

STANDARDS CHANGES CATALOG (SCC)

SCC NUMBER: SCC #132

CHANGE PROPOSAL TITLE: MIL-STD-2045-47001C, Application Header,
Authentication Data (A) Calculation and
Authentication Data (B) Calculation

ORIGINATOR and ADDRESS: Commanding Officer
US Army CECOM
ATTN: AMSEL-SE-CD
Fort Monmouth, NJ 07703
Stephen Turczyn, (732)532-8453
stephen.turczyn@mail1.monmouth.army.mil
Russell A. Moriarty
russell.moriarty@mail1.monmouth.army.mil

ORIGINATOR'S INTERNAL NUMBER:

AFFECTED DOCUMENT: MIL-STD-2045-47001C

PRECEDENCE: Routine

RECOMMENDATIONS:

RECORD OF PROCESSING

<u>DATE:</u>	<u>ACTION:</u>
18 Sep 02	Proposal
24 Sep 02	Work Item
17 Dec 02	Draft (R2)
14 Jan 03	(R3) Approved for MIL-STD-2045-47001C

1. STATEMENT OF THE PROBLEM: Paragraph D.4.1.1.5 of MIL-STD-2045-47001C describes how to calculate the hash value for the Authentication data (A). However, it refers to a 320-bit signature value; this is incorrect. The value could be from 64 bits to 8192 bits. Also, the method of not hashing the signature value itself is not specified.
2. PROBLEM ANALYSIS: Authentication data (A) can be any value from 64 bits to 8192 bits in 64-bit increments. Also, the method of ignoring the Authentication data (A) itself is not specified.
3. PROPOSED SOLUTION: The following modifications are to be made to Appendix D:

D.4.1.1.5 Authentication data (A).

D.4.1.1.5.1 Message is an original message.

The Authentication Data (A) field provides for data origin authentication, connectionless integrity and non-repudiation with proof of origin. It is generated by digitally signing the hash of both the application header and user data. The 160-bit hash is computed by the SHA-1 hashing algorithm. Note that the SHA-1 algorithm requires padding to be added to the original message to ensure it is a multiple of 512 bits, but this padding is utilized only by SHA-1 and should not be transmitted. The 320-bit signature is then computed from this 160-bit hash by the Digital Signature Algorithm (DSA). For purposes of hashing, the Authentication data (A) field shall be set to 320 zeroes; once the 320-bit signature has been generated from the 160-bit hash, the Authentication data (A) field shall be set to this 320-bit signature value. The signature algorithm is the DSA. The hashing algorithm is SHA-1. All values of the application header are hashed except for the 320-bit signature value. The input to the hash starts with the LSB of the first field of the application header. This corresponds with the header version field. It ends with the last byte of the uncompressed user message. When multiple user messages are present, a signature is calculated for each user message for which authentication is desired by digitally signing the hash of both the application header (with all Authentication data (A) fields zeroed out) and that particular instance of the user message.

D.4.1.1.5.2 Message is a signed acknowledgement.

When the message being prepared is a signed acknowledgement, both the Authentication data (A) and Authentication data (B) fields are required (see Section 5.7.2.1.7). When computing the hash of a signed acknowledgement, the Authentication data (A) field will be zeroed out but the Authentication data (B) field will contain its appropriate signature (see Section D.4.1.1.6 below). Since there is no user message in a signed acknowledgement, the hash will be computed from the header alone. When multiple signed acknowledgements are present, a signature is calculated for each one by digitally signing the hash of the entire application header (with all Authentication data (A) fields zeroed out and all Authentication data (B) fields containing their appropriate values). Thus, when multiple signed acknowledgements are present they will all have identical Authentication (A) fields.

D.4.1.1.6 Authentication data (B).

The Authentication Data (B) field provides for non-repudiation with proof of delivery (signed acknowledgment). It is generated by digitally signing the hash of both the entire original application header and the user data of the message being acknowledged. In this case the Authentication data (A) fields of the original message being acknowledged signature of the originator is are included within the hash calculation. The signature algorithm is the DSA. The hashing algorithm is SHA-1. The signature algorithm is the DSA. The input to the hash starts with the LSB of the first field of the original application header. This corresponds with the header version field. It ends with the last byte of the uncompressed original user data of the message being acknowledged.

The following modifications are to be made to Appendix E:

TABLE I. MIL-STD-2045-47001C application header (Continued)					
Item Number	Field Name	Reference	Status		Notes
			Tx	Rx	
			Support		
			Tx	Rx	
2.7.17.4.a	NOT PRESENT	5.5.3	2.7.17.4:M.<2> 2.7.17.1.a:M	Yes ___ ___ No ___ ___	
2.7.17.4.b	PRESENT	5.5.3	2.7.17.4:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.4.1	KEY TOKEN LENGTH	5.6.33 D.4.1.1.4	2.7.17.4.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.4.2	FRI (17)	5.5.2	2.3, 2.4, 2.5, 2.7.17.4:C	Yes ___ ___ No ___ ___	
2.7.17.4.2.a	NOT REPEATED	5.5.2	2.7.17.4.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.4.2.b	REPEATED	5.5.2	2.7.17.4.2:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.4.3	KEY TOKEN	5.6.34	2.7.17.4.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.5	GPI FOR G14 (AUTHENTICATION GROUP (A))	5.5.3 5.7.2.2.13 D.4.1.1.5	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.5.a	NOT PRESENT	5.5.3	2.7.17.5:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.5.b	PRESENT	5.5.3	2.7.17.5:M.<2> 2.7.17.1.a:M	Yes ___ ___ No ___ ___	
2.7.17.5.1	AUTHENTICATION DATA (A) LENGTH	5.6.35	2.7.17.5.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.5.2	AUTHENTICATION DATA (A)	5.6.36 D.4.1.1.5.1	2.7.17.5.b:M 2.7.17.1:C	Yes ___ ___ No ___ ___	
2.7.17.6	GPI FOR G15 (AUTHENTICATION GROUP (B))	5.5.3 5.7.3.4 D.4.1.1.6	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.6.a	NOT PRESENT	5.5.3	2.7.17.6:M.<2>	Yes ___ ___ No ___ ___	
2.7.17.6.b	PRESENT	5.5.3	2.7.17.6:M.<2> 2.7.17.7:C 2.7.14.b:C	Yes ___ ___ No ___ ___	
2.7.17.6.1	AUTHENTICATION DATA (B) LENGTH	5.6.37	2.7.17.6.b:M	Yes ___ ___ No ___ ___	
2.7.17.6.2	AUTHENTICATION DATA (B)	5.6.38 D.4.1.1.6	2.7.17.6.b:M	Yes ___ ___ No ___ ___	
2.7.17.7	SIGNED ACKNOWLEDGE REQUEST INDICATOR	5.6.39 5.7.2.2.14 5.7.3.4 D.4.1.1.7	2.7.17.b:M	Yes ___ ___ No ___ ___	
2.7.17.8	GPI FOR G16 (MESSAGE SECURITY PADDING GROUP)	5.5.3 5.7.2.2.13	2.7.17.b:M	Yes ___ ___ No ___ ___	

4. ALTERNATIVE SOLUTIONS: None.

5. SYSTEM CHANGES REQUIRED: None.

6. CONFIGURATION ITEM DOCUMENTATION CHANGES: MIL-STD-2045-47001C
7. IMPACT ON INTEROPERABILITY: Specification of method of ignoring the signature value in the hash calculation is necessary to ensure interoperability.
8. IMPACT ON RELATED DOCUMENTS: None.
9. IMPLEMENTATION DATES: Immediately upon acceptance.
10. OTHER CONSIDERATIONS: None.
11. REFERENCES: None.
12. TROUBLE REPORTS (TRs) ADDRESSED IN THIS SCC: None