3GPP TSG SA WG3 Security — S3#20 **S3-010462**

16 - 19 October, 2001

Sydney, Australia

Source: Siemens Atea

Title: MAPsec counter mode of operation

Document for: Discussion / Decision

Agenda item: MAP security

Abstract

This contribution proposes to use the counter mode of operation as described in NIST 800-XXX 'Recommendation for Block Cipher Modes' that will be stable end of this year in stead of the counter mode of operation as drafted in SC 27 N 2711 (Enhancement of ISO IEC 10116) that is intended to become a new standard in 2003.

1 Introduction and problem statement

At SA3#18 in Phoenix an SA3-subgroup used a first draft version of an updated ISO IEC 10116 (carrying the ISO internal name SC 27 N 2711) to specify the MAPsec Encryption Algorithm within clause 5.6.1.1 of TS 33.200. It was unknown to the other SA3-participants that a draft-ISO document was used, and that the target date for completion of this standard update did not fit with the 3GPP rel-4 timeframe.

In the next paragraphs the status of 2 alternatives counter mode specifications (ISO or NIST) are described and an evaluation is performed.

2 Status of draft ISO IEC 10116 on 'Modes of operation for an n-bit block cipher algorithm'

The 1997-version of ISO IEC 10116 is the latest published official version, which does not describe the counter mode of operation.

At the time of writing of this contribution there is a second working draft available of ISO IEC 10116 [SC 27 N 2895].

According to the chairman of ISO JTC1/SC 27 (ISO workgroup which controls the development of ISO IEC 10116), the new version of the standard will be publicly available in 2003. The intermediate milestones are following: The first CD ballot[1] is expected for 11/2001, and the final DIS[2] ballot for 11/2002.

[1] Committee Draft = OSI Internal document

[2] Draft International Standard = Publicly available draft document

3 Status of draft NIST 800-XX on ‘Recommendation for Block Cipher Modes of Operation’

End of July NIST has published a draft recommendation for Block Cipher Modes of operation that includes a counter mode description. (See http://csrc.nist.gov/encryption/modes/ or embedded PDF object). This draft NIST recommendation is currently undergoing a public review. The target date for completion is scheduled at 11/2001, which is around the same time as the final approval of the AES block cipher.

"NIST-modes of
operations Draft.pdf"

The proposed counter mode of clause 5.5 perfectly matches the needs for MAPsec encryption.

4 ISO IEC 10116:200x or NIST 800-XX ?

From chapter 2, it is clear that the milestones for updating ISO IEC 10116 are too late with respect to MAPsec Rel-4 implementation. Referring intermediate draft versions of ISO IEC 10116:200x is no solution as it is only available to the members that participate within the ISO-organization. Additionally 3GPP could risk incompatible implementations of the counter mode when small changes are introduced between different draft versions.

The possible solution to temporarily copy all available draft ISO IEC 10116 counter mode information into an annex of TS 33.200 is not favored, as it is a cumbersome process and again risks to introduce incompatibilities.

From chapter 3, we know that the timeline for finishing the official NIST Publication on ‘Block Cipher Modes of Operation’ is end of this year.   This is more than 1 year in advance of ISO IEC 10116:200x. In addition, the NIST-document is currently publicly available for review. It contains a suitable counter mode of operation for AES, just as envisaged by SA3#18 in Phoenix.

5 Status of discussions of MAPsec Adhoc in Sophia Antipolis 13 September 2001 (from MAPsec Adhoc draft report)

TD S3z010090 Introduced by Siemens. Proposed that MAPsec Encryption Mode be based on counter mode described in NIST 800-XX. It was reported that this draft had been removed from the internet site, probably for additional changes (unknown by the group). It was also noted that ISO/IEC 10116 was also not stable, and was targeted for completion in 2003. After some discussion over the use of algorithm specs, it was decided to postpone this issue to SA WG3#20 meeting where the status of the algorithms could be reviewed. **The majority of those present at the ad-hoc meeting were in favour of using the NIST standard.** The CR could not be agreed as the NIST standard had not been finalised.

6 Conclusions

Siemens proposes that the MAPsec Encryption Mode shall be based on the counter mode that is described in the upcoming NIST 800-XX ‘Recommendation for Block Cipher Modes of Operation’ targetted for 11/2001. This shall be implemented in a CR to TS 33.200.

3GPP TSG SA WG3 Security — S3#20 **S3-010xxx**

16 - 19 October, 2001

Sydney, Australia

CR-Form-v4

CHANGE REQUEST

⌘	**33.200**	**CR**		⌘	ev	**-**	⌘	Current version:	**4.1.0**	⌘

*For **HELP** on using this form, see bottom of this page or look at the pop-up text over the ⌘ symbols.*

Proposed change affects: ⌘ (U)SIM ☐ ME/UE ☐ Radio Access Network ☐ Core Network ☒

Title: ⌘	MEA encryption algorithm update		
Source: ⌘	Siemens Atea		
Work item code: ⌘	MAPsec	***Date:*** ⌘	09-Oct-2001
Category: ⌘	**F**	***Release:*** ⌘	Rel-4

Use <u>one</u> of the following categories:
- ***F*** *(correction)*
- ***A*** *(corresponds to a correction in an earlier release)*
- ***B*** *(addition of feature),*
- ***C*** *(functional modification of feature)*
- ***D*** *(editorial modification)*

Detailed explanations of the above categories can be found in 3GPP TR 21.900.

Use <u>one</u> of the following releases:

2	*(GSM Phase 2)*
R96	*(Release 1996)*
R97	*(Release 1997)*
R98	*(Release 1998)*
R99	*(Release 1999)*
REL-4	*(Release 4)*
REL-5	*(Release 5)*

Reason for change: ⌘	The counter mode of operation, that is currently referred too, is described in a not publicly available draft version of an ISO standard that is targetted for completion in 2003.
Summary of change: ⌘	The NIST specified counter mode of operation shall be used.
Consequences if not approved: ⌘	Inconsistent counter mode implementations may arise as there will be no official ISO IEC 10116:200x available including a counter mode of operation until begin 2003. A publicly available draft version will be available end of 2002. This may delay the implementation and use of MAPsec Rel-4.

Clauses affected: ⌘	2 ; 5.6.1	
Other specs affected: ⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘
Other comments: ⌘		

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] 3G TS 21.133: Security Threats and Requirements.

[2] 3G TS 21.905: 3G Vocabulary.

[3] 3G TS 23.060: General Packet Radio Service (GPRS); Service description; Stage 2.

[4] 3G TS 29.002: Mobile Application Part (MAP) specification.

[5] NIST Special Publication 800-XX Recommendation for Block Cipher Modes of Operation July 2001 ~~ISO/IEC 10116: "Information technology -- Security techniques -- Modes of operation for an n-bit block cipher", Ed.2, 1997-04-17.~~

[6] ISO/IEC 9797: "Information technology -- Security techniques -- Message Authentication Codes (MACs) -- Part 1: Mechanisms using a block cipher"**,** Ed.1, 1999-12-16.

***** next modified chapter ****

5.6 MAPsec algorithms

5.6.1 Mapping of MAP-SA encryption algorithm identifiers

The MEA algorithm indication fields in the MAP-SA are used to identify the encryption algorithm and algorithm mode to be used. The mapping of algorithm identifiers is defined below.

Table 1: MAP encryption algorithm identifiers

MAP Encryption Algorithm identifier	Description
0	Null
1	AES in counter Mode with 128-bit key length~~in a stream cipher mode~~ (MANDATORY)
:	-not yet assigned-
15	-not yet assigned-

5.6.1.1 Description of MEA-1

The MEA-1 algorithm is AES used in counter mode with a 128-bit key and 128-bit counter blocks as described ~~is the~~ in clause 5.5 of FIPS 800-XX Recommendation for Block Cipher Modes of Operation [5]. The initial counter block T_1 is initialized with IV. Successive counter blocks T_j (J>1) are derived by applying an incrementing function over the entire block T_{j-1} (J>=2) (see Appendix B.1: The standard incrementing function of [5]) .

The MAPsec cleartext shall be cut into P_j blocks of 128 bits . If the last block P_n has less than 128-bits (z bits), then it shall be encrypted by bitwise addition with only the first z bits of output block n (Clause 5.5 of [5]).

~~ISO/IEC 10116 Counter Mode with parameter j=128 bits, SV=IV and truncation of the last block is according to the method described in ISO/IEC 10116 Annex A.5.3. See ISO/IEC 10116 [5] for more information.~~

~~Editor's Note: More specification on the mode of operation for MEA-1 may be required.~~