Public Comments on Draft FIPS PUB 46-3,
"Data Encryption Standard (DES)"

(Comments were submitted in response to the Federal Register Notice of January 15, 1999, (Volume 64, Number 10) on Pages 2625-2628. The first three comments were submitted electronically to desreview@nist.gov.)

From: Roland Lockhart <roland.lockhart@entrust.com>
To: "'desreview@nist.gov'" <desreview@nist.gov>
Subject: Comments on draft FIPS PUB 46-3
Date: Thu, 21 Jan 1999 15:37:10 -0500
X-Mailer: Internet Mail Service (5.5.1960.3)

Hi Jim and company,

I have a few comments on the FIPS PUB 46-3 draft. They are mainly typographical and cosmetic in nature.

Page 9, figure 1. Figure caption is missing

Page 9, figure 1. Horizontal arrowheads are distorted.

Page 9, figure 1. The lefthand side of the pre-output blocks should be L16=L15 xor f(R15,K16) rather than R16, should it not, given that there is no transposition after the final round? Likewise shouldn't the right hand side be R16=R15?

Page 9, figure 1. The page number appears inside the figure space (at least on my printout).

Page 13, figure 2. Figure caption is missing.

Page 13, figure 2. Horizontal arrowheads are distorted.

A general question: is it implied that in order to conform with 46-3 a device or system must implement both DEA and triple-DEA?

- cheers,
Roland Lockhart
Entrust Technologies Ltd.
Ottawa, ON

From: "Costantini, Frank " <Frank.Costantini@ccmail.l-3com.com>
To: desreview@nist.gov
Subject: DES / 3-DES Review
Date: Mon, 8 Feb 1999 16:26:00 -0500
X-Mailer: Internet Mail Service (5.5.2232.9)

NIST:

I would like to respectfully request and recommend that Counter Mode operation be included in the approved modes of operation in FIPS-46-3. This mode has certain advantages over the other permitted modes in real-time, connection oriented, packet-based communications. Specifically, this mode requires little synchronization overhead, even in lossy communications channels where data is lost, and allows the keystream to be precomputed before the plaintext/ciphertext data is available. This is critical in low-delay applications (like full duplex voice).

If you require any additional information on this request, please feel free to contact me. Thank you for your consideration.

Respectfully,

Frank Costantini
Principal Member Engineering Staff
L-3 Communications Systems East
Camden, NJ 08102
609-338-3480
frank.costantini@L-3com.com

From: mchawrun@its.cse.dnd.ca
To: desreview@nist.gov
Cc: nmlabreche@its.cse.dnd.ca
Subject: FIPS 46-3
Date: Fri, 26 Feb 1999 12:06:16 -0500
X-Mailer: Internet Mail Service (5.5.2232.9)

The following comments are submitted for consideration.

General:

In contrast to FIPS 46-1, FIPS 46-2 has an additional annex. Therefore, it is suggested that using the search and replace feature, "appendix" be replaced with "appendix 1."

Minor technical

1. Page 13, figure 2:

   The inputs to the S boxes should have 6 inputs (vice 4) and 4 outputs (vice 3).

Editorial

2. Page 1, Article 3, second paragraph, first line:
   Change "O" to indicate the numeric font of zero, (i.e., "0").

3. Page 3, Article 7:
   It is suggested that this article be broken up into two paragraphs.
   The first paragraph would end with the sentence "Communications security ... receiving point."
   The statement "DEA forms the basis for TDEA" appears to be an orphan. It is a true statement, however, it belongs elsewhere.
   The second paragraph would begin with "File security ... storage medium."

4. Page 4, article 12, point 3:
   Delete the comma after "where."

5. Page 5, article 13:
   Increase the space between, this article and the preceding one.

6. Page 6, article 17, second paragraph, second last line:
   Insert a comma followed by a space after the word "Decisions."

7. Page 7, article 19, fourth line:
   The information appearing in brackets appears not in the right format.

8. Page 8, Introduction, second line.

It is suggested that the footnote be numbered rather than indicated with an asterisk.

9. Page 9:

The diagram appears to large for the page and it lacks a label (figure 1 ...).

10. Page 10, top paragraph, lines three and four:

Insert a space after "B_2 ...".

"Enciphering" is the title heading and should appear on another line, in a consistent format.

11. Page 10, fourth paragraph:

Insert a comma after "that is."

12. Page 11:

Insert and extra "new line" after the first paragraph.

13. Page 12:

The symbol for function that appears in the heading should be the same as the symbol appearing the text of that paragraph.

14. Page 17:

The zeros that appear in the chart appear to be the character for O rather than the numeric font for zero.

15. Page 19:

This more of a question that may need to be clarified. Are the subscripts that appear after C and D zeros or open brackets followed by closed brackets? If they are open and closed brackets, it may be helpful to add a short explanation or insert a space between the brackets.

In the last paragraph, the notation that follows immediately after D should appear as subscript.

16. Page 20:

For consistency, the title should appear outside and under the border.

U.S. Department of Justice
Immigration and Naturalization Service

40/11.2.4

425 I Street NW
Washington, DC 20536

April 14, 1999

Information Technology Laboratory
ATTN: Review of Draft FIPS 46-3
National Institute of Standards and Technology
100 Bureau Drive, STOP 8970
Gaithersburg, MD 20899-8970

Subject: INS HQRSS Comments on Draft FIPS 46-3

Dear Sir/Madam:

The Immigration and Naturalization Service (INS) Headquarters Radio Systems Section (HQRSS) is pleased to submit comments in response to Draft Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES).

BACKGROUND

As the largest Federal law enforcement agency, the INS operates one of the most extensive civilian law enforcement wireless communications systems in the world operating in the HF, VHF, UHF, and microwave bands. INS HQRSS is responsible for the design, engineering, implementation, and operation and maintenance of the INS' wireless communications systems Service-wide.

Currently, the INS' wireless communications systems support the operational communications requirements of over 17,000 INS law enforcement personnel in urban, suburban, and rural areas. The INS provides wireless communications throughout the continental United States, Alaska, Hawaii, Guam, and Puerto Rico. INS law enforcement personnel are distributed throughout three (3) Regions, 21 Sectors, and 36 Districts. These INS agents/officers staff over 250 air, land, and sea ports of entry and patrol over 8,000 miles of international boundaries in land vehicles, aircraft, or boats, as well as on horseback or on foot. In addition, the INS operates ten (10) detention facilities known as Service Processing Centers (SPCs).

The INS has over 17,000 handheld/portable radios and over 15,000 mobile/vehicular radios that support both INS personnel and multi-agency task forces comprised of Federal, state, and local law enforcement personnel. These 32,000 radios operate over a nationwide wireless communications systems consisting of approximately 1,400 base stations/repeater stations.

The INS has an extensive wireless communications infrastructure that includes, but is not limited to: VHF and UHF mobile relay/repeaters, satellite voting receivers, command and control (C2) centers, microwave backbone infrastructure, base stations, control base stations, HF stations, antennas, towers, shelters, etc.

The INS has deployed and continues to deploy cryptographically protected narrowband digital wireless equipment as part of its Encrypted Voice Radio Program (EVRP).

SINGLE KEY DES (DEA)

The INS, like most other federal law enforcement agencies, makes extensive use of the DES cryptographic algorithm in the DEA (single key DES) form, to protect the privacy of its wireless communications.

In addition, the INS has been a long time participant and supporter of the APCO/TIA Project 25 international law enforcement communications standards effort. In this regard Project 25 has adopted the use of DEA as the Type-3 cryptology for use in Project 25. To date, there has been no effort within the Project 25 community to press for the adoption of any other cryptographic algorithm.

The INS appreciates NIST's concerns regarding the protection provided by DEA (single key DES). The INS HQRSS, in its wireless operational training, stresses to all INS operational users that DEA is not "secure" and, therefore INS, encrypted wireless systems are not "secure". The INS HQRSS instructs INS personnel that its DEA-protected equipment affords privacy protection with respect to the threat posed by certain categories of adversary.

As NIST is aware, the INS has had representation at the two Advanced Encryption Standard (AES) conferences. The INS is greatly encouraged by the AES effort and looks forward to its expedient conclusion. It is the INS' intent to advance the adoption of AES, and the strong cryptographic protection provided, within the Project 25 process, upon its selection by NIST.

In this regard, the continued provision for DEA (single key DES) will permit the INS and other agencies to procure, in the future, dual algorithm (DEA and AES) cryptographic modules that will allow for a graceful migration and transition from DEA to AES.

The INS HQRSS is committed to the continued interoperability of law enforcement wireless communications system that employ DEA (single key DES). Encrypted interoperability between and amongst agencies that employ DEA, is essential to INS law enforcement operations.

It is the INS' experience that graceful migration to new technologies and backward compatibility with legacy systems are essential elements in a law enforcement wireless communications environment. The INS EVRP strategy has long been predicated upon both backward compatibility and graceful technology migration.

Recommendation – Single Key DES
The INS HQRSS recommends that the Draft FIPS 46-3 permit the continued use of DEA (single key DES) in those wireless communications systems, and their associated support infrastructures, where interoperability is required between and amongst federal, state and local law enforcement agencies.

The INS also recommends that DEA (single key DES) be referenced for use in cryptographic modules that also contain the future AES algorithm to facilitate backward compatibility with legacy systems and to promote graceful migration to the AES.

ELECTRONIC CRYPTOGRAPHIC KEY DISTRIBUTION
Over-The-Air-Rekey (OTAR)
The INS also makes extensive use of electronic cryptographic key management and distribution techniques. Cryptographically protected INS wireless equipment has its cryptographic key variables changed by means of an Over-The-Air-Rekey (OTAR) protocol. The OTAR process currently employed by INS, in its EVRP systems, is not based upon ANSI X9.17 or ANSI X9.42, but rather is optimized for the unique environment that characterizes wireless communications.

Moreover, the INS EVRP strategy calls for migrating toward the Project 25-compliant OTAR protocol, as defined in the TIA/EIA APCO Project 25 Over-The-Air-Rekeying (OTAR) Protocol, TSB102.AACA. This Project 25 law enforcement wireless communications standard is likewise not based upon ANSI X9.17 or ANSI X9.42.

Recommendation - OTAR
The INS recommends that FIPS 46-3 recognize and permit continued use of existing OTAR protocols, such as that currently employed by the INS, and that the Project 25 OTAR protocol be referenced for use in wireless communications systems.

Thank your for the opportunity to submit comments on this critically important subject. Should you have any questions, please contact Dr. Gregory M. Stone on 301.925.9773.

Sincerely,

David G. Butler
Chief
Radio Systems Section

MOTOROLA

April 13, 1999

Information Technology Laboratory
ATTN: Review of Draft FIPS 46-3
National Institute of Standards and Technology
100 Bureau Drive, STOP 8970
Gaithersburg, MD 20899-8970
Email: desreview@nist.gov

Motorola comments on Draft FIPS 46-3.
Response to NIST invitation to comment on the reaffirmation of the FIPS PUB 46-3 standard, as published in the Federal Register January 15, 1999. The comment period closes April 15, 1999.

Motorola actively supports the National Institute of Standards and Technology (NIST) in its efforts to continue the approval and endorsement of Data Encryption Standard (DES) products through the FIPS 46-3 standard activities. To date, Motorola has six cryptographic modules that implement the DES and have been validated to the FIPS 140-1 standard, including the first product to be validated by a US company. We intend to continue to produce cryptographic modules compliant to FIPS 46-3 and FIPS 140-1.

GENERAL COMMENTS

NIST should continue to permit and approve the use of single key DES (i.e., DEA) to support existing standards. Manufacturers due to interoperability requirements cannot arbitrarily modify these standards to implement Triple DES (TDEA). Specifically, TIA/EIA standards for the Association of Public Safety Communication Officers (APCO) Project 25 specify the use of single key DES. NIST should continue to approve the use of single key DES in these applications until the applicable standard bodies formally specify the requirement for Triple DES and/or Advanced Encryption Standard (AES) as well as the time frame for implementation.

The task of managing keys across large systems has become increasing complex. A technique to manage this complexity is to employ automatic key distribution mechanisms in the systems. FIPS 46-3 makes references to couple key distribution mechanisms, FIPS PUB 171, *Key Management Using ANSI X9.17* and ANSI X9.42, *Agreement of Symmetric Keys on Using Diffie-Hellman and MQV Algorithms*. Motorola feels that NIST should recognize other key management standards specifically designed for wireless environments. For example, the Over-The-Air-Rekeying protocol defined in TSB102.AACA *TIA/EIA APCO Project 25 Over-The-Air-Rekeying (OTAR) Protocol* should be referenced for wireless applications.

Motorola supports the FIPS 46-3 standard and feels that NIST should continue to support the validation of cryptographic modules that implement the standard. We hope that NIST will consider our comments that we believe would augment the benefits for those devices that comply with the standard.

Regards,

Richard Barth

Richard C. Barth, Ph.D.
Vice President and Director
Telecommunications Strategy and Regulation

SPECIFIC COMMENTS

This section provides comments on syntax problems in the document and is only being provided for informational purposes.

1. Announcement, Section 13 (page 5)– A carriage return should be inserted before Section 13.

   > NIST provides technical assistance to Federal agencies in implementing data encryption through the issuance of standards, guidelines and through individual reimbursable projects.
   >
   > **13. Specifications.** Federal Information Processing Standard (FIPS) 46-3, Data Encryption Standard (DES) (affixed).

2. Announcement, Section 15 (page 5) - For consistency, the first paragraph in Section 15 should immediately start after the title. The carriage return should be removed after **Qualifications**.

   > **15. Qualifications.** Both this standard and possible threats reducing the security provided through the use of this standard will undergo review by NIST as appropriate, taking into account newly available technology. In addition, the awareness of any breakthrough in technology or any mathematical weakness of the algorithm will cause NIST to reevaluate this standard and provide necessary revisions.

3. Announcement, Section 17 (page 6) – The bullet items in this section should be indented for consistency. Also, a comma should be inserted in the address.

   > **17. Waiver Procedure.** Under certain exceptional circumstances, the heads of Federal departments and agencies may approve waivers to Federal Information Processing Standards (FIPS). The head of such agency may redelegate such authority only to a senior official designated pursuant to section 3506(b) of Title 44, United States Code. Waiver shall be granted only when:
   >
   > a. Compliance with a standard would adversely affect the accomplishment of the mission of an operator of a Federal computer system; or
   >
   > b. Compliance with a standard would cause a major adverse financial impact on the operator which is not offset by Government-wide savings.
   >
   > Agency heads may act upon a written waiver request containing the information detailed above. Agency heads may also act without a written waiver request when they determine that conditions for meeting the standard cannot be met. Agency heads may approve waivers only by a written decision which explains the basis on which the agency head made the required finding(s). A copy of each decision, with procurement sensitive or classified portions clearly identified, shall be sent to: National Institute of Standards and Technology; ATTN: FIPS Waiver Decisions,100 Bureau Drive, Stop 8970, Gaithersburg, MD 20899-8970

4. Specifications, Figure 1 (page 9) – The figure should be scaled to fit on the page. The figure should also be labeled.

5. Specifications, Enciphering (page 10) – Two carriage returns should be inserted before the **Enciphering** header.

The following notation is convenient: Given two blocks ***L*** and ***R*** of bits, ***LR*** denotes the block consisting of the bits of ***L*** followed by the bits of ***R***. Since concatenation is associative, ***B1B2...B8***, for example, denotes the block consisting of the bits of ***B1*** followed by the bits of ***B2***...followed by the bits of ***B8***.

Enciphering

A sketch of the enciphering computation is given in **Figure 1**.

6. Specifications, Enciphering (page 11, 1st paragraph) – A carriage return should be inserted after the first paragraph.

The computation which uses the permuted input block as its input to produce the preoutput block consists, but for a final interchange of blocks, of 16 iterations of a calculation that is described below in terms of the cipher function ***f*** which operates on two blocks, one of 32 bits and one of 48 bits, and produces a block of 32 bits.

Let the 64 bits of the input block to an iteration consist of a 32 bit block ***L*** followed by a 32 bit block ***R***. Using the notation defined in the introduction, the input block is then ***LR***.

7. Specifications, Enciphering (page 11, 3rd paragraph) – A carriage return should be inserted before the equations label (1) for consistency.

Let ***K*** be a block of 48 bits chosen from the 64-bit key. Then the output ***L'R'*** of an iteration with input ***LR*** is defined by:

$$L' = R \qquad (1)$$
$$R' = L \oplus f(R,K)$$

where ⊕ denotes bit-by-bit addition modulo 2.

8. Specifications, (page 14) – There appears to be a page break on page 14 which should not be there.

9. Specification – Triple Data Encryption Algorithm (page 16) – The bullet items in this section should be indented for consistency. A carriage return should be inserted before the equation in bullet item 1.

Let ***EK(I)*** and ***DK(I)*** represent the DEA encryption and decryption of ***I*** using DEA key ***K*** respectively. Each TDEA encryption/decryption operation (as specified in ANSI X9.52) is a compound operation of DEA encryption and decryption operations. The following operations are used:

1. TDEA encryption operation: the transformation of a 64-bit block ***I*** into a 64-bit block ***O*** that is defined as follows:

$$O = E_{K3}(D_{K2}(E_{K1}(I))).$$

2. TDEA decryption operation: the transformation of a 64-bit block ***I*** into a 64-bit block ***O*** that is defined as follows:

$$O = D_{K1}(E_{K2}(D_{K3}(I)))$$

The standard specifies the following keying options for bundle (K_1, K_2, K_3)

1. Keying Option 1: $\boldsymbol{K_1}$, $\boldsymbol{K_2}$ and $\boldsymbol{K_3}$ are independent keys;

2. Keying Option 2: $\boldsymbol{K_1}$ and $\boldsymbol{K_2}$ are independent keys and $\boldsymbol{K_3 = K_1}$;

3. Keying Option 3: $\boldsymbol{K_1 = K_2 = K_3}$.

A TDEA mode of operation is backward compatible with its single DEA counterpart if, with compatible keying options for TDEA operation,

10. General Comment – Through out the document there is a inconsistency in the paragraph justification. The entire document should be left-right justified.

11. General Comment – Though out the document there are extra spaces, either at the beginning or the end of a line, if a period occurs at the end of line.