzes*: The assessor will ask the laboratory manager to assist in arranging times for individual interviews with laboratory staff members and/or proficiency/roundtable quizzes of staff. While it is not necessary for the assessor to talk to all staff members if individual interviews are requested, he/she may select staff members representing all different aspects of the laboratory. If proficiency/roundtable quizzes are to be conducted onsite as a means of resolving technical nonconformities resulting from the written or oral exam, all members of the relevant staff shall be scheduled to be available and participate. Also, if after the completion of the roundtable quizzing of the laboratory staff it is deemed necessary by the assessor(s), further interviews with individual laboratory staff members may be requested.

c) *Records review*: During the onsite visit, the assessor(s) will also review the laboratory's documentation, including:

- conformance of the management system with ISO/IEC 17025 and NIST Handbook 150;
- equipment and maintenance records;
- record-keeping procedures;
- testing procedures;
- laboratory test reports;
- personnel competency records;
- personnel training records including, but not limited to, training plans, areas of training, and training materials;
- version of the test tools and/or other test program-specific software;
- procedures for updating pertinent information; and
- safeguards and separation for the protection of confidential, vendor-sensitive, proprietary and applicable International Traffic in Arms Regulations (ITAR) information.

One (or more) laboratory staff member(s) shall be available to answer questions; however, the assessor may wish to review documents alone. Under some circumstances, the assessor may request to review management system documents outside of the laboratory during the assessment such as a revised quality manual, proficiency test data, or new procedures. The material will be returned or destroyed atthe laboratory's direction.

The assessor will check personnel information for job descriptions, resumes, training records, and technical performance reviews. The assessor will not request information that violates individual privacy such as salary, medical information, or performance reviews outside the scope of the laboratory's accreditation. At the discretion of the laboratory, a member of its human resources department (or equivalent) may be present during the review of personnel information.

d) *Internal audit and management review*: The assessor(s) will review and discuss the laboratory's internal audit and management review activities with the laboratory staff. The discussion will include

all aspects of those activities including the management system procedures, the audit findings, the results of the management review, and the actions taken to resolve problems identified.

e) *Equipment*: The assessor(s) will examine test method-specific computer hardware, software, supporting test equipment, and facilities for appropriateness, capability, adherence to specifications, etc.

f) *Laboratory walk-through*: The assessor(s) will inspect the laboratory in the following areas during a walk-through:

- physical layout of the laboratory including entrance/exit points;
- all test equipment and tools, including computer hardware, servers used for records retention, and physical storage area;
- work environment regarding provision of adequate testing workspace (including adequate separation of work activities as appropriate or by programmatic requirement), heating, lighting, etc.; and
- physical security including access control procedures and records.

g) *Proficiency evaluations*: Although the written and/or oral examination is provided prior to the initial onsite assessment, the group round-table quizzes and individual demonstrations conducted as required during the initial and renewal onsite assessments are considered part of the proficiency evaluations. When necessary, there may be additional proficiency artifact and/or operational exams required as part of the assessment. Unless otherwise instructed prior to the onsite visit, the proficiency artifact and/or operational exam described in 3.1.2 and which completes the initial proficiency evaluations will be either provided at the end of the onsite visit or will be sent to the laboratory after the onsite visit. NVLAP reserves the right to modify this rule, when appropriate, on a case-by-case basis.

h) *Closing meeting*: At the end of the onsite visit, a closing meeting is held with the laboratory manager and staff to discuss findings documented by the assessor(s) during the visit. See 3.3.3 and 3.3.4 of NIST Handbook 150 for more information regarding the assessment report, nonconformities, and the final resolution.

3.3.2 Onsite assessment report

The assessor completes the Onsite Assessment Report that summarizes the findings. Copies of the completed checklists are also provided at the closing meeting. The report is signed by the assessor(s) and the laboratory's Authorized Representative. The original report and checklists are forwarded to NVLAP. A copy of the report is given to the laboratory. The decision to grant or renew accreditation is not made by the assessor team but is made by NVLAP in accordance with the procedures described in NIST Handbook150.

3.3.3 Nonconformities, comments, and recommendations

3.3.3.1 Any nonconformity that has been corrected during the onsite assessment by the laboratory using its corrective action process and any recommendations will be specifically noted on the onsite assessment report by the assessor. The assessor will also note how the nonconformity was resolved.

3.3.3.2 Comments in the report should be given serious consideration by the laboratory, however a corrective action response is not required to be submitted to NVLAP. Actions that arise from comments are made at the laboratory's discretion. Comments are those areas of concern where a nonconformity may arise; however, no objective evidence is available to support citation of a nonconformity. Historically, it has been noted that comments often rise to the level of nonconformities on subsequent assessments. As such, comments noted in the assessment will be reviewed at the next onsite assessment to ensure that these issues

have not risen to the level of nonconformities since the last onsite visit.

3.3.3.3 Positive findings from the assessment will also be recorded in the onsite assessment report.

3.4 Proficiency Testing

3.4.1 General

3.4.1.1 The CST LAP mandates program-specific proficiency testing participation, where available. Laboratories are required to participate in proficiency testing, if available, as designated in the annex associated with the specific test methods.

3.4.1.2 The proficiency test concept is designed to allow the evaluation of the laboratory's ability to produce repeatable and reproducible test data. To properly evaluate a laboratory, the proficiency testing consists of several parts previously described in 3.3a.

3.4.2 Types of proficiency testing

The LAP's proficiency testing may consist of one or more of the following exercises:

a) Demonstration of correct identification and use of the NIST-mandated test tools. The laboratory shall demonstrate that all appropriate personnel, including those performing testing, understand the test tools and/or component use and operation. This shall be demonstrated by the laboratory personnel exercising the use of the publicly available or provided test tools under the assessor(s)' direct observation.

b) Demonstration of an understanding and correct interpretation of all data transformation and of all test results reported by the test tools.

c) Demonstration of report generation in an approved format and with the content identical to the results produced by the test tools.

d) Demonstration of a solid background, theoretical knowledge, and technical expertise in the selected test methods for the scope of accreditation. The laboratory shall be provided with a proficiency quiz to be responded to by all appropriate personnel including those performing testing. The quiz also poses questions for each test method for which the laboratory is seeking accreditation.

   These questions will test for:

   - basic cryptographic and security knowledge as applicable to the technical area determined by the selected test methods on the scope of accreditation;
   - familiarity with the governing standards and specifications;
   - familiarity with the test methods that are part of the scope of accreditation;
   - ability to determine how a cryptographic or security test should be performed for a set of test requirements; and
   - how a specific algorithm, module, or component should be tested to the governing specification.

e) Demonstration of IUT or SUT conformance testing proficiency. The laboratory shall perform a conformance test of a specially designed artifact, referred to as IUT or SUT, with one or more features that is/are not in conformance with the standard. The laboratory shall discover the nonconformities, document them, and indicate which standard's requirements have failed due to the presence of the nonconformities.

   Unless otherwise specified by NVLAP, the proficiency artifact for the initial accreditation will be delivered to the laboratory at the end of the onsite assessment or later. Also, unless otherwise stated, the proficiency artifact shall be considered the property of the programmatic body and shall be considered confidential property not to be shared, divulged, or changed without permission from the associated programmatic body. Any use of the artifact outside of the specified task may result in adverse action regarding the laboratory's accreditation.

NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests.

3.4.3 Analysis and reporting

The results of the proficiency testing are presented by the assessor(s) and/or the validation program to NVLAP as soon as the testing process is completed. The results are then reported to the laboratory.

3.4.4 Proficiency testing nonconformities

Unsatisfactory performance in proficiency testing is a technical nonconformity that shall be resolved by the laboratory through its corrective action process to maintain its accreditation for the testing activity in question. If the laboratory performs unsatisfactorily in any proficiency test, it shall take corrective action to investigate and resolve nonconformities in a timely manner, according to the requirements in 7.10 of ISO/IEC 17025 for the control of nonconforming work.

Unsatisfactory performance in proficiency testing or substantial errors in the reports submitted to any of the validation programs may result in suspension or revocation of accreditation. For more information, see clause 3.10.

3.5 Accreditation decision

There are no requirements additional to those set forth in NIST Handbook 150.

3.6 Granting accreditation

It is important to note that the laboratory is granted initial accreditation after effectively implementing the management system, produced appropriate records of all management system activities, including conducting at least one internal audit and one management review, and successfully completed the initial Proficiency Testing (PT) activity.

3.7 Renewal of accreditation

There are no requirements additional to those set forth in NIST Handbook 150.

3.8 Monitoring visits

There are no requirements additional to those set forth in NIST Handbook 150.

3.9 Changes to scope of accreditation

There are no requirements additional to those set forth in NIST Handbook 150.

3.10 Suspension of accreditation

3.10.1 Failure to appropriately address and resolve complaints from customers or other interested parties may result in a NVLAP monitoring visit, additional proficiency testing, and/or suspension or revocation of accreditation.

3.10.2 Significant changes in a laboratory's key technical personnel or facilities may result in a NVLAP monitoring visit(s), and/or suspension of accreditation of the affected test method(s) from the scope of accreditation if the new personnel fail to meet the competency requirements in support of the testing. Loss of key personnel without immediate adequate replacement may result in suspension of the laboratory's accreditation for the test method(s) affected by the loss of key personnel.

3.10.3 If the laboratory does not demonstrate continued competence to perform CST conformance testing, NVLAP may suspend or revoke the laboratory's accreditation. The accreditation may be suspended or revoked if any of the following statements is true:

- reports submitted for validation within the accreditation cycle are incorrect, invalid, or deficient as defined by each validation program;
- the loss of key technical personnel from the laboratory;
- nonconformities found during any onsite visit are not appropriately addressed through corrective actions taken by the laboratory; or
- the laboratory has not submitted the required number of vendor product test reports to the validation authority within the accreditation cycle.

3.11 Denial and revocation of accreditation

There are no requirements additional to those set forth in NIST Handbook 150.

3.12 Voluntary termination of accreditation

There are no requirements additional to those set forth in NIST Handbook 150.

3.13 Appeals

There are no requirements additional to those set forth in NIST Handbook 150.

4 General requirements

4.1 Impartiality

4.1.1 The laboratory shall establish and maintain policies and procedures for maintaining laboratory impartiality and integrity in the conduct of cryptographic and security testing.

NOTE: A CST laboratory may provide clarification of the standards, the Derived Test Requirements, and other associated documents at any time during the life cycle of the IUT or SUT which is not deemed a conflict of interest.

4.1.2. A third-party CST laboratory shall have no financial interest for the work performed under the present scope of accreditation other than its conformance testing and/or validation fees. A first-party CST laboratory may be part of the same company that produced the IUT/SUT but must be organizationally independent.

4.1.3 The laboratory shall not perform conformance testing on a module for which the laboratory staff has:

a) designed any part of the IUT or SUT;

b) developed original documentation for any part of the IUT or SUT;

c) built, coded, or implemented any part of the IUT or SUT; or

d) had any ownership or vested interest in the IUT or SUT.

NOTE: Provided that a CST laboratory has met the other requirements, to be considered a third-party laboratory, the laboratory may perform conformance testing on IUT or SUT produced by a company when:

- the laboratory has no ownership in the company;
- the laboratory has a separate management from the company; and
- business between the CST laboratory and the company is performed under contractual agreements, as done with other clients.

4.1.4 A CST laboratory may take existing vendor documentation for an IUT or SUT (post-design and post-development) and consolidate or reformat the information (from multiple sources) into a set format. If this occurs, the vendor and the validation programs shall be notified of this when the conformance test report is submitted.

4.2 Confidentiality

The management system shall include policies and procedures to ensure the protection of proprietary information. The policies and procedures shall specify how proprietary information will be protected from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons.

5 Structural requirements

The laboratory shall have a policy and procedure(s) for maintaining a strict separation, both physical and electronic, between the laboratory testers and company's consultant teams, product developers, system integrators, and others who may have an interest in and/or may unduly influence the testing outcome.

6 Resource requirements

6.1 General

The laboratory's management system shall contain all documentation that ensures the laboratory's implementation of the technical requirements in ISO/IEC 17025, NIST Handbook 150, this handbook, and other stakeholder requirements as necessary (e.g., CMVP Implementation Guidance).

6.2 Personnel

6.2.1 Within each laboratory's elected scope of accreditation, the laboratory shall maintain responsible supervisory personnel and competent technical staff who are:

a) knowledgeable of all programmatic test methods, test metrics, and implementation guidance;

b) knowledgeable of all relevant FIPS, NIST SP, and references in this handbook and on the CST LAP website;

c) familiar with cryptographic terminology and families of cryptographic algorithms and security functions with emphasis on the FIPS-approved and/or NIST-recommended security functions; and

d) familiar with the cryptographic and security testing tools.

6.2.2 The laboratory shall identify, define, and document the key personnel designated to satisfy NVLAP requirements and their assigned roles. Key Personnel shall include, but not be limited to:

a) laboratory director;

b) laboratory manager(s);

c) staff members(s) responsible for maintaining management system;

d) authorized representative;

e) approved signatories; and

f) other key technical persons in the laboratory (e.g., testers).

NOTE: Significant changes in a laboratory's key technical personnel or facilities may result in a NVLAP monitoring visit. Loss of key personnel without immediate adequate replacement may result in the laboratory's suspension of accreditation.

6.2.3 When the laboratory employs staff members through contracting, the laboratory shall ensure any key personnel who are contractors are identified. NVLAP and the affected validation program shall be informed when a change in the key personnel employed through contracting occurs or when the direct supervision of this category of personnel is not possible. Contracted laboratory staff shall also be subject to the CST LAP's proficiency exam process (See 3.3).

NOTE: When any change occurs in contracted key personnel, the laboratory shall ensure NVLAP and the validation program are notified.

6.2.4 An individual may be assigned or appointed to serve in more than one position provided it does not create a conflict of interest and maintains impartiality of the testing activities. To the extent possible, the laboratory director and the person responsible for implementing and maintaining the management system should be independently staffed.

6.2.5 The laboratory person(s) responsible for implementing and maintaining the management system shall receive management system training preferably in ISO/IEC 17025. If training is not available in ISO/IEC 17025, minimum training shall be acquired in the ISO 9000 series, especially ISO 9001 or equivalent with emphasis on internal auditing

6.2.6 The laboratory staff responsible for the testing activities shall have knowledge and skills commensurate with the scope of work such as a technical degree (e.g., a bachelor's degree in computer science, computer engineering, electrical engineering, etc.), similar technical discipline, or equivalent experience (e.g., professional certification, etc.). For more details regarding the staff members' required expertise for each program, see the annex associated with the specific test methods.

6.2.7 The laboratory personnel who manage, perform, or verify work affecting the results of laboratory activities shall possess knowledge and have undergone training on/in the areas listed below:

a) general requirements of the test methods, including generation of test reports;

b) system security concepts;

c) physical security;

d) identification and authentication technologies and techniques;

e) familiarity with cryptographic and security methods and terminology;

f) standards compliance;

g) familiarity with all FIPS publications referenced in this document and NIST Handbook 150;

h) operation and maintenance of NVLAP/Validation Program-mandated testing tools.

6.2.8 Only the laboratory personnel shall take all actions necessary to perform the testing activities and record the results, including the loading, compiling, configuring, and execution of mandatory test tools.

6.2.9 The laboratory shall have a competency review program and procedures for the evaluation and maintenance of the competency of each staff member for each test method the staff member is authorized to conduct. An evaluation and an observation of performance shall be conducted annually for each staff member by the immediate supervisor or a designee appointed by the laboratory director. A record of the annual evaluation of each staff member shall be dated and signed by the supervisor and the employee.

6.3 Facilities and environmental conditions

6.3.1 The laboratory shall have its internal networks protected from unauthorized access and malicious software.

6.3.2 If the laboratory is conducting multiple simultaneous testing activities, a system of separation between IUTs and SUTs from different vendors and conformance testing activities shall be maintained as necessary.

6.3.3 The laboratory shall have access to the most current documentation and test tools from NIST/ITL, NVLAP, or other appropriate sites and secure e-mail capabilities for communication with NVLAP, NIST/ITL, CCCS, and the laboratory's customers.

6.3.4 The testing laboratory shall ensure that, when applicable, the correct version of the program-specific testing tools is used and that the tools have not been altered in any way that might lead to incorrect results.

6.3.5 For all conformance testing and validations, the laboratory shall ensure that any file containing past results or past test programs on the IUT or SUT is isolated from the current test programs and test or validation results.

6.3.6 If a laboratory must conduct conformance testing at sites away from its permanent facilities, testing activities shall be carried out in such a way as to meet the requirements of this document.

6.3.7 Testing at permanent remote locations

6.3.7.1 Where the laboratory performs IUT testing activities at permanent remote locations the laboratory shall meet the requirements listed in sections 6.3.7.2 to 6.3.7.7.

6.3.7.2 The laboratory shall have a procedure for the protection of all IUT information. The procedure shall address, but not be limited to:

a) VPN connections that may be used to transmit IUT information between laboratory locations;

b) workstations, laptops, and storage devices (e.g., memory sticks, hard drives, etc.);

c) authenticated access to workstations, laptops, etc. by lab personnel only;

d) protection, access, use, storage, and disposal of data (i.e., source code, HDL, documentation, etc.) shall be defined and documented for both electronic and physical documents.

NOTE 1: Permanent remote locations are considered those locations outside of the laboratory facility and which occur at a known location (e.g., work-at-home, remote offices).

NOTE 2: Temporary off-site locations may be used for performing physical testing (e.g., vendor sites or specialized physical testing facility such as a university laboratory).

NOTE 3: Mobile facilities are not approved for any cryptographic and security testing activities.

6.3.7.3 All workstations or test equipment shall be supplied by and under the control of the laboratory. Programmatic tools shall only be installed on laboratory-owned equipment.

6.3.7.4 Hardware IUTs shall not be present at a remote location.

6.3.7.5 Software or firmware IUT operating environment platforms shall not be present at a remote location. If software or firmware IUT operational testing is performed from a remote location, the laboratory shall utilize a VPN connection to the operating environment platform(s) located at the permanent laboratory facility.

NOTE: Documentation review and code review are permitted at remote locations.

6.3.7.6 The laboratory shall disclose to the IUT vendor that the vendor's IUT information may be maintained at remote locations.

6.3.7.7 All records shall be retained at the laboratory's permanent location.

6.3.7.8 The laboratory shall document the work performed at any remote location (e.g., ACVTS, document review, source code review, CRYPTIK entry, etc.).

6.4 Equipment

6.4.1 The laboratory shall ensure that any test tool used to conduct cryptographic and security testing is performing properly according to the validation authority specifications. The laboratory shall also ensure that the tool does not interfere with the conduct of the test and does not modify or impact the IUT or SUT.

6.4.2 Confirmation of the use of the most current version of testing tools shall be ensured before conducting a test. Records of these confirmations shall be maintained.

NOTE 1: For more information regarding types of equipment and information required for conducting the conformance tests, see the annex associated with the specific test method(s). Special equipment may be necessary for test methods as derived from the scope of accreditation.

NOTE 2: Test equipment refers to software and hardware products and/or other assessment mechanisms used by the laboratory to support the cryptographic and security testing of the IUT or SUT.

6.4.3 For conformance testing, the laboratory shall maintain, load, and run a copy of the testing tool(s) provided by the validation program and produce test results using the tool(s) as appropriate. The testing tools provided by the validation program shall not be altered or changed and shall not be distributed outside the laboratory except to the validation program.

NOTE: A list of the required testing tools is provided in the annex associated with the specific test method(s) and/or the CST LAP website.

6.4.4 Whenever major or minor changes are made to any testing tool, a testing laboratory shall have procedures to assure the accurate execution and correct performance of the test tool. The procedures shall include, at a minimum, the complete set of regression testing of the test tool. This is necessary to ensure that consistency is maintained, as appropriate, with other testing laboratories and that correctness is maintained with respect to the relevant standard(s) or specification(s).

6.4.5 When no suitable validation service or no suitable reference implementation is available, the laboratory shall define the procedures used to verify the correct operation of the test tool. Verification records shall be maintained for whenever the test tool is modified.

6.4.6 The laboratory shall document appropriate procedures whenever a test tool is found to contain errors that make the tool defective or unfit for use. These procedures shall include identification of the error and reporting the error to the appropriate maintenance authority or validation authority. If, after correction of the test tool, the results of the test require modification, the modified test results shall be transmitted to the vendor and validation authority.

6.4.7 The laboratory shall maintain records of the configuration of test equipment (hardware and software) and the analyses to ensure the suitability of test equipment to perform the desired testing.

6.4.8 Equipment records shall include hardware and software upgrades and periods of use.

6.5 Measurement traceability

6.5.1 Test results produced by the testing laboratory shall be traceable to standard test suites when appropriate, or otherwise to the applicable authoritative test suite.

NOTE 1: For cryptographic and security testing, "traceability" (see 1.5.38) is interpreted to mean that the validation test tools shall be traceable back to the underlying requirements of the normative standards listed in 1.4, in the annex associated with the specific test methods, and on the CST LAP website.

NOTE 2: Each abstract test case and the associated evaluation methodology are traceable to a specific cryptographic or security requirement listed in the governing documentary standard. The abstract tests cases are achieved via the assertions and associated DTRs documented in the testing tool in use.

6.5.2 Calibration of test equipment

6.5.2.1 If applicable, equipment used for conformance tests shall be maintained and calibrated in accordance with the manufacturer's recommendation, as specified in the test method, or as specified in the annex associated with the specific test method(s).

6.5.2.2 When calibrations are performed in-house, the requirements of NIST Handbook 150, Annex B shall be met.

6.5.3 Testing

6.5.3.1 The laboratory shall use the test methods specified in the applicable Annex. When deviations to the test methods are necessary, in addition to receiving vendor-approval, the validation program shall also be informed.

6.5.3.2 Any deviation shall be sufficiently documented to ensure the correct and required precision and interpretation of the program-specific test method are maintained.

6.5.3.3 Any deviation to the test method shall be identified in the test report.

NOTE: The validation authority may use identified test method deviations to update the test methods whenappropriate.

6.5.3.4 When a difference is identified between the program-specific test objectives and the testing tool's abstract test cases, the laboratory shall record how each realization of a test case is derived faithfully from the governing document (e.g., FIPS, NIST, SP, etc.) with preservation of assignment of verdicts or measurements to the corresponding sets of observations.

NOTE: For more details on the specific test methods in the CST Accreditation program, see the annex associated with the specific test methods and the CST LAP website: https://www.nist.gov/nvlap/nvlap-cst-lap.cfm.

6.6 Externally provided products and services

If an external laboratory provides testing activities (i.e., on a subcontract) during the conformance testing process, the external laboratory shall be itself a NVLAP-accredited laboratory whose scope includes the applicable test method(s).

7 Process requirements for accreditation

7.1 Review of requests, tenders, and contracts

7.1.1 Policies for document storage and maintenance of contracts under confidentiality, nondisclosure agreements, marked as secret, or copyright protected, shall be defined according to the document's status.

7.1.2 These documents shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel.

7.1.3 When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be the applicable version of FIPS 140 validated and operating in FIPS mode.

7.1.4 The testing laboratory and vendor shall agree, in writing, what constitutes the IUT or SUT and what constitutes the environment within the IUT. For this program, the environment includes, but it is not limited to:

a) the specific test platform;

b) the test configuration; and

c) the external environment.

7.2 Selection verification and validation of methods

There are no requirements additional to those set forth in ISO/IEC 17025.

7.3 Sampling

There are no requirements additional to those set forth in ISO/IEC 17025.

7.4 Handling of test items

7.4.1 The laboratory shall protect all IUTs, SUTs, and test tools from modifications of any kind and from unauthorized access.

7.4.2 Cryptographic mechanisms utilized to protect information shall be the applicable version of FIPS 140validated and operating in FIPS mode.

7.4.3 When the IUT or SUT consists of software components, the laboratory shall ensure that configuration management is in place to prevent inadvertent modifications. This configuration management shall uniquely identify each IUT or SUT and control and document modifications to any of the software components.

7.5 Technical records

7.5.1 The test results and the test reports generated using cryptographic or security testing tools for the IUT or SUT shall be kept by the laboratory following the completion of testing for the life of the IUT or SUT, or as specified by the validation authority and/or vendor in writing.

7.5.2 Records may include hard or digital copies of the official test results and the test results error file(s). Records shall be stored in a manner that assures survivability, confidentiality, integrity, and accessibility.

7.5.3 When cryptography is utilized as the mechanism for protection of information, the cryptographic module used shall be the applicable version of FIPS 140 validated and operating in FIPS mode.

7.5.4 A copy of the final test results and/or the test reports generated using cryptographic or security testing tools for the IUT shall be submitted to the validation program.

7.5.5 All records shall be retained at the laboratory's permanent location.

7.6 Evaluation of measurement of uncertainty

There are no requirements additional to those set forth in ISO/IEC 17025.

7.7 Ensuring the validity of results

There are no requirements additional to those set forth in ISO/IEC 17025.

7.8 Reporting of results

7.8.1 General

7.8.1.1 The laboratory shall issue test reports of its work that accurately, clearly, and unambiguously present the test conditions, the test setup when it varies from the standard protocol, the test results, and all other information necessary to reproduce the test.

7.8.1.2 Any deviations or omissions from the relevant program-specific requirements shall be clearly indicated.

7.8.2 Test reports

7.8.2.1 Test reports issued to customers shall meet contractual as well as validation program requirements, in addition to meeting the requirements of NIST Handbooks 150 and 150-17.

7.8.2.2 If a validation program-supplied test report tool or other reporting methodologies are provided, the laboratory shall follow those requirements and use those supplied test tools.

7.8.2.3 If the laboratory includes opinions, interpretations, or results in a test report that are not covered by their accreditation, the laboratory shall state clearly which statements are outside the scope of its accreditation.

7.8.2.4 For test cases that require an analysis of the observations by the testing staff to interpret the results before issuing a test report, the laboratory shall have procedures to be followed by the test operators performing the analysis. These procedures shall ensure the repeatability, reproducibility, and objectivity of the analysis.

7.8.2.5 Test reports bearing the NVLAP symbol may be written for more than one purpose:

a) reports that are produced under contract and intended for use only by the vendor, which shall meet vendor/laboratory contract obligations and be complete but need not necessarily meet all validation program requirements;

b) reports to be submitted to a validation authority for IUT or SUT validation under a specific validation program.

7.8.2.6 Test reports intended for submission to any of the validation programs under the CST LAP shall meet the requirements of the associated DTRs and the implementation guidance (IG) when applicable, as well as the requirements of NIST Handbook 150 and NIST Handbook 150-17.

7.8.2.7 The laboratory shall perform an independent technical quality review of the test report submission documents prior to submission to the validation program. This review shall address accuracy, completeness, sufficient testing evidence, and consistency. A record of this review shall be maintained.

7.8.2.8 The test reports for each project shall identify the work performed at each laboratory location, if applicable (e.g., ACVTS, document review, source code review, CRYPTIK entry, etc.).

7.8.2.9 Test reports shall provide all necessary information to permit reproduction of the test and to obtain consistent results.

7.8.3 Electronic transmission of results to the validation programs

7.8.3.1 A laboratory may submit a test report as instructed by the validation program. An electronic version shall have the same content as the printed reports and shall be generated using a software application that is acceptable to the validation program.

7.8.3.2 The laboratory shall ensure that the test results are transmitted with an integrity and confidentiality mechanism appropriate to the sensitivity of the data and the requirements of the validation program and/or governments regulations.

7.8.3.3 When cryptography is utilized as the mechanism for the protection of information, the cryptographic module shall be the applicable version of FIPS 140 validated and operating in FIPS mode.

NOTE 1: The transmission mechanism of the test report to the validation program is employed to ensure that the test report is only disclosed to the intended recipient(s).

NOTE 2: An integrity mechanism exists to ensure that the test report is not modified.

7.8.4 Amendments to test reports

7.8.4.1 When amendments are made to the test results for the purpose of the validation program, the laboratory shall issue corrections or additions to a test report using the method that meets the requirements of the respective validation program and to the requirements set forth in ISO/IEC 17025.

7.8.4.2 For test reports created for purposes other than official IUT validation, the laboratory shall issue corrections or additions to a test report only by a supplementary document suitably marked, e.g., "Supplement to test report serial number […]." If the change involves a test assertion, this document shall specify which test assertion is in question, the content of the result, the explanation of the result, and the reason for acceptance of the result.

7.9 Complaints

There are no requirements additional to those set forth in ISO/IEC 17025.

7.10 Non-conforming work

There are no requirements additional to those set forth in ISO/IEC 17025.

7.11 Control of data information management

There are no requirements additional to those set forth in ISO/IEC 17025.

8 Management system requirements for accreditation

8.1 Options

There are no requirements additional to those set forth in ISO/IEC 17025.

8.2 Management system documentation

The reference documents listed in 1.4, the annex associated with the specific test methods, as well as any other standards and publications related to the CST LAP, shall always be available to all appropriate personnel.

8.3 Control of management system documents

There are no requirements additional to those set forth in ISO/IEC 17025.

8.4 Control of records

8.4.1 The laboratory shall maintain a functional record-keeping system for each customer. Records shall be readily accessible. Digital media shall be logged and effectively marked, and they shall be properly and securely backed-up and disposed of once the retention period has been exceeded. Entries in paper-based laboratory notebooks shall be dated, signed, or initialed.

8.4.2 Software and data protected by nondisclosure agreements or classified as confidential shall be stored according to the vendor and/or government requirements and commensurate with the data sensitivity, and access shall be granted only to the authorized personnel. An access log file shall be maintained.

8.4.3 If a vendor's system on which testing is conducted is potentially open to access by third parties, the testing laboratory shall ensure that the testing environment is controlled to prevent unauthorized access to the system during testing.

8.4.4 All records including training, internal audits, and management reviews shall be retained for future reviews, and the integrity of electronic documents shall be assured. Documents in hard copy form shall be marked and stored in a secure location and, if necessary, a file logging any access, change, or addition shall be maintained to preserve a document's integrity and prevent unauthorized changes.

8.4.5 The laboratory shall maintain records of the configuration of test equipment and all analyses to ensure the suitability of test equipment to perform the desired testing.

NOTE: Additional requirements regarding technical records are given in 7.5.

8.5 Actions to address risk and opportunities

There are no requirements additional to those set forth in ISO/IEC 17025.

8.6 Improvement

There are no requirements additional to those set forth in ISO/IEC 17025.

8.7 Corrective action

There are no requirements additional to those set forth in ISO/IEC 17025.

8.8 Internal audits

8.8.1 The laboratory shall perform at least one full internal audit prior to the initial onsite assessment.

8.8.2 In the case where only one member of a laboratory staff is competent in some technical aspects of the program or is the only expert in conducting a specific aspect of the conformance testing, that part of the audit shall be carried out by an external expert.

NOTE: The laboratory's permanent remote locations are within the criteria and scope of the internal audit.

8.9 Management reviews

The laboratory shall perform at least one full management review prior to the first onsite assessment.

9 Additional requirements

See the following annexes for requirements specific to each technical program and its associated test methods.

Annex A: Additional information about tests offered by the CST LAP (informative)

A.1 Additional general information

Annex A provides additional information as it pertains to the specific test methods for the various testing programs with the CST LAP. Section A.2 describes the various testing programs and the associated test methods available for accreditation under the CST LAP.

Figure A.1 is included to make a clear distinction between the accreditation program and the validation program, as well as to emphasize the separation of duties for each key player in these processes. This informative diagram illustrates the validation process and the rapport between:

- the validation authority (validation program, i.e., CAVP, CMVP, NPIVP, GSAP, DHSIPCM, SCAP);
- the laboratory; and
- the consumers (e.g., U.S. Government agencies).

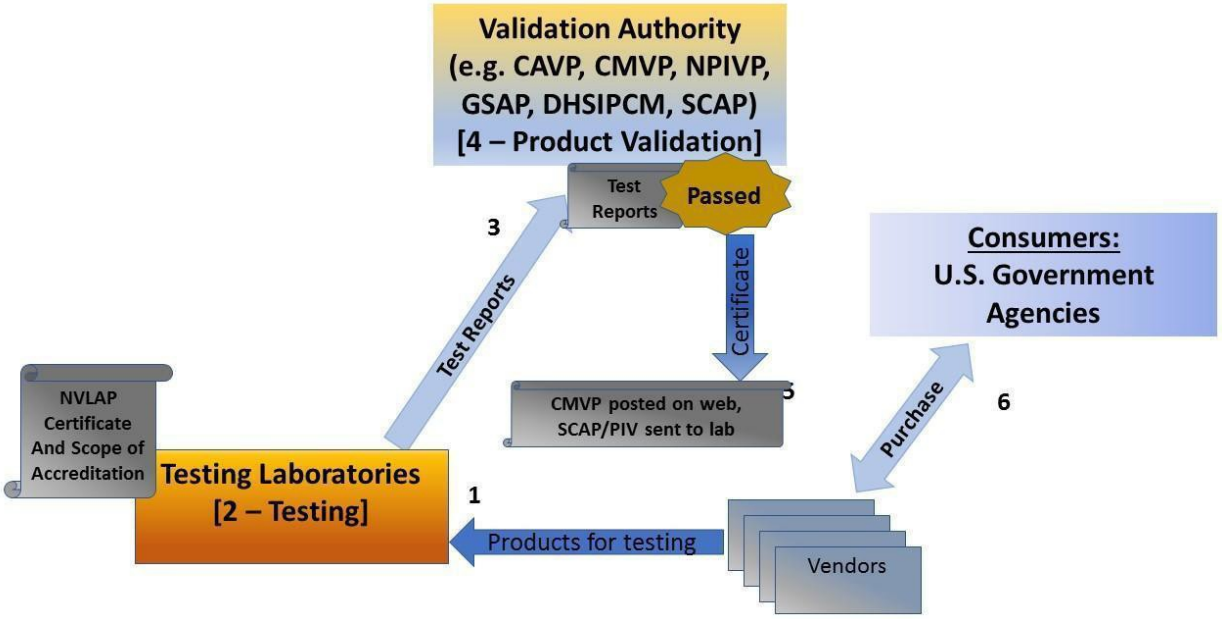

Figure A.1. Validation process.

A.2 Scope of accreditation and test methods

NVLAP offers all interested laboratories a flexible, dynamic system of selecting a compound scope of accreditation under the CST LAP that best fits the laboratory's level of expertise and equipment.

A chained list showing all currently offered test methods is presented below. For the most current information on methods available, see the CST LAP website at http://www.nist.gov/nvlap/nvlap-cst-lap.cfm.

The list below indicates that the selection of any descendent test method mandates the selection of all preceding test methods. For example, the selection of the 17PIV test, mandates the selection of the 17CM, 17ACVT tests, as well.

☐ **17ACVT** Automated Cryptographic Validation Testing (mandatory for 17CM)

☐ **17CM** Cryptographic Modules – Testing
(applicable version of FIPS 140, Security Levels 1 to 4)

☐ **17PIV** Personal Identity Verification Testing (NPIVP, FIPS 201)

☐ **17GSAP** General Services Administration Precursor Testing
(GSAP test methods, FIPS 201)

☐ **17DHSIPCM** Department of Homeland Security Identity and Privilege Credential Management Testing

☐ **17SCAP** Security Content Automation Protocol Testing
(SCAP, XCCDF, OVAL, OCIL, CVE, CCE, CPE, CCSS, CVSS, Asset Identification, ARF, and TMSAD)

Figure A.2 provides a graphical representation of the list presented above. Also indicated are the dependencies and the compounding rules for the available test methods. For example, if the Personal Identity Verification Testing (17PIV) test is elected, the Cryptographic Modules Testing (17CM), and Automated Cryptographic Validation Testing (17ACVT) become mandatory prerequisites.

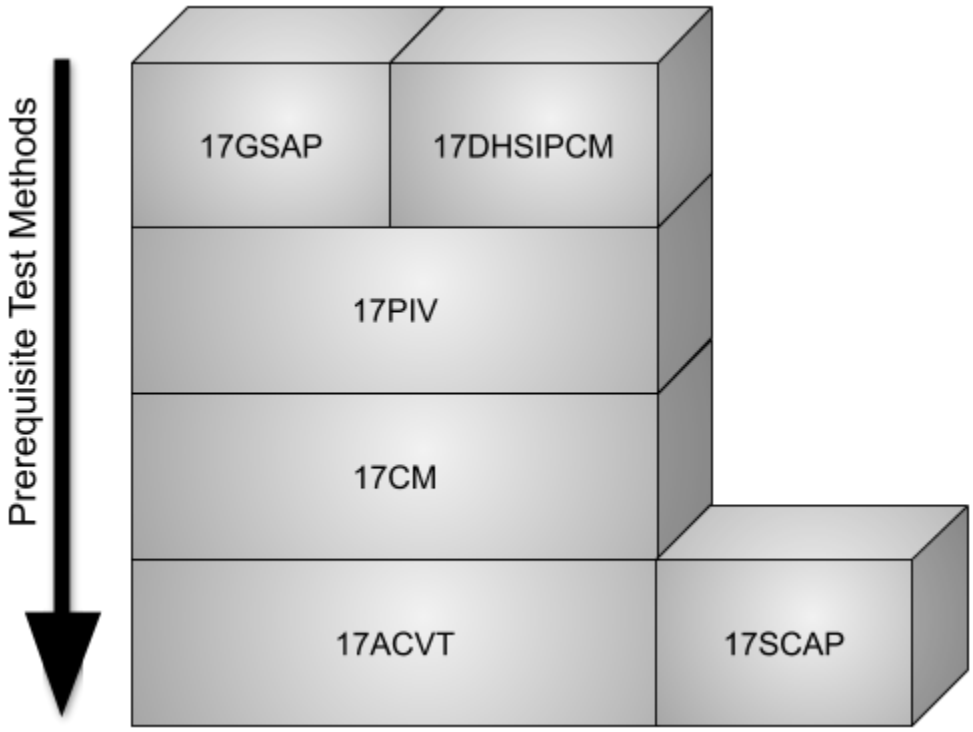

Figure A.2. CST test methods

Legend:

17ACVT	=	Automated Cryptographic Validation Testing
17CM	=	Cryptographic Modules –Testing (Security Levels 1 to 4)
17PIV	=	Personal Identity Verification Testing
17GSAP	=	GSA-Precursor Testing
17DHSIPCM	=	DHS Identity and Privilege Credential Management Testing
17SCAP	=	Security Content Automation Protocol Testing

Annex B: Cryptographic Algorithms and Cryptographic Modules Testing (normative)

B.1 Additional general information

The CAVP and the CMVP are separate, collaborative programs based on a partnership between NIST's Computer Security Division and the Canadian Centre for Cyber Security (CCCS), a division of the Communication Security Establishment (CSE). The programs provide federal agencies — in the United States and Canada — confidence that a validated cryptographic algorithm has been implemented correctly and that a validated cryptographic module meets a claimed level of security assurance. The CAVP and the CMVP validate algorithms and modules used in a wide variety of products, including secure Internet browsers, secure radios, smart cards, space-based communications, munitions, security tokens, storage devices, and products supporting Public Key Infrastructure and electronic commerce. A module may be a stand-alone product such as a VPN, smartcard, or toolkit or one module may be used in several products, so a small number of modules may be incorporated within hundreds of products. Likewise, the CAVP validates cryptographic algorithms that may be integrated in one or more cryptographic modules.

The two validation programs provide documented methodologies for conformance testing through defined sets of security requirements. Algorithm validation documentation is found at CAVP web site https://csrc.nist.gov/projects/automated-cryptographic-validation-testing. The documents are designed for each FIPS-Approved and NIST-Recommended cryptographic algorithm. For the CMVP, these security requirements are found in applicable version of FIPS 140, *Security Requirements for Cryptographic Modules* and the associated test metrics and methods in Derived Test Requirements for applicable version of FIPS 140, *Security Requirements for Cryptographic Modules*. The applicable version of FIPS 140 Annexes reference the underlying cryptographic algorithm standards or methods. Federal agencies are required to use modules that are validated as conforming to the provisions of applicable version of FIPS 140. The CMVP developed applicable version of FIPS 140 and the associated Derived Test Requirements to define the security requirements and test metrics and methods to ensure repeatability of tests and equivalency in results across the testing laboratories.

B.2 Scope of accreditation, test methods, additional references, terms, and definitions

B.2.1 Scope of accreditation

NVLAP offers laboratories a flexible, dynamic system of selecting a compound scope of accreditation under the CST LAP that best fits the laboratory's level of expertise and equipment.

The prerequisite required expertise for Cryptographic Module (17CM) test methods is Automated Cryptographic Validation Test (17ACVT).

NOTE: Firmware and hybrid modules are defined in applicable version of FIPS 140 and supporting documents.

B.2.2 Test methods

B.2.2.1 Cryptographic Modules - Modules Testing (17CM)

17CM Test methods for FIPS 140 incorporate testing for all Security Levels (1 through 4) and all Types (Software, Firmware, Hardware, and Hybrids).

B.2.2.2 Automated Cryptographic Validation Testing (17ACVT)

The 17ACVT requirements are defined in Annex G and are a prerequisite for 17CM.

B.2.3 Additional references for Cryptographic Algorithms and Cryptographic Modules Testing

B.2.3.1 FIPS 140-2 references

— Federal Information Processing Standards Publication FIPS 140-2, *Security Requirements for Cryptographic Modules*, (see https://csrc.nist.gov/publications/fips/fips140-2/fips1402.pdf)

— *Implementation Guidance for FIPS 140-1 and the Cryptographic Module Validation Program* (see https://csrc.nist.gov/groups/STM/cmvp/documents/fips140-1/FIPS1401IG.pdf)

— Annex A: Approved Security Functions for FIPS 140-2, *Security Requirements for Cryptographic Modules* (see https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf)

— Annex B: Approved Protection Profiles for FIPS 140-2, *Security Requirements for Cryptographic Modules* (see https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexb.pdf)

— Annex C: Approved Random Number Generators for FIPS 140-2, *Security Requirements for Cryptographic Modules* (see https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexc.pdf)

— Annex D: Approved Key Establishment Techniques for FIPS 140-2, *Security Requirements for Cryptographic Modules* (see https://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf)

— Derived Test Requirements (DTR) for FIPS 140-2, *Security Requirements for Cryptographic Modules* (see https://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402DTR.pdf)

— *Implementation Guidance for FIPS 140-2 and the Cryptographic Module Validation Program* (see https://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/FIPS1402IG.pdf)

— *FIPS 140-2 Cryptographic Module Validation Program Management Manual* (see https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/CMVPMM.pdf)

B.2.3.2 FIPS 140-3 references

— Federal Information Processing Standards Publication FIPS 140-3, *Security Requirements for Cryptographic Modules* (see https://doi.org/10.6028/NIST.FIPS.140-3)

— ISO/IEC 19790:2012, *Information technology — Security techniques — Security requirements for cryptographic modules* (see https://www.iso.org/standard/52906.html)

— ISO/IEC 24759:2017 *Information technology — Security techniques — Test requirements for cryptographic modules* (see https://www.iso.org/standard/72515.html)

— NIST Special Publication 800-140, *FIPS 140-3 Derived Test Requirements (DTR): CMVP Validation Authority Updates to ISO/IEC 24759* (see https://doi.org/10.6028/NIST.SP.800-140)

— NIST Special Publication 800-140 A, *CMVP Documentation Requirements: CMVP Validation Authority Updates to ISO/IEC 24759* (see https://doi.org/10.6028/NIST.SP.800-140A)

— NIST Special Publication 800-140 B, *CMVP Security Policy Requirements: CMVP Validation Authority Updates to ISO/IEC 24759 and ISO/IEC 19790 Annex B* (see https://doi.org/10.6028/NIST.SP.800-140B)

— NIST Special Publication 800-140 C, *CMVP Approved Security Functions: CMVP Validation Authority Updates to ISO/IEC 24759* (see https://doi.org/10.6028/NIST.SP.800-140C)

— NIST Special Publication 800-140 D, *CMVP Approved Sensitive Parameter Generation and Establishment Methods: CMVP Validation Authority Updates to ISO/IEC 24759* (see https://doi.org/10.6028/NIST.SP.800-140D)

— NIST Special Publication 800-140 E, *CMVP Approved Authentication Mechanisms: CMVP Validation Authority Requirements for ISO/IEC 19790 Annex E and ISO/IEC 24579 Section 6.17* (see https://doi.org/10.6028/NIST.SP.800-140E)

— NIST Special Publication 800-140 F: *CMVP Approved Non-Invasive Attack Mitigation Test Metrics: CMVP Validation Authority Updates to ISO/IEC 24759* (see https://doi.org/10.6028/NIST.SP.800-140F)

— *Implementation Guidance for FIPS 140-3 and the Cryptographic Module Validation Program* (see http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-3/FIPS1403IG.pdf)

— *FIPS 140-3 Cryptographic Module Validation Program Management Manual* (see https://csrc.nist.gov/CSRC/media/Projects/Cryptographic-Module-Validation-Program/documents/CMVPMM.pdf)

B.2.4 Additional terms and definitions

B.2.4.1
ACVTS
Automated Cryptographic Validation Testing System Tool.

B.2.4.2
CRYPTIK
Cryptographic Module Validation Requirements Test Documentation Tool.

B.2.4.3
METRIX
CMVP and CAVP Programmatic Metrics Collection Program.

B.3 Additional requirements for accreditation process

B.3.1 Additional requirements for accreditation for 17CM testing

For an applicant laboratory to qualify for any of the Cryptographic Modules Testing (17CM), the laboratory shall achieve accreditation by NVLAP in the Automated Cryptographic Validation Testing (17ACVT).

Non-commercial laboratories (i.e. labs that operate as part of a government institution) are prohibited from applying for accreditation to 17CM and those related test methods based on 17CM.

B.3.2 Additional management system evaluation activities (prior to assessment)

There are no requirements additional to those provided in clause 3.2 of this handbook.

B.3.3 Additional requirements for onsite assessment

There are no requirements additional to those provided in clause 3.3 of this handbook.

B.3.4 Additional requirements for proficiency testing

B.3.4.1 General

A proficiency testing artifact (Clause 3.1.2b) is a step in the initial accreditation process for the 17CM test method. The artifact is a cryptographic module developed by the CMVP for laboratory testing for conformance to the applicable version of FIPS 140 and supporting documents, or successors. The artifact conformance testing will demonstrate the laboratory's knowledge of the supporting standards as applied in an actual implementation, knowledge of the programmatically required test methods and metrics, and the laboratory's testing skills and use of appropriate tools.

During the testing process, the proficiency artifact will also mimic the relationship a laboratory will have with a module vendor and the CMVP in following up with questions and guidance as the proficiency artifact design and documentation may be purposely incomplete or non-compliant. All these elements are brought together with the submission of the proficiency artifact test report to the CMVP using the CRYPTIK tool. The timeframe for completion of the testing is determined by the laboratory. The laboratory test report submission shall demonstrate that the laboratory is familiar with the entire testing and reporting process.

The validation program may also use a proficiency artifact as part of the renewal process once accreditation is granted.

NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests. Repeated failures in the reports submitted to any of the validation programs may result in the laboratory's suspension or revocation of the accreditation. For more information, see clause B.3.10 of this handbook.

B.3.4.2 Additional requirements for proficiency testing for 17CM testing

B.3.4.2.1 The Cryptographic Validation Program (CVP) Certified Tester exam is an individual certification exam administered by a third-party organization. The certification exam encompasses the same domains as listed in this annex.

B.3.4.2.2 The reexamination period maintaining the certification for CVP certified testers is four-years. In the event of major program updates, such as the adoption of a new FIPS 140 standard, the reexamination frequency may be temporarily reduced to account for new technical requirements.

B.3.4.2.3 All approved signatories are required to pass the CVP certified tester exam to continue in their roles. All testing must be performed by a CVP certified tester. In the case of testing is performed by a tester-in-training, a CVP certified tester shall be present and be responsible for the results.

B.3.4.2.3.a *Initial Accreditation*: Both a CVP certified tester exam and a proficiency artifact aremandatory for the 17CM scope. The CVP certified tester exam must be passed with a score of 75% or greater.

NOTE: An onsite assessment will not be scheduled until the laboratory has a minimum of two members on staff pass the CVP certified tester exam. The proficiency artifact will be provided to the laboratory for testing at the end of the initial onsite assessment.

B.3.4.2.3.b *Renewal Accreditation*: The laboratory is required to have a minimum of two Cryptographic Validation Program (CVP) FIPS 140 Certified Testers throughout the accreditation period. The laboratory will continue to be required to notify NVLAP and CMVP of any personnel changes within thirty (30) days. Failure to communicate laboratory changes to NVLAP and CMVP may result in the suspension of accreditation.

NOTE: Passing the certification exam is the only requirement for becoming a CVP certified tester. CMVP will receive a copy of all exam results and maintain a list of CVP certified testers.

B.3.4.2.4 A proficiency artifact may be administered to a laboratory at the discretion of the validation authority to assess ongoing proficiency.

B.3.5 Additional requirements for accreditation decision for 17CM testing

B.3.5.3 Minimum number of vendor product test reports

Test report submissions are used by the validation authority as a measure to determine the laboratory's ongoing proficiency. Failure to meet the CMVP minimum requirements for report submission is grounds for suspension.

B.3.5.3.a *Initial Accreditation*: There is no requirement for a test report submission during the first year of accreditation. For all successive years of accreditation, the requirements under Renewal Accreditation apply.

B.3.5.3.b *Renewal Accreditation*: An accredited CST laboratory shall submit to the validation authority a minimum of three (3) test reports within the two-year period of the accreditation cycle. The laboratory shall submit to the validation authority a minimum of one (1) test report within each successive one-year period. A submission shall be either a Scenario 3 or a Scenario 5 as defined in the CMVP Implementation Guidance to meet this requirement.

B.3.6 Additional requirements for granting accreditation for 17CM testing

There are no requirements additional to those provided in clause 3.6 of this handbook.

B.3.7 Additional requirements for renewal of accreditation for 17CM testing

There are no requirements additional to those provided in clause 3.7 of this handbook.

B.3.8 Additional requirements for monitoring visits for 17CM testing

There are no requirements additional to those provided in clause 3.8 of this handbook.

B.3.9 Additional requirements for changes to the scope of accreditation for 17CM testing

There are no requirements additional to those provided in clause 3.9 of this handbook.

B.3.10 Additional requirements for suspension of accreditation for 17CM testing

B.3.10.1 Minimum number of Cryptographic Validation Program (CVP) FIPS 140 Certified Testers

The laboratory is required to have a minimum of two Cryptographic Validation Program (CVP) FIPS 140 Certified Testers throughout the accreditation period (See B.6.2).

B.3.10.2 Test report quality

An accredited laboratory shall maintain an Extended Cost Recovery (ECR) point total of less than 12 points during the two-year period of accreditation. If a laboratory accumulates 12 or more points during the two-year period, the accreditation for the 17CM testing will be suspended. For further details, reference the CMVP Management Manual.

B.3.11 Additional requirements for denial and revocation of accreditation for 17CM testing

There are no requirements additional to those provided in clause 3.11 of this handbook.

B.3.12 Additional requirements for voluntary termination of accreditation for 17CM testing

There are no requirements additional to those provided in clause 3.12 of this handbook.

B.3.13 Additional requirements for appeals for 17CM testing

There are no requirements additional to those provided in clause 3.13 of this handbook.

B.4 Additional general requirements for accreditation for 17CM testing

There are no requirements additional to those provided in clause 4 of this handbook.

B.5 Additional structural requirements for accreditation for 17CM testing

There are no requirements additional to those provided in clause 5 of this handbook.

B.6 Additional resource requirements for accreditation for 17CM testing

B.6.1 Additional general requirements

There are no requirements additional to those provided in clause 6.1 of this handbook.

B.6.2 Additional personnel requirements for the 17CM testing

B.6.2.1 For a laboratory to qualify for accreditation under the CST LAP, the laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that their personnel have basic knowledge of cryptographic and security practice for information systems and that the laboratory is aware of the governing standards and publications, especially the ones listed in this handbook.

Cryptographic Validation Program (CVP) certified tester exam – The test will be an individual certification exam administered by a third-party organization. The certification exam will encompass the domains listed below:

a) Physical Security
b) Authentication, Roles, Services, and Operational Environment
c) Algorithms and Self-Tests
d) Key Establishment
e) Key Management
f) Security Assurances.

NOTE: Refer to the CMVP Management Manual for additional information.

B.6.2.2 The laboratory shall continuously maintain a minimum of two CVP certified testers during the accreditation cycle for the laboratory in its entirety to be deemed proficient for the 17CM scope.

The laboratory is required to notify NVLAP and CMVP of any personnel changes within thirty (30) days. Failure to communicate laboratory changes to NVLAP and CMVP may result in an adverse action regarding accreditation. Passing the certification exam is the only requirement for becoming a CVP certified tester. CMVP will receive a copy of all exam results and maintain a list of CVP certified testers.

The reexamination period maintaining the certification for CVP certified testers is four-years. In the event of major program updates, such as the adoption of a new FIPS 140 standard, the reexamination frequency may be temporarily reduced to account for new technical requirements.

All approved signatories are required to pass the CVP certified tester exam to continue in their roles. All testing must be performed by a CVP certified tester. In the case testing is performed by a tester-in-training, a CVP certified tester shall be present and be responsible for the results.

B.6.3 Additional facilities and environmental condition requirements

B.6.3.1 General

The laboratory shall have appropriate areas, including appropriate ventilation and safety, for the use of test methods using chemical solvents and heating/cooling apparatus.

B.6.3.2 Additional facilities and environmental requirements for the 17CM testing

B.6.3.2.1 Implementations-under-test, IUT-specific documentation, IUT-specific test jigs, harnesses, supporting test apparatus, or test results shall be protected (e.g., from physical, logical, or visual access) from persons outside the laboratory, from visitors to the laboratory, from laboratory personnel without a need to know, and from other unauthorized persons.

B.6.3.2.2 The laboratory manager shall identify and document for each specific IUT the laboratory personnel who either have a need to know or have authorized access of the IUT, documentation, and testing-related apparatus including rationale for such access.

B.6.3.2.3 An audit log shall be maintained documenting personnel who have had access to each IUT during the contracted timeframe and all supporting documentation and testing related apparatus. Authorized vendor personnel for the IUT under contract may be granted access by the laboratory per the contract.

B.6.3.3 Temporary off-site locations may be used for performing physical testing (e.g., vendor sites or specialized physical testing facility such as a university lab).

B.6.3.5 Requirements for testing at permanent remote locations

Refer to section 6.3.7 of this handbook.

B.6.4 Additional equipment requirements for the 17CM testing

B.6.4.1 General

B.6.4.1.1 The laboratory applying for accreditation for the 17CM testing shall own at least one designated workstation and compatible operating system that will run the *CRYPTIK* and *METRIX* tools.

B.6.4.1.2 The designated workstation shall have internet access and e-mail capability (for report submission). Workstations shall have interfaces for loading images from a digital camera and acquiring scanned document images and/or scanning hard copy printouts. Workstations shall have enough storage capability, performance, and features as specified by the tool provider.

B.6.4.2 The laboratory shall also meet the following minimum test equipment requirements for hardware, software, and firmware components:

a) Hardware components: Security Levels 1 to 4:
   1) tools to conduct testing of tamper evidence on coatings;
   2) tools to conduct enclosure removal/penetration test;
   3) tools to conduct physical and thermal coating/potting removal/penetration tests;
   4) tools to conduct opacity and probing tests;
   5) tools to conduct tests on locks;
   6) tools to conduct mechanical/thermal/chemical tests on tamper evidence label removability;
   7) tools to test tamper detection mechanisms/switches on doors and removable covers;
   8) digital camera with flash and macro (near focus) features (phones are not acceptable);
   9) tools to conduct tests on fasteners (e.g., drills);
   10) tools to monitor/capture/exercise the data input/output of cryptographic module interfaces, at logical level (procured, rented, or leased, as needed)

b) Hardware components: Additional requirements for Security Levels 3 to 4:

   1) variable power supply;
   2) temperature chamber (procured, rented, or leased, as needed);
   3) digital storage oscilloscope or logic analyzer (procured, rented, or leased, as needed)

NOTE: Here the bandwidth will be greater than or equal to the clock frequency of the IUT. It is said that digital oscilloscopes with bandwidth of 2,5 GHz or higher have built-in preamplifiers superior to those of narrower band width. Also, high resolution (i.e. A/D conversion bits with more than 8-bit) may be used to discriminate subtle difference in information leakage, which would affect the number of waveforms required to perform side-channel analysis.

c) Hardware components: Additional requirements for Security Level 4:
   1) tools to conduct enclosure testing (e.g., drilling, milling);
   2) tools to test tamper detection envelope;
   3) solvents to conduct chemical coating removal tests

d) Software components (Security Levels 1 to 2)/Firmware components (Security Levels 1 to 4):
   1) Tools to conduct software testing - appropriate compilers, debuggers, and binary editors

e) Reporting tools:
   1) access to the Validation Program-originated *CRYPTIK* (latest version);
   2) access to the Validation Program-originated *METRIX* (latest version)

NOTE: Refer to the CMVP Management Manual for a suggested tool list.

B.6.4.3 The laboratory shall maintain a record of the tools used for each test report involving physical testing

B.6.5 Additional measurement traceability requirements for 17CM

Traceability to the requirements in the applicable version of FIPS 140 is achieved via the assertions, the associated DTRs documents, *CRYPTIK* test reporting tool, and access to ACVTS. The DTRs are divided into two sets of requirements: one levied on the vendor and one levied on the tester of the cryptographic module.

B.6.6 Additional externally provided products and services requirements for 17CM

The laboratory shall use the reporting tools (*CRYPTIK* and *METRIX*) to provide submissions and communications to the CMVP. See the CMVP Management Manual for a description and usage of these tools.

B.7 Additional process requirements for accreditation for 17CM

B.7.1 Additional requirements for requests, tenders and contracts

There are no requirements additional to those provided in clause 7.1 of this handbook.

B.7.2 Additional requirements for selection verification and validation of methods

B.7.2.1 The laboratory shall use the test methods described in the Derived Test Requirements for FIPS 140, Security Requirements for Cryptographic Modules (or successor), with clarifications provided in the Implementation Guidance for FIPS 140 and the Cryptographic Module Validation Program (or successor).

B.7.2.2 When deviations to the test methods are necessary, the validation authority (CAVP and/or CMVP) shall be informed, and details shall be described in the test report. The laboratory should submit a Request for Guidance (RFG) to document and receive official guidance from the validation programs.

B.7.2.3 When the *CRYPTIK* tool cannot support submission of the test result information, the laboratory shall provide documentation to ensure that the correct interpretation of the test assertions is maintained.

B.7.2.4 The *CRYPTIK* tool shall not be distributed, provided, or used by anyone other than laboratory personnel.

B.7.2.5 The laboratory shall use the test methods and tests for the security functions listed at the websites: http://csrc.nist.gov/groups/STM/cavp/index.html, and http://csrc.nist.gov/groups/STM/cmvp/index.html.

B.7.2.6 When testing is performed away from the main laboratory location or permanent remote locations, only the laboratory personnel shall have access to the *CRYPTIK* or *METRIX* tools supplied by the validation program.

B.7.3 Additional requirements for Sampling

There are no requirements additional to those provided in clause 7.3 of this handbook.

B.7.4 Additional requirements for handling of test items

The laboratory shall be capable of reproducing test results using a current version of the IUT.

B.7.5 Additional requirements for technical records

Validation test records shall be kept for a minimum of five years.

B.7.6 Additional requirements for the evaluation of measurement uncertainty

There are no requirements additional to those provided in clause 7.6 of this handbook.

B.7.7 Additional requirements for ensuring the validity of results

[See B.3.4]

B.7.8 Additional requirements for the reporting of results

B.7.8.1 The *CRYPTIK* tool shall be used for the 17CM test report submission.

B.7.8.2 The *METRIX* tool shall be used to submit quarterly, or as specified by the validation program, results of test statistics.

B.8 Additional management system requirements for accreditation

There are no requirements additional to those provided in clause 8 of this handbook.

Annex C: Personal Identity Verification (PIV) Testing (normative)

C.1 Additional general information

NIST established the NIST Personal Identity Verification Program (NPIVP) to validate Personal Identity Verification (PIV) components required by FIPS 201 within ITL. NVLAP accredits NPIVP laboratories for testing of PIV Card Application and PIV Middleware implementations for conformance to the NIST SP800-73, Interfaces for Personal Identity Verification, which is normatively referenced from FIPS 201. The Personal Identity Verification (PIV) objectives to validating PIV components by NPIVP are:

- to validate the conformance of two PIV components: PIV Middleware and PIV Card Application with the specifications in NIST SP 800-73-4 or successors; and
- to provide assurance that the set of PIV Middleware and PIV Card Applications that have been validated by NPIVP are interoperable.

C.2 Scope of accreditation, test methods, additional references, terms, and definitions

C.2.1 Scope of accreditation

The prerequisite required expertise for Personal Identity Verification Testing (17PIV) test methods requires selection of 17ACVT and 17CM test methods.

C.2.2 Test methods

C.2.2.1 General

For each testing program, the test methods are listed below. When a hierarchically higher test method is elected, all test methods associated with the prerequisite scopes also become mandatory.

C.2.2.2 Personal Identity Verification Testing (17PIV)

Both Cryptographic Module (17CM) and Automated Cryptographic Validation Testing (17ACVT) are prerequisites for 17PIV testing.

Further, both test methods (17PIV/01 and 17PIV/02) are required for accreditation in the PIV Testing Program.

17PIV/01 PIV Card Applications Conformance Test Suite for products meeting specifications in the FIPS 201 and NIST Special Publication 800-73 or successors.

17PIV/02 PIV Middleware Conformance Test Suite for products meeting specifications in the FIPS 201 and NIST Special Publication 800-73 or successors.

C.2.3 Additional references for the Personal Identity Verification Testing (17PIV)

C.2.3.1 Federal Information Processing Standards

— FIPS 201-2 or successors, *Personal Identity Verification of Federal Employees and Contractors*, 2013 or successor (https://doi.org/10.6028/NIST.FIPS.201-2)

C.2.3.2 NIST Special Publications (SPs) and tools for PIV

NOTE: All NIST SPs listed below are available for download at the following site: https://csrc.nist.gov/publications/sp.

— NIST SP 800-56A Rev. 2, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography, General*, NIST, April 2018 or latest (https://doi.org/10.6028/NIST.SP.800-56Ar3)

— NIST SP 800-57 Rev. 4, *Recommendation for Key Management - Part 1 General*, NIST, May 2002 or latest (https://doi.org/10.6028/NIST.SP.800-57pt1r5)

— NIST SP 800-57, *Recommendation for Key Management - Part 2, Best Practices for Key Management Organization*, NIST, May 2019 or latest (https://doi.org/10.6028/NIST.SP.800-57pt2r1)

— NIST SP 800-73 (Revision 4: 800-73-4), *Interfaces for Personal Identity Verification*, NIST, May 2015 or latest (https://dx.doi.org/10.6028/NIST.SP.800-73-4)

— NIST SP 800-76-2, *Biometric Data Specification for Personal Identity Verification*, NIST, July 2013 or latest (https://dx.doi.org/10.6028/NIST.SP.800-76-2)

— NIST SP 800-78-4 or successors, *Cryptographic Algorithms and Key Sizes for Personal Identity Verification*, NIST, May 2015 or latest (https://dx.doi.org/10.6028/NIST.SP.800-78-4)

— NIST SP 800-79-2, *Guidelines for the Accreditation of Personal Identity Verification Card Issuers*, NIST, July 2015 or latest (https://dx.doi.org/10.6028/NIST.SP.800-79-2)

— NIST SP 800-85A-4, *PIV Card Application and Middleware Interface Test Guidelines*, NIST, April 2016 or latest (https://dx.doi.org/10.6028/NIST.SP.800-85A-4)

— NIST SP 800-96, or successor, *PIV Card to Reader Interoperability Guidelines*, NIST, September 2006 or latest (https://dx.doi.org/10.6028/NIST.SP.800-96)

— PIV Card Application and Middleware Test Runner for NPIVP (https://csrc.nist.gov/projects/nist-personal-identity-verification-program/software-downloads)

C.2.3.3 ISO/IEC standards for the PIV testing

— ISO/IEC 7810

— ISO/IEC 7816

— ISO/IEC 14443

C.2.4 Additional terms and definitions

There are no additional terms and definitions to those provided in Section 1.5 of this handbook.

C.3 Additional accreditation process requirements for the PIV testing

C.3.1 Additional application requirements

All laboratories applying for accreditation in the test methods associated with 17PIV testing shall be based in North America. The cryptographic modules in the PIV systems (both on-card and issuer software) are required to be validated to the applicable version of FIPS 140 with an overall Security Level 2 (or higher) while the cryptographic module on the PIV card is required to provide physical Security Level 3 to protect the PIV private keys in storage.

As such, for an applicant laboratory to qualify for any of the Personal Identification Verification testing, the laboratory shall achieve accreditation by NVLAP in the Automated Cryptographic Validation Testing (17ACVT), Cryptographic Module Testing (17CM).

Further, the applicant laboratory cannot choose only one (17PIV/01 or 17PIV/02) test method. Both test methods must be elected to qualify for 17 PIV testing.

C.3.2 Additional management system evaluation activities (prior to assessment)

There are no requirements additional to those provided in clause 3.2 of this handbook.

C.3.3 Additional requirements for onsite assessment

There are no requirements additional to those provided in clause 3.3 of this handbook.

C.3.4 Additional requirements for proficiency testing

C.3.4.1 *Initial Accreditation*: Proficiency testing for the 17PIV tests will require proof of the laboratory's ability to handle the *PIV Card Application* and *PIV Middleware* (NIST SP 800-85A) test tools, provided by NIST/ITL or NVLAP. The laboratory shall demonstrate that all appropriate personnel are familiar withthe tools, can configure the tools, can run the conformance tests, can verify the results, and can generate the report.

C.3.4.2 *Renewal of Accreditation*: NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests. Unsatisfactory performance in proficiency testing or substantial errors in the reports submitted to any of the validation programs may result in suspension or revocation of accreditation. For more information, see clause 3.10.

C.3.5 Additional requirements for accreditation decisions for 17PIV testing

There are no requirements additional to those provided in clause 3.5 of this handbook.

C.3.6 Additional requirements for granting accreditation for 17PIV testing

There are no requirements additional to those provided in clause 3.6 of this handbook.

C.3.7 Additional requirements for renewal of accreditation for 17PIV testing

There are no requirements additional to those provided in clause 3.7 of this handbook.

C.3.8 Additional requirements for monitoring visits for 17PIV testing

There are no requirements additional to those provided in clause 3.8 of this handbook.

C.3.9 Additional requirements for changes to the scope of accreditation for 17PIV testing

There are no requirements additional to those provided in clause 3.9 of this handbook.

C.3.10 Additional requirements for suspension of accreditation for the 17PIV testing

There are no requirements additional to those provided in clause 3.10 of this handbook.

C.3.11 Additional requirements for denial and revocation of accreditation for 17PIV testing

There are no requirements additional to those provided in clause 3.11 of this handbook.

C.3.12 Additional requirements for voluntary termination of accreditation for 17PIV testing

There are no requirements additional to those provided in clause 3.12 of this handbook.

C.3.13 Additional requirements for appeals for 17PIV testing

There are no requirements additional to those provided in clause 3.13 of this handbook.

C.4 Additional general requirements for accreditation in 17PIV testing

There are no requirements additional to those provided in clause 4 of this handbook.

C.5 Additional structural requirements for accreditation in 17PIV testing

There are no requirements additional to those provided in clause 5 of this handbook.

C.6 Additional resource requirements for accreditation in 17PIV testing

C.6.1 General

There are no requirements additional to those provided in Section 6.1 of this handbook.

C.6.2 Additional personnel requirements

C.6.2.1 The laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that their personnel have basic knowledge of cryptographic and security practice for

information systems and that the laboratory is aware of the governing standards and publications, especially the ones listed in this handbook.

C.6.2.2 The laboratory's personnel shall have experience, training, or familiarity in the areas of:

a) cryptography - symmetric versus asymmetric algorithms and uses;
b) cryptography - encryption protocols and implementations;
c) key management techniques and concepts;
d) the families of cryptographic algorithms;
e) FIPS-approved and NIST-recommended security functions (applicable version of FIPS 140);
f) cryptography - Public Key Infrastructure (PKI);
g) access control security models;
h) smart cards;
i) smart card readers (contact and contactless);
j) Application Protocol Data Unit (APDU);
k) Basic Encoding Rules (BER);
l) biometric authentication techniques;
m) concepts of the operational PIV systems; and
n) contact and contactless interface standards.

C.6.3 Additional requirements for the review of request, tenders, and contracts

There are no requirements additional to those provided in Section 6.3 of this handbook.

C.6.4 Additional equipment requirements

C.6.4.1 The laboratory shall own at least one designated compatible PC equipped with, at minimum, a compact disk rewritable (CD-RW) drive or other secure digital storage media and running Microsoft Windows 10[1] (or later) or compatible.

C.6.4.2 The laboratory shall also meet the following minimum hardware, software, and operating system requirements for the platform on which the *PIV Card Application* and *PIV Middleware* tools (also known as *PIV Test Runner*) will run:

a) Hardware:

1) a test computer running Windows 10 or later and with at least 4 MB of available space on the hard disk;
2) contact and contactless smart card reader or a dual interface reader;
3) a dual interface FIPS 201 conformant PIV card loaded with SP 800-73 conformant PIV card application; and

[1] Certain commercial entities, equipment, or materials may be identified in this document to describe a requirement adequately. Such identification is not intended to imply recommendation or endorsement by NIST.

b) Software:

1) Oracle Java Runtime Environment (JRE) version 1.8 or later; and
2) *PIV Card Application* and *PIV Middleware* test toolkit application software provided by NIST/ITL or NVLAP (version 5.0.1 or later).

C.7 Additional process requirements for accreditation for the 17 PIV testing

C.7.1 Additional requirements for review of requests tenders and contracts

There are no requirements additional to those provided in clause 7.1 of this handbook.

C.7.2 Additional requirements for the selection, verification, and validation

C.7.2.1 The laboratory shall use the test methods and tests listed in the NIST SP 800-85A-4: *PIV Card Application and Middleware Interface Test Guidelines* (or latest) for conformance testing of the PIV card application and PIV middleware. For additional clarifications, check the documentation listed on the NPIVP website: https://csrc.nist.gov/groups/SNS/piv/index.html.

C.7.2.2 FIPS 201 Appendix B.3 specifies that a PIV system/component is "FIPS 201-compliant" after each of IUT's constituent parts have met individual validation requirements. For a PIV card, the constituent parts requiring validation include:

- PIV card application validation for conformance to NIST SP 800-73-4 (or latest) through NPIVP; and
- cryptographic module validation for applicable version of FIPS 140, *Security Requirements for Cryptographic Modules* (or latest) conformance of the cryptographic module that hosts the PIV card application.

C.7.3 Additional requirements for sampling

There are no requirements additional to those provided in clause 7.3 of this handbook.

C.7.4 Additional requirements for handling of test items

There are no requirements additional to those provided in clause 7.4 of this handbook.

C.7.5 Additional requirements for technical records

There are no requirements additional to those provided in clause 7.5 of this handbook.

C.7.6 Additional requirements for the evaluation of measurement uncertainty

There are no requirements additional to those provided in clause 7.6 of this handbook.

C.7.7 Additional requirements for ensuring the validity of results

[See C.3.4]

C.7.8 Additional requirements for the reporting of results

There are no requirements additional to those provided in clause 7.8 of this handbook.

C.8 Additional management system requirements for accreditation

There are no requirements additional to those provided in clause 8 of this handbook

Annex D: General Services Administration Precursor (GSAP) Testing (normative)

D.1 Additional general information

The FIPS 201 Evaluation Program (EP) is a U.S. Government entity administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency. The goal of the FIPS 201 Evaluation Program (EP) is to evaluate products and services against the requirements outlined in FIPS 201 and its supporting documents. In addition to derived test requirements developed to test conformance to the National Institute of Standards and Technology (NIST) standard, GSA has also established interoperability and performance metrics to further determine product suitability. To facilitate testing of these requirements, the EP has developed a set of approval and test procedures for 33 Product Categories, which outline the evaluation criteria, approval mechanisms, and test process employed by the laboratory during its evaluation of a supplier's product or service against the requirements for that category. The EP Laboratories (EPLs) utilize these approval procedures and test procedures to test Products for FIPS 201 conformance.

D.2 Scope of accreditation, test methods, additional references, terms, and definitions

D.2.1 Scope of accreditation

NVLAP offers all interested laboratories a flexible, dynamic system of selecting a compound scope of accreditation under the CST LAP that best fits the laboratory's level of expertise and equipment.

The prerequisite expertise for General Services Administration Precursor (17GSAP) test methods also requires selection of the 17PIV test methods.

D.2.2 Test methods

D.2.2.1 General

For each testing program, the test methods are listed below. When a hierarchically higher test method is elected, all test methods associated with the prerequisite scopes also become mandatory.

D.2.2.2 General Services Administration Precursor Testing (17GSAP)

17GSAP/01 FIPS 201 Evaluation Program – Electromagnetically Opaque Sleeve

17GSAP/02 FIPS 201 Evaluation Program – Electronic Personalization

17GSAP/03 FIPS 201 Evaluation Program – PIV Card

17GSAP/04 FIPS 201 Evaluation Program – PIV Card Reader - Authentication Key

17GSAP/05 FIPS 201 Evaluation Program – PIV Card Reader - Biometric

17GSAP/06 FIPS 201 Evaluation Program – PIV Card Reader - CHUID (Contact)

17GSAP/07 FIPS 201 Evaluation Program – PIV Card Reader - CHUID (Contactless)

17GSAP/08 FIPS 201 Evaluation Program – PIV Card Reader - Transparent

17GSAP/09 FIPS 201 Evaluation Program – Template Generator

17GSAP/10 FIPS 201 Evaluation Program – Card Printer Station

17GSAP/11 FIPS 201 Evaluation Program – PIV Card Reader - CHUID Authentication (Contact)

17GSAP/12 FIPS 201 Evaluation Program – PIV Card Reader - CHUID Authentication (Contactless)

17GSAP/13 FIPS 201 Evaluation Program – Graphical Personalization

17GSAP/14 FIPS 201 Evaluation Program – Facial Image Capturing Camera

17GSAP/15 FIPS 201 Evaluation Program – Biometric Authentication System

17GSAP/16 FIPS 201 Evaluation Program – CAK Authentication System

17GSAP/17 FIPS 201 Evaluation Program – Certificate Validator

17GSAP/18 FIPS 201 Evaluation Program – Certificate Validator (without authentication)

17GSAP/19 FIPS 201 Evaluation Program – Card Reader – Biometric Authentication

17GSAP/20 FIPS 201 Evaluation Program – CHUID Authentication System

17GSAP/21 FIPS 201 Evaluation Program – Facial Image Capturing (Middleware)

17GSAP/22 FIPS 201 Evaluation Program – PIV Authentication System

17GSAP/23 FIPS 201 Evaluation Program – SCVP Client

17GSAP/24 FIPS 201 Evaluation Program – SCVP Client (without authentication)

D.2.3 Additional references for General Services Administration Precursor testing (17GSAP)

— HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004 (http://www.dhs.gov/xabout/laws/gc_1217616624097.shtm)

— NIST SP 800-85B, *PIV Data Model Test Guidelines*, NIST, September 2009 (http://csrc.nist.gov/publications/drafts/800-85B-1/draft-sp800-85B-1.pdf)

— FIPS 201 Evaluation Program – Authentication Key Reader Test Procedure, v 4.0.0.0 or later

— FIPS 201 Evaluation Program – Biometric Reader Test Procedure, v 4.0.0 or later

— FIPS 201 Evaluation Program – CHUID Reader (Contact) Test Procedure, v 4.0.0 or later

— FIPS 201 Evaluation Program – CHUID Reader (Contactless) Test Procedure, v 4.0.0 or later

— FIPS 201 Evaluation Program – CHUID Authentication Reader (Contact) Test Procedure, v 2.0.0 or later

— FIPS 201 Evaluation Program – CHUID Authentication Reader (Contactless) Test Procedure, v 2.0.0 or later

— FIPS 201 Evaluation Program – Electromagnetically Opaque Sleeve Test Procedure, v 3.0.0 or later

— FIPS 201 Evaluation Program – Electronic Personalization Test Procedure, v 5.0.0 or later

— FIPS 201 Evaluation Program – PIV Card Test Procedure, v 3.0.0 or later

— FIPS 201 Evaluation Program – Template Generator Test Procedure, v 2.0.0 or later

— FIPS 201 Evaluation Program – Transparent Card Reader Test Procedure, v 5.0.0 or later

— FIPS 201 Evaluation Program – Graphical Personalization Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – Facial Image Capturing Camera Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – Card Printer Station Test Procedure, v 2.0.0 or later

— FIPS 201 Evaluation Program – Biometric Authentication System Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – CAK Authentication System Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – Certificate Validator Test Procedure, v 3.0.0 or later

— FIPS 201 Evaluation Program – Certificate Validator (without authentication) Test Procedure, v 2.0.0 or later

— FIPS 201 Evaluation Program – Biometric Authentication Card Reader Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – CHUID Authentication System Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – Facial Image Capturing Middleware Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – PIV Authentication System Test Procedure, v 1.0.0 or later

— FIPS 201 Evaluation Program – SCVP Client Test Procedure, v 2.0.0 or later

— FIPS 201 Evaluation Program – SCVP Client (without authentication) Test Procedure, v 1.0.0 or later

NOTE: The most current version of the documents listed above can be downloaded from the GSA's website: http://fips201ep.cio.gov/ (click on the "Test Procedures" link).

D.2.4 Additional terms and definitions

D.2.4.1
GSA FIPS 201 EP

U.S. Government entity responsible for ensuring that products are validated against FIPS 201 and its supporting requirements. The EP is administered by the Office of Government-wide Policy (OGP), within the General Services Administration (GSA) agency.

D.2.4.2
EP Laboratories (EPLs)

Accredited laboratories that are authorized to perform FIPS 201 conformance testing on products submitted by vendors. The EPLs perform testing in accordance with GSA FIPS 201 EP approval procedures and test procedures.

D.2.4.3
Approved FIPS 201 Products and Services List (APL)

A list of qualified products that have been validated for FIPS-201 conformance.

D.2.4.4
Removed Products List (RPL)

A list of products that are no longer conformant with requirements specified in the FIPS 201 and its supporting documents. When APL products become non-conformant, they are placed on the RPL.

D.2.4.5
Central Certificate Validator (CCV)

A free service hosted by GSA that can be used to determine if a presented identity credential (PKI certificate) is valid, i.e., was legitimately issued and has not expired or been terminated. The CCV uses the processes of path discovery and path validation to verify the binding between the subject identifier and the subject public key in the certificate.

D.3 Additional accreditation process requirements

D.3.1 Additional accreditation requirements for the 17GSAP testing

For a laboratory to qualify as a General Services Administration (GSA) FIPS 201 Evaluation Laboratory, the laboratory shall achieve accreditation by NVLAP in the GSA FIPS 201 test methods (17GSAP), including all 17GSAP/xx test methods listed herein, or the updated list from the CST LAP website. Before the laboratory qualifies to apply to GSA as a GSA FIPS 201 Evaluation Program laboratory (GSA EP), the laboratory shall prove to GSA that the laboratory can perform all evaluations for all FIPS 201 categories of products and services, not just the test methods for which NVLAP accredits. The laboratory shall also satisfy other technical and business requirements as specified by GSA.

All laboratories applying for the 17GSAP testing shall:

- first, achieve accreditation by NVLAP as an Automated Cryptographic Validation Testing Laboratory in the 17ACVT test method;
- second, achieve accreditation by NVLAP for Cryptographic Module (17CM) test method;
- third, achieve accreditation by NVLAP (as a NPIVP Testing Laboratory) in both 17PIV/01 and 17PIV/02 test methods.

D.3.2 Additional management system evaluation activities (prior to assessment) for 17GSAP testing

There are no requirements additional to those provided in clause 3.2 of this handbook.

D.3.3 Additional onsite assessment requirements for the 17GSAP testing

There are no requirements additional to those provided in clause 3.3 of this handbook.

D.3.4 Additional proficiency testing requirements for the 17GSAP testing

D.3.4.1 NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests. Unsatisfactory performance in proficiency testing or substantial errors in the reports submitted to any of the validation programs may result in suspension or revocation of accreditation. For more information, see clause 3.10.

D.3.4.2 Proficiency testing for the 17GSAP tests will require proof of the laboratory's competence to set up and configure a testing hardware and software environment as instructed in the test, to use a PIV card(s) (with T=0 and/or T=1 protocols) and a PIV card reader, to perform all the operations instructed in the test (e.g., electronically personalize the card(s), generate key pair(s), generate and load personalized data objects, authenticate the card holder), and to run the tests as instructed.

D.3.5 Additional requirements of Accreditation Decision for the 17GSAP testing

There are no requirements additional to those provided in clause 3.3 of this handbook.

D.3.6 Additional granting accreditation requirements for the 17GSAP testing

There are no requirements additional to those provided in clause 3.3 of this handbook.

D.3.7 Additional renewal of accreditation requirements for the 17GSAP testing

There are no requirements additional to those provided in clause 3.3 of this handbook.

D.3.8 Additional monitoring visits requirements for the 17GSAP testing

There are no requirements additional to those provided in clause 3.3 of this handbook.

D.3.9 Additional requirements for changes to the scope of accreditation for the 17GSAP testing

There are no requirements additional to those provided in clause 3.3 of this handbook.

D.3.10 Additional suspension of accreditation for the 17GSAP testing

D.4 Additional general requirements for accreditation

There are no requirements additional to those provided in clause 4 of this handbook.

D.5 Additional structural requirements for accreditation

There are no requirements additional to those provided in clause 5 of this handbook.

D.6 Additional resource requirements for accreditation

D.6.1 General

There are no requirements additional to those provided in Section 6.1 of this handbook.

D.6.2 Additional personnel requirements for the 17GSAP testing

D.6.2.1 The laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that their personnel have basic knowledge of cryptographic and security practice for information systems and that the laboratory is aware of the governing standards and publications, especially the ones listed in this handbook.

D.6.2.2 Prior to accreditation, the laboratory's personnel shall have experience, training, or familiarity in the areas of:

a) cryptography - symmetric versus asymmetric algorithms and uses;

b) cryptography - encryption protocols and implementations;

c) key management techniques and concepts;

d) cryptographic self-test techniques;

e) the families of cryptographic algorithms;

f) FIPS-approved and NIST-recommended security functions (applicable version of FIPS 140);

g) cryptography - Public Key Infrastructure (PKI);

h) access control security models;

i) smart cards;

j) smart card readers (contact and contactless);

k) Application Protocol Data Unit (APDU);

l) Basic Encoding Rules (BER);

m) biometric authentication techniques;

n) concepts of the operational PIV systems;

o) contact and contactless interface standards; and

p) Server-Based Certificate Validation Protocol (SCVP).

D.6.3 Additional facilities and environmental condition requirements for the 17GSAP testing

The laboratory shall have appropriate areas, including appropriate ventilation and safety, for the use of test methods using chemical solvents and heating/cooling apparatus.

D.6.4 Additional equipment requirement for the 17GSAP testing

Supplemental to the additional equipment requirements listed for 17PIV testing (section C.5.5.2), the laboratory shall also meet the following minimum hardware, software, and operating system requirements

for any platform on which the *PIV Data Model Tester* (SP800-85B) and the *Test Fixture Software* tools required for GSAP testing will run:

a) Hardware:

1) at least 1 USB and 1 serial port available on the Windows XP test computer;
2) Golden Contact PIV Card Reader - Gemalto GemPC twin USB HW111459A[2];
3) Breakout Box - For connecting physical access readers - for additional information see GSA Laboratory Specification, section 3.3.4.3 - latest version from http://fips201ep.cio.gov/. The USB and serial communication cables from the breakout box will be connected to the IBM-compatible PC system;
4) 22 AWG Wire - category 5 or similar Ethernet; and
5) tools needed for the breakout box:
   - drill;
   - screwdriver;
   - glue.

b) Software:

1) BouncyCastle crypto provider, version 1.32 (bcprov-jdk15-132.jar) - available from http://www.bouncycastle.org/download/bcprov-jdk15-132.jar;
2) BouncyCastle mail utilities, version 1.32 (bcmail-jdk15-132.jar) - available from http://www.bouncycastle.org/download/bcmail-jdk15-132.jar;
3) Crypto++ DLL version 5.2.3 - available from http://www.cryptopp.com;
4) *PIV Test Data Software* (which includes the *JPIV Test Data Generator* jar file and the *PIV Data Loader* executable) provided by NIST/ITL website, http://csrc.nist.gov/piv-program - latest release available;
5) unless otherwise specified by NVLAP on the CST LAP website, a *Gemplus GemPIV applet* v1.01 on Gemplus GemCombi Xpresso R4 E72K Smart Card (to be used when a "Golden Class A PIV Card" (PIVcard-ClassA) or "Golden T=0 PIV Card" or "PIVcard-T0" will be referred);
6) unless otherwise specified by NVLAP on the CST LAP website, a *PIV EP v.108 Java Card Applet* on Oberthur ID-One Cosmo v5 64K Smart Card - to be used when a "Golden T=1 PIV Card" or "PIVcard-T1" will be referred;
7) card reader driver provided by the manufacturer;
8) SP 800-85B Data Conformance Test Tool v6.2.0 - Used to test data model conformance for a populated PIV Card. Available from http://fips201ep.cio.gov/tools.php;
9) Cardholder Facial Image Test Tool v1.0.1 – used to test the conformance of the PIV Facial Image to the specifications of SP 800-76-1 and INCITS 385. Available from http://fips201ep.cio.gov/tools.php;
10) SCVP Client Test Tool v2.0.0 – A client application that interacts (using the RFC 5055 as the protocol) with the GSA Central Certificate Validator (CCV) service in order to determine validity for any given PIV Certificate using PKI-based path discovery and validation. Available from http://fips201ep.cio.gov/tools.php;
11) Data Populator Tool v2.3.0 - Used to randomly generate conformant data and load them on the PIV Card. Available from http://fips201ep.cio.gov/tools.php.

D.6.5 Additional requirements measurement traceability for the 17GSAP testing

[2] Certain commercial entities, equipment, or materials may be identified in this document to describe a requirement adequately. Such identification is not intended to imply recommendation or endorsement by NIST.

There are no requirements additional to those provided in clause 6.5 of this handbook.

D.6.6 Additional requirements for externally provided products and services for 17GSAP testing

There are no requirements additional to those provided in clause 6.6 of this handbook.

D.7 Additional process requirements for accreditation

D.7.1 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.1 of this handbook.

D.7.2 Additional requirements for the selection, verification, and validation of methods for 17GSAP testing

D7.2.1 The laboratory shall use the test methods listed at the website http://fips201ep.cio.gov/contact.php under the "Test Procedures."

D.7.2.2 Prior to testing the IUT, the laboratory shall inventory all the equipment received and tag all systems.

D.7.2.3 The IUT shall be NPIVP-certified before being considered for the GSA EP conformance testing, as the NPIVP is a prerequisite to the GSAP program.

D.7.2.4 During the conformance testing, the laboratory shall use and complete the following documentation:

a) Approval Procedure;
b) Test Procedures; and
c) Evaluation Report.

NOTE: The core function of a GSAP laboratory is to analyze and evaluate the IUT for conformance with FIPS 201 specifications. Based on the laboratory evaluation results, an authorized GSA official, the Approval Authority, makes the final determination as to whether the IUT should be approved.

D.7.3 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.3 of this handbook.

D.7.4 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.4 of this handbook.

D.7.5 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.5 of this handbook.

D.7.6 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.6 of this handbook.

D.7.7 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.7 of this handbook.

D.7.8 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.8 of this handbook.

D.7.9 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.9 of this handbook.

D.7.10 Additional requirements for review of requests, tenders and contracts for 17GSAP testing

There are no requirements additional to those provided in clause 7.10 of this handbook.

D.8 Additional management system requirements for accreditation

There are no requirements additional to those provided in Section 6.1 of this handbook.

Annex E: Security Content Automation Protocol Testing (SCAP) (normative)

E.1 Additional general information for Security Content Automation Protocol Testing (17SCAP)

Please see E.2.3 for references to additional information regarding SCAP.

E.2 Scope of accreditation, test methods, additional references, terms, and definitions

E.2.1 Scope of accreditation

NVLAP offers all interested laboratories a flexible, dynamic system of selecting a compound scope of accreditation under the CST LAP that best fits the laboratory's level of expertise and equipment.

E.2.2 Test methods

For each testing program, the test methods are listed below. When a hierarchically higher test method is elected, all test methods associated with the prerequisite scopes also become mandatory.

The SCAP testing is comprised of testing for the 12 component specifications within SCAP, and the SCAP protocol (17SCAP/13), which covers the interaction of the component specifications.

17SCAP/01 eXtensible Configuration Checklist Description Format (XCCDF)

17SCAP/02 Open Vulnerability and Assessment Language (OVAL)

17SCAP/03 Open Checklist Interactive Language (OCIL)

17SCAP/04 Common Vulnerabilities and Exposures (CVE)

17SCAP/05 Common Configuration Enumeration (CCE)

17SCAP/06 Common Platform Enumeration (CPE)

17SCAP/07 Software Identification (SWID)

17SCAP/08 Common Configuration Scoring System (CCSS)

17SCAP/09 Common Vulnerability Scoring System (CVSS)

17SCAP/10 Asset Identification

17SCAP/11 Asset Reporting Format (ARF)

17SCAP/12 Trust Model for Security Automation Data (TMSAD)

17SCAP/13 Security Content Automation Protocol (SCAP)

E.2.3 Additional references for the Security Content Automation Protocol testing (17SCAP)

E.2.3.1 NIST Special Publications (SP) for SCAP

— NIST SP 800-126, *The Technical Specification for the Security Content Automation Protocol* (see http://csrc.nist.gov/publications/PubsSPs.html)

— NIST SP 800-117, *Guide to Adopting and Using the Security Content Automation Protocol (SCAP)* (see http://csrc.nist.gov/publications/PubsSPs.html)

— NIST SP 800-40, *Creating a Patch and Vulnerability Management Program*, version 2 or later (see http://csrc.nist.gov/publications/PubsSPs.html)

— NIST SP 800-100, *Information Security Handbook: A Guide for Managers* (see http://csrc.nist.gov/publications/PubsSPs.html)

E.2.3.2 Other references for SCAP

For the latest versions, see https://scap.nist.gov, unless otherwise noted.

— NIST IR 7511, Security Content Automation Protocol (SCAP) Validation Program Derived Test Requirements

— Security Content Automation Protocol (SCAP) Validation Program Implementation Guide (contact scap@nist.gov for latest version)

— NIST IR 7275, Specification for the Extensible Configuration Checklist Description Format (XCCDF)

— Open Vulnerability Assessment Language (OVAL)

— NIST IR 7692, Open Checklist Interactive Language (OCIL)

— Common Vulnerabilities and Exposures (CVE)

— Common Configuration Enumeration (CCE)

— NIST IR 7695, NIST IR 7696, NIST IR 7697, NIST IR 7698, Common Platform Enumeration (CPE)

— NIST IR 8060, Software Identification (SWID)

— NIST IR 7502, The Common Configuration Scoring System (CCSS)

— NIST IR 7435, The Common Vulnerability Scoring System (CVSS)

— NIST IR 7693, Asset Identification

— NIST IR 7694, Asset Report Format (ARF)

— NIST IR 7802, Trust Model for Security Automation Data

E.2.4 Additional terms and definitions

E.2.4.1
Asset Identification
Provides constructs to uniquely identify assets based on known identifiers and/or known information about the assets. This specification describes the purpose of asset identification, a data model for identifying assets, methods for identifying assets, and guidance on how to use asset identification.

E.2.4.2
Asset Reporting Format (ARF)
A data model for expressing the transport format of information about assets, and the relationships between assets and reports.

E.2.4.3
Common Configuration Enumeration (CCE)
Provides unique identifiers to system configuration issues to facilitate correlation of configuration data across multiple information sources and tools.

E.2.4.4
Common Platform Enumeration (CPE)
A structured naming scheme for information technology systems, platforms, and packages.

E.2.4.5
Software Identification (SWID) Tags
A format for representing software identifiers and associated metadata.

E.2.4.6
Common Vulnerabilities and Exposures (CVE)
A dictionary of publicly known information security vulnerabilities and exposures.

E.2.4.7
Common Configuration Scoring System (CCSS)
A system to provide a standardized method for measuring the severity of software security configuration issues.

E.2.4.8
Common Vulnerability Scoring System (CVSS)
A system to provide a standardized method for measuring the impact of the IT vulnerabilities.

E.2.4.9
Open Checklist Interactive Language (OCIL)
A specification for expressing a set of questions to be presented to a user and corresponding procedures to interpret responses to these questions.

E.2.4.10
Open Vulnerability Assessment Language (OVAL)
An information security community standard that facilitates measuring a machine state, and is often used for vulnerability, configuration and patch checking.

E.2.4.11
Trust Model for Security Automation Data (TMSAD)
A data model for establishing trust for security automation data.

E.2.4.12
eXtensible Configuration Checklist Document Format (XCCDF)
A specification language for writing security checklists, benchmarks, and related documents. An XCCDF document represents a structured collection of security configuration rules for one or more applications and/or systems.

E.3 Additional accreditation process requirements

E.3.1 Additional accreditation requirements

There are no requirements additional to those provided in clause 3.1 of this handbook.

E.3.2 Additional activities prior to an onsite assessment

There are no requirements additional to those provided in clause 3.2 of this handbook.

E.3.3 Additional onsite assessment requirements

There are no requirements additional to those provided in clause 3.3 of this handbook.

E.3.4 Additional proficiency testing requirements

E.3.4.1 *Initial Accreditation*: Proficiency testing for the 17SCAP tests require proof of the laboratory's competence to set up and configure a testing environment as instructed in the test. Using a sample artifact provided by NIST/ITL, the laboratory shall determine which test requirements are appropriate for the provided artifact, conduct the test procedures associated with those requirements, verify the results, and generate a report indicating the proposed validation status of the artifact.

E.3.4.2 *Renewal of Accreditation*: NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests. Unsatisfactory performance in proficiency testing or substantial errors in the reports submitted to any of the validation programs may result in suspension or revocation of accreditation. For more information, see clause 3.10.

E.4 Additional general requirements for accreditation for SCAP testing

There are no requirements additional to those provided in clause 4 of this handbook.

E.5 Additional structural requirements for accreditation for SCAP testing

There are no requirements additional to those provided in clause 5 of this handbook.

E.6 Additional resource requirements for accreditation for the Security Content Automation Protocol testing (17SCAP)

E.6.1 General

There are no requirements additional to those provided in Section 5.1 of this handbook.

E.6.2 Additional personnel requirements

E.6.2.1 The laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that personnel have basic knowledge of cryptographic and security practice for information systems and that the laboratory is aware of the governing standards and publications, especially the ones listed in this handbook.

E.6.2.2 The laboratory personnel shall have experience, training, basic knowledge, or familiarity in:

a) vulnerability and configuration management (NIST SP 800-40 v2 or later and NIST SP 800-100);

b) XML and how to read XML documents (W3C Extensible Markup Language (XML) 1.1 (Second Edition) or later);

c) all SCAP specifications (XCCDF, OVAL, OCIL, CVE, CCE, CPE, SWID, CCSS, CVSS, Asset Identification, ARF, and TMSAD, including NIST SP 800-126) – latest versions (for more information, see https://scap.nist.gov); and

d) the installation and configuration of operating systems or platforms (e.g., Microsoft Windows, Red Hat Linux, Apple MacOS) listed on the https://scap.nist.gov/validation/ page.

E.6.3 Additional facilities and environmental conditions requirements

There are no additional requirements.

E.6.4 Additional equipment requirements

The laboratory shall be equipped with the following minimum hardware, software, and operating system requirements:

1) Hardware:

   Any IT system capable of properly executing the operating systems supported by the validation program, and a domain controller such as Windows Server.
   a) This can be a real system or supported through virtualization architecture.
   b) Must be capable of executing the product under test as indicated by the documentation accompanying the product or as otherwise specified by the vendor of the product.

2) Software:[3]

a) Microsoft Windows running on the IT system.
   i) The operating system must be configured according to the configuration requirements in the Implementation Guide.
   ii) The OS must have Internet Explorer and\or Microsoft Edge installed according to the requirements specified in the Implementation Guide.
   iii) The OS must be able to be joined to a test domain.

b) Red Hat Enterprise Linux running on the IT system.

   The operating system must be configured according to the configuration requirements in the Implementation Guide.

c) Apple Mac OS running on the IT system.

   The operating system must be configured according to the configuration requirements in the Implementation Guide.

d) XML schema validation tool. The tester must be able to perform XML schema validation against XML results produced by the product under test. The tool must be able to reference NIST provided schemas.

e) Access to the National Vulnerability Database located at https://nvd.nist.gov.

f) Access to the SCAP Validation Program Publications and Resources located at https://scap.nist.gov/validation

E.6.5 Additional requirements for measurement traceability

There are no requirements additional to those provided in clause 6.5 of this handbook.

E.6.6 Additional requirements for externally provided products and services

There are no requirements additional to those provided in clause 6.6 of this handbook.

E.7 Additional process requirements for accreditation for the Security Content Automation Protocol testing (17SCAP)

There are no requirements additional to those provided in clause 7 of this handbook.

[3] Certain commercial entities, equipment, or materials may be identified in this document to describe a requirement adequately. Such identification is not intended to imply recommendation or endorsement by NIST.

E.8 Additional management system requirements for accreditation for the Security Content Automation Protocol testing (17SCAP)

There are no requirements additional to those provided in clause 8 of this handbook.

Annex F: DHS Identity and Privilege Credential Management Testing (normative)

F.1 Additional general information

The United States Congress mandated the Transportation Worker Identification Credential (TWIC) in the Maritime Transportation Security Act of 2002 (MTSA) as amended by the Security and Accountability for Every Port Act of 2006 (SAFE Port Act). The mission is to design and field a common credential for all transportation workers requiring unescorted physical and logical access to secure areas of the nation's transportation system and their associated information systems. Under such a program, a credential (referred to as "TWIC Card") is issued to maritime workers requiring unescorted access to secure areas ofport facilities, outer continental shelf facilities, and vessels regulated under the MTSA, and all U.S. Coast Guard credentialed merchant mariners.

F.2 Scope of accreditation, test methods, additional references, terms, and definitions

F.2.1 Scope of accreditation

NVLAP offers all interested laboratories a flexible, dynamic system of selecting a compound scope of accreditation under the CST LAP that best fits the laboratory's level of expertise and equipment.

A valid accreditation including the PIV test methods is required prior to applying for the Identity and Privilege Credential Management (17DHSIPCM) test methods.

F.2.2 Test methods

17DHSIPCM Transportation Worker Identification Credential (TWIC) Card – Fixed Reader Conformance Testing

NOTE: NVLAP, in collaboration with the DHS Identity and Privilege Credential Management Program, reserves the right to modify or add test methods as the program evolves and transitions from its initial stage to its mature stage.

F.2.3 Additional references

Additional references for the Department of Homeland Security Identity and Privilege Credential Management testing (17DHSIPCM)

In addition to the references specified for the 17PIV test methods in Annex C, the following references are recommended:

— Transportation Worker Identification Credential (TWIC®) Reader Hardware and Card Application Implementation Guidance, Version 1.0, 10 February 2011, or later.

— Transportation Worker Identification Credential (TWIC®) Qualified Technology List (QTL) Program Administrative Manual, Version 1.1, 08 February 2010, or later.

— Transportation Worker Identification Credential (TWIC®) Qualified Technology List (QTL) Program Fixed Physical Access Control Reader Approval Procedures, Version 0.7, 20 December 2010, or later.

— Transportation Worker Identification Credential (TWIC®) Qualified Technology List (QTL) Program Fixed Physical Access Control Reader Test Procedures, Version 0.8, 18 March 2011, or later.

— Transportation Worker Identification Credential (TWIC®) Qualified Technology List (QTL) Program Portable Physical Access Control Reader Approval Procedures, Version 0.6, 08 February 2010, or later.

— Transportation Worker Identification Credential (TWIC®) Qualified Technology List (QTL) Program Portable TWIC® Reader Test Procedures, Version 0.8, 18 March 2011, or later.

— Transportation Worker Identification Credential (TWIC®) Qualified Technology List (QTL) Program Derived Test Requirements, Version 0.7, 08 February 2011, or later.

F.2.4 Additional terms and definitions

Transportation Worker Identification Credential (TWIC)
The Transportation Security Administration's program for the design, issuance and maintenance of credentials of all maritime transportation workers requiring unescorted access to secure areas of regulated facilities and vessels and for the verification of their identity.

F.3 Additional accreditation process requirements

F.3.1 Additional accreditation requirements for the 17DHSIPCM testing

For an applicant laboratory to qualify as a DHS Identity and Privilege Credential Management (17DHSIPCM) testing laboratory, it shall achieve accreditation by NVLAP in the DHSIPCM test method.

All laboratories applying for the 17DHSIPCM testing shall:

- first, achieve accreditation by NVLAP as an Automated Cryptographic Validation Testing (17ACVT), Cryptographic Module Testing (17CM) laboratory;
- second, achieve accreditation by NVLAP as a NPIVP Testing Laboratory, in both 17PIV/01 and 17PIV/02 test methods.

F.3.2 Additional activities prior to an onsite assessment

There are no requirements additional to those provided in clause 3.2 of this handbook.

F.3.3 Additional onsite assessment requirements

There are no requirements additional to those provided in clause 3.3 of this handbook.

F.3.4 Additional proficiency testing requirements for the 17DHSIPCM testing

F3.4.1 *Initial Accreditation*: Proficiency testing for the 17DHSIPCM tests require proof of the laboratory's competence to set up and configure a testing hardware and software environment as instructed in the test, to use a TWIC card(s) and a specified card reader, to perform all the operations instructed in the test (e.g., electronically personalize the card(s), generate key pair(s), generate and load personalized data objects, authenticate the card holder), and to run the tests as instructed.

F.3.4.2 *Renewal of Accreditation*: NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests. Unsatisfactory performance in proficiency testing or substantial errors in the reports submitted to any of the validation programs may result in suspension or revocation of accreditation. For more information, see clause 3.10.

F.3.5 Additional requirements of Accreditation Decision for the 17DHSIPCM testing

There are no requirements additional to those provided in clause 3.5 of this handbook.

F.3.6 Additional granting accreditation requirements for the 17DHSIPCM testing

There are no requirements additional to those provided in clause 3.6 of this handbook.

F.3.7 Additional renewal of accreditation requirements for the 17DHSIPCM testing

There are no requirements additional to those provided in clause 3.7 of this handbook.

F.3.8 Additional monitoring visits requirements for the 17DHSIPCM testing

There are no requirements additional to those provided in clause 3.8 of this handbook.

F.3.9 Additional requirements for changes to the scope of accreditation for 17DHSIPCM testing

There are no requirements additional to those provided in clause 3.9 of this handbook.

F.3.10 Additional suspension of accreditation for the 17DHSIPCM testing

There are no requirements additional to those provided in clause 3.10 of this handbook

F.4 Additional general requirements for accreditation

There are no requirements additional to those provided in clause 4 of this handbook.

F.5 Additional structural requirements for accreditation

There are no requirements additional to those provided in clause 5 of this handbook.

F.6 Additional resource requirements for accreditation for the 17DHSIPCM testing

F.6.1 General

There are no requirements additional to those provided in Section 6.1 of this handbook.

F.6.2 Additional personnel requirements

F.6.2.1 For a laboratory to qualify for accreditation under the CST LAP, the laboratory shall demonstrate, in addition to the technical expertise required by each test method as described below, that their personnel

have basic knowledge of cryptographic and security practice for information systems and that the laboratory is aware of the governing standards and publications, especially the ones listed in this handbook.

F.6.2.2 Additional personnel requirements for the 17DHSIPCM testing

The laboratory personnel shall have experience, training, or familiarity in the areas of:

a) cryptography – symmetric versus asymmetric algorithms and uses;
b) cryptography – encryption protocols and implementations;
c) key generation and digital certificate encoding;
d) key management techniques and concepts;
e) cryptographic self-test techniques;
f) the families of cryptographic algorithms;
g) FIPS-approved and NIST-recommended security functions (applicable version of FIPS 140);
h) cryptography - Public Key Infrastructure (PKI);
i) TWIC and PIV Reader Authentication Modes;
j) access control models;
k) privilege management;
l) smart cards;
m) smart card readers (contact and contactless; portable and non-portable);
n) fingerprint readers;
o) Application Protocol Data Unit (APDU);
p) Basic Encoding Rules (BER);
q) biometric authentication techniques;
r) biometric enrollment, quality measure, and authentication techniques;
s) biometric testing;
t) concepts of the operational PIV systems;
u) contact and contactless interface standards;
v) Physical Access Control System (PACS) registration systems;
w) biometric device installation, integration and operation;
x) Personal Identifiable Information (PII) data protection and management;
y) data review, reduction and analysis;
z) statistical analysis methodologies; and
aa) the TWIC reader testing tools and their operation.

F.6.3 Additional facilities and environmental condition requirements

The laboratory shall have appropriate areas, including appropriate ventilation and safety, for the use of test methods using chemical solvents and heating/cooling apparatus.

F.6.4 Additional equipment requirements for the 17DHSIPCM testing

Supplemental to the additional equipment requirements listed for 17PIV testing (section C.5.5.2), the laboratory shall also meet the following minimum hardware, software and operating system requirements for any platform on which the testing tools required for DHSIPCM testing will run:

a) Hardware:
   1) at least 1 USB and 1 serial port available on the Windows XP[4] test computer;
   2) one or more sets of testing cards provided by the DHSIPCM Program Management Office (PMO); and
   3) Contact/Contactless Smart Card Reader, Magstripe Reader.

b) Software: testing tool provided by the DHSIPCM PMO.

F.6.5 Additional requirements for measurement traceability

There are no requirements additional to those provided in clause 6.5 of this handbook.

F.6.6 Additional requirements for externally provided products and services

There are no requirements additional to those provided in clause 6.6 of this handbook.

F.7 Additional process requirements for accreditation for the 17DHSIPCM testing

There are no requirements additional to those provided in clause 7 of this handbook.

F.8 Additional management system requirements for accreditation for the 17DHSIPCM testing

There are no requirements additional to those provided in clause 8 of this handbook.

[4] Certain commercial entities, equipment, or materials may be identified in this document to describe a requirement adequately. Such identification is not intended to imply recommendation or endorsement by NIST.

Annex G: Automated Cryptographic Validation Testing (ACVT) (normative)

G.1 Additional general information

The CAVP is a program based on a partnership between NIST's Computer Security Division and the Canadian Centre for Cyber Security (CCCS). The program provides federal agencies — in the United States and Canada — confidence that a validated cryptographic algorithm has been implemented correctly The CAVP validates cryptographic algorithms that may be integrated in one or more cryptographic modules validated by the CMVP.

The CAVP provides documented methodologies for conformance testing through defined sets of security requirements. For the CAVP, these are found in the individual validation system documents containing the validation test suites required to assure the algorithm has been implemented correctly. The validation system documents are designed for each FIPS-Approved and NIST-Recommended cryptographic algorithm.

The Cryptographic Algorithm Validation Program (CAVP) provides validation testing of FIPS-approved and NIST recommended cryptographic algorithms and is a prerequisite for the Cryptographic Module Validation Program (CMVP)[5]. The 17ACVT test method is based on the Automated Cryptographic Validation Protocol (ACVP) service and may be used by both first-party and third-party testing laboratories for CAVP testing.[6]

Laboratories accredited under this scope are permitted to perform conformance testing of FIPS-approved and NIST recommended algorithms using the 17ACVT test method and submit test results to the CAVP for validation. Conformance testing measures whether the implementation-under-test correctly implements the specification. The Cryptographic Algorithm Validation Program retains the role of validation authority and will award validation certificates for implementations that successfully satisfy the test requirements. Laboratories accredited under this scope must leverage the ACVTS service as their "means of testing"[7] to maintain accreditation.

G.2 Scope of accreditation, test methods, additional references, terms, and definitions

G.2.1 Scope of accreditation

NVLAP offers all interested laboratories a flexible, dynamic system of selecting a compound scope of accreditation under the CST LAP that best fits the laboratory's level of expertise and equipment.

[5] 17ACVT test methods satisfy the prerequisite testing for the 17CM test method.

[6] ISO/IEC 17000:2004 defines first-party conformity assessment activities as those that are performed by the person or organization that provides the object. Third-party conformity assessment activities are those that are performed by a person or body that is independent of the person or organization that provides the object, and of user interests in that object.

[7] ISO/IEC 9646-1 defines "means of testing" as the hardware and/or software, and the procedures for its use, including the executable test suite itself, used to carry out the testing required.

17ACVT is not a standalone test method for third party labs and shall be selected with 17CM. 17ACVT is a standalone test method for first party labs.

If only 17ACVT is selected, then only algorithm conformance testing may be performed.

G.2.2 Test methods

The only test method defined in this scope is 17ACVT.

17ACVT Automated Cryptographic Validation Testing (ACVT) for all FIPS-approved and/or NIST-recommended security functions as required in applicable version of FIPS 140 Annexes (and all superseded versions) – see http://csrc.nist.gov/groups/STM/cavp/index.html.

G.2.3 Additional references for Cryptographic Algorithms Testing

— *Cryptographic Algorithm Validation Program Management Manual*
(see http://csrc.nist.gov/groups/STM/cavp/documents/CAVPMM.pdf)

— *Frequently Asked Questions for the Cryptographic Algorithm Validation Program Concerning the Validation of Cryptographic Algorithm Implementations*
(see http://csrc.nist.gov/groups/STM/cavp/documents/CAVPFAQ.pdf)

— *NIST – Cryptographic Technology – Cryptographic Standards and Guidelines*
(see https://csrc.nist.gov/projects/cryptographic-standards-and-guidelines)

— Cryptographic Algorithm Validation Program CAVP
(see https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program)

G.2.4 Additional terms and definitions

G.2.4.1
ACVT
Automated Cryptographic Validation Testing

G.2.4.2
ACVP
Automated Cryptographic Validation Protocol

G.3 Additional accreditation process requirements for 17ACVT testing

G.3.1 Additional accreditation requirements

Non-commercial laboratories (i.e. labs that operate as part of a government institution) are prohibited from applying to 17ACVT and related test methods based on 17ACVT.

G.3.2 Additional activities prior to an onsite assessment

Archives of the output of the test harness from test runs submitted to the validation authority shall be kept for a minimum of five years.

G.3.3 Additional onsite assessment requirements

There are no requirements additional to those provided in clause 3.3 of this handbook.

G.3.4 Additional proficiency testing requirements 17ACVT testing

G.3.4.1 *Initial Accreditation*: A proficiency test is a step in the initial accreditation process for the 17ACVT test method. The laboratory shall demonstrate the ability to use and maintain a test environment that correctly works with the ACVTS servers. The laboratory shall also communicate a plan for responsibly managing the NIST issued key used to access the ACVTS server and for maintaining the test harness in a configuration management system.

G.3.4.2 *Renewal of Accreditation*: NVLAP, in collaboration with all CST validation programs, considers validation submissions to the validation programs as ongoing proficiency tests. Unsatisfactory performance in proficiency testing or substantial errors in the reports submitted to any of the validation programs may result in suspension or revocation of accreditation. For more information, see clause 3.10.

G.3.5 Accreditation decision

There are no requirements additional to those provided in clause 3.5 of this handbook.

G.3.6 Granting accreditation

There are no requirements additional to those provided in clause 3.6 of this handbook.

G.3.7 Renewal of accreditation

There are no requirements additional to those provided in clause 3.7 of this handbook.

G.3.8 Monitoring visits

There are no requirements additional to those provided in clause 3.8 of this handbook.

G.3.9 Changes to scope of accreditation

There are no requirements additional to those provided in clause 3.9 of this handbook.

G.3.10 Suspension of accreditation

The laboratory shall submit at least two new algorithm validations within the accreditation onsite assessment period. Failure to do so may result in the suspension of the accreditation. For more information, see clause 3.10 of this handbook.

G.3.11 Denial and revocation of accreditation

There are no requirements additional to those provided in clause 3.11 of this handbook.

G.3.12 Voluntary termination of accreditation

There are no requirements additional to those provided in clause 3.12 of this handbook.

G.3.13 Appeals

There are no requirements additional to those provided in clause 3.13 of this handbook.

G.4 Additional general requirements for accreditation 17ACVT testing

There are no requirements additional to those provided in clause 4 of this handbook.

G.5 Additional structural requirements for accreditation 17ACVT testing

There are no requirements additional to those provided in clause 5 of this handbook.

G.6 Additional resource requirements for accreditation 17ACVT testing

G.6.1 General

There are no requirements additional to those provided in Section 6.1 of this handbook.

G.6.2 Additional personnel requirements

G.6.2.1 General

The laboratory shall identify personnel who have basic knowledge of cryptographic and security practice for information systems. This is in addition to the technical expertise required by each test method. The laboratory shall be aware of the governing standards and publications, especially those listed in this handbook.

G.6.2.2 Key Roles

The laboratory shall identify two or more personnel who fill key roles. The laboratory is expected to approach this personnel requirement such that laboratory performance is optimized.

Key Roles (all roles listed below must be independent of development):

- Approved Signatory
  NIST Handbook 150 defines an Approved Signatory. The name of at least one Approved Signatory shall appear on the test report.

- Lab Manager
  The Lab Manager shall be responsible for managing the NIST-issued key and for ensuring the correct usage of the ACVTS servers. Failure to comply with published accreditation parameters (e.g., usage of the ACVTS servers. Failure to comply with published accreditation parameters (e.g., invalid signatory, etc.) can trigger the laboratory's suspension or revocation of the accreditation.

- Cryptography Subject Matter Expert (SME)
  Minimum/General Experience: This position requires 5 years' general experience and 3 years' specialized experience. Five years' general experience includes all aspects of cryptography, and a mixture of experience from the mathematical disciplines and the demonstrated ability to work independently or under only general supervision. Three years' specialized experience includes developing cryptographic and hash algorithms including but not limited to AES, SHA, etc.

Demonstrated experience in developing, analyzing, testing, and researching Public Key Infrastructures using X.509 certificates, symmetric and public key algorithms, hash functions, and quantum cryptography.

Functional Responsibilities: Duties may include but are not limited to: performing complex analysis, design, development, integration, testing and debugging cryptographic and hashing algorithms; and applying cryptography-based solutions to contemporary use cases such as evaluating for FIPS 140 compliance, electronic voting, smart grid, health care, and resource-constrained environments including but not limited to smart meters, smart cards, and medical devices.

Minimum Education: A Master's degree in Cryptography, Computer Science, Engineering, Mathematics, or other related scientific or technical discipline is required; or a bachelor's degree in one of the above-mentioned fields plus 8 years' related experience; or a PhD with 2 years' related experience.

- Independent Tester:
  A tester who is not a part of the development team.

G.6.2.3 The Lab Manager (or delegate) shall be responsible for managing the NIST-issued key and for ensuring correct usage of the ACVTS Demo and ACVTS Production servers.

G.6.2.4 The Cryptography SME and Tester shall have basic knowledge, experience, and training, in FIPS-approved and NIST-recommended cryptographic algorithms and shall have a working knowledge of the test environment and ACVTS services.

G.6.3 Additional facilities and environmental conditions requirements

G.6.3.1 Implementations-under-test (IUT), IUT-specific documentation, IUT-specific test harnesses, supporting test apparatus, or test results, shall be protected (e.g., from physical, logical, or visual access) from unauthorized access that could compromise the integrity of the test and corresponding records.

G.6.3.2 The laboratory manager shall identify and document for each specific IUT the laboratory personnel who either have a need to know or have authorized access of the IUT, server credentials, documentation, and testing-related apparatus including rationale for such access.

G.6.3.3 An audit log shall be maintained documenting personnel who have had access to each IUT during the contracted timeframe and all supporting documentation and testing related apparatus.

NOTE: Authorized vendor personnel for the IUT under contract may be granted access by the laboratory per the contract.

G.6.3.4 Requirements for testing at permanent remote locations

There are no requirements additional to those provided in Section 6.3.7 of this handbook.

G.6.4 Additional equipment requirements

The laboratory shall specify all hardware and software (e.g., compilers, debuggers, simulators, etc.) that fully define the test configuration for each IUT. This information shall be maintained as part of the validation test records.

G.6.5 Additional requirements for measurement traceability

Test vectors and results for cryptographic algorithm testing shall be generated and checked using the ACVT service.

G.6.6 Additional requirements externally provided products and services

The laboratory shall use the tools defined in the CAVP web page (https://csrc.nist.gov/projects/automated-cryptographic-validation-testing).

G.7 Additional process requirements for accreditation 17ACVT testing

G.7.1 Additional requirements for requests, tenders and contracts

There are no requirements additional to those provided in clause 7.1 of this handbook.

G.7.2 Additional requirements for selection verification and validation of methods

There are no requirements additional to those provided in clause 7.2 of this handbook.

G.7.3 Additional requirements for sampling

There are no requirements additional to those provided in clause 7.3 of this handbook.

G.7.4 Additional requirements for handling of test items

The laboratory shall be capable of reproducing test results using a current version of the IUT.

G.7.5 Additional requirements for technical records

Validation test records shall be kept for a minimum of five years.

G.7.6 Additional requirements for the evaluation of measurement uncertainty

There are no requirements additional to those provided in clause 7.6 of this handbook.

G.7.7 Additional requirements for ensuring the validity of results

[See G.3.4]

G.7.8 Additional requirements for the reporting of results

G.7.8.1 The ACVP service shall be used for algorithm validation submissions that use the 17ACVT test method.

G.7.8.2 When testing is performed at the vendor site or other mutually agreed upon site, only the laboratory personnel shall use or have access to the NIST-issued key.

G.8 Additional management system requirements for accreditation

There are no requirements additional to those provided in clause 8 of this handbook.

Annex H: Acronyms and abbreviations
(informative)

The following acronyms and abbreviations are used throughout this handbook:

ACVP	Automated Cryptographic Validation Program
ACVT	Automated Cryptographic Validation Testing
ACVTS	Automated Cryptographic Validation Testing System
ANSI	American National Standards Institute
APDU	Application Protocol Data Unit
ARF	Asset Reporting Format
BER	Basic Encoding Rules
CAVP	Cryptographic Algorithm Validation Program
CCE	Common Configuration Enumeration
CCSS	Common Configuration Scoring System
CMT LAP	Cryptographic Module Testing Laboratory Accreditation Program
CMVP	Cryptographic Module Validation Program
CPE	Common Platform Enumeration
CSD	Computer Security Division
CSE	Communications Security Establishment Canada
CST LAP	Cryptographic and Security Testing Laboratory Accreditation Program
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHSIPCM	Department of Homeland Security Identity and Privilege Credential Management
DMM	Digital Multi-Meter
DTR	Derived Test Requirements
FIPS	Federal Information Processing Standard
GSA EP	General Service Administration Evaluation Program
GSAP	General Service Administration Precursor
IEC	International Electrotechnical Commission
IG	Implementation Guidance
INCITS	InterNational Committee for Information Technology Standards
ISO	International Organization for Standardization
ITL	Information Technology Laboratory
IUT	Implementation-Under-Test

JRE	Java Runtime Environment
MB	Megabytes
NPIVP	NIST Personal Identity Verification Program
NVLAP	National Voluntary Laboratory Accreditation Program
OCIL	Open Checklist Interactive Language
OVAL	Open Vulnerability Assessment Language
PIV	Personal Identity Verification
PKI	Public Key Infrastructure
QM	Quality Manual
SCAP	Security Content Automation Protocol
SP	Special Publication
TMSAD	Trust Model for Security Automation Data
TWIC	Transportation Worker Identification Credential
USB	Universal Serial Bus
VCS	Version Control System
VHD	Virtual Hard Disk
VM	Virtual Machine
VOM	Volt-Ohm-Meter
XCCDF	eXtensible Configuration Checklist Document Format