National Institute of Standards and Technology

Cryptographic Module Validation Program

DES Transition Plan

Federal Register / Vol. 70, No. 96 / Thursday, May 19, 2005 / Notices

National Institute of Standards and Technology
[Docket No. 040602169–5002–02]

Announcing Approval of the Withdrawal of Federal Information Processing Standard (FIPS) 46–3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation

SUMMARY: The Secretary of Commerce has approved the withdrawal of FIPS 46–3, Data Encryption Standard (DES); FIPS 74, Guidelines for Implementing and Using the NBS Data Encryption Standard; and FIPS 81, DES Modes of Operation. These FIPS are withdrawn because FIPS 46–3, DES, no longer provides the security that is needed to protect Federal government information. FIPS 74 and 81 are associated standards that provide for the implementation and operation of the DES. Federal government organizations are now encouraged to use FIPS 197, Advanced Encryption Standard (AES), which was approved for Federal government use in November 2001. FIPS 197 specifies a faster and stronger algorithm than the DES for encryption. For some applications, Federal government departments and agencies may use the Triple Data Encryption Algorithm to provide cryptographic protection for their information. This algorithm and its uses have been specified in NIST Special Publication 800–67, Recommendations for the Triple Data Encryption Algorithm (TDEA) Block Cipher, issued in May 2004. FIPS 197 and SP 800–67 are available on NIST's Web pages. The content of these withdrawn standards will remain available at http://csrc.nist.gov/publications/fips/index.html as reference documents and these three FIPS will be listed as withdrawn, rather than current FIPS.

Comment: NIST should provide a timetable and a transition strategy for the discontinuation of the use of DES implementations. NIST should clarify the transition from the use of applied and embedded DES products.
Response: A proposed transition strategy for validating algorithms and cryptographic modules has been posted for public comment on NIST's Web page at http://csrc.nist.gov/groups/STM/cmvp/index.html under ''Notices.'' The transition plan addresses the use by Federal agencies of DES implementations, which are incorporated in cryptographic modules, and which have been validated under the Cryptographic Module Validation Program. The transition plan allows Federal agencies and vendors to make a smooth transition to stronger cryptographic algorithms such as AES or Triple-DES.

Future use of DES by Federal agencies is to be permitted only as a component function of the Triple Data Encryption Algorithm (TDEA or Triple-DES) (NIST Special Publication 800-67). Triple-DES may continue to be used for the foreseeable future for the protection of Federal information; however, NIST encourages agencies to implement the faster and stronger algorithm specified by FIPS 197, Advanced Encryption Standard (AES).

The Cryptographic Module Validation Program (CMVP) **DES Transition Plan** addresses the use of single key DES by Federal agencies, which are incorporated in cryptographic modules, validated to FIPS 140-1 or FIPS 140-2. Single key DES has been an Approved security function since the inception of the CMVP and the signing of FIPS 140-1 on January 11, 1994. The DES transition plan was developed to allow Federal agencies and vendors to smoothly transition to the stronger Approved security functions, specifically AES and Triple-DES.

1. Effective May 19, 2005: Federal Agencies may continue to use DES as a NIST recommended Approved security function in a FIPS Approved mode of operation in FIPS

140-1 or FIPS 140-2 validated cryptographic modules for a period of 2 years (until May 19, 2007). This provides a transition period to migrate to AES or Triple-DES.

   a. Cryptographic modules validated to FIPS 140-1 or FIPS 140-2 that implement DES as an Approved security function will have the DES algorithm entry on the module validation list changed to include the caveat “transitional phase only – valid until May 19, 2007”
   b. The Cryptographic Algorithm Validation Program (CAVP) has discontinued the issuance of new DES algorithm validation certificates as of February 9, 2005 (Note: DES implementations under contract for testing by a CMT Laboratory prior to February 9, 2005 will be completed).
   c. Agencies must understand that NIST strongly recommends against any continued use of DES. Agencies must accept the security risks of the continued use of DES during the transition phase. In short, DES does not provide adequate protection for data whose confidentiality must be assured for more than near-transitory implementations.

2. After the 2-year transition period ends on May 19, 2007:

   a. The reference to single DES will be removed from FIPS 140-2 Annex A, *Approved Security Functions*.
   b. The CMVP will move all references of DES from an Approved security function to the non-Approved security function line on all FIPS 140-1 and FIPS 140-2 cryptographic module validation certificates. Modules validated to FIPS 140-1 or FIPS 140-2 that *only* implement DES as an Approved security function will have their entry on the module validation list annotated as not meeting FIPS 140-1 or FIPS 140-2 requirements anymore and can no longer be used by a Federal agency.
   c. The DES validation list will be saved for historical reference only but annotated as no longer being Approved for use.

3. This transition also applies to DES MAC.

4. The use of DES in National Institute of Standards and Technology, Digital Signature Standard (DSS), Federal Information Processing Standards Publication 186-2, January 27, 2000 – Appendix 3.2 is not affected.

The point of contact regarding this plan is Allen Roginsky (CMVP) at allen.roginsky@nist.gov. Please contact Allen regarding any questions.