Annex D: Approved Key Establishment Techniques for FIPS PUB 140-2, *Security Requirements for Cryptographic Modules*

June 30, 2005
Draft

Jean Campbell
Randall J. Easter

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

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

Technology Administration
Phillip J. Bond, Under Secretary for Technology

National Institute of Standards and Technology
Hratch G. Semerjian, Director (*Acting*)

Annex D: Approved Key Establishment Techniques 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 Communications Security Establishment (CSE - www.cse-cst.gc.ca) 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 FIPS Approved key establishment techniques applicable to FIPS PUB 140-2.

Table of Contents

ANNEX D: APPROVED KEY ESTABLISHMENT TECHNIQUES

Annex D provides a list of the FIPS Approved key establishment techniques applicable to FIPS PUB 140-2.

Symmetric Key Establishment Techniques

National Institute of Standards and Technology, *Key Management using ANSI X9.17*, Federal Information Processing Standards Publication 171, April 27, 1992.

National Institute of Standards and Technology, *AES Key Wrap Specification (Draft),* 16 November 2001

Asymmetric Key Establishment Techniques

There are no FIPS Approved asymmetric key establishment techniques at this time. Until such time as a FIPS Approved asymmetric key establishment technique is established, techniques such as:

- Diffie-Hellman (key agreement)
- EC Diffie-Hellman (key agreement)
- Key Transport using asymmetric keys (key wrapping)
- MQV
- EC MQV

are allowed for use in a FIPS Approved mode.

The CMVP may approve other techniques for use in a FIPS Approved mode but they shall meet all the following requirements:

- are industry accepted;
- are commercially available;
- are widely used by government and industry; and
- are known in the public domain.

The final determination of an approved technique for use in a FIPS Approved mode is made by the CMVP.

Note: Please review National Institute of Standards and Technology, Implementation Guidance for FIPS PUB 140-1 and the Cryptographic Module Validation Program, Sections 8.2 and 8.8 for historical additional guidance.

End of Document