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

August 12, 2020

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 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 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/). Modules validated as conforming to FIPS 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 140-2.

Contents

ANNEX D: APPROVED KEY ESTABLISHMENT TECHNIQUES

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

Transitions

National Institute of Standards and Technology, *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*, Special Publication 800-131A, Revision 2, March 2019. Sections relevant to this Annex: 1, 5, 6, 7 and 8.

Key Establishment Techniques

1. Key establishment techniques *allowed* in a FIPS Approved mode of operation with appropriate restrictions are listed in *FIPS 140-2 Implementation Guidance* Section D.2.

2. National Institute of Standards and Technology, *Digital Signature Standard (DSS)*, Federal Information Processing Standards Publication 186-4, July 2013. (DSA, RSA and ECDSA)

3. National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Special Publication 800-56A Revision 3, April 2018.

4. National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography*, Special Publication 800-56A Revision 2, May 2013.

5. National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes using Discrete Logarithm Cryptography*, Special Publication 800-56A Revised, March 2007.

6. National Institute of Standards and Technology, *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography*, Special Publication 800-56B Revision 2, March 2019.

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

8. National Institute of Standards and Technology, *Recommendation for Key Derivation Using Pseudorandom Functions*, Special Publication 800-108, October 2009, Revised.

9. National Institute of Standards and Technology, *Recommendation for Password-Based Key Derivation, Part 1: Storage Applications*, Special Publication 800-132, December 2010.

10. National Institute of Standards and Technology, *Recommendation for Existing Application-Specific Key Derivation Functions*, Special Publication 800-135rev1, December 2011.

11. Internet Engineering Task Force (IETF), *The Transport Layer Security (TLS) Protocol Version 1.3, Section 7.1*, RFC 8446, August 2018.

12. National Institute of Standards and Technology, *Recommendation for Key-Derivation Methods in Key-Establishment* Schemes, Special Publication 800-56C Revision 1, April 2018.

13. National Institute of Standards and Technology, *Recommendation for Key Derivation through Extraction-then-Expansion*, Special Publication 800-56C, November 2011.

14. National Institute of Standards and Technology, *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, Special Publication 800-38F, December 2012.

15. National Institute of Standards and Technology, *Recommendation for Cryptographic Key Generation*, Special Publication 800-133 Revision 2, June 2020.

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 Revision 1
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
11/24/2010	**Symmetric Key Establishment Techniques**, Number 1: Changed reference from FIPS 140-2 Implementation Guidance 7.1 to D.2.
	Asymmetric Key Establishment Techniques Split section into three parts.
	Asymmetric Key Establishment Techniques, Number 3 Changed reference from FIPS 140-2 Implementation Guidance 7.1 to D.2.
01/04/2011	**References reorganized**
	Added reference FIPS 186-3 – asymmetric key generation
	Added reference Special Publication 800-108
	Added reference Special Publication 800-132
	Added reference Special Publication 800-135
07/26/2011	**Added new Section: Transitions** Added: *Recommendation for Transitioning the Use of Cryptographic Algorithms and Key Lengths*
12/20/2011	**Key Establishment Techniques** Added: *Recommendation for Key Derivation through Extraction-then-Expansion*, Special Publication 800-56C
04/23/2011	**Key Establishment Techniques** Updated: *Recommendation for Existing Application-Specific Key Derivation Functions* to Revision 1.

01/02/2013	**Key Establishment Techniques** Added: *Recommendation for Block Cipher Modes of Operation: Methods for Key Wrapping*, Special Publication 800-38F
02/24/2014	**Key Establishment Techniques** Updated: *Digital Signature Standard (DSS)* from FIPS 186-3 to FIPS 186-4 Updated: *Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography* from Revision 1 to Revision 2
02/26/2014	**Key Establishment Techniques** Added: *Recommendation for Cryptographic Key Generation,* Special Publication 800-133
10/08/2014	**Key Establishment Techniques** Updated: *Recommendation for Pair-Wise Key Establishment Schemes Using Integer Factorization Cryptography* to Revision 1.
05/10/2017	**Transitions** Updated: SP 800-131Arev1 replaces SP 800-131A **Key Establishment Techniques** Added: SP 800-56A and included a reference to IG D1-rev2 **Overall Document** Modified section titles, added a note and fixed broken links.
06-10-2019	**Transitions** Updated: SP 800-131Arev2 replaces SP 800-131Arev1 **Key Establishment Techniques** Added: SP 800-56A Revision 3, April 2018 Added: SP 800-56B Revision 2, March 2019 Added: SP 800-56C Revision 1, April 2018
11/15/2019	**Key Establishment Techniques** Added: SP 800-133 Revision 1, July 2019
04/03/2020	**Key Establishment Techniques** Added: SP 800-56B, August 2009 Removed: SP 800-56B Revision 1, September 2014 Removed: note referencing IG D.1-rev2.
08/12/2020	**Key Establishment Techniques** Added: RFC 8446, Section 7.1, August 2018 Added: SP 800-133 Revision 2, June 2020 Removed: SP 800-133, December 2012 Removed: SP 800-133 Revision 1, July 2019