

STANDARDS AUSTRALIA

Amendment No. 1
to
AS 2805.4.1—2001
Electronic funds transfer—Requirements for interfaces
Part 4.1: Message authentication—Mechanism using a block cipher

REVISED TEXT

The 2001 edition of AS 2805.4.1 is amended as follows; the amendment(s) should be inserted in the appropriate place(s).

SUMMARY: This Amendment applies to Contents, Clauses 2, 5.3, 5.5, 5.7 and Appendix A.

Published on 14 February 2006.

Page 4 Table of Contents

Add new listing as follows:

APPENDIX A SECURITY ANALYSIS OF THE MAC ALGORITHMS 11

Page 5 Clause 2

Add the following to the list:

AS

2805.5.1 Ciphers—Data encipherment algorithm 1 (DEA 1)

ISO/IEC

9797 Information technology—Security techniques—Message Authentication Codes (MACs)

9797-1 Part 1: Mechanisms using a block cipher

Page 7 Clause 5.3

Delete Clause 5.3 and *replace* with the new Clause 5.3 as follows:

5.3 Data representation and padding**5.3.1 General**

The authentication elements to be input to the MAC algorithm will form a data string D of length L_D bits. Initially the data string will be padded to a multiple of 64 bits, using Padding Method 1 or Padding Method 2. The padded data string will be accepted as concatenated blocks of 64 bits, $D_1 \dots D_n$.

5.3.2 Padding Method 1

The data string D shall be right-padded with as few (possibly none) '0' bits as necessary to obtain a data string whose length (in bits) is a positive integer multiple of 64.

NOTE: MAC algorithms using Padding Method 1 may be subject to trivial forgery attacks. See Appendix A for further details.

5.3.3 Padding Method 2

The data string D shall be right-padded with a single '1' bit. The resulting string shall then be right-padded with as few (possibly none) '0' bits as necessary to obtain a data string whose length (in bits) is a positive integer multiple of 64.

Page 7 Clause 5.5

Replace Clause title with the following:

5.5 MAC method 1

Page 8 Clause 5.7

Add a new Clause 5.7 as follows:

5.7 MAC method 2

MAC algorithm 2 provides a lower level of security than MAC algorithm 1 and is suitable for use when a comprehensive risk analysis has shown that a reduced level of security is acceptable for the intended application. MAC algorithm 2 uses DEA 1 as specified in AS 2805.5.1.

The 128-bit key used in this algorithm is decomposed into two 64-bit DEA-1 keys, KL and KR. To prevent exhaustion attacks against these sub-keys this MAC algorithm is only suitable when the entire process, including the key decomposition, is executed within the confines of a Secure Cryptographic Device from which no intermediate results are ever released.

If MAC algorithm 2 is to be used attention should be paid to the security analysis contained in Appendix A. Additionally, the number of MACs generated using the same key shall be restricted to the extent necessary to prevent shortcut key recovery attacks as described in reference [1] in Appendix A.

MAC algorithm 2 is illustrated in Figure 2.

NOTE: MAC Algorithm 2 is functionally identical to MAC Algorithm 3 as defined in ISO/IEC 9797-1.

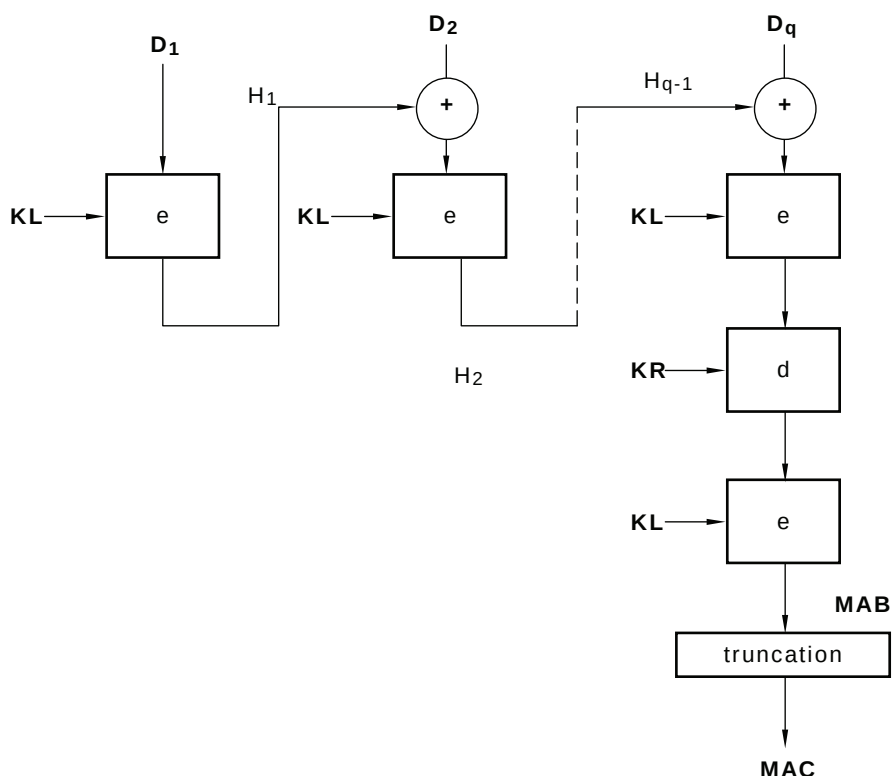


FIGURE 2 MAC ALGORITHM 2