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

October 08, 2009
Draft

Jean Campbell
Randall J. Easter

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

U.S. Department of Commerce
Gary Locke, Secretary

National Institute of Standards and Technology
Patrick Gallagher, Deputy Director

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 Canada (CSEC - www.cse-cst.gc.ca). Modules 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 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 Approved key establishment techniques applicable to FIPS PUB 140-2.

Symmetric Key Establishment Techniques

1. The symmetric key establishment techniques are listed in *FIPS 140-2 Implementation Guidance* Section 7.1.

Asymmetric Key Establishment Techniques

1. National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revision1)*, Special Publication 800-56A, March 2007.

2. National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, Special Publication 800-56B, August 2009

3. Additional asymmetric key establishment schemes are allowed in a FIPS Approved mode of operation. These schemes are listed with appropriate restrictions in *FIPS 140-2 Implementation Guidance* Section 7.1.

Document Revisions

Date	Change
05/20/2003	**Symmetric Key Establishment Techniques** Reference to FIPS 171 added for symmetric keys
08/28/2003	**Asymmetric Key Establishment Techniques** Clarification of Asymmetric Key Establishment Techniques for use in a FIPS Approved mode
02/23/2004	**Asymmetric Key Establishment Techniques** MQV and EC MQV added as Asymmetric Key Establishment Techniques for use in a FIPS Approved mode
06/30/2005	**Asymmetric Key Establishment Techniques** Clarification regarding the use of asymmetric keys for key wrapping as a key transport method for key establishment
09/15/2005	**Asymmetric Key Establishment Techniques** Information regarding allowed asymmetric key establishment methods moved to FIPS 140-2 IG 7.1
01/24/2007	**Asymmetric Key Establishment Techniques** *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* - Added
03/19/2007	**Asymmetric Key Establishment Techniques** *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography (Revised)* – Updated to revised document
06/26/2007	**Symmetric Key Establishment Techniques** Removed reference to FIPS 171. FIPS 171 was withdrawn February 08, 2005. **Asymmetric Key Establishment Techniques** Added references for additional schemes in FIPS 140-2 IG Section 7.1.
10/18/2007	Updated links
01/16/2008	**Symmetric Key Establishment Techniques** Change reference to FIPS 140-2 Implementation Guidance 7.1.
10/08/2009	**Asymmetric Key Establishment Techniques** *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography* - Added

End of Document