




Standards Council of Canada
Conseil canadien des normes



Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities

CAN-P-1621
November 2006

REQUIREMENTS FOR THE ACCREDITATION OF CRYPTOGRAPHIC MODULE AND ALGORITHM TESTING FACILITIES

***EXIGENCES RELATIVES À L'ACCREDITATION DES
INSTALLATIONS D'ESSAIS DE MODULES ET D'ALGORITHMES
CRYPTOGRAPHIQUES***

CAN-P-1621

November 2006

Copyright © Standards Council of Canada, 2006

All rights reserved. No part of this publication may be reproduced, stored in a retrieval system, or transmitted, in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of the publisher:



Standards Council of Canada
270 Albert Street, Suite 200
Ottawa, Ontario
K1P 6N7
Canada
Tel.: (613) 238-3222
Fax.: (613) 569-7808
Internet: info@scc.ca

NOTE : On peut obtenir un exemplaire anglais de ce document en écrivant au :

Conseil canadien des normes
270 rue Albert, bureau 200
OTTAWA (Ontario)
K1P 6N7
Tél.: (613) 238-3222
Fax.: (613) 569-7808
Courriel: info.palcan@scc.ca
Site web: www.scc.ca

NOTE: An English version of this document is available from the:

Standards Council of Canada
270 Albert Street, Suite 200,
OTTAWA, Ontario
K1P 6N7
Tel.: (613) 238-3222
Fax.: (613) 569-7808
Email: info.palcan@scc.ca
Website: www.scc.ca

TABLE OF CONTENTS

FOREWORD	I
PREFACE	II
INTRODUCTION	1
GENERAL REQUIREMENTS	4
1 REFERENCES.....	4
2 DEFINITIONS.....	6
3 SCOPE OF ACCREDITATION	7
4 DEMONSTRATING TECHNICAL COMPETENCE.....	8
4.1 <i>Composition of the Assessment Team</i>	8
4.2 <i>Preparation of On-Site Assessment</i>	8
4.3 <i>Proficiency Testing</i>	8
4.4 <i>On-Site Assessment</i>	9
4.5 <i>Accreditation</i>	11
4.6 <i>Denying, Suspending and Withdrawing Accreditation</i>	11
5 AMPLIFICATION OF CAN-P-1591B REQUIREMENTS.....	11
5.1 <i>General</i>	11
5.2 <i>Organization [CAN-P1591B Section 5.2]</i>	11
5.3 <i>Quality System [CAN-P1591B Section 5.3]</i>	11
5.4 <i>Review of Requests, Tenders and Contracts [CAN-P-1591B Section 5.4]</i>	12
5.5 <i>Control of Records [CAN-P1591B Section 5.5]</i>	12
5.6 <i>Personnel [CAN-P1591B Section 5.6]</i>	12
5.7 <i>Accommodation and Environmental Conditions [CAN-P1591B Section 5.7]</i>	14
5.8 <i>Test and Calibration Methods and Method Validation [CAN-P1591B Section 5.8]</i>	14
5.9 <i>Equipment [CAN-P1591B Section 5.9]</i>	14
5.10 <i>Measurement Traceability [CAN-P1591B Section 5.10]</i>	15
5.11 <i>Reporting the Results [CAN-P1591B Section 5.11]</i>	15

FOREWORD

The Standards Council of Canada ("Council") is a crown corporation established by an Act of Parliament in 1970, amended in 1996, to foster and promote efficient and effective voluntary standardization in Canada. It is independent of government in its policies and operations, although it is financed partially by Parliamentary appropriation. The Council consists of members from government and the private sectors.

The mandate of the Council is to promote the participation of Canadians in voluntary standards activities, promote public-private sector cooperation in relation to voluntary standardization in Canada, coordinate and oversee the efforts of the persons and organizations involved in the National Standards System, foster quality, performance and technological innovation in Canadian goods and services through standards-related activities, and develop standards-related strategies and long-term objectives.

In essence, the Council promotes efficient and effective voluntary standardization in Canada in order to advance the national economy, support sustainable development, benefit the health, safety and welfare of workers and the public, assist and protect consumers, facilitate domestic and international trade and further international cooperation in relation to standardization.

In addition, the Council serves as the government's focal point for voluntary standardization and represents Canada in international standardization activities, sets out policies and procedures for the development of National Standards of Canada, and for the accreditation of standards development organizations, of product certification bodies, of testing and calibration laboratories, of quality and environmental management systems registration bodies and of quality management systems and environmental auditor certifiers and training course providers, and promotes and supports the principle of recognition of accreditation or equivalent systems as a means of decreasing the number of multiple assessments and audits, both in Canada and with Canada's trading partners.

This document is one of several issued by the Standards Council of Canada to define the policies, plans, and procedures established by the Council to help achieve its mandate.

Requests for clarification and recommendations for amendment of this document, or requests for additional copies should be addressed to the publisher directly.

PREFACE

CAN-P-1621 presents the specific requirements of the Standards Council of Canada for testing facilities seeking accreditation for conformance testing of cryptographic modules conducted against FIPS PUB 140-2 *Security Requirements for Cryptographic Modules*. The FIPS 140-2 standard has been developed by the National Institute for Standards and Technology of the Government of the United States and the Communications Security Establishment of the Government of Canada.

This document is intended for information and use by accreditors, staff of accredited cryptographic module and algorithm testing facilities, those facilities seeking accreditation, other laboratory accreditation systems, customers of facility services and organizations or individuals needing information about the requirements for accreditation under the Cryptographic Module and Algorithm Testing Facilities accreditation program.

This document is a specific guideline document that amplifies CAN-P-1591B: 2001, *Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities*. Technical requirements are explained to indicate how these specific guidelines are applied.

Any facility (including commercial, manufacturer, university, and federal or provincial government laboratory) that performs any of the test methods that comprise the cryptographic module and algorithm testing may apply for SCC accreditation. Accreditation will be granted to a facility that conforms to the requirements for accreditation as defined in this document and those of PALCAN Handbook, *Program for the Accreditation of Laboratories Canada*. Accreditation does not imply a guarantee of facility performance or of product test data; it is a finding of facility competence.

The terms *laboratory* and *testing facility* are used interchangeably through this document and are considered synonyms.

INTRODUCTION

a) **Cryptographic Module Validation Program**

On July 17, 1995, the National Institute of Standards and Technology (NIST), Department of Commerce, Government of the United States and the Communications Security Establishment (CSE) announced the establishment of the Cryptographic Module Validation Program (CMVP). The Cryptographic Module Validation Program will validate commercial products for conformance to FIPS 140-2, *Security Requirements for Cryptographic Modules*. Products validated by this program will be accepted for use in both Canada and the United States for the protection of sensitive, unclassified information.

The CMVP requires accredited, independent, third-party testing facilities to test products for FIPS 140-2 validation. The National Voluntary Laboratory Accreditation Program (NVLAP) of NIST historically accredits testing facilities for meeting the requirements contained in NIST Handbook 150, *NVLAP Procedures and General Requirements* and NIST Handbook 150-17 *Cryptographic Module Testing*.

CAN-P-1621 provides accreditation of testing facilities under the Standards Council of Canada (SCC) to perform conformance testing to the FIPS 140-2 and be recognized under the CMVP.

b) **FIPS 140-2 Security Requirements for Cryptographic Modules**

The FIPS 140-2 specifies the security requirements that are to be satisfied by a cryptographic module utilized within a security system protecting unclassified information within computer and telecommunication systems (including voice systems). The security requirements cover areas related to the secure design and implementation of a cryptographic module. These areas include basic design and documentation, module ports and interfaces, authorized roles, services and authentication, physical security, software security, operational environment, cryptographic key management, electromagnetic interference/electromagnetic compatibility (EMI/EMC), self-testing, design assurance and mitigation of other attacks.

FIPS 140-1 has been in effect since January 1994 and has recently been revised by NIST and CSE to realign the standard with current technology. This revision occurs every five years. The revised standard has been labeled as FIPS 140-2 *Security Requirements for Cryptographic Modules*.

c) CAN-P-1621 Requirements for the Accreditation of Cryptographic Module and Algorithm Testing Facilities

CAN-P-1621 specifies the requirement specific to cryptographic module and algorithm testing for conformance testing to FIPS 140-2. The generic testing facility requirements specified in Handbook 150 and Handbook 150-17 were identified and mapped to the requirements specified in PALCAN, CAN-P-4E and CAN-P-1591B. The remaining requirements were specific to cryptographic module and algorithm testing and were grouped in this document. Therefore, the linking of the requirements specified in CAN-P-4E, CAN-P-1591B and CAN-1621 maps all requirements specified in Handbook 150 and Handbook 150-17. Figure 1 illustrates the requirements mapping.

The purpose of this document is to establish the requirements, additional to those given in CAN-P-4E and in CAN-P-1591B in technical and organizational matters, for testing facility accreditation for conformance testing of cryptographic modules conducted in accordance with FIPS PUB 140-2, *Security Requirements for Cryptographic Modules* and conformance testing of associated cryptographic algorithms.

CAN-P-1622 *Checklist for the Assessment of Cryptographic Module and Algorithm Testing Facilities* is the checklist to be used for the assessment of testing facilities for conformance to the requirements specified in this document.

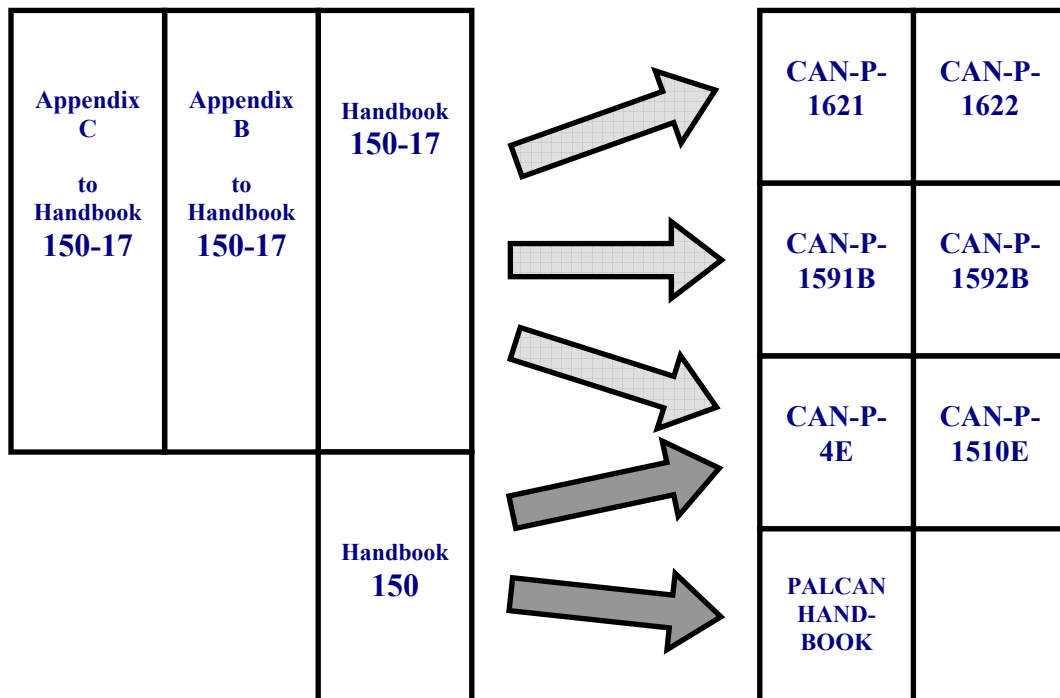


Figure 1 – Requirements mapping from NIST Handbooks to SCC document

d) SCC Accreditation Framework

SCC has elaborated an accreditation framework where a standard supplements other more general standards. Refer to Figure 2 below. PALCAN (not shown) describes the testing facility accreditation process. CAN-P-4E specifies the general requirements that every testing facility needs to meet to become such a facility. CAN-P-1591B supplements CAN-P-4E for the Information Technology Security Evaluation and Testing (ITSET) specialty area. This document further specifies the requirements an ITSET facility must meet to perform cryptographic module and algorithm testing. This framework provides the possibility of adding other specialized areas of testing.

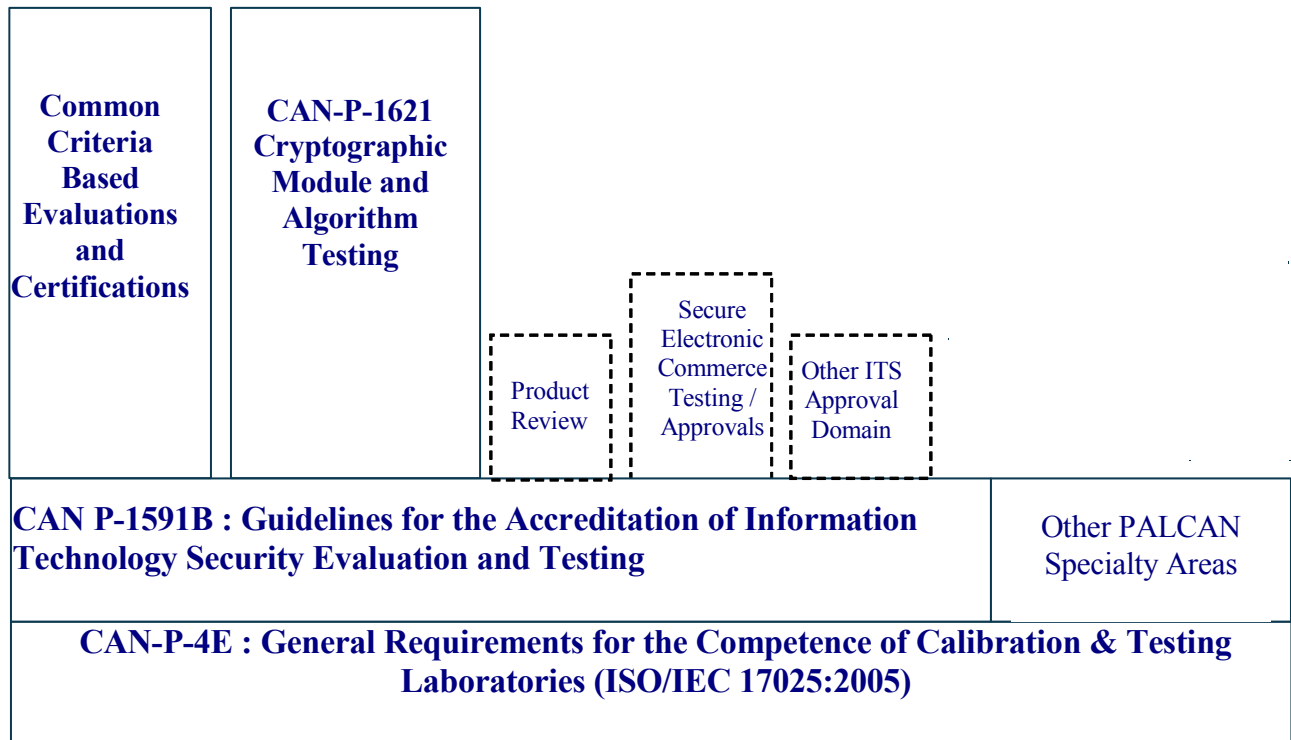


Figure 2 - SCC Accreditation Framework

GENERAL REQUIREMENTS

The testing facility interested in receiving the accreditation to this standard must also meet the requirements of the following documents:

- a) PALCAN Handbook, *Program for the Accreditation of Laboratories Canada*;
- b) CAN-P-4E: 2005, *General Requirements for the Accreditation of Testing and Calibration Laboratories*; and
- c) CAN-P-1591B: 2006, *Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities*

1 REFERENCES

1.1 The following reference documentation is applicable to this standard and available from the SCC:

CAN-P-1570 PALCAN Handbook, *Program for the Accreditation of Laboratories Canada*, Standards Council of Canada

CAN-P-4E: 2005, *General Requirements for the Accreditation of Testing and Calibration Laboratories*, Standards Council of Canada

CAN-P-1510E: *Assessment Rating Guide for use with CAN-P-4E*, Standards Council of Canada

CAN-P-1591B: 2006, *Guidelines for the Accreditation of Information Technology Security Evaluation and Testing Facilities*, Standards Council of Canada

SCC documentation may be ordered from:

Standards Council of Canada
270 Albert Street, Suite 200
Ottawa, Ontario K1P 6N7
Canada
Tel: (613) 238-3222
Fax: (613) 569-7808

Several documents are available on-line by visiting the SCC's website at http://www.scc.ca/can_p/canplist.html

1.2 The following reference documentation is applicable to this standard and available from the National Voluntary Laboratory Accreditation Program (NVLAP):

NIST Handbook 150, *NVLAP Procedures and General Requirements*, 2001 Edition

NIST Handbook 150-17, *NVLAP Cryptographic Module Testing*, June 2000

NVLAP publications may be ordered from:
National Voluntary Laboratory Accreditation Program
National Institute of Standards and Technology
100 Bureau Drive, Stop 2140
Gaithersburg, Maryland
United States of America 20899-2140
Tel: (301) 975-4016
Fax: (301) 926-2884
E-mail: nvlap@nist.gov

NIST Handbook 150 and NIST Handbook 150-17 are also available on the NVLAP web site:
<http://ts.nist.gov/nvlap> .

1.3 The following reference documentation is applicable to this standard and available from the National Institute of Standards and Technology/ Information Technology Laboratory (NIST/ITL):

Derived Test Requirements for FIPS PUB 140-2, Security Requirements for Cryptographic Modules, 25 May 2001 (hereinafter called *140-2:Derived Test Requirements*);

Implementation Guidance for FIPS PUB 140-2 and the Cryptographic Module Validation Program, updated periodically (hereinafter called *140-2: Implementation Guidance*);

Cryptographic Module Validation Program Management Processes Manual (Draft); and
Cryptographic Support Test Tool- Cryptik

Software packages of cryptographic algorithm tests and test procedures.

NIST/ITL publications and software may be ordered from:
Information Technology Laboratory (ITL)
Cryptographic Module Validation Program
National Institute of Standards and Technology
100 Bureau Drive, Stop 8930
Gaithersburg, Maryland
United States of America 20899-8930

Tel: (301) 975-2934
Fax: (301) 948-1233.

The NIST/ITL publications are also available on-line at the indicated URL:

140-2: Derived Test Requirements may also be obtained from the web site:
<http://csrc.nist.gov/cryptval/>.

140-2: Implementation Guidance may also be obtained from the web site:
<http://csrc.nist.gov/cryptval/>.

Cryptographic algorithm tests and test procedures may also be obtained from the web site: <http://csrc.nist.gov/cryptval>.

FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*, available from:
National Technical Information Service
5285 Port Royal Road
Springfield, Virginia
United States of America 22161
Tel: (800) 553-6847
Fax: (703) 605-6900
E-mail: orders@ntis.fedworld.gov.
FIPS PUB 140-2 is also available on the web site: <http://csrc.nist.gov/cryptval>.

2 DEFINITIONS

2.1 All definitions in CAN-P-4E (i.e. laboratory, testing laboratory, calibration laboratory, calibration, test, calibration method, test method, verification, quality management system, quality manual, reference standard, reference material, certified reference material, traceability, proficiency testing, accreditation requirements), CAN-P-1591B (i.e. approved signatories, approval, assessor, architectural design, conformance, conformance testing, cryptographic module, evaluation, information technology security evaluation and testing facility, facility, facility accreditation, implementation guidance, ITS Approval domain, key technical personnel, on-site assessment, product, proficiency testing, records, recognized ITS competent authority¹, security, security requirements, technical expert, technical review, testing tools) and those applicable from ISO/IEC 17000 (e.g. quality assurance, quality control) apply, as well as the following items specific to this document:

CMV: Cryptographic module validation is the act of determining if a cryptographic module conforms to the requirements of FIPS PUB 140-2

CMVP: The Cryptographic Module Validation Program administered jointly by NIST/ITL and CSE

CSE: Communications Security Establishment

Cryptik: The Cryptographic Support Test Tool (CSTT), defined below

Cryptographic algorithm testing: Input/output testing to determine whether the implementation conforms with the specification

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

¹ The term is only used in the context of the CAN-P-1591B and is not used in the context of CAN-P-1621 and the CMVP.

CSTT: Cryptographic Support Test Tool, used for documenting cryptographic module test results. This is the *Cryptik* database of abstract test cases (referred to as the *Cryptik* database)

DTR: Derived Test Requirements for FIPS PUB 140-2

FIPS: Federal Information Processing Standard

IG: Implementation Guidance for FIPS PUB 140-2

SCC: Standards Council of Canada

Validation: The administrative acts by NIST/ITL and CSE of determining the level of conformance of an implementation to specified requirements.

3 SCOPE OF ACCREDITATION

3.1 CAN-P-1621 contains four scopes of accreditation. For acceptance by the CMVP, testing facilities shall be accredited to at least Scope 1 - Group 1 and Scope 2. Accreditation to Scope 1 - Group 2 and Scope 1 - Group 3 is optional.

3.2 The four scopes of accreditation are:

Scope 1

NIST-CSTT: 140-2; National Institute of Standards and Technology - Cryptographic Support Test Tool (CSTT) for the Federal Information Processing Standard 140-2 (FIPS 140-2), "Security Requirements for Cryptographic Modules."

Group 1 All test methods derived from FIPS 140-2 and specified in the CSTT, except those listed in Group 2 and Group 3.

Group 2 Test methods for Physical Security, Level 4 derived from FIPS 140-2 and specified in the CSTT.

Group 3 Test methods for Software Security, Level 4 derived from FIPS 140-2 and specified in the CSTT.

Scope 2

FIPS-Approved Cryptographic Algorithms (see <<http://csrc.nist.gov/cryptval>>) as required in FIPS PUB 140-2.

4 DEMONSTRATING TECHNICAL COMPETENCE

4.1 Composition of the Assessment Team

4.1.1 Accreditation to the CAN-P-1621 is a method of demonstration of competence accepted by the CMVP to perform conformance testing on cryptographic modules. Other accepted means are found in the CMVP Management Processes Manual. CSE and NIST jointly manage the CMVP. Therefore, in addition to the SCC's assessors, NIST and CSE shall participate as technical assessors during the on-site assessment and the proficiency testing.

4.2 Preparation of On-Site Assessment

4.2.1 The assessors will review the facility Quality Manual and the completed proficiency testing prior to the on-site assessment. This documentation must be submitted to the assessors not less than 15 business days prior to the date scheduled for the assessment. Any problems discovered with the submitted documentation will be discussed at the assessment.

4.3 Proficiency Testing

4.3.1 Facilities are required to participate in proficiency testing for identified test methods. Successful completion of proficiency testing is required prior to initial accreditation and periodically thereafter. Facilities renewing their accreditation must have satisfactorily participated in all required proficiency testing during their previous accreditation period.

4.3.2 To properly evaluate a facility, proficiency testing may consist of several parts. The proficiency test concept is designed to allow the evaluation of the facility's ability to produce repeatable and reproducible test data. Portions of the testing process may be "highlighted" in proficiency testing; e.g., software, hardware, data analysis, etc. Proficiency testing may consist of one or more of the following methods at the discretion of the assessment team:

- a) A quiz to be responded to by all appropriate test personnel. The quiz shall pose questions for each test method that is included in each accreditation unit for which the facility is seeking accreditation. These questions will test for familiarity with the test methods, ability to determine how a particular cryptographic module should be tested for a particular test requirement, and how a specific algorithm should be tested to a specification;
- b) Testing of a specially designed artifact with one or more features that may or may not be in conformance with FIPS PUB 140-2. The facility must discover the non-conformities, document them, and indicate which FIPS PUB 140-2 requirements have failed due to the presence of the nonconformities;
- c) Examination of a specially designed finite state machine (FSM) with one or more features that are not in conformance with FIPS PUB 140-2. For example, the FSM may indicate that there is a direct transition from an error state to a user state. The facility must discover the nonconformities, document them, and indicate which FIPS PUB 140-2 requirements have failed because of the presence of the nonconformities;

- d) Demonstration of correct use of The Cryptographic Support Test Tool (*Cryptik*). The facility must demonstrate that all appropriate personnel understand its use and operation. This may be demonstrated by the assessor observing the use of *Cryptik* by facility personnel;
- e) Ability to produce a report in the approved format and with the identical content of that produced with *Cryptik*;
- f) Ability to understand test results reported in *Cryptik*.

4.3.3 The on-site assessor may hand carry proficiency test samples to the facility. Alternatively, the on-site assessor may deliver proficiency test samples to the facility prior to the on-site assessment.

4.3.4 The results of proficiency testing will be reported to the participants in appropriate documents and reports. Problems indicated by proficiency testing will be discussed with appropriate facility personnel responsible for developing and implementing plans for resolving the problems.

4.4 On-Site Assessment

4.4.1 SCC/CSE/NIST assessors will usually perform an on-site assessment for the cryptographic module testing facilities in one or two days at the facility's location. All observations made by the assessors during the assessment are held as sensitive, company confidential information.

4.4.2 The facility should be prepared to conduct test demonstrations, have equipment in good working order, and be ready for examination according to the requirements identified in this document, CAN-P-4E, CAN-P-1591B and the facility's quality manual. Efforts will be made to keep disruption to the normal working routines at a minimum. The assessor will need time and work space to complete assessment of documentation during the time at the testing facility.

4.4.3 The assessor will use the CAN-P-1622, *Checklist for the Assessment of Cryptographic Module and Algorithm Testing Facilities* and any relevant SCC checklists from CAN-P-4E and CAN-P-1591B. The checklists serve to ensure that the assessment is complete and that all assessors cover the same items at each facility. The checklists are written to cover all possibilities; therefore, not all questions apply in all circumstances. On the other hand, the assessor may go beyond the checklist in order to delve more deeply into a technical issue.

4.4.4 The agenda for a typical assessment is as follows:

- a) The assessor meets with facility management and supervisory personnel to explain the purpose of the on-site assessment and to discuss the schedule for the assessment activities. Information provided by the facility on its application form may be discussed during this meeting. At the discretion of the facility manager, other staff may attend this meeting;

- b) The assessor will ask the facility manager to assist in arranging times for interviews with facility staff members. While it is not necessary for the assessor to talk to all staff members, he/she may select staff members representing all aspects of the facility;
- c) Facility personnel should not answer any question they feel unqualified to answer. Knowing whom to ask or where to find the answer is usually considered an acceptable response by the assessor;
- d) The assessor reviews facility's quality system, including the quality manual, equipment and maintenance records, software versions, record keeping procedures, testing procedures, test reports, personnel competency records, personnel training plans and records, procedures for updating pertinent information (e.g., IG and validated product list), and safeguards for the protection of vendor-sensitive and proprietary information;
- e) The assessor will have reviewed the quality manual submitted to SCC before the on-site assessment. The assessor will discuss the manual with the designated facility staff and return the manual to the facility;
- f) One (or more) facility staff member(s) must be available to answer questions; however, the assessor may wish to review the documents alone. The assessor does not usually ask to remove any documents from the facility;
- g) The assessor will check personnel information for job descriptions, resumes, and technical performance reviews. The assessor need not be given information which violates individual privacy such as salary, medical information, or performance reviews outside the scope of the facility's accreditation. At the discretion of the facility, a member of its Human Resources Department may be present during the review of personnel information;
- g) The assessor examines hardware and software equipment and facilities for appropriateness, capability, adherence to specification, etc;
- h) At the end of the on-site assessment, an exit briefing is held with the facility manager and staff to discuss the assessor's findings. Deficiencies are discussed and resolutions may be mutually agreed upon. Items that must be addressed before accreditation can be granted are emphasized and outstanding deficiencies require a subsequent planning response to SCC within 30 days indicating a course of action that must be completed within 90 days. Items that have been corrected during the on-site assessment and any recommendations are specifically noted;
- i) Comments concerning improvements that are not identified as deficiencies by the assessors should be given serious consideration, but are taken at the facility's discretion. Any disagreements between the facility and the assessor should be referred to SCC, CSE and NIST for further evaluation; and
- j) The assessor completes an On-Site Assessment Report which summarizes the findings. The assessor attaches copies of the completed checklists to this report during the exit briefing.

The report is signed by the assessor and the facility's Authorized Representative. A copy of the report and of all the checklists is given to the facility representative for retention.

4.5 Accreditation

4.5.1 The decision to grant or renew accreditation is not made by the assessor team but by SCC in accordance with the procedures described in the PALCAN Handbook.

4.6 Denying, Suspending and Withdrawing Accreditation

4.6.1 Failure to comply with all SCC requirements, as specified in this document, CAN-P-1591B and CAN-P-4E may result in the denial, suspension, or withdrawal of a facility's accreditation. This includes failure to resolve noted deficiencies and failure to successfully participate in proficiency testing activities.

5 AMPLIFICATION OF CAN-P-1591B REQUIREMENTS

5.1 General

5.1.1 This section of the document is to be used in conjunction with CAN-P-1591B. It provides guidance in the form of interpretation and/or amplification of some clauses of CAN-P-1591B for which procedures specifically applicable to cryptographic module and algorithm testing will be used. The CAN-P-1591B clause numbers are indicated in brackets beside the headings.

5.2 Organization [CAN-P1591B Section 5.2]

There are no additional requirements for this section.

5.3 Quality System [CAN-P1591B Section 5.3]

5.3.1 The quality system requirements are designed to promote facility's practices which ensure technical integrity of the analyses and adherence to quality assurance practices appropriate to CMV and cryptographic algorithm conformance testing.

5.3.2 The facility must maintain a quality manual which fully documents the facility's policies and practices and the specific steps taken to ensure the quality of CMV conformance testing.

5.3.3 The quality manual and related documentation must contain, or refer to, documentation that describes and details the facility's implementation of procedures covering all of the technical requirements in this document. SCC assessors will review this information during on-site assessments.

5.3.4 The reference documents, standards, and publications for the CMVP listed in Section 1 of this document shall be available as references in developing and maintaining the quality system.

5.3.5 In order for the CMVP to audit technical aspects of the testing facility's operation, it may be necessary to have external audits performed by SCC or another appropriate organization, to have the facility submit validation test reports to NIST/ITL and CSE, and/or to have telephone interviews with the facility staff.

5.3.6 A testing facility shall have procedures defining the evaluation to be performed whenever major or minor changes are made to *Cryptik* or other test tools. This is necessary to ensure that harmonization is maintained as appropriate with other testing facilities and that correctness is maintained with respect to the relevant standard(s) or specification(s). (Note: cryptographic algorithm tests that are not supplied by NIST must be purchased through the appropriate standards bodies.)

5.3.7 The procedures for carrying out the test tool validation and for using the *Cryptik* database shall be documented by the facility.

5.4 Review of Requests, Tenders and Contracts [CAN-P-1591B Section 5.4]

There are no additional requirements for this section.

5.5 Control of Records [CAN-P1591B Section 5.5]

5.5.1 Records covering the following are required and will be reviewed during the on-site assessment by selective sampling:

- a) *Cryptik* versions and updates;
- b) *Cryptik* documentation; and
- c) Correspondence file including questions submitted, as defined in 140-2: Implementation Guidance, and responses.

5.5.2 Final test reports generated using *Cryptik* and final test values for the algorithm test item shall be kept by the facility following the completion of testing for the life of the cryptographic module or as specified by the client.

5.6 Personnel [CAN-P1591B Section 5.6]

5.6.1 The facility shall maintain a competent administrative and technical staff appropriate for FIPS PUB 140-2 and cryptographic algorithm conformance testing.

5.6.2 The facility shall maintain position descriptions and resumes for the staff members assigned to FIPS PUB 140-2 and cryptographic algorithm testing related positions and responsible supervisory personnel.

5.6.3 The facility shall document the required qualifications for each staff position involved in the CMV and cryptographic algorithm conformance testing processes.

5.6.4 Training for the facility staff shall concentrate on the following areas:

- a) general requirements of the test methods, including generation of test reports;
- b) familiarity with classes of hardware platforms (for software-based cryptographic algorithms);
- c) voltage and temperature measurement (Environmental Failure Protection/Environmental Failure Testing (EFP/EFT) for Level 4 only);
- d) computer security concepts;
- e) finite state model analysis;
- f) production grade, tamper evident, and tamper detection techniques;
- g) software design specifications, including high-level languages and formal models;
- h) key management techniques and concepts;
- i) Electromagnetic Interference/ Electromagnetic Compatibility (EMI/EMC) techniques;
- j) cryptographic self-test techniques;
- k) FIPS-approved cryptographic algorithms;
- l) operating system concepts;
- m) familiarity with all FIPS PUBs relating to cryptography;
- n) familiarity with cryptographic terminology and families of cryptographic algorithms;
- o) familiarity with the Common Criteria (ISO/IEC 15408:1999);
- p) operation and maintenance of *Cryptik*, and
- q) familiarity with the Internet and Internet-related software, and the ability to locate and download references and information from the CMVP web site <http://csrc.nist.gov/cryptval>.

5.6.5 The facility shall have a detailed documented description of its training program for new and current staff members. The training program shall focus, as a minimum, in the areas identified at paragraph 5.6.4 above.

5.6.6 Current staff members must receive additional training when hardware and/or software are changed, when new cryptographic algorithms are approved, when new responsibilities are assigned, or when relevant cryptographic FIPS are modified or developed.

5.6.7 This training shall include applying new test methods and 140-2: Implementation Guidance and performing tests.

5.7 Accommodation and Environmental Conditions [CAN-P1591B Section 5.7]

5.7.1 The facility shall meet the equipment and environment requirements specific to CMV testing and cryptographic algorithm testing specified in the DTR.

5.7.2 Electronic mail capability and Internet access are required by the CMVP.

5.7.3 Test reports and other communications may be sent to NIST/ITL and CSE by e-mail.

5.8 Test and Calibration Methods and Method Validation [CAN-P1591B Section 5.8]

5.8.1 When testing is performed at a client site, only the test facility personnel shall perform all actions necessary to conduct the tests and record the results, including the loading, compiling, configuring, and running of *Cryptik*.

5.8.2 The facility shall use the test methods described in the 140-2: Derived Test Requirements, with clarifications provided in 140-2: Implementation Guidance. 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 is maintained. These reports may be used to update *Cryptik* and its accompanying documentation.

5.8.3 The facility shall use the test methods and tests for the cryptographic algorithms listed at the web site <http://csrc.nist.gov/cryptval>.

5.9 Equipment [CAN-P1591B Section 5.9]

5.9.1 For its scope of accreditation, the facility shall have appropriate hardware, software, and computer facilities to conduct cryptographic module testing. This includes test and measurement equipment and tools for physical tests.

5.9.2 Facilities accredited to perform Level 4 conformance tests shall have the following types of equipment and their associated information:

- a) variable power supply;
- b) temperature chamber; and
- c) formal model texts.

5.9.3 The facility shall own, load and run a NIST/ITL-originated copy of *Cryptik* and produce printed output of the test results using the *Cryptik* database.

5.9.4 The facility shall own a computer platform that can load and effectively run a NIST/ITL-originated copy of *Cryptik*.

5.9.5 The facility shall document procedures for the following actions that involve *Cryptik*: updates; copying original software onto the appropriate media; and transporting database information from one site to another.

5.10 Measurement Traceability [CAN-P1591B Section 5.10]

5.10.1 The traceability of the abstract test cases is assured through the use of *Cryptik*. Traceability to the requirements in the FIPS PUB 140-2 documentary standard is achieved via the assertions and associated DTRs documented in the database in the *Cryptik* tool. The assertions are direct quotes from FIPS PUB 140-2. The DTRs are divided into two sets of requirements: one levied on the vendor and one levied on the tester of the cryptographic module.

5.10.2 The equipment used for conducting the conformance tests must be maintained/recalibrated:

- a) in accordance with the manufacturer's recommendation;
- b) as specified in the test method; or
- c) yearly.

Whichever results in shorter time periods between calibrations.

5.10.3 Traceability to the latest version of *Cryptik* must be assured before conducting a test. This may be accomplished through configuration management for all hardware and software, or through software version control.

5.10.4 In those technical areas where there is a difference between FIPS PUB 140-2 requirements and the *Cryptik* database of abstract test cases, the facility shall show how each realization of a test case is derived faithfully from FIPS PUB 140-2, with preservation of assignment of verdicts or measurements to the corresponding sets of observations.

5.11 Reporting the Results [CAN-P1591B Section 5.11]

5.11.1 Test reports to clients shall meet contractual requirements in addition to meeting the requirements of FIPS PUB 140-2 and of CAN-P-4E and CAN-P-1591B.

5.11.2 If the facility includes comments, analysis or results in a test report that are not covered by the requirements of FIPS PUB 140-2, then they shall be clearly identified as being outside the scope of this accreditation.

5.11.3 Test reports intended for submission to the CMVP must meet the requirements of 140-2: Derived Test Requirements and 140-2: Implementation Guidance as well as the accreditation requirements.

5.11.4 Test results created for cryptographic algorithm testing must include the values generated by the test item.

5.11.5 In addition to printed reports, the facility may submit reports to NIST/ITL and CSE in electronic form using media such as floppy disks. The electronic version shall have the same content as the printed reports and shall use a software application that is acceptable to NIST/ITL and CSE.

5.11.6 Reports that are produced by *Cryptik* are acceptable as CMVP test reports.

5.11.7 For test reports created for validation purposes and submitted to the CMVP, the facility shall issue corrections or additions to a test report only by a further document that is suitably marked and that meets the requirements of the CMVP.