Annex D:
Allowed SSP Management Techniques for FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*

July 10, 2009
Draft

NIST Computer Security Division

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

U.S. Department of Commerce
Secretary Gary Locke

Technology Administration
Under Secretary for Technology

National Institute of Standards and Technology
Deputy Director Patrick D. Gallagher

Annex D: Allowed SSP Management Techniques for FIPS PUB 140-3, *Security Requirements for Cryptographic Modules*

1. Introduction

Federal Information Processing Standards Publication (FIPS PUB) 140-3, 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 Interfaces
3. Roles, Authentication and Services
4. Software/Firmware Security
5. Operating Environment
6. Physical Security
7. Physical Security - Non-Invasive Attacks
8. Sensitive Security Parameter Management
9. Self-Tests
10. Life-Cycle Assurance
11. Mitigation of Other Attacks

The Cryptographic Module Validation Program (CMVP - www.nist.gov/cmvp) validates cryptographic modules for conformance to FIPS PUB 140-3 and other cryptography based standards. The CMVP is a joint effort between NIST and the Communications Security Establishment Canada (CSEC - www.cse-cst.gc.ca). Modules validated as conforming to FIPS PUB 140-3 are accepted by the Federal agencies of both countries for the protection of sensitive information (United States) or Designated information (Canada).

Under 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 Allowed SSP Management Techniques applicable to FIPS PUB 140-3.

Table of Contents

ANNEX D: ALLOWED SSP MANAGEMENT TECHNIQUES

Annex D provides a list of the Allowed SSP Management Techniques applicable to FIPS PUB 140-3.

Symmetric Techniques

Allowed symmetric SSP Management techniques can be found in *FIPS 140-3 Implementation Guidance*, Section 8.

Asymmetric Techniques

Allowed asymmetric SSP Management techniques can be found in *FIPS 140-3 Implementation Guidance*, Section 8.

Document Revisions

Date	Change
03/02/2009	**Initial Draft**

End of Document