NIST HANDBOOK 150-17
2008 Edition

National Voluntary Laboratory Accreditation Program

CRYPTOGRAPHIC AND SECURITY TESTING

Michaela Iorga and Carroll Brickenkamp

National Voluntary Laboratory Accreditation Program
Standards Services Division
Technology Services

May 2008

U.S. Department of Commerce
Carlos M. Gutierrez, Secretary

National Institute of Standards and Technology
James Turner, Deputy Director

NVLAP AND THE NVLAP LOGO

The term *NVLAP* and the NVLAP logo are registered marks of the Federal Government, which retains exclusive rights to control the use thereof. Permission to use the term and symbol (NVLAP logo with approved caption) is granted to NVLAP-accredited laboratories for the limited purpose of announcing their accredited status, and for use on reports that describe only testing and calibration within the scope of accreditation. NVLAP reserves the right to control the quality of the use of the NVLAP term, logo, and symbol.

Contents

Acknowledgments

The authors (Michaela Iorga of MiTech Consulting, Inc. and Carroll Brickenkamp of Pi Group, Inc.) would like to thank the many people who reviewed and contributed to this document. In particular, the following individuals provided invaluable feedback: Ray Snouffer, William MacGregor, Randy Easter, Magdalena Benitez, Hildy Ferraiollo and Peter Mell (NIST/ITL/CSD); Jean Campbell and Claudia Popa (CSEC); Carol Cantlon and Erin Connor (EWA-Canada); and Steve Ratcliff (ICSALab).

Foreword

The 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 is comprised of 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. They tailor the general criteria found in NIST Handbook 150 to the specific tests, calibrations, or types of tests or calibrations covered by a LAP.

NIST Handbook 150-17 presents technical requirements and guidance for the accreditation of laboratories under the National Voluntary Laboratory Accreditation Program (NVLAP) Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP), formerly known as Cryptographic Module Testing (CMT) LAP. The handbook is intended for information and use by accredited laboratories, assessor(s) conducting on-site visits, 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 the NIST Handbook 150. If ambiguity unintentionally arises, the NIST Handbook 150 requirements shall be followed.

The 2008 edition of NIST Handbook 150-17 incorporates changes resulting from the release of the newest editions of ISO/IEC 17025, *General requirements for the competence of testing and calibration laboratories*, ISO/IEC 17011, *Conformity assessment—General requirements for accreditation bodies accrediting conformity assessment bodies*, ISO 9001, *Quality management systems—Requirements*, NIST Handbook 150, *NVLAP Procedures and General Requirements*, addition of new scopes of accreditation, and editorial improvements. The requirements of NIST Handbook 150, the interpretations and specific requirements in NIST Handbook 150-17, and the requirements in program-specific checklists shall be combined to produce the criteria for accreditation in the NVLAP Cryptographic and Security Testing Laboratory Accreditation Program.

The 2008 edition of NIST Handbook 150-17 supersedes and replaces the 2000 edition.

The numbering and titles of the first five clauses of this handbook correspond to those of NIST Handbook 150. The primary subclauses in clauses 3, 4 and 5 (e.g., 4.1, 4.2, etc.) are also numbered and titled to correspond with those of NIST Handbook 150, even when there are no requirements additional to those in NIST Handbook 150.

This handbook is also available on the NVLAP website (http://www.nist.gov/nvlap).

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 NIST Handbook 150, *NVLAP Procedures and General Requirements* by gathering the technical requirements of the 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, protocols), and of cryptographic and security modules. Technical requirements are explained to indicate how the NVLAP criteria are applied to accreditation for conformance testing under the Cryptographic and Security Testing (CST) LAP.

Any laboratory (including commercial, manufacturer, university, federal, state, or local government laboratory, foreign or domestic) that performs any of the test methods covered by the CST LAP may apply for NVLAP accreditation. Accreditation will be granted to a laboratory that complies with the conditions for accreditation as defined in this document. Accreditation does not imply a guarantee of laboratory performance or of system-under-testing test data; 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 of security policy compliance and vulnerability management modules. For more information see the CST LAP's website <http://ts.nist.gov/Standards/Accreditation/CST-LAP.cfm>.

Types of security functions covered: A security function is a part, a subset of parts, or the whole set of the System-Under-Test (SUT) that has to 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 FIPS 140-2 Annex A (and all superseded and future versions).

Types of cryptographic modules covered: A cryptographic module is defined as a set of hardware and/or software that implements FIPS-approved and/or NIST-recommended security functions and that is contained within the predefined 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 considered to be 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 considered to be 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 Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP). It supplements the NVLAP procedures and general requirements found in NIST Handbook 150, by tailoring the general criteria found in NIST Handbook 150 to the specific types of tests covered by the CST LAP.

1.1.2 NIST Handbook 150, this handbook, and their respective checklists (see 1.6 and Annex A) constitute the collective body of requirements that must be met by a laboratory seeking NVLAP accreditation for the CST LAP.

1.1.3 The interpretive comments and additional requirements contained in this handbook make the general NVLAP criteria specifically applicable to the CST LAP.

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

1.2 Organization of handbook

1.2.1 The numbering and titles of the first five clauses of this handbook are patterned after Handbook 150:2006, *NVLAP Procedures and General Requirements*, to allow easy cross-reference. The primary subclauses in clauses 3, 4 and 5 (e.g., 4.1, 4.2) are also numbered and titled to correspond with those of NIST Handbook 150, even when there are no requirements additional to those in NIST Handbook 150.

1.2.2 In addition, the handbook contains two annexes that supplement the text. Annex A (normative) lists the available scopes of accreditation offered by the CST LAP, provides additional information and links to the CST LAP, NVLAP and NIST websites where the most current information and resources are located, and lists the additional requirements per specific scope of accreditation in terms of personnel proficiency, managerial and technical requirements, specific tools, quality manual, and other documentation. Annex B (informative) provides a list of additional acronyms.

1.2.3 The procedures and general requirements of NIST Handbook 150 and the interpretations and specific requirements in this handbook must be combined to produce the criteria for accreditation under the CST LAP.

1.3 Program description

1.3.1 The Cryptographic and Security Testing (CST) Laboratory Accreditation Program (LAP), formerly named Cryptographic Module Testing (CMT), was established by the National Voluntary Laboratory Accreditation Program (NVLAP) to accredit laboratories that perform cryptographic algorithms and cryptographic module validation conformance testing. As the LAP expanded in 2006 and 2007 and offered additional security scopes of accreditation, the 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 National Institute of Standards and Technology, Information Technology Laboratory (NIST/ITL), initially requested establishment of this LAP to accredit laboratories that conformance test cryptographic modules under the Cryptographic Module Validation Program (CMVP). As the CMVP expanded, a new program was developed within ITL to encompass the validation of all FIPS-approved and NIST-recommended security functions. Laboratory accreditation for the Cryptographic Algorithm Validation Program (CAVP) was added in July 1995 as a component of the accreditation for the CMVP, and became a separate program in 2006.

1.3.3 The Cryptographic Algorithm Validation Program (CAVP) is a validation program developed by NIST/ITL and administered jointly by NIST/ITL and the Communications Security Establishment Canada (CSEC) of the Government of Canada for the validation of all FIPS-approved and NIST-recommended security functions. NIST/ITL developed a validation test suite for testing the correctness of a security function's implementation. All algorithm-specific test suites are bundled in a tool kit provided by NIST/ITL for all laboratories obtaining accreditation. Unless otherwise specified, the CAVP test tool is provided by NIST/ITL.

1.3.4 The Cryptographic Module Validation Program (CMVP) is a validation program developed by NIST/ITL and administered jointly by NIST/ITL and the Communications Security Establishment Canada (CSEC) of the Government of Canada. The testing requirements for this program are derived by NIST/ITL from FIPS 140-2: *Security Requirements for Cryptographic Modules* or successors. The requirements are specified in the *Derived Test Requirements (DTR) for FIPS 140-2, 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.

1.3.5 In response to the Homeland Security Presidential Directive (HSPD) 12 of August 2004, the NIST Computer Security Division (NIST/CSD) 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. Later that year, NIST established the NIST Personal Identity Verification Program (NPIVP) to validate Personal Identity Verification (PIV) components required by FIPS 201 within ITL. NVLAP added the PIV Test Methods to the CST LAP in April 2006. NVLAP accredits NPIVP laboratories to test *PIV Card Application* and *PIV Middleware* implementations for conformance to the NIST SP 800-73, *Interfaces for Personal Identity Verification*, which is normatively referenced from FIPS 201. The Personal Identity Verification (PIV) components required by FIPS 201-1 and validated by the NPIVP are:

- to validate the conformance of two PIV components: *PIV Middleware* and *PIV Card Application* with the specifications in NIST SP 800-73-1 or successors; and
- to provide assurance that the set of *PIV Middleware* and *PIV Card Applications* that have been validated by NPIVP are interoperable.

1.3.6 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 could already attain 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.

1.3.7 The GSA EP was established to evaluate and approve products and services as compliant with specified FIPS 201 requirements and ensure product interoperability (see <http://fips201ep.cio.gov/>. 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 GSA Precursor (GSAP) in this handbook

1.3.8 In response to the Office of Management and Budget (OMB) Memorandum M-07-18 of July 31, 2007, the NIST/CSD initiated a new program for validating the implementation of the Security Content Automation Protocol (SCAP) standards within security software modules. To meet the needs defined in the Memorandums M-07-11 and M-07-18, NVLAP established the accreditation of SCAP conformance testing laboratories in December 2007.

1.3.9 The SCAP enables automated vulnerability management, measurement, and policy compliance evaluation; enumerates vulnerabilities, misconfigurations, platforms, and impact; and provides machine-readable security configuration checklists. SCAP is composed of six open standards:

- Common Vulnerabilities and Exposure (CVE) – a dictionary of security related software flaws;
- Common Configuration Enumeration (CCE) – a dictionary of software misconfigurations;
- Common Platform Enumeration (CPE) – a standard nomenclature and dictionary for product naming;
- eXtensible Configuration Checklist Description Format (XCCDF) – a standard XML for specifying checklists;
- Open Vulnerability Assessment Language (OVAL) – a standard XML for checking the machine state; and
- Common Vulnerability Scoring System (CVSS) – a standard for scoring the impact of vulnerabilities.

1.3.10 For additional information regarding SCAP see the program website http://scap.nist.gov.

1.3.11 Information regarding the most current additions, enhancements and extensions to the CST LAP scopes of accreditation at the time of this publication can be found in Annex A.

1.3.12 NVLAP reserves the right to expand the CST LAP and offer to interested laboratories additional scopes of accreditation not listed in this handbook. Laboratories are advised to review the CST LAP's website for the most current information (see http://ts.nist.gov/Standards/Accreditation/CST-LAP.cfm).

1.3.13 All of the cryptographic and security testing performed under any of the CST LAP's programs (e.g., CMVP, CAVP) are handled by third-party test facilities that are accredited as Cryptographic and Security Testing laboratories by NVLAP as described in this handbook.

1.3.14 The Figure 1, below, provides a generic overview of the accreditation process and the relationship between:

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

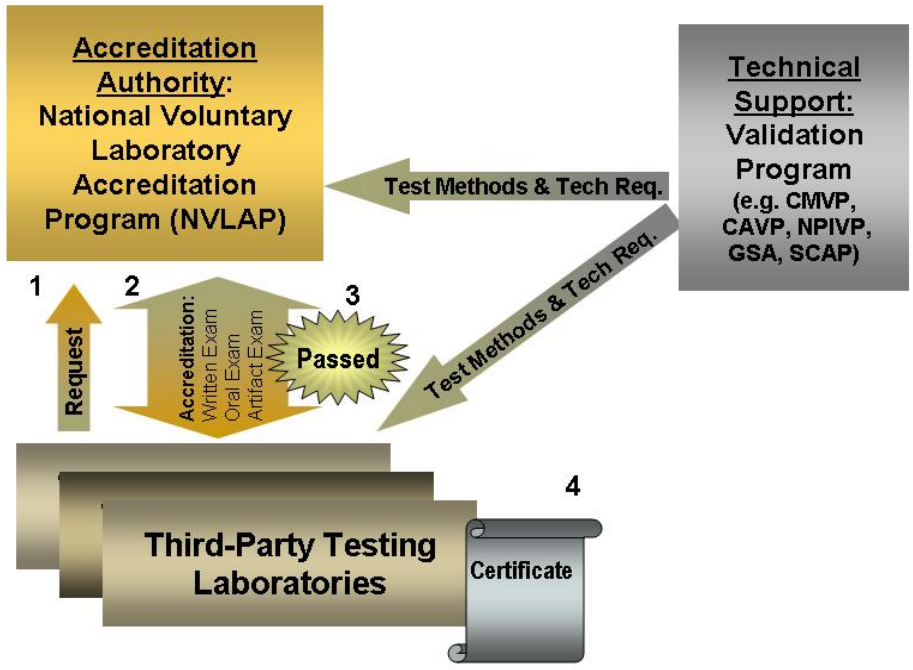


Figure 1: Accreditation process

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* http://ts.nist.gov/Standards/Accreditation/upload/nist-handbook-150.pdf.

1.4.2 FIPS publications

For FIPS references specific to particular scopes of accreditation and/or test methods, see Annex A.

1.4.3 ISO/IEC publications

In addition to the ISO/IEC references listed in NIST Handbook 150, ISO/IEC references specific to particular scopes of accreditation and/or test methods are listed in Annex A. These may be purchased from http://www.iso.org,

— ISO/IEC Guide 43-2, *Proficiency testing by interlaboratory comparisons- Part2: Selection and use of proficiency testing schemes by laboratory accreditation bodies*, 1997.

1.4.4 NIST Special Publications (SP)

For NIST/ITL references specific to particular scopes of accreditation or test methods, see Annex A. The CST LAP website <http://ts.nist.gov/Standards/Accreditation/CST-LAP.cfm> also provides a complete, up-to-date list of links to the Special Publications (SP) and validation programs sites where the Testing Tools are located. The references listed on the website supersede the information provided herein unless otherwise specified. If no link is indicated, NIST Special Publications relevant to this program can be downloaded from the CST LAP website.

1.4.5 Other NIST publications and tools

See Annex A for scope-specific descriptions of the Cryptographic and Security Testing tools relevant to the desired scope of accreditation.

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 the NIST Handbook 150. For a list of all acronyms, see Annex A. Terms specific to the CST LAP are defined as follows:

1.5.1

Additional scope-specific terms and definitions are provided in Annex A, subclause A.2

1.5.2

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

1.5.3

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

1.5.4

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

1.5.5

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

1.5.6

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

1.5.7

confidentiality
Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.

1.5.8

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.

1.5.9

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.

1.5.10

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

1.5.11

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.

1.5.12

Cryptographic Algorithm Validation Program (CAVP)
The Cryptographic Algorithm Validation Program administered jointly by NIST/ITL and CSEC. The laboratory's accreditation for conformance testing under this program is covered by the CST LAP. For more information regarding CAVP see the validation program website:
<http://csrc.nist.gov/groups/STM/cavp/index.html>.

1.5.13

Cryptographic Algorithm Validation System (CAVS)
The NIST CAVP Security Function Test Tool Kit, also known as the Cryptographic Algorithm Validation System.

1.5.14

Cryptographic Module Validation Program (CMVP)
The Cryptographic Module Validation Program administered jointly by NIST/ITL and CSEC. The laboratory's accreditation for conformance testing under this program is covered by the CST LAP. For more information regarding CMVP see the validation program website:
<http://csrc.nist.gov/groups/STM/cmvp/index.html>.

1.5.15

Cryptographic and Security Testing Laboratory Accreditation Program (CST LAP)
The current name given to *this* LAP. The new nomenclature supersedes the Cryptographic Module Testing (CMT) LAP naming.

1.5.16

derived test requirements (DTR)
Description of the methods that will be used by accredited laboratories to test whether the 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 <http://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. (Implementation guidance cannot change or add requirements to the given standard.)

1.5.19

integrity
Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.

1.5.20

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

1.5.21

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

1.5.22

NIST Personal Identity Verification Program (NPIVP):
The NIST Personal Identity Verification Program established to validate Personal Identity Verification (PIV) components required by FIPS 201. The program is administered by NIST/ITL. The laboratory's accreditation for conformance testing under this program is covered by the CST LAP. For more information regarding the NPIVP, see the validation program website:
<http://csrc.nist.gov/groups/SNS/piv/npivp/index.html>.

1.5.23

Personal Identity Verification (PIV)
The NIST initiative created in response to the HSPD 12 for improving the identification and authentication of Federal employees and contractors for access to Federal facilities and information systems. For more information, see the program website
<http://csrc.nist.gov/groups/SNS/piv/index.html>.

1.5.24

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

1.5.25

Security Content Automation Protocol (SCAP)
A method for using specific standards to enable automated vulnerability management, measurement, and policy compliance evaluation. SCAP tools (systems) can be used by an end user (agency, corporation) to automatically evaluate the user's compliance to the targeted requirements (e.g., FISMA compliance, FDCC compliance). For more information, see the program's website <http://scap.nist.gov>.

1.5.26

Security Content Automation Protocol (SCAP) Validation Program
The Security Content Automation Protocol validation program administered by NIST/ITL. The laboratory's accreditation for conformance testing under this program is covered by the CST LAP. For more information regarding the SCAP validation program, see the website <http://scap.nist.gov>.

1.5.27

security functions
A part, a subset of parts or the whole set of the System-Under-Test (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.

1.5.28

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

1.5.29

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.

1.5.30

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.

1.5.31

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.

1.5.32

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.

1.5.33

validation
The administrative acts by the governing Validation Program (e.g., CMVP, CAVS, NPIVP, etc) of determining conformance of an implementation to specified standards and requirements (e.g., FIPS 140-2 or successor, FIPS 201-1 or successor) based on test results from the accredited laboratories.

1.5.34

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 it interpreting, detailing and expanding portions of NIST Handbook 150 for CST LAP use. Assessor(s) use(s) NVLAP checklists to ensure that each laboratory receives an assessment consistent with that received by other laboratories. Checklists assist assessor(s) in documenting the assessment to the NVLAP requirements found in NIST Handbook 150, in this handbook, and in the checklists themselves. 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 <http://www.nist.gov/nvlap>.

1.6.2 NIST Handbook 150 Checklist

All NVLAP programs use the NIST Handbook 150 Checklist (formerly called the General Operations Checklist), which contains the requirements published in NIST Handbook 150. The checklist items are numbered to correspond to clauses 4 and 5 and annexes A and B of NIST Handbook 150. The current version of the checklist is available from the NVLAP website at <http://www.nist.gov/nvlap>.

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 at <http://ts.nist.gov/Standards/Accreditation/CST-LAP.cfm>.

1.6.3.2 The *CST Program-Specific Checklist* applies only to cryptographic and security testing. The checklist focuses on the testing requirements and the special personnel and equipment requirements corresponding to the scopes of accreditations elected by the applicant laboratory. Annex A provides additional information on the scopes of accreditation and derived requirements.

1.6.3.3 The *CST Program-Specific Checklist* also includes a place to record the assessor's observations of round-table proficiency quizzes, proficiency testing results when applicable, and of test demonstrations when performed (for more information see 1.6.5, 3.3.1.6 and 3.4.2). This checklist may be revised, when appropriate, to reflect changes in the technical requirements, scope, and/or technology of the program.

1.6.3.4 The checklist concludes with a *Comments and Nonconformities* section used by the assessor(s) to explicitly identify and describe all nonconformities noted in the body of the checklist. Additionally, the assessor(s) may use the form to document comments on any aspect of the laboratory or its performance.

1.6.4 Scopes of Accreditation and Test Method Selection

1.6.4.1 The CST LAP offers a set of scopes for accreditation. Depending on the breadth of its testing capabilities, the applicant laboratory may select scope(s) of accreditation from the list of offered scopes. The minimum required scope of accreditation is the Basic Cryptographic and Security (BCS) scope, as defined in Annex A and on the CST LAP website. Some of the scopes have additional accreditations as prerequisites, such as the GSAP test methods that require PIV accreditation.

1.6.4.2 The scope of accreditation is determined by the test methods on the *Test Method Selection List*, which is provided to a laboratory seeking accreditation as part of the NVLAP application package for the program.

1.6.5 Test Method Review Summary

The assessor(s) use(s) the *Test Method Review Summary*, when necessary, to document their review of the laboratory's ability to perform the test methods pertaining to the elected scope(s) of accreditation. The review of the test methods by the assessor(s) ranges from having laboratory staff describe the test procedures, conducting round-table quizzes, or evaluating the laboratory's proficiency based on the step-by-step documented execution of a test suite on a given artifact and testing scenario. The assessor(s) notes on the *Test Method Review Summary* the depth into which each part of the test method was reviewed (Observed Test, Examined Apparatus, Conducted Quiz, Walked/Talked Through Test, Listened to Description of Procedures, Step-by-Step Documented Test Report).

1.6.6 NVLAP Lab Bulletins

NVLAP Lab Bulletins are issued to laboratories and assessor(s), when needed, to clarify program-specific requirements and to provide information about the most current program additions and changes.

1.6.7 Other Publications

Some of the scopes of accreditation and associated test methods reference additional documentation that can be found in Annex A and/or on the CST LAP website. The scopes of accreditation are available on the NVLAP website at <http://ts.nist.gov/Standards/Accreditation/handbook.cfm>.

2 LAP establishment, development and implementation

2.1 Bases for establishment

This subclause contains no information additional to that provided in NIST Handbook 150, 2.1.

2.2 Development of technical requirements

All technical requirements mandated for a laboratory under accreditation tailor the requirements discussed in Clauses 4 and 5 which are derived from the elected scope of accreditation and associated test methods for which a candidate requests accreditation.

2.3 Announcing the establishment of a LAP

This subclause contains no information additional to that provided in NIST Handbook 150, 2.3.

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 website: <http://www.nist.gov/nvlap>.

2.5 Termination of a LAP

This subclause contains no information additional to that provided in NIST Handbook 150, 2.5.

3 Accreditation Process

3.1 Application for initial accreditation

3.1.1 A laboratory interested in accreditation for any of the scopes of accreditations offered under the CST LAP shall review and become familiar with all the requirements listed in NIST Handbook 150 and in this handbook, review the CST LAP website at <http://ts.nist.gov/Standards/Accreditation/CST-LAP.cfm>, and contact NVLAP for the most current updates on the requirements and application process.

3.1.2 The accreditation process starts with the submission of the laboratory's application, fees payment, continues with the on-site visit and laboratory's proficiency evaluation which includes the a) through d) steps represented below, and ends with NVLAP's final decision regarding the laboratory's accreditation.

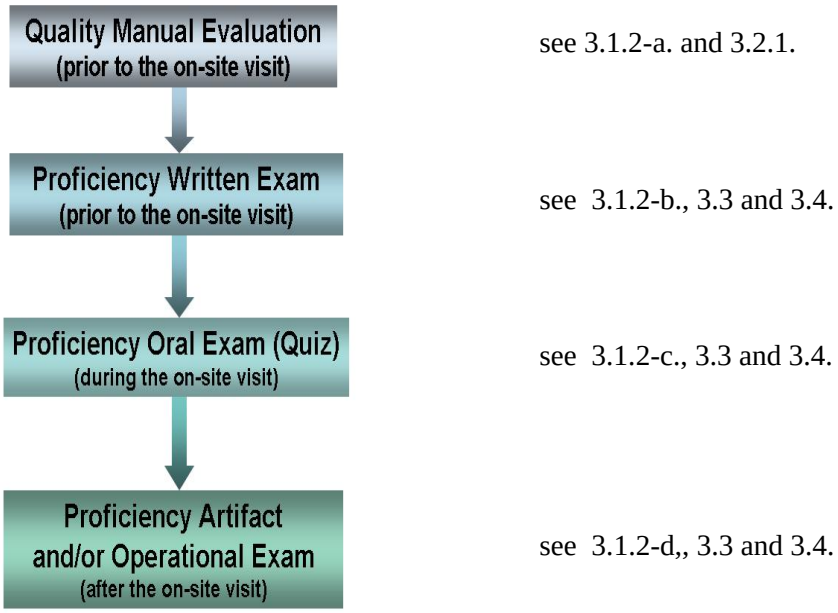


Figure 2: Accreditation flow chart

a) Quality manual evaluation - When the laboratory is applying for initial accreditation, the assessor(s) must first determine that the management system meets the requirements.

b) Proficiency written exam - If the assessor(s) determine that the management system meets the requirements, a written exam is then provided to the applicant laboratory, with a 5-business-day deadline for response, unless otherwise specified. This exam evaluates the laboratory personnel's technical expertise and knowledge of the standards and test methods applicable to the scope(s) of accreditation for which the laboratory is applying. The laboratory shall score greater than 75 % correct responses for the accreditation process to continue and the on-site visit to be scheduled.

c) On-site visit and proficiency/round-table quiz - Once the written exam is passed, an on-site visit is scheduled at a mutually agreed date and time. During the on-site visit, the laboratory's personnel will be quizzed and team dynamics observed for proficiency and expertise in the technical area for which the laboratory is applying for accreditation. 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 greater than 75 % correct responses for the accreditation process to continue.

d) Proficiency artifact and/or operational exam - Once the assessor(s) determines that the laboratory has satisfactorily completed the on-site visit, a proficiency artifact and/or operational exam is provided to the applicant laboratory (at the end of the initial on-site visit or after on-site visit). Unless otherwise specified by NVLAP, the laboratory shall complete the test by the scope-dependent deadline. The proficiency artifact and/or operational exam is designed to evaluate the laboratory's understanding of and competence to apply the Cryptographic and Security Testing conformance testing methodology specific to the scope(s) of accreditation for which the laboratory is applying. The laboratory shall successfully complete the proficiency test as evaluated by the technical expert assessor(s) in order to be accredited by NVLAP. The proficiency artifact and/or operational exam requirement applies only to initial accreditation.

3.2 Activities prior to initial on-site assessment

3.2.1 The quality manual and related documentation shall contain or refer to documentation that describes and details the implementation of procedures covering all of the technical requirements in this handbook. This information will be reviewed by NVLAP assessor(s) prior to the on-site assessments. If the quality manual is judged unsatisfactory, the on-site visit will be postponed. Otherwise, defects and recommendations for management system enhancements will be discussed during the on-site visit.

3.2.2 For some of the scopes of accreditation, 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 scopes 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 on-site evaluation. 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 on-site visit.

3.3 On-site assessments

3.3.1 Conduct of on-site assessment

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

- the laboratory has completed and passed the written exam [3.1.1.2] (normally conducted before the initial on-site assessment);
- the laboratory passed the proficiency quiz [3.1.1.3] (normally conducted during the on-site assessment);
- the laboratory has completed and passed the proficiency artifact test and/or operational exam [3.1.1.4] (normally conducted after the initial on-site assessment);
- the laboratory staff has demonstrated understanding of and competence to apply the Cryptographic and Security Testing conformance testing methodology as evaluated by the results of the proficiency test; and
- the laboratory has exercised the management system and has produced appropriate records of all management system activities.

3.3.1.2 The on-site assessment is scheduled at a mutually agreed date between NVLAP's assessor(s) and the laboratory. The on-site assessment will most likely span about two days and will most likely be performed by two or more NVLAP assessor(s). All observations made by the assessor(s) during the assessment are held in the strictest confidence.

3.3.1.3 In some cases, the on-site 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 between the assessor(s) and laboratory management, but still part of the approximately two day on-site visit. If the geographic distance to the separate test site requires significant travel, then this is deemed by NVLAP to be a separate laboratory that will have to be separately accredited with its own separate on-site assessment.

3.3.1.4 The assessor(s) will use, in addition to the general checklist based on NIST Handbook 150, the *CST Program-Specific Checklist* derived from the technical specifics contained in this handbook. Even though the CST checklist is derived dynamically from the elected scopes 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 equivalent chosen scopes of accreditation.

3.3.1.5 Additionally, the assigned assessor(s) have the right and the responsibility to go beyond the checklist whenever need rises (e.g., new updated requirement are available on the CST LAP's website but are not incorporated yet in the checklist), in order to delve more deeply into technical issues.

NOTE: NVLAP will document all technical requirements prior to assessments.

3.3.1.6 The agenda for a typical on-site assessment is given below.

a) *Opening meeting:* During the on-site visit, the assessor(s) conduct(s) an entry briefing with laboratory management and supervisory personnel to explain the purpose of the on-site 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/round-table 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/round-table quizzes are to be conducted, all members of the relevant staff should be scheduled to be present and participate.

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

- conformance of the quality system with ISO 17025-2005 and NIST Handbook 150,
- quality manual,
- equipment and maintenance records;
- record-keeping procedures,
- testing procedures,
- laboratory test reports,
- personnel competency records,
- personnel training plans and records,
- version of the validation tools and/or other validation program-specific software,
- procedures for updating pertinent information (e.g., Implementation Guidance and the validated products list for the CMVP), and
- safeguards for the protection of confidential, vendor-sensitive and proprietary information.

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

The assessor will check personnel information for job descriptions, resumes, training records and technical performance reviews. The assessor shall not be given information which 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 will examine computer hardware, software, auxiliary 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 and exit points;
- all test equipment and tools, including computer hardware, servers used for records retention and physical storage area;
- work environment in regard to providing adequate testing work space, heating, lighting, etc.; and
- physical security including access control procedures and records.

g) *Proficiency evaluations:* Although the written examination provided prior to the initial on-site assessment; the group round-table quizzes and individual demonstrations conducted during the initial and renewal on-site 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 initial assessment. Unless otherwise instructed prior to the on-site 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 on-site visit or will be sent to the laboratory after the on-site 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 on-site visit, a closing meeting is held with the laboratory manager and staff to discuss the assessor's findings. See 3.3.3.6 and 3.3.3.7 of NIST Handbook 150 for more information regarding the assessment report, nonconformities and the final resolution.

3.3.2 On-site assessment report (OSAR)

The assessor completes an *On-Site Assessment Report* (OSAR) that summarizes the findings. Copies of the completed checklists are also attached to the OSAR at the closing meeting. The report is signed by the assessor and the laboratory's Authorized Representative. A copy of the report and of the checklists is given to the laboratory representative for retention. 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 Handbook 150.

3.3.3 Nonconformities, comments, and recommendations

3.3.3.1 Nonconformities that have been corrected during the on-site assessment and any recommendations will be specifically noted on the OSAR.

3.3.3.2 Comments in the OSAR should be given serious consideration by the laboratory, but no action is mandated and changes are made at the laboratory's discretion. However, assessor(s) frequently note that comments often rise to the level of nonconformities on subsequent assessments.

3.3.3.3 Positive feedback will also be recorded on the OSAR.

3.4 Proficiency Testing

3.4.1 General

3.4.1.1 The CST LAP mandates program-specific proficiency testing. All applicant laboratories are required to participate in proficiency testing for all test methods derived from their scope(s) of accreditation, as designated in Annex A.

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 3.1.2. See Annex A for more details regarding the proficiency testing for each scope of accreditation.

3.4.2 Types of proficiency testing

NVLAP follows ISO/IEC Guide 43-2 for all of the types of proficiency testing used within the CST LAP, therefore, the LAP's proficiency testing may consist of one or more of the following exercises:

a) Demonstration of *correct identification and use* of the NVLAP/NIST-mandated test tools. The laboratory shall demonstrate that all appropriate personnel 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 the *understanding and correct interpretation* of all data transformation and of all test results reported by the test tools.

c) Demonstration of the *reports generation* in the 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 area of the elected scope(s) of accreditation. The laboratory shall be provided with a *proficiency quiz* to be responded to by all appropriate test personnel. The quiz also poses questions for each test method that is included in each accreditation unit 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 elected scope(s) of accreditation;
- familiarity with the governing standards and specifications;
- familiarity with the test methods derived from the elected scope(s) of accreditation;
- ability to determine how a particular cryptographic or security test should be performed for a particular set of test requirements; and
- how a specific algorithm, module or component should be tested to the governing specification.

e) Demonstration of SUT conformance testing proficiency. The laboratory shall perform a *conformance test* of a specially designed artifact, referred to as 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 and/or operational exam* for the initial accreditation will be delivered to the laboratory at the end of the on-site assessment or later.

f) NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests. A large number of errors in the reports submitted to any of the validation programs can trigger the suspension or revocation of a laboratory's accreditation. For more information see 3.10.

3.4.3 Analysis and reporting

The results of the proficiency testing are presented by the assessor(s) to NVLAP as soon as the testing process is completed. The results are then reported in appropriate documents to the candidate laboratory within 30 days from the completion of the testing process.

3.4.4 Proficiency testing nonconformities

Problems indicated by proficiency testing will be discussed with appropriate laboratory personnel responsible for developing and implementing plans for resolving the problems. Nonconformities identified by proficiency testing during an on-site assessment, a scheduled proficiency testing, or submission of a test report for validation of a vendor's product shall be resolved by the laboratory in order to attain and/or maintain accreditation.

3.5 Accreditation decision

This subclause contains no information additional to that provided in NIST Handbook 150, 3.5.

3.6 Granting accreditation

This subclause contains no information additional to that provided in NIST Handbook 150, 3.6.

3.7 Renewal of accreditation

It is important to note that the laboratory cannot be granted the renewal of the accreditation unless the laboratory has effectively implemented the management system and has produced appropriate records of all management system activities, including conducting at least one internal audit and management review before initial accreditation.

3.8 Monitoring visits

This subclause contains no information additional to that provided in NIST Handbook 150, 3.8.

3.9 Changes to scope of accreditation

3.9.1 A laboratory can request at any time a change in its scope of accreditation. A laboratory that requests additions to its scope of accreditation may be required to successfully complete additional proficiency tests.

3.9.2 In some instances when the laboratory's request is to increase the original scope, NVLAP may require an on-site assessment.

3.10 Suspension of accreditation

3.10.1 Failure to appropriately address and resolve complaints from customers or other interested parties may result in NVLAP surveillance activity, 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 if the new personnel prove inadequately prepared or unsuited for the job. Loss of key personnel without immediate adequate replacement may result in laboratory's suspension.

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

- 25 % or more of the reports submitted for validation within one year are incorrect, invalid or deficient as defined by each validation program;
- more than 60 % of the personnel that participated in the latest (re)accreditation process have left the laboratory; or

- nonconformities are found during any on-site visit and are not addressed through corrective actions taken by the laboratory .

3.11 Denial and revocation of accreditation

This subclause contains no information additional to that provided in NIST Handbook 150, 3.11.

3.12 Voluntary termination of accreditation

This subclause contains no information additional to that provided in NIST Handbook 150, 3.12.

3.13 Appeals

This subclause contains no information additional to that provided in NIST Handbook 150, 3.13.

4 Management requirements for accreditation

4.1 Organization

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. To avoid any conflict of interest, the laboratory policies and procedures shall ensure that neither the applicant laboratory nor other divisions within their parent corporation can perform conformance testing if is currently providing or has previously provided consulting services to the vendor for the SUT (e.g., develop testing evidence, design advice).

NOTE A CST laboratory may perform consulting services to provide clarification of the standards, the Derived Test Requirements, and other associated documents at any time during the life cycle of the SUT.

4.1.2 For any other services of the laboratory's parent corporation not listed in the subclause 4.1.1, the laboratory shall have an explicit policy and a set of procedures 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.

4.1.3 A 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.

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

1. designed any part of the SUT,
2. developed original documentation for any part of the SUT,
3. built, coded or implemented any part of the SUT, or
4. any ownership or vested interest in the SUT.

NOTE Provided that a CST laboratory has met the other requirements, the laboratory may perform conformance testing on SUT produced by a company when:

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

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

4.1.6 For additional guidance on laboratory organization, additional interpretations and clarifications concerning the conflict of interest and strategies for avoiding it, consult also the guidance provided by each validation program. If any discrepancy in the provided information regarding accreditation process and/or conflict of interest rises, NVLAP's guidance supersedes any other program-specific documentation.

4.2 Management system

4.2.1 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.

4.2.2 The laboratory shall comply with all policies and procedures to ensure technical integrity of the conformance testing analyses and results.

4.2.3 The quality system shall provide policy and procedures to ensure routine checks of the competence of the staff involved in the conduct and evaluation of the conformance testing.

4.2.4 The reference documents listed in 1.4, Annex A, and the program's website, as well as any other standards and publications related to the CST LAP, shall be available to all appropriate personnel at all times.

4.3 Document control

The quality manual and related documentation shall include procedures and policies for handling software and maintaining the software's integrity according to the copyright and secrecy status.

4.4 Review of requests, tenders and contracts

4.4.1 The contract review shall be conducted to ensure that a laboratory is capable of providing the service, and that the requirements, rights, and responsibilities of the parties are understood.

4.4.2 If the laboratory conducts testing at clients sites or any selected site other than the laboratory's site accredited for conformance testing, the site shall meet all requirements pertinent to the conformance testing of the SUT as the accredited testing laboratory.

NOTE The laboratory may use checklists and/or contract agreements to satisfy this requirement.

4.4.3 The laboratory shall establish and maintain documented procedures for the review of contracts between the laboratory and clients. Policies for documents storage and maintenance of contracts under confidentiality, non-disclosure agreements, marked as secret, or copyright protected, shall be well defined according to the document's status. These documents shall be protected commensurate with their classification and/or sensitivity, and access to them shall be given only to authorized personnel.

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

- the specific test platform,
- the test configuration, and
- the external environment.

4.5 Subcontracting of tests and calibrations

4.5.1 If the mechanism by which the laboratory employs staff members is through subcontracting, any key personnel who are contractors shall be identified and listed in the laboratory's application for accreditation. When a change in the key personnel employed through subcontracting occurs or when the direct supervision of this category of personnel is not possible, a report shall be submitted to NVLAP and to the affected validation program.

NOTE Any of the above-listed changes in the personnel employed through subcontracting can affect laboratory's accreditation status.

4.5.2 If subcontracting is used as a mechanism by which the laboratory fulfills and/or enhances the conformance testing process, the subcontracting laboratory shall employ either services provided only by NVLAP-accredited laboratories or by laboratories that satisfy all testing requirements as indicated in the NIST Handbook 150, NIST Handbook 150-17 and all documents pertaining to the validation program. In the later instance, the subcontracting laboratory:

1. shall justify the selection explaining why this particular subcontractor was selected and how the subcontractor satisfies the testing requirements; and
2. shall assume full responsibility for the outcome of the conformance testing performed by the subcontractor.

4.6 Purchasing services and supplies

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

4.7 Service to the customer

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

4.8 Complaints

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

4.9 Control of nonconforming testing and/or calibration work

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

4.10 Improvement

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

4.11 Corrective action

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

4.12 Preventive action

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

4.13 Control of records

4.13.1 General

4.13.1.1 The laboratory shall maintain a functional record keeping system for each client. Records shall be readily accessible and complete. Digital media shall be logged and properly marked, and they shall be properly and securely backed-up. Entries in paper-base laboratory notebooks shall be dated and signed or initialed.

4.13.1.2 Digital records shall contain entries of pertinent staff/date information for data as required in the quality manual and, as an established safeguard, shall have means to preserve integrity of records, and shall have means for maintenance without later unauthorized modifications.

4.13.1.3 Software and data protected by non-disclosure 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.

4.13.1.4 The testing laboratory shall take steps to ensure that no third party can gain access to on-line records or to hard copies of he records, either during, or after testing.

4.13.1.5 If a client's system on which testing is conducted is potentially open to access by third parties, the testing laboratory shall ensure that the client controls the testing environment so that the third parties do not gain access to that system during testing.

4.13.1.6 Records of all management system activities including training, internal audits, and management reviews shall be securely saved for future reviews. The integrity of electronic documents shall be insured assure by means commensurate with the data sensitivity. 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 document's integrity and prevent unauthorized changes.

4.13.1.7 Laboratories shall maintain records of the configuration of test equipment and all analyses to ensure the suitability of test equipment to perform the desired testing.

4.13.2 Technical records

4.13.2.1 During the on-site assessment, the records that will be reviewed include, but are not limited to:

1. management system;
2. staff training dates and competency reviews;
3. validation program-specific software versions and updates;
4. versions and updates of mandated testing tools;
5. documentation for mandated testing tools;
6. statement of security policy;
7. conditions for testing when applicable;
8. test equipment and instrumentation calibration (software documentation updates, if applicable);
9. acceptance/rejection of cryptographic and/or security modules, systems or components submitted for test;
10. comprehensive logs for tracking samples and test activities;
11. records of problems with test equipment or system(s), records that demonstrate such equipment or system(s) were removed from service, records of repairs or resolution of problems;
12. test data (including any diagrams, algorithm test suites, photos, and graphic images) and official reports; and
13. correspondence files including questions submitted and responses.

4.13.2.2 The final test results and/or the test reports generated using cryptographic or security testing tools for the SUT shall be kept by the laboratory following the completion of testing for the life of the SUT, or as specified by the client in writing. 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, accessibility and retrievability.

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

4.14 Internal audits

4.14.1 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, in order to audit this technical aspect, an external audit by an appropriate expert shall be necessary.

4.14.2 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, audits shall include, at a minimum, but not be limited to:

1. a review of documentation and instructions,
2. adherence to procedures and instructions, and
3. documentation of the audit findings.

4.15 Management reviews

4.15.1 The laboratory shall perform at least one management review prior to the first full on-site assessment.

4.15.2 The most recent management review report shall be available for review before or during the NVLAP on-site assessment visit.

5 Technical requirements for accreditation

5.1 General

The quality manual shall contain, or refer to documentation that describes and details the laboratory's implementation of procedures covering all of the technical requirements in NIST Handbook 150 and this handbook.

5.2 Personnel

5.2.1 The laboratory shall maintain responsible supervisory personnel and competent administrative and technical staff that are:

1. knowledgeable of all FIPS and NIST Special Publications (SP) listed as references in this handbook and on the CST LAP website,

2. familiar with cryptographic terminology and families of cryptographic algorithms and security functions with particular emphasis on the FIPS-approved and NIST-recommended security functions, and
3. familiar with the cryptographic and security testing tools as required by the laboratory's elected scope of accreditation.

5.2.2 The laboratory shall maintain a list of the key personnel designated to satisfy NVLAP requirements, including their assigned roles and a brief summary of their latest training qualifications. The list shall include, but shall not be limited to:

1. laboratory's director,
2. Authorized Representative,
3. Approved Signatories, and
4. key technical persons in the laboratory.

NOTE Significant changes in a laboratory's key technical personnel or facilities may result in a NVLAP monitoring visit(s), and/or suspension of accreditation if the new personnel prove inadequately prepared or unsuited for the job(s). Loss of key personnel without immediate adequate replacement may result in the laboratory's suspension.

5.2.3 The laboratory shall identify a staff member as quality manager with overall responsibility for quality assurance and for maintenance of the quality manual. An individual may be assigned or appointed to serve in more than one position; however, to the extent possible, the laboratory director and the quality manager positions should be independently staffed.

5.2.4 The quality manager shall receive management system training preferably in ISO/IEC 17025. If training is not available in ISO/IEC 17025, minimum training should be acquired in the ISO 9000 series, especially ISO 9001, or equivalent with particular emphasis on internal auditor training.

5.2.5 The laboratory shall have staff members with at least a Bachelor degree in Computer Science, Computer Engineering, Electrical Engineering or similar technical discipline or equivalent experience – such as a minimum of three years experience – in security products, development, testing, and/or evaluation practice. For more details regarding the staff members' required expertise for each validation program, see Annex A.

5.2.6 The laboratory's personnel shall be trained or have three years of direct work experience, prior to accreditation, in the area of information security best practices, security technologies and events relevant to practicing information security.

5.2.7 The laboratory shall ensure adequate training for the laboratory staff as directed in this subclause and in Annex A, for the specific training requirements derived from the laboratory's scope(s) of accreditation. The personnel shall possess knowledge of, or be trained prior to accreditation on/in the areas listed below:

1. general requirements of the test methods, including generation of test reports;
2. system security concepts;

3. physical security;
4. identification and authentication technologies and techniques;
5. familiarity with cryptographic and security terminology;
6. standards compliance;
7. familiarity with all FIPS publications referenced in this document and NIST Handbook 150;
8. operation and maintenance of NVLAP/NIST-mandated testing tools; and
9. familiarity with the Internet and Internet-related software and the ability to locate and securely download references and information from a given website.

5.2.8 The laboratory shall have a detailed, documented description of their training program for new and current staff members. Each new staff member shall be trained for assigned duties. Current staff members shall receive additional training when hardware and/or software are changed, when new security functions are to be tested, when new responsibilities are assigned, or when relevant cryptographic or security FIPS and/or NIST publications are modified or developed. This training shall include applying new test methods, abiding by FIPS and NIST SPs relevant for the laboratory's elected scope(s) of accreditation, and performing required tests. Each staff member may receive training for assigned duties either through on-the-job training, formal classroom study, or another appropriate mechanism.

5.2.9 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.

5.2.10 If more than 60 % of the personnel that participated in the latest (re)accreditation process has left the laboratory, the laboratory shall inform NVLAP. NVLAP will assign a nonconformity to the laboratory due to the inability to demonstrate competence. The laboratory shall address the nonconformity through corrective and preventive actions. NVLAP reserves the right to require a reassessment if considered necessary.

5.2.11 For scope of accreditation and test method-specific requirements additional to those set forth in 5.2, see Annex A.

5.3 Accommodation and environmental conditions

5.3.1 The laboratory shall have adequate facilities to meet the requirements for NVLAP accreditation. This includes facilities for security conformance testing, record-keeping, document storage, and hardware and software storage. The laboratory shall have access to staff training facilities.

5.3.2 The laboratory shall provide a secure system capable of safeguarding proprietary hardware, software, test data, electronic and paper records, and other materials. This system shall protect all proprietary materials and information from laboratory personnel not authorized to perform conformance testing and product evaluation, and/or visitors to the laboratory.

5.3.3 The laboratory shall have its internal networks protected from unauthorized access by external entities, as well as protection against malicious software, worms, viruses, spybots, etc.

5.3.4 If the laboratory is conducting multiple simultaneous validations, a system of separation between products of different customers and conformance testing activities shall be maintained.

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

5.3.6 The laboratory shall meet the environmental requirements specific to cryptographic and security testing specified in the test methods and/or specific DTR.

5.3.7 The testing laboratory shall ensure that, when applicable, the correct version of the NIST/ITL-or NVLAP-provided testing tools are used and that the tools have not been altered in any way that might lead to incorrect results.

5.3.8 For all conformance testing and validations, the laboratory shall ensured that any file containing old results or old test programs on the SUT is isolated from the current test programs and test or validation results.

5.3.9 If a laboratory must conduct conformance testing at the customer site or other location outside the laboratory facility, the environment shall conform, as appropriate, to the requirements for the laboratory site, and shall be checked by the NVLAP-accredited laboratory as a responsible party for the security of the environment and the integrity of all tests and recorded results. For additional information see subclause 4.4.3.

5.3.10 For scope of accreditation and test method specific requirements additional to those set forth in 5.3, see Annex A.

5.4 Test and calibration methods and method validation

5.4.1 General

Tests may be conducted at the client or laboratory site or at another mutually agreed upon site. When testing is performed at a client site, all NVLAP requirements pertaining to equipment and environment as they apply to the tests scheduled outside the laboratory's accredited location, shall apply. Moreover, only the personnel of the NVLAP-accredited laboratory shall perform all actions necessary to conduct the tests and record the results, including the loading, compiling, configuring, and execution of any of the mandated testing tools.

5.4.2 Selection of methods

Laboratories shall use the test methods and tests derived from their scopes of accreditation. For more specific information regarding methods selection for each scope of accreditation, see Annex A.

5.5 Equipment

5.5.1 Testing equipment or verification records shall include, when applicable, the following:

- **a)** equipment name or description;
- **b)** model, style, serial number or other unique identifier;
- **c)** manufacturer;
- **d)** date received and date placed in service;
- **e)** current location, where appropriate;
- **f)** condition when received (e.g., new, used, reconditioned);
- **g)** copy of the manufacturer's instructions, where available;
- **h)** notation of all equipment variables requiring verification;
- **i)** the range of verification;
- **j)** the resolution of the instrument and its allowable error;
- **k)** date of next calibration and/or verification;
- **l)** date and result of last calibration and/or verification;
- **m)** details of maintenance carried out to date and planned for the future;
- **n)** history of any damage, malfunction, modification or repair;
- **o)** identity of the laboratory individual or external service responsible for calibration; and
- **p)** source of reference standard and traceability.

5.5.2 For its scope of accreditation, the laboratory shall have appropriate hardware, software, and computer facilities to conduct cryptographic and security testing. This includes but is not limited to:

- **a)** required software test suites;
- **b)** testing equipment for physical tests; and
- **c)** all special equipment necessary to perform all tests derived from the most current version of the standard.

5.5.3 Special equipment may be necessary for particular test methods as derived from the scope of accreditation. Generic types of equipment and information required for conducting the conformance tests are listed below:

- **a)** standard laboratory bench equipment (see Annex A for more information);
- **b)** digital storage oscilloscope, logic analyzer or at minimum a digital voltmeter (DVM) (to view outputs from ports);
- **c)** tools to perform physical security conformance tests if appropriate (see Annex A for more information); and
- **d)** access to all relevant validated/evaluated products lists.

See Annex A for additional information.

5.5.4 The equipment used for conducting cryptographic and security testing shall be maintained in accordance with the manufacturer's recommendations and in accordance with internally documented laboratory procedures, as applicable. 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 SUT.

5.5.5 A list of the required testing tools for each scope of accreditation is provided in Annex A and/or the CST LAP website. For conformance testing, the laboratory shall own, 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.

5.5.6 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).

5.5.7 For a given test tool, there may be no suitable validation service available outside the testing laboratory to which accreditation is applicable, and no suitable reference implementation that could be used by the testing laboratory to validate the test tool. In this situation, the testing laboratory shall define and document the procedures and methods that it uses to check on the correct operation of the test tool, and provide evidence that these procedures and methods are applied whenever the test tool is modified.

5.5.8 The testing laboratory shall document and follow appropriate procedures whenever a test tool is suspected or found to contain errors which make the tool defective or unfit for use. These procedures shall include establishing that there is a genuine error, reporting the error to the appropriate maintenance authority, withdrawing the test tool or test case(s) from service, as appropriate, correcting the errors, and then revalidating the test tool, as appropriate. If the conformance testing results change for a SUT after correcting the test tool then the information shall be transmitted to the customer and validation authority.

5.5.9 For scope of accreditation and test method-specific requirements additional to those set forth in 5.5, see Annex A.

5.6 Measurement traceability

5.6.1 General

5.6.1.1 For Cryptographic and Security Testing, "traceability" [see 1.5.32] 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, Annex A, and on the CST LAP website. This means that each abstract test case and the associated evaluation methodology are traceable to a specific cryptographic or security requirement listed

in the governing documentary standard, and that the abstract tests cases are achieved via the assertions and associated DTRs documented in the testing tool in use.

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

5.6.1.2 For cryptographic and security testing purposes, "calibration" means verification of correctness and suitability.

5.6.1.3 For scope of accreditation and test method specific requirements additional to those set forth in 5.6, see Annex A.

5.6.2 Calibration

5.6.2.1 Test tools

5.6.2.1.1 Any test tool used to conduct cryptographic and security testing and which is not part of the unit under testing shall be studied in isolation to make sure the tool correctly represents and assesses the test assertions it claims. The laboratory should also examine to ensure that the tool does not interfere with the conduct of the test and does not modify or impact the product under test.

5.6.2.1.2 Validation of the use of the most current version of testing tools shall be assured before conducting a test.

5.6.2.2 Test equipment

5.6.2.2.1 Laboratories shall maintain records of the configuration of test equipment and all analysis to ensure the suitability of test equipment to perform the desired testing.

5.6.2.2.2 If applicable, the equipment used for conducting the conformance tests shall be maintained and recalibrated in accordance with the manufacturer's recommendation, as often as the laboratory's equipment control charts indicate, or as specified in the test method, or as specified below, whichever results in shorter time periods between calibrations.

Apparatus/Instrumentation	*Frequency*
ohmmeters	annually
voltmeters	annually
wattmeters	annually
oscilloscopes	annually
logic analyzer	annually
temperature chamber	annually
IBM-compatible computers	annually

5.6.2.2.3 All calibrations performed in the laboratory shall be executed by properly trained staff using calibrated standards, or through a contract with a competent external calibration service (see NIST Handbook 150, Annex B). All calibrations and characterizations shall be done against reference standards that are traceable to national standards maintained by NIST or by an equivalent foreign national standard authority.

5.6.2.2.4 For calibrations performed in-house, the reference standards used and the environmental conditions at the time of calibration shall be documented for all calibrations. Calibration records and evidence of the traceability of the reference standards used shall be made available for inspection during the on-site visit.

5.6.2.2.5 The calibration of the hardware and software shall be accomplished through:

a) configuration management for all hardware and software, or through
b) a version control system.

5.6.2.2.6 Records shall be kept of the date and extent of all hardware and software upgrades and updates.

5.6.3 Testing

5.6.3.1 The laboratory shall request the most current versions of the CST test tools from the respective program (e.g., CAVP, CMVP, NPIVP), NIST/ITL, or from NVLAP. No CST test tools provided by the accreditation or validation programs shall be redistributed outside the laboratory without written permission from the respective authority.

5.6.3.2 Laboratories shall use the test methods described in the program's specific DTRs. When exceptions are deemed necessary for technical reasons, the client and the validation program shall be informed and details shall be described in the test report. Substantive documentation shall be provided on exceptions taken to the testing tool to ensure that the correct and required precision and interpretation of the test assertion is maintained. When necessary, these reports may be used by the validation authority to update testing tools and the accompanying documentation.

The validation of a test tool is the process of verifying as far as possible that the test tool will behave properly and produce results that are consistent with the specifications of the relevant test suites, with any relevant standards and, if applicable, with a previously validated version of the test tool (see 5.6.2.1).

5.6.3.3 In those technical areas where there is a difference between FIPS requirements and the testing tool's abstract test cases, the testing laboratory shall show how each realization of a test case is derived

faithfully from the governing FIPS, with preservation of assignment of verdicts or measurements to the corresponding sets of observations.

For more details on the specific test methods corresponding to different scopes of accreditation see Annex A and the CST LAP.

5.7 Sampling

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

5.8 Handling of test and calibration items

5.8.1 Laboratories shall protect all products under testing and test tools from modifications of any kind or unauthorized access and use.

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

5.9 Assuring the quality of test and calibration results

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

5.10 Reporting the results

5.10.1 General

The laboratory shall issue test reports of its work which accurately, clearly, and unambiguously present the test conditions, the test setup when varies from the standard protocol, the test results, and all other information necessary to reproduce the test. Any deviations or omissions from the standard shall be clearly indicated. Test reports to clients shall meet contractual requirements in addition to meeting the requirements of NIST Handbooks 150 and 150-17, governing FIPS and other standards. Test reports shall provide all necessary information to permit reproduction of the test and to obtain consistent results.

5.10.2 Test reports

5.10.2.1 If a NIST/ITL-supplied test report tool or other reporting methodologies are provided, the laboratory shall follow those requirements and use those supplied test tools.

5.10.2.2 If the testing laboratory includes comments, analysis or results in a test report that are not covered by the requirements of the governing FIPS, the laboratory shall state clearly which statements are outside the scope of its accreditation.

5.10.2.3 Whenever test cases are such that an analysis of the observations by the testing staff is required in order to interpret the results before stating them in a test report, the testing laboratory shall have objective procedures to be followed by the test operators performing the analysis, sufficient to ensure that the repeatability, reproducibility, and objectivity of the test results can be maintained.

5.10.2.4 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 by the client*

Reports intended for use only by the client shall meet client/laboratory contract obligations and be complete, but need not necessarily meet all Validation Program requirements.

b) *Reports to be submitted to NIST/ITL and CSEC for product validation under a specific Validation Program*

Test reports intended for submission to any of the Validation Programs under the CST LAP shall meet the requirements of the associated DTRs and IG when applicable, as well as the requirements of NIST Handbook 150, NIST Handbook 150-17 and any other programmatic documentation guidance.

5.10.3 Electronic transmission of results to the Validation Programs

5.10.3.1 A laboratory may submit either a printed or an electronic report as instructed by the Validation Program. The 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. A controlled copy of the report shall be placed in the laboratory's records. A mechanism that ensures the control copy's integrity and confidentiality commensurable with the data sensitivity and/or programmatic requirements shall exist.

5.10.3.2 The laboratory shall provide an integrity and confidentiality mechanism commensurable with the data sensitivity and/or programmatic requirements and/or government requirements when electronic delivery of the test reports to the Validation Program is employed. Confidentiality mechanisms shall be employed to ensure that the test report cannot be disclosed to anyone other than the intended recipient(s), while an integrity mechanism shall exist to ensure that the test report is not maliciously modified.

5.10.4 Amendments to test reports and calibration certificates

5.10.4.1 For test reports created for validation purposes and submitted to any Validation Program under the CST LAP, the laboratory shall issue corrections or additions to a test report only by a

supplementary document that is suitably marked and that meets the requirements of the respective Validation Program.

5.10.4.2 For test reports created for purposes other than official SUT 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.

6 Additional requirements

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

Annex A

(normative)

A.1 Additional general information

Annex A provides additional information and requirements as those pertain to each scope of accreditation. A.2 describes the scopes of accreditation available under the CST LAP, and supplements the reference list provided in 1.4 and the terms and definitions list from 1.5 with the scope-specific information. A.3, A.4 and A.5 are structured to map directly to clauses 3, 4, and 5 of the handbook and to provide per scope of accreditation all necessary information and requirements (e.g., A.3.4 "Additional Proficiency testing requirements" supplements the 3.4 "Proficiency testing").

To make a clear distinction between the accreditation program and the validation program and to emphasize the separation of duties for each key player in these processes, NVLAP is including here an informative diagram (see Figure A.1) of the validation process and the rapport between:

- the validation authority (validation program, i.e., CMVP, NPIVP, SCAP),
- the third-party laboratory, and
- the consumers (e.g., U.S. Government agencies)

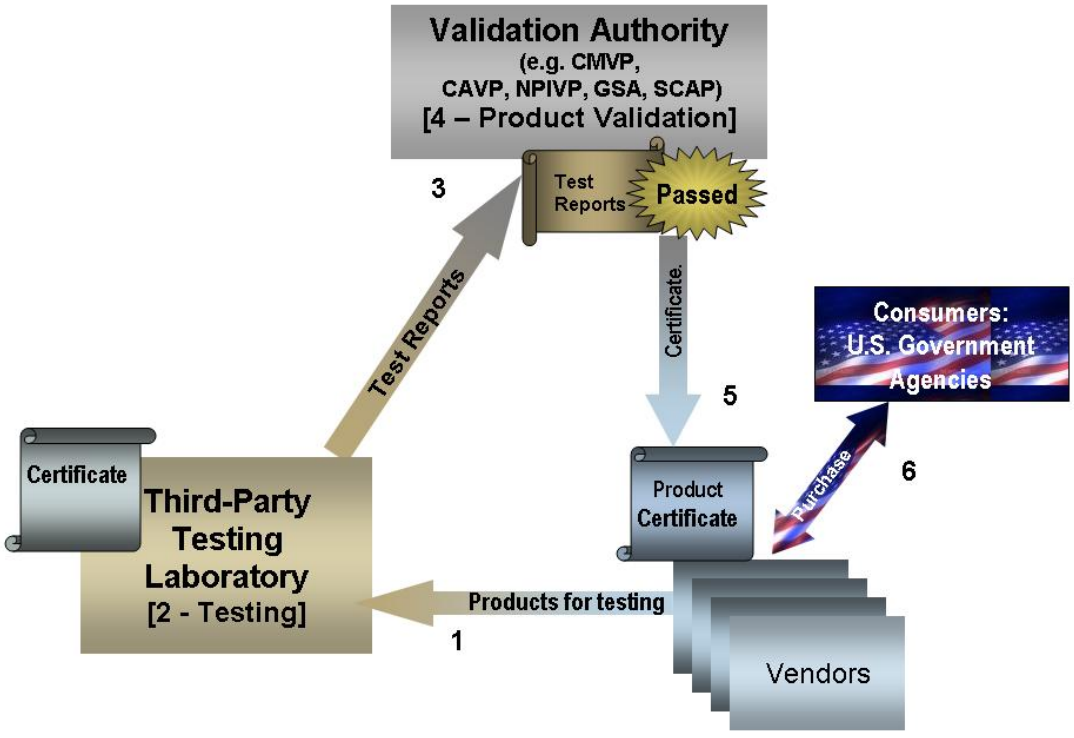


Figure A.1: Validation Process

A.2 Scopes of accreditation, test methods, additional references, terms and definitions

A.2.1 Scopes 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 minimum level of required expertise is described as "Basic Cryptographic and Security (BCS)" testing and is considered the foundation of all scopes of accreditations for the CST LAP. The Basic Cryptographic and Security (17BCS) testing scope is not a standalone scope and it is mandated as a prerequisite for all other scopes.

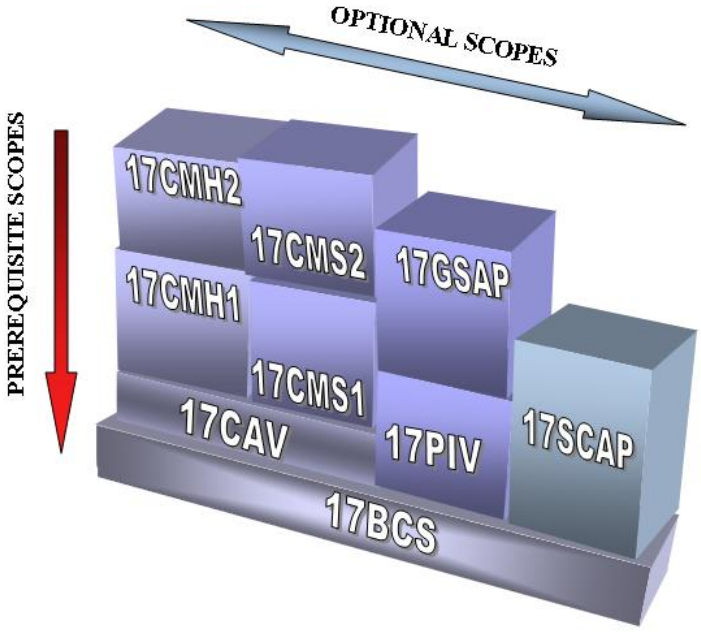
A chained list showing all currently offered scopes of accreditation is presented below. For the most current information on scopes available, see the CST LAP website at:
<http://ts.nist.gov/Standards/Accreditation/CST-LAP.cfm>.

The list below indicates that the election of any descendent scope of accreditation mandates the election of all preceding scopes of accreditation. For example, the selection of the 17CMH2 scope, mandates the selection of the 17CMH1, 17CAV and 17BCS (included automatically) scopes, as well.

☒ **17BCS** Basic Cryptographic and Security Testing

- ☐ **17CAV** Cryptographic Algorithm Validation Testing
  - ☐ **17CMS1** Cryptographic Modules – Software 1 Testing
    (FIPS 140-2 or successor, Security Level 1 to 3)
    - ☐ **17CMS2** Cryptographic Modules – Software 2 Testing
      (FIPS 140-2 or successor, Security Level 4 and above)
  - ☐ **17CMH1** Cryptographic Modules – Hardware 1 Testing
    (FIPS 140-2 or successor, Security Level 1 to 3)
    - ☐ **17CMH2** Cryptographic Modules – Hardware 2 Testing
      (FIPS 140-2 or successor, Security Level 4 and above)
- ☐ **17PIV** Personal Identity Verifier Testing (NPIVP, FIPS 201)
  - ☐ **17GSAP** General Services Administration Precursor Testing
    (GSAP test methods, FIPS 201)
- ☐ **17SCAP** Security Content Automation Protocol Testing
  (SCAP, CVE, CCE, CPE, CVSS, XCCDF and OVAL)

Figure A.2 provides a graphical representation of the list presented above. Also indicated are the dependencies and the compounding rules for the available scopes of accreditation. For example, if the Cryptographic Modules – Software 2 (17CMS2) scope is elected, the Cryptographic Modules – Software 1 testing (17CMS1), Cryptographic Algorithm Validation testing (17CAV) and Cryptographic and Security testing (17BCS) scopes become mandatory prerequisites.



Legend:

17BCS = Basic Cryptographic and Security Testing
17CAV = Cryptographic Algorithm Validation Testing
17CMS1 = Cryptographic Modules – Software 1 Testing (Security Levels 1 to 3)
17CMS2 = Cryptographic Modules – Software 2 Testing (Security Levels 4 and above)
17CMH1 = Cryptographic Modules – Hardware 1 Testing (Security Levels 1 to 3)
17CMH2 = Cryptographic Modules – Hardware 2 Testing (Security Levels 4 and above)
17PIV = Personal Identity Verifier Testing
17GSAP = GSA-Precursor Testing
17SCAP = Security Content Automation Protocol Testing

Figure A.2: Scopes of Accreditations

A.2.2 Test methods

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

A.2.2.1 *Basic Cryptographic and Security Test Methods (17BCS)*

The minimum level of required expertise is described as "Basic Cryptographic Security (BCS)" testing and is considered the foundation of all scopes of accreditations for the CST LAP. The Basic Cryptographic and Security (17BCS) testing scope is not a stand-alone scope and it is mandated as a prerequisite for all other scopes.

A.2.2.2 *Cryptographic Algorithm Validation Testing (17CAV)*

17CAV/01 NIST - Cryptographic Algorithm Validation System (CAVS) for all FIPS-approved and NIST-recommended security functions as required in FIPS 140-2 Annex A (and all superseded versions) –
see http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf.

A.2.2.3 *Cryptographic Modules – Software 1 Testing (17CMS1)*

17CMS1/01 All test methods in accordance with FIPS 140-1, except those listed in 17CMS2/01.

17CMS1/02 All test methods in accordance with FIPS 140-2, except those listed in 17CMS2/02 and CAVS.

NOTE The 17CMS1/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.

A.2.2.4 *Cryptographic Modules – Software 2 Testing (17CMS2)*

17CMS2/01 Test methods for Software Security Level 4, in accordance with FIPS 140-1.

17CMS2/02 Test methods for Software Security Level 4, in accordance with FIPS 140-2.

NOTE The 17CMS2/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.

A.2.2.5 *Cryptographic Modules – Hardware 1 Testing (17CMH1)*

17CMH1/01 All test methods in accordance with FIPS 140-1, except those listed in 17CMH2/01.

17CMH1/02 All test methods in accordance with FIPS 140-2, except those listed in 17CMH2/02 and CAVS.

NOTE The 17CMH1/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.

A.2.2.6 *Cryptographic Modules – Hardware 2 Testing (17CMH2)*

17CMH2/01 Test methods for Physical Security Level 4, in accordance with FIPS 140-1.

17CMH2/02 Test methods for Physical Security Level 4, in accordance with FIPS 140-2.

NOTE The 17CMH2/01 test methods are not available for new products but only for products that have been already validated and must be retested for reasons outside the scope of this document.

A.2.2.7 *Personal Identity Verifier Testing (17PIV)*

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.

A.2.2.8 *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

A.2.2.9 *Security Content Automation Protocol Testing (17SCAP)*

The SCAP scope of accreditation is comprised of six test methods for the testing of the six component standards within SCAP, and a test suite (17SCAP/07) for the six components used in conjunction with, and for the specific capabilities.

17SCAP/01 Common Vulnerability and Exposures (CVE)

17SCAP/02 Common Configuration Enumeration (CCE)

17SCAP/03 Common Platform Enumeration (CPE)

17SCAP/04 Common Vulnerability Scoring System (CVSS)

17SCAP/05 eXtensible Configuration Checklist Document Format (XCCDF)

17SCAP/06 Open Vulnerability Assessment Language (OVAL)

17SCAP/07 Security Content Automation Protocol (SCAP)

A.2.3 Additional references

A.2.3.1 *Additional reference for all Cryptographic Algorithms and Cryptographic Modules Testing Scopes of Accreditation*

— Federal Information Processing Standards Publication FIPS PUB 140-1, *Security Requirements for Cryptographic Modules* (see http://csrc.nist.gov/publications/fips/fips140-1/fips1401.pdf).

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

— Derived Test Requirements for FIPS 140-1
(see http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-1/1401test.pdf.)

— Derived Test Requirements (DTR) for FIPS 140-1 APPENDIX A, *A Cryptographic Module Security Policy* (see. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-1/1401testA.pdf).

— Implementation Guidance for FIPS 140-1 and the Cryptographic Module Validation Program (see http://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 http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexa.pdf).

— Annex B: Approved Protection Profiles for FIPS 140-2, *Security Requirements for Cryptographic Modules* (see http://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 http://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 http://csrc.nist.gov/publications/fips/fips140-2/fips1402annexd.pdf).

— Derived Test Requirements (DTR) for FIPS 140-2 APPENDIX A, *A Cryptographic Module Security Policy* (see. http://csrc.nist.gov/groups/STM/cmvp/documents/fips140-2/1402DTR.pdf).

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

A.2.3.2 *Additional references for the Personal Identity Verifier Testing (17PIV) Scope of Accreditation*

— FIPS 201 or successors, Personal Identity *Verification for Governmental Employees and Contractors*, 2005 or successor, http://csrc.nist.gov/publications/fips/fips201-1/FIPS-201-1-v5.pdf.

NIST Special Publications (SP) and tools for PIV

All NIST Special Publications (SP) listed below are available for download at the following site: http://csrc.nist.gov/publications/nistpubs.

— NIST SP 800-18, Guide for Developing Security Plans for Federal Information Systems, Revision 1, February 2006 or latest. http://csrc.nist.gov/publications/nistpubs/800-18-Rev1/sp800-18-Rev1-final.pdf

— NIST SP 800-21-1, Guideline for Implementing Cryptography in the Federal Government, second edition, NIST, December 2005 or latest. http://csrc.nist.gov/publications/nistpubs/800-21-1/sp800-21-1_Dec2005.pdf

— NIST SP 800-53, Recommended Security Controls for Federal Information Systems, February 2005 or latest. http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

— NIST SP 800-57, Recommendation for Key Management - Part 1, General, NIST, March 2007. http://csrc.nist.gov/publications/nistpubs/800-57/sp800-57-Part1-revised2_Mar08-2007.pdf

— NIST SP 800-57, Recommendation for Key Management - Part 2, Best Practices for Key Management Organization, NIST, August 2005 or latest. http://csrc.nist.gov/publications/nistpubs/800-57/SP800-57-Part2.pdf

— NIST SP 800-73 (Revision 1: 800-73-1), Interfaces for Personal Identity Verification, NIST, March 2006 or latest http://csrc.nist.gov/publications/nistpubs/800-73-1/sp800-73-1v7-April20-2006.pdf

— NIST Errata for NIST SP 800-73-1, NIST, May 2006. http://csrc.nist.gov/publications/nistpubs/800-73-1/Errata-for-sp800-73-1-050206.pdf

— NIST SP 800-76, Biometric Data Specification for Personal Identity Verification, NIST, January 2007 or latest. http://csrc.nist.gov/publications/nistpubs/800-76-1/SP800-76-1_012407.pdf

— NIST SP 800-78 or successors, Cryptographic Standards and Key Sizes for Personal Identity Verification, NIST, April 2005 or latest. http://csrc.nist.gov/publications/nistpubs/800-78/sp800-78-final.pdf

— NIST SP 800-79, Guidelines for the Certification and Accreditation of PIV Card Issuing Organizations, NIST, July 2005 or latest. http://csrc.nist.gov/publications/nistpubs/800-79/sp800-79.pdf

— NIST SP 800-85A, PIV Card Application and Middleware Interface Test Guidelines, NIST, April 2006 or later. http://csrc.nist.gov/publications/nistpubs/800-85A/SP800-85A.pdf

— NIST SP 800-96, or successor, PIV Card / Reader Interoperability Guidelines.

— Cryptographic Module Interface conformance tool for NPIVP.

ISO/IEC standards for PIV

— ISO/IEC 7810;
— ISO/IEC 7816;
— ISO/IEC 14443;
— ISO/IEC 10373.

Other references for PIV

— ANSI INCITS 322, *Card Durability Tests Methods*, 2002 or later.

A.2.3.3 *Additional references for the General Services Administration Precursor Testing (17GSAP) Scope of Accreditation*

— HSPD 12, *Policy for a Common Identification Standard for Federal Employees and Contractors*, August 27, 2004, http://www.whitehouse.gov/news/releases/2004/08/20040827-8.html

— NIST SP 800-85B, *PIV Data Model Conformance Test Guidelines*, NIST, July 2006, http://csrc.nist.gov/publications/nistpubs/800-85B/SP800-85b-072406-final.pdf

— FIPS 201 Evaluation Program - Authentication Key Reader Test Procedure, v 3.0.0.0 or later
— FIPS 201 Evaluation Program - Biometric Reader Test Procedure, v 3.0.0 or later
— FIPS 201 Evaluation Program - CHUID Reader (Contact) Test Procedure, v 3.0.0 or later
— FIPS 201 Evaluation Program - CHUID Reader (Contactless) Test Procedure, v 3.0.0 or later
— FIPS 201 Evaluation Program - CHUID Authentication Reader (Contact) Test Procedure, v 1.0.0 or later
— FIPS 201 Evaluation Program - CHUID Authentication Reader (Contactless) Test Procedure, v 1.0.0 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 3.0.0 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 4.0.0 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

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).

A.2.3.4 *Additional references for the Security Content Automation Protocol Testing (17SCAP) Scope of Accreditation*

NIST Special Publications (SP) for SCAP

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

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

Other references for SCAP

— *Security Content Automation Protocol (SCAP) Derived Test Requirements*, the latest version from http://scap.nist.gov.

— *Security Content Automation Protocol Testing Implementation Guidance*, the latest version from http://scap.nist.gov.

— The Common Vulnerability Scoring System (CVSS) and Its Applicability to Federal Agency Systems, NIST IR-7435 - see http://scap.nist.gov.

— Specification for the Extensible Configuration Checklist Description Format (XCCDF) - see http://scap.nist.gov.

— *Common Platform Enumeration (CPE) – Specification* – see http://scap.nist.gov.

— *Common Vulnerabilities and Exposures (CVE)* - see http://scap.nist.gov.

— *Common Configuration Enumeration (CCE)* - see http://scap.nist.gov.

— *Open Vulnerability Assessment Language (OVAL)* - see http://scap.nist.gov.

A.2.4 Additional terms and definitions

A.2.4.1

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

A.2.4.2

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

A.2.4.3

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

A.2.4.4

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

A.2.4.5

CRYPTIK
Cryptographic Module Validation Test Documentation Tool.

A.2.4.6

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.

A.2.4.7

METRIX
Software tool used for collecting CMVP and CAVP metrics.

A.2.4.8

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

A.2.4.9

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.

A.3 Additional accreditation process requirements

A.3.1 Additional initial accreditation requirements

A.3.1.1 *Additional Initial Accreditation Requirements for the 17CMH1 and 17CMS1 Scopes of Accreditation*

In order for a NVLAP laboratory to qualify for any of the Cryptographic Modules – Software and/or Hardware scopes of accreditation, Security Levels 1 to 3 (17CMS1 and/or 17CMH1), the laboratory shall become accredited under NVLAP in the Cryptographic Algorithm Validation Testing (17CAV) scope, in the 17CAV/01 test method listed herein, or in the most current list from the CST LAP website.

A.3.1.2 *Additional Initial Accreditation Requirements for the 17PIV Scope of Accreditation*

All laboratories applying for the 17PIV scope of accreditation shall be able to perform accreditation tests according to FIPS 140-2 or successors to an overall Security Level 2 (or higher) and a physical Security Level 3, as the cryptographic modules in the PIV systems (both on-card and issuer software) are required to be validated to FIPS 140-2 with an overall Security Level 2 (or higher) while the PIV Card is required to provide Level 3 physical security to protect the PIV private keys in storage.

A.3.1.3 *Additional Initial Accreditation Requirements for the 17GSAP Scope of Accreditation*

In order for a NVLAP laboratory to qualify as a General Services Administration (GSA) FIPS 201 Evaluation Laboratory, the laboratory shall become accredited under NVLAP in the GSA FIPS 201 test methods, scope 17GSAP, in 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 can accredit. In addition, the applicant laboratory shall satisfy other laboratory and business requirements as specified by GSA.

All laboratories applying for the 17GSAP scope of accreditation shall:

- firstly, become accredited under NVLAP as a Basic Cryptographic and Security Testing (17BCS) laboratory;
- secondly, become accredited under NVLAP as a NPIVP Testing Laboratory, in both 17PIV/01 and 17PIV/02 test methods.

A.3.2 Additional activities prior to initial on-site assessment

There are no additional requirements other than those provided in clause 3.2 of this document.

A.3.3 Additional on-site assessment requirements

There are no additional requirements other than those provided in clause 3.3 of this document.

A.3.4 Additional proficiency testing requirements

NVLAP, in collaboration with all CST validation programs, considers the validation reports submitted to the validation programs as ongoing proficiency tests. A large number of flaws in the reports submitted to any of the validation programs can trigger the laboratory's suspension or revocation of the accreditation. For more information see 3.10.

A.3.4.1 *Additional proficiency testing requirements for the 17CAV, 17CMH and17CMS scopes of accreditation*

The proficiency artifact or operational exam for the 17CMH1, 17CMH2, 17CMS1 and 17CMS2 scopes of accreditation will require proof of the laboratory's ability to use *CRYPTIK* that has been pre-populated with data by the NIST/ITL. The laboratory shall demonstrate that all appropriate personnel are familiar with the procedures for resetting the pass/fail indicators for each pre-validated test.

A.3.4.2 *Additional proficiency testing requirements for the 17PIV scope of accreditation*

Proficiency testing for the 17PIV scopes of accreditation 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 with the tools, are capable of configuring the tools, running the conformance tests, verifying the results and generating the report.

A.3.4.3 *Additional proficiency testing requirements for the 17GSAP scope of accreditation*

Proficiency testing for the 17GSAP scope of accreditation will require proof of the laboratory's competence to set up and configure a testing hardware and software 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.

A.3.4.4 *Additional proficiency testing requirements for the 17SCAP scope of accreditation*

Proficiency testing for the 17SCAP scope of accreditation will require proof of the laboratory's competence to set up and configure a testing hardware and software environment as instructed in the test. Using a sample artifact provided by NIST/CSD, 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.

A.4 Additional management requirements for accreditation

There are no additional requirements other than those provided in clause 4 of this document.

A.5 Additional technical requirements for accreditation

A.5.1 General

The laboratory's quality manual shall contain or reference procedures and instructions covering the technical requirements for each scope of accreditation and corresponding test methods.

A.5.2 Additional personnel requirements

For a laboratory to qualify for accreditation under the CST LAP, the laboratory shall prove, in addition to the technical expertise required by each scope of accreditation as described below, that their personnel has 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.

A.5.2.1 *Additional personnel requirements for the 17CAV, 17CMH and17CMS scopes of accreditation*

The laboratory's personnel shall have experience or be trained prior to accreditation 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)** familiarity with the families of cryptographic algorithms;
- **f)** FIPS-approved and NIST-recommended security functions (FIPS 140-2 or successors);

g) voltage and temperature measurement (Environmental Failure Protection/Environmental Failure Testing (EFP/EFT) for Security Level 4 testing only, as defined in FIPS 140-2 or successors);
h) finite state machine model analysis;
i) production grade, tamper evident, and tamper detection techniques;
j) software design specifications, including high-level languages and formal models.

A.5.2.2 *Additional personnel requirements for the 17PIV and 17GSAP scopes of accreditation*

The laboratory personnel shall have experience or be trained prior to accreditation 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) familiarity with the families of cryptographic algorithms;
f) FIPS-approved and NIST-recommended security functions (FIPS 140-2 or successors);
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.

A.5.2.3 *Additional personnel requirements for the 17SCAP scope of accreditation*

The laboratory personnel shall have experience or be trained prior to accreditation in:

a) basic knowledge of vulnerability and configuration management (NIST SP 800-40 v2 or later and NIST SP 800-100);
b) basic knowledge of XML and how to read XML documents (W3C Extensible Markup Language (XML) 1.1 (Second Edition) or later);
c) familiarity with all SCAP standards (CVE, CCE, CPE, CVSS, XCCDF, OVAL) – latest versions (for more information see http://scap.nist.gov);
d) familiarity with Virtual Machines (VM) Virtual Hard Disks (VHD).

A.5.3 Additional accommodation and environmental conditions

There are no additional requirements to those provided in 5.3.

A.5.4 Additional test and calibration methods and method validation

There are no additional requirements to those provided in 5.4.

A.5.5 Additional equipment requirements

A.5.5.1 *Additional equipment requirements for the 17CAV, 17CMH and17CMS scopes of accreditation*

The laboratory applying for accreditation for the 17CAV, 17CMH or 17CMS scopes of accreditation shall own at least one designated IBM[1)] compatible PC equipped with, at minimum, a compact disk rewritable (CD-RW) drive or other secure digital storage media and running Microsoft Windows XP[1)] (or later) or compatible.

The laboratory shall also meet the following minimum hardware and software requirements, including the operating system requirements for the platform on which *CRYPTIK* will run:

a) Hardware:
- **1.** power supplies (set of variable power supplies if accreditation for Level 4 is desired);
- **2.** temperature chamber (only if accreditation for Level 4 is desired);
- **3.** formal model texts (only if accreditation for Level 4 is desired);
- **4.** at least 100 MB of available space on the hard disk;
- **5.** X-Acto "Type" knives (including various blades);
- **6.** strong artificial light source (Wavelength range of 400 nm to 750 nm);
- **7.** magnifying glass;
- **8.** Dremmel[1)] "Type" rotary tool (including accessory bits: cutting, grinding, drilling, carving, etc.);
- **9.** jeweler's screwdrivers (e.g., flat, Phillips, Robertson, torx, hex key);
- **10.** dentist picks and mirrors;
- **11.** hobbyist saw;
- **12.** small pliers (e.g., needle nose, standard nose, long nose, curved nose, side cutters);
- **13.** hammer;
- **14.** chisels;
- **15.** fine (small) files;
- **16.** hair dryer/ heat source;
- **17.** Volt-Ohm-Meter (VOM) or Digital Multi-Meter (DMM) (basic functions to include an ammeter, voltmeter and ohmmeter);
- **18.** digital camera;
- **19.** digital scanner;
- **20.** printer;
- **21.** miscellaneous protection equipment for chemical testing (e.g., goggles, gloves) – optional.

b) Software:
- **1.** appropriate compilers;
- **2.** a NIST/ITL-originated copy of *CRYPTIK* (latest version);
- **3.** a NIST/ITL-originated copy of *CAVS* (latest version);
- **4.** a CSEC-originated copy of *METRIX* (latest version).

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

A.5.5.2 *Additional equipment requirements for the 17PIV scope of accreditation*

.

The laboratory applying for accreditation for the 17PIV scope of accreditation shall own at least one designated IBM compatible PC[1)] equipped with, at minimum, a compact disk rewritable (CD-RW) drive or other secure digital storage media and running Microsoft Windows XP[1)] (or later) or compatible.

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-CTTK* and *Test Runner*) will run:

a) Hardware:
   1. a test computer running Windows XP[1)] 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;
   4. a printer for reporting and documenting the test results;

b) Software:
   1. SUN[1)] Microsystems Java Runtime Environment (JRE) version 1.5 or later,
   2. *Java Cryptography Extension* (JCE) Unlimited Strength Jurisdiction Policy Files 5.0";
   3. *PIV Card Application* and *PIV Middleware* test toolkit application software provided by NIST/ITL or NVLAP (version 2.9.8 or later).

A.5.5.3 *Additional equipment requirements for the 17GSAP scope of accreditation*

Supplemental to the additional equipment requirements listed for 17PIV scope of accreditation (section A.5.5.2, the laboratory applying for accreditation for the 17GSAP scope of accreditation 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[1)];
   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;
   5. tools needed for the breakout box:
      - Drill,
      - Screw driver,
      - Glue.

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

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. Crpto++ 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[1)] (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.

A.5.5.4 *Additional equipment requirements for the 17SCAP scope of accreditation*

The laboratory applying for accreditation for the 17SCAP scope of accreditation shall be equipped with IBM compatible PC(s) that meet the following minimum hardware, software and operating system requirements:

a) Hardware:

1. 1 GHz or better, virtualization enabled CPU (examples: Intel Core 2 Duo with VT);
2. 2 GB of RAM;
3. 100 GB of available Hard Disk Space.

b) Operating Systems:

1. Microsoft Windows XP SP2 (or later) or Microsoft Windows Vista.

c) Software:

1. Sun Java Runtime Environment (JRE) 1.5 or later;
2. Microsoft Virtual PC (VPC) available at http://www.microsoft.com/virtualpc;
3. XML capable viewer/editor;
4. CPE Validation Utility (provided by NIST/CSD);
5. a set of Virtual Hard Drives (VHD) (provided by NIST/CSD).

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

A.5.6 Additional measurement traceability

A.5.6.1 *Additional general requirements*

There are no additional requirements to those provided in 5.6.1 of this document.

A.5.6.2 *Additional calibration requirements*

There are no additional requirements to those provided in 5.6.2. of this document.

A.5.6.3 *Additional testing requirements*

A.5.6.3.1 Additional testing requirements for the 17CAV, 17CMH and 17CMS scopes of accreditation

The traceability of the abstract test cases is assured through the use of *CRYPTIK*. Traceability to the requirements in the FIPS 140-2 (or successor) documentary standard is achieved via the assertions, the associated DTRs documents and the *CRYPTIK* tool. The assertions are direct quotes from FIPS 140-2 (or successors). The DTRs are divided into two sets of requirements: one levied on the vendor and one levied on the tester of the cryptographic module.

In those technical areas where there is a difference between FIPS 140-2 (or successor) requirements and the *CRYPTIK* tool, the testing laboratory shall show how each realization of a test is derived faithfully from FIPS 140-2 (or successor), with preservation of assignment of verdicts or measurements to the corresponding sets of observations.

When testing is performed at the client site or other mutually agreed upon site, only the laboratory personnel shall perform use the *CRYPTIK* tool.

Laboratories shall use the test methods described in the document *140-2: Derived Test Requirements* (or successor), with clarifications provided in the document *140-2: Implementation Guidance* (or successor). When exceptions are deemed necessary for technical reasons, the client shall be informed and details shall be described in the test report. Substantive documentation shall be provided on exceptions taken to *CRYPTIK* to ensure that the correct and required precision and interpretation of the test assertion are maintained. When necessary, laboratory's reports may be used to update *CRYPTIK* and the accompanying documentation.

Test results created for cryptographic algorithm testing shall include the values generated by the SUT.

Laboratories shall use the test methods and tests for the security functions listed at the website http://csrc.nist.gov/groups/STM/cmvp/index.html.

All Systems-Under-Test (SUT) accepted for validation shall meet all federal regulations including the Federal Communication Commission (FCC) regulations.

Questions regarding the FCC regulations and FCC requirements may be directed to the FCC, Office of Engineering and Technology Laboratory at < labinfo@fcc.gov >.

The U.S Code of Federal Regulations may be found at < http://www.gpoaccess.gov/nara/index.html >.

A.5.6.3.2 Additional testing requirements for the 17PIV scope of accreditation

Laboratories shall use the test methods and tests listed in the NIST SP 800-85A*: PIV Card Application and Middleware Interface Test Guidelines* (or successors) for conformance testing of the PIV card application and PIV middleware. For additional clarifications, check the documentation listed on the NPIVP website < http://npivp.nist.gov >.

FIPS 201 Appendix B.3 specifies that a PIV system/component is "*FIPS 201-compliant*" after each of SUT'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 through NPIVP, and
- cryptographic module validation for FIPS 140-2 *Security Requirements for Cryptographic Modules* (or successors) conformance of the cryptographic module that hosts the PIV card application.

A.5.6.3.3 Additional testing requirements for the 17GSAP scope of accreditation

Laboratories shall use the test methods listed at the website http://fips201ep.cio.gov/contact.php under the "*Test Procedures*".

Prior to testing the SUT, the laboratory shall create an inventory list with all the equipment received and tag all systems. The SUT shall be NPIVP-certified before being considered for the GSA EP conformance testing, as the NPIVP is a prerequisite to the GSAP program.

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

1. Approval Procedure,
2. Test Procedures, and
3. Evaluation Report

The core function of a GSAP laboratory is to analyze and evaluate the SUT 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 SUT should be approved.

Annex B

(informative)

The following acronyms and abbreviations are used throughout this handbook:

APDU: Application Protocol Data Unit

BCS: Basic Cryptographic and Security

BER: Basic Encoding Rules

CAVP: Cryptographic Algorithm Validation Program

CAVS: Cryptographic Algorithm Validation System

CCE: Common Configuration Enumeration

CHUID: Card Holder Unique Identifier

CMT LAP: Cryptographic Module Testing Laboratory Accreditation Program

CMVP: Cryptographic Module Validation Program

CST LAP: Cryptographic and Security Testing Laboratory Accreditation Program

CPE: Common Platform Enumeration

CSD: Computer Security Division

CSEC: Communications Security Establishment Canada

CVE: Common Vulnerabilities and Exposures

CVSS: Common Vulnerability Scoring System

DMM: Digital Multi-Meter

DTR: Derived Test Requirements

DVM: Digital Voltmeter

FIPS: Federal Information Processing Standard

GB: Gigabytes

GSA EP: General Service Administration Evaluation Program

GSAP: General Service Administration Precursor

IEC: International Electrotechnical Commission

IG: Implementation Guidance

ISO: International Organization for Standardization

ITL: Information Technology Laboratory

JRE: Java Runtime Environment

MB: Megabytes

NPIVP: NIST Personal Identity Verification Program

NVLAP: National Voluntary laboratory Accreditation Program

OSAR: On-Site Assessment Report

OVAL: Open Vulnerability Assessment

PIV: Personal Identity Verification

PKI: Public Key Infrastructure

QM: Quality Manual

SCAP: Security Content Automation Protocol

SP: Special Publication

SUT: System-Under-Test

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