Ruminations on applying FIPS 140-2 to IEEE 802.1af

Brian Weis

Typical FIPS 140-2 Evaluation

- The crypto module consists of existing protocol specifications, where the protocol specification uses approved procedures and/or procedures for which implementation guidance already exists.
  - E.g., IPsec, IEEE 802.11i
- What is effectively being evaluated? That the protocol specifications have been correctly & safely implemented.
  - The evaluation proving correctness comes at a somewhat predictable cost and on a somewhat predictable timeline.

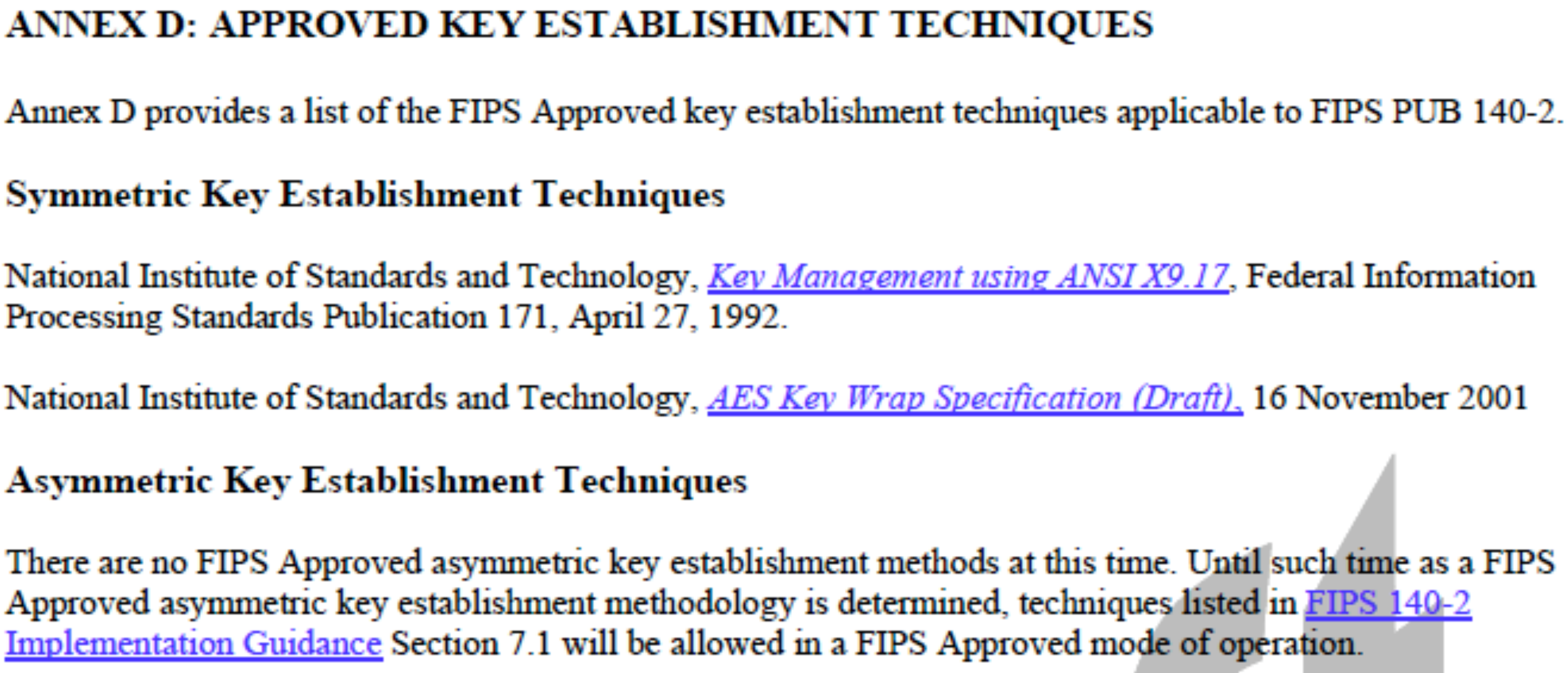
Risk of new procedures

- If there are novel and/or unapproved procedures used in the crypto module, these new procedures must first be defended to the evaluation lab, which must defend them to NIST.
  - This must be done concluded before any analysis of correct & safe implementation!
  - This process represents an additional unbounded cost in terms of time and money.

Time Delays

- NIST isn’t going to independently rule on any new procedure
- They’re going to want a review from the cryptographic community.
  - Cryptographers need time to analyze
  - It can take years! They aren’t on a schedule :-)
- Eventually NIST may update its implementation guidance to allow/restrict the new procedure

Current approved key establishment methods



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.

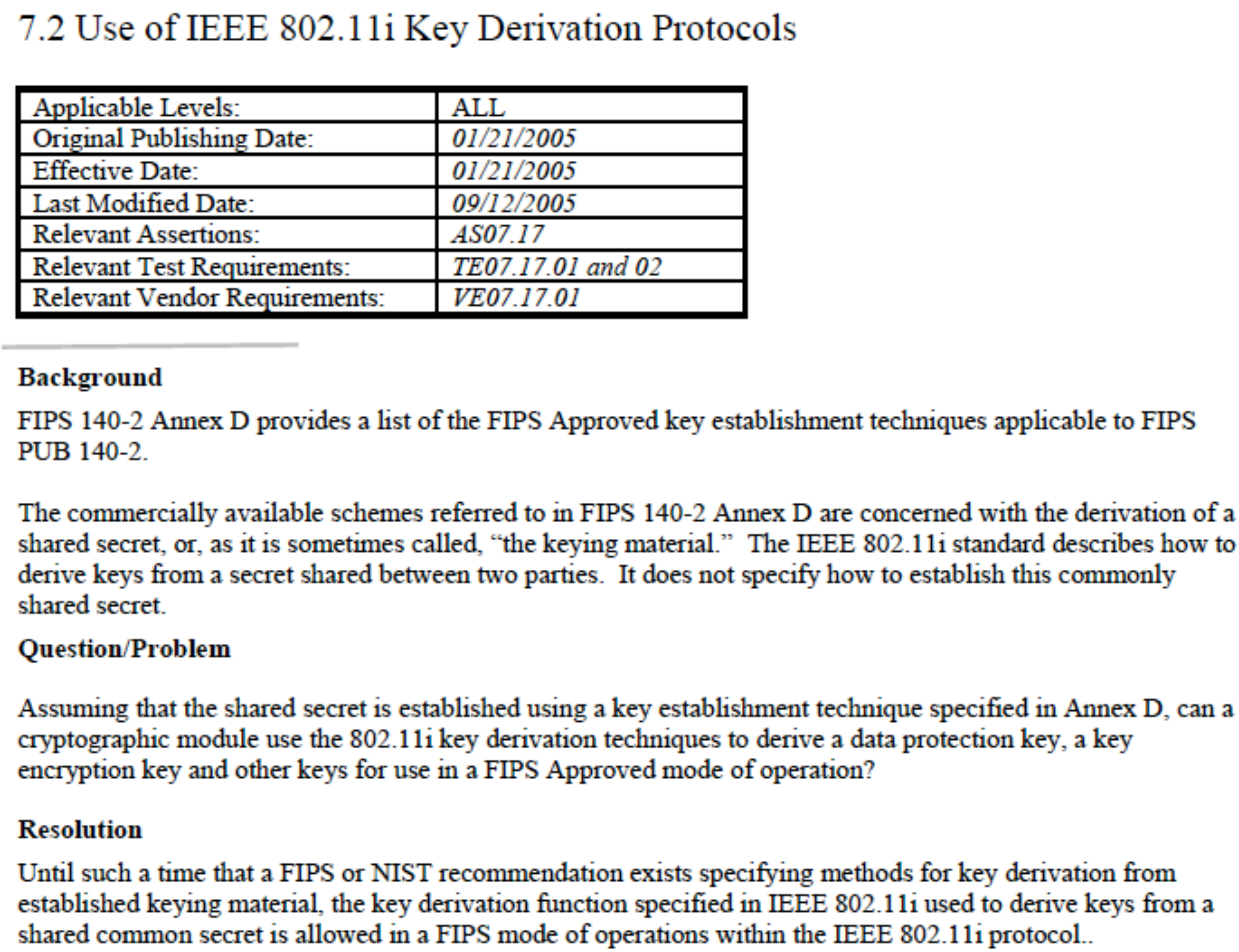
National Institute of Standards and Technology, *AES Key Wrap Specification (Draft)*, 16 November 2001

Asymmetric Key Establishment Techniques

There are no FIPS Approved asymmetric key establishment methods at this time. Until such time as a FIPS Approved asymmetric key establishment methodology is determined, techniques listed in FIPS 140-2 Implementation Guidance Section 7.1 will be allowed in a FIPS Approved mode of operation.

802.11i experience

- 802.11i uses the AES Key Wrap for distributing a group key
- But this was was not sufficient to avoid needing implementation guide. They needed it for
  - a new 4-way handshake protocol
  - a new key derivation method



7.2 Use of IEEE 802.11i Key Derivation Protocols

Applicable Levels:	ALL
Original Publishing Date:	*01/21/2005*
Effective Date:	*01/21/2005*
Last Modified Date:	*09/12/2005*
Relevant Assertions:	*AS07.17*
Relevant Test Requirements:	*TE07.17.01 and 02*
Relevant Vendor Requirements:	*VE07.17.01*

Background

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

The commercially available schemes referred to in FIPS 140-2 Annex D are concerned with the derivation of a shared secret, or, as it is sometimes called, "the keying material." The IEEE 802.11i standard describes how to derive keys from a secret shared between two parties. It does not specify how to establish this commonly shared secret.

Question/Problem

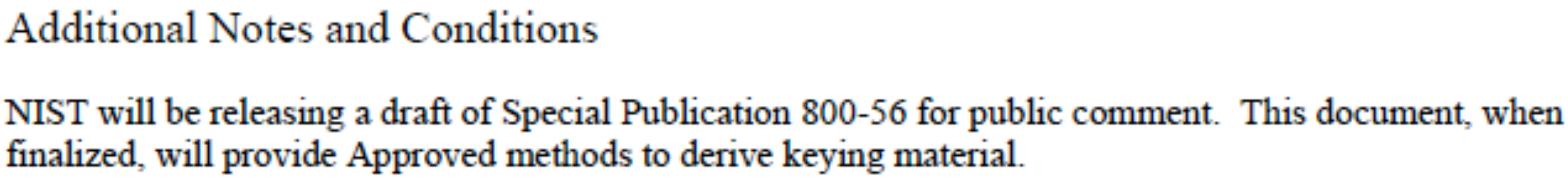
Assuming that the shared secret is established using a key establishment technique specified in Annex D, can a cryptographic module use the 802.11i key derivation techniques to derive a data protection key, a key encryption key and other keys for use in a FIPS Approved mode of operation?

Resolution

Until such a time that a FIPS or NIST recommendation exists specifying methods for key derivation from established keying material, the key derivation function specified in IEEE 802.11i used to derive keys from a shared common secret is allowed in a FIPS mode of operations within the IEEE 802.11i protocol..

Future Requirements

- NIST also said in the 802.11i guidance:



Additional Notes and Conditions

NIST will be releasing a draft of Special Publication 800-56 for public comment. This document, when finalized, will provide Approved methods to derive keying material.

- SP 800-56A has been published

  "Recommendation for Pair-Wise Key Establishment Schemes Using Discrete Logarithm Cryptography"

- 800-56A doesn't apply to the IEEE 802.1af environment

Conclusion

- SAK
  - Deriving a key from Key Contributions will need implementation guidance similar to 802.11i
  - Deriving a key obtained from an approved RNG, and distributing it protected by the AES Key Wrap should be acceptable
- CAK
  - Inventing a new method for deriving a CAK may need implementation guidance similar to 802.11i
  - Re-using the definition in 802.11i might not require additional implementation guidance