Annex B: Approved Protection Profiles for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

June 10, 2019

Draft

Information Technology Laboratory
National Institute of Standards and Technology
Gaithersburg, MD 20899-8930

U.S. Department of Commerce
Penny Pritzker, *Secretary*

National Institute of Standards and Technology
Willie E. May (acting), *Under Secretary for Standards and Technology and Director*

Annex B: Approved Protection Profiles for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-2, Security Requirements for Cryptographic Modules, specifies the security requirements that are to be satisfied by the cryptographic module utilized within a security system protecting sensitive information within computer and telecommunications systems (including voice systems). The standard provides four increasing, qualitative levels of security: Level 1, Level 2, Level 3, and Level 4. These levels are intended to cover the wide range of potential applications and environments in which cryptographic modules may be employed. The security requirements cover eleven areas related to the secure design and implementation of the cryptographic module. These areas include the following:

1. Cryptographic Module Specification
2. Cryptographic Module Ports and Interfaces
3. Roles, Services, and Authentication
4. Finite State Model
5. Physical Security
6. Operational Environment
7. Cryptographic Key Management
8. Electromagnetic Interference/Electromagnetic Compatibility (EMI/EMC)
9. Self Tests
10. Design Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules to FIPS PUB 140-2 and other cryptography based standards. The CMVP is a joint effort between NIST and the Canadian Centre for Cyber Security (CCCS - https://cyber.gc.ca/en/) of the Government of Canada. Products validated as conforming to FIPS PUB 140-2 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

In the CMVP, vendors of cryptographic modules use independent, accredited testing laboratories to have their modules tested. Organizations wishing to have validations performed would contract with the laboratories for the required services.

2. Purpose

The purpose of this document is to provide a list of the Approved protection profiles applicable to FIPS PUB 140-2.

Contents

ANNEX B: APPROVED PROTECTION PROFILES

Annex B provides a list of the Approved protection profiles applicable to FIPS PUB 140-2.

Current

1. *NIAP Approved Protection Profile for General Purpose Operating Systems*
2. *NIAP Approved Protection Profile for Mobile Device Fundamentals*

These two protection profiles are available here: *NIAP Approved Protection Profiles*

NIAP no longer identifies the Protection Profiles as meeting the CC evaluation assurance EAL levels. For the purpose of meeting the FIPS 140-2 Section 4.6 validation requirements, an operational environment evaluated to one of the profiles in this annex is considered as meeting the functional requirements for security level 2.

Note: Software modules can only be validated up to security level 2.

Archived

1. U.S. Government Approved Protection Profile - U.S. Government Protection Profile for General-Purpose Operating Systems in a Networked Environment – CC Version 3.1, 30 August 2010
2. Controlled Access Protection Profile (CAPP), Version 1.d, Protection Profile NoPP006, 8 October 1999.
3. Protection Profile for Single-Level Operating Systems in Environments Requiring Medium Robustness, Version 1.22, 23 May 2001. **Sunset Date:** 16 September 2007, replaced by Protection Profile for Single-level Operating Systems in Environments Requiring Medium Robustness, Version 1.91.
4. Protection Profile for Single-level Operating Systems in Environments Requiring Medium Robustness, Version 1.91, 16 March 2007.

Document Revisions

Date	Change
06-14-2007	Updated document links. Added *Protection Profile for Single-level Operating Systems in Environments Requiring Medium Robustness*, Version 1.91
08-12-2011	Updated document links. Added *U.S. Government Approved Protection Profile - U.S. Government Protection Profile for General-Purpose Operating Systems in a Networked Environment* – CC Version 3.1, 30 August 2010
11-18-2015	**Added:** Common Criteria Protection Profiles for General Purpose Operating Systems - until June 30, 2016, NIAP-approved Protection Profiles for Operating Systems NIAP Approved Protection Profile for Mobile Device Fundamentals **Retired:** U.S. Government Protection Profile for General-Purpose Operating Systems in a Networked Environment – CC Version 3.1, 30 August 2010
12-21-2016	**Added:** Clarification for the operating environment for security level 2 modules. **Retired:** *Common Criteria Protection Profiles for General Purpose Operating Systems* – only valid through June 30, 2016.
06-10-2019	Added a URL for NIAP approved Protection Profiles and removed old URLs.