3GPP TSG CN Plenary Meeting #12 Tdoc NP-010348
Stockholm, Sweden, 13th - 15th June 2001

Source: TSG CN WG4

Title: CRs on Rel-4 Work Item Security Enhancement

Agenda item: 8.10

Document for: APPROVAL

Introduction:

This document contains 2 CRs on Rel-4 Work Item ”Security”, that have been agreed by TSG CN WG4, and are forwarded to TSG CN Plenary meeting #12 for approval.

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
29.002	168	5	N4-010778	Rel-4	Security Header modification	C	4.3.0
29.002	289	2	N4-010790	Rel-4	Component level granularity of protection	F	4.3.0

3GPP TSG-CN-WG4 Meeting #08_1_Ad_Hoc
Teleconference, 6 - 7 June 2001

N4-010778

CR-Form-v3

CHANGE REQUEST

⌘	**29.002**	**CR**	**168**	⌘	rev	**5**	⌘	Current version:	**4.3.0** ⌘

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:	⌘	Security Header modification			
Source:	⌘	Siemens			
Work item code:	⌘	Security	***Date:***	⌘	7 June 2001
Category:	⌘	C	***Release:***	⌘	REL-4

Use one of the following categories:
F *(essential 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 one 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:	⌘	To align 29.002 with 33.200
Summary of change:	⌘	Security header definition is modified
Consequences if not approved:	⌘	TS 29.002 is not inline with TS 33.200

Clauses affected:	⌘	2, 7.6.12.1, 17.7.14	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘	linked with approval of 33.200 all references to 3GPP 33.102 shall be replaced with a reference to 3GPP 33.200	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

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.

[1] 3G TS 21.905: "3G Vocabulary".

[2] GSM 02.01: "Digital cellular telecommunications system (Phase 2+); Principles of telecommunication services supported by a GSM Public Land Mobile Network (PLMN)".

[3] 3G TS 22.002: "Bearer Services Supported by a GSM Public Land Mobile Network (PLMN)".

[4] GSM 02.03: "Digital cellular telecommunications system (Phase 2+); Teleservices Supported by a GSM Public Land Mobile Network (PLMN)".

[5] 3G TS 22.004: "General on Supplementary Services".

[6] GSM 02.09: "Digital cellular telecommunications system (Phase 2+); Security aspects".

[7] 3G TS 22.016: "International Mobile station Equipment Identities (IMEI)".

[8] 3G TS 22.041: "Operator Determined Barring".

[9] 3G TS 22.081: "Line identification supplementary services - Stage 1".

[10] 3G TS 22.082: "Call Forwarding (CF) supplementary services - Stage 1".

[11] 3G TS 22.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services - Stage 1".

[12] 3G TS 22.084: "Multi Party (MPTY) Supplementary Services - Stage 1".

[13] 3G TS 22.085: "Closed User Group (CUG) supplementary services - Stage 1".

[14] 3G TS 22.086: "Advice of charge (AoC) Supplementary Services - Stage 1".

[15] 3G TS 22.088: "Call Barring (CB) supplementary services - Stage 1".

[16] 3G TS 22.090: "Unstructured Supplementary Service Data (USSD); - Stage 1".

[17] 3G TS 23.003: "Numbering, addressing and identification".

[18] GSM 03.04: "Digital cellular telecommunications system (Phase 2+); Signalling requirements relating to routeing of calls to mobile subscribers".

[19] 3G TS 23.007: "Restoration procedures".

[20] 3G TS 23.008: "Organisation of subscriber data".

[21] 3G TS 23.009: "Handover procedures".

[22] 3G TS 23.011: "Technical realization of Supplementary Services - General Aspects".

[23] 3G TS 23.012: "Location registration procedures".

[24] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions".

[25] 3G TS 23.038: "Alphabets and language".

[26] 3G TS 23.040: "Technical realization of the Short Message Service (SMS) Point to Point (PP)".

[26a] GSM 03.71: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Functional Description; Stage 2".

[27] 3G TS 23.081: "Line Identification Supplementary Services - Stage 2".

[28] 3G TS 23.082: "Call Forwarding (CF) Supplementary Services - Stage 2".

[29] 3G TS 23.083: "Call Waiting (CW) and Call Hold (HOLD) Supplementary Services - Stage 2".

[30] 3G TS 23.084: "Multi Party (MPTY) Supplementary Services - Stage 2".

[31] 3G TS 23.085: "Closed User Group (CUG) Supplementary Services - Stage 2".

[32] 3G TS 23.086: "Advice of Charge (AoC) Supplementary Services - Stage 2".

[33] 3G TS 23.088: "Call Barring (CB) Supplementary Services - Stage 2".

[34] 3G TS 23.090: "Unstructured Supplementary Services Data (USSD) - Stage 2".

[34a] 3G TS 33.200: "3G Security; Network domain security; MAP application layer security– ~~Stage 2~~".

[35] 3G TS 24.008: "Mobile Radio Interface Layer 3 specification; Core Network Protocols - Stage 3".

[36] 3G TS 24.010: "Mobile radio interface layer 3 Supplementary Services specification - General aspects".

[37] 3G TS 24.011: "Point-to-Point (PP) Short Message Service (SMS) support on mobile radio interface".

[37a] GSM 04.71: "Digital cellular telecommunications system (Phase 2+); Mobile radio interface layer 3 location services specification".

[38] 3G TS 24.080: "Mobile radio interface layer 3 supplementary services specification - Formats and coding".

[39] 3G TS 24.081: "Line identification supplementary services - Stage 3".

[40] 3G TS 24.082: "Call Forwarding (CF) Supplementary Services - Stage 3".

[41] 3G TS 24.083: "Call Waiting (CW) and Call Hold (HOLD) supplementary services - Stage 3".

[42] 3G TS 24.084: "Multi Party (MPTY) Supplementary Services - Stage 3".

[43] 3G TS 24.085: "Closed User Group (CUG) Supplementary Services - Stage 3".

[44] 3G TS 24.086: "Advice of Charge (AoC) Supplementary Services - Stage 3".

[45] 3G TS 24.088: "Call Barring (CB) Supplementary Services - Stage 3".

[46] 3G TS 24.090: "Unstructured Supplementary Services Data - Stage 3".

[47] GSM 08.02: "Digital cellular telecommunications system (Phase 2+); Base Station System - Mobile-services Switching Centre (BSS - MSC) interface principles".

[48] GSM 08.06: "Digital cellular telecommunications system (Phase 2+); Signalling transport mechanism specification for the Base Station System - Mobile-services Switching Centre (BSS - MSC) interface".

[49] GSM 08.08: "Digital cellular telecommunications system (Phase 2+); Mobile Switching Centre - Base Station System (MSC - BSS) interface Layer 3 specification".

[49a] GSM 08.08: "Digital cellular telecommunications system (Phase 2+); Mobile Switching Centre - Base Station System (MSC - BSS) interface Layer 3 specification".

[49a1] GSM 08.31: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre (SMLC) – Serving Mobile Location Centre (SMLC); SMLC Peer Protocol (SMLCPP)".

[49b] GSM 08.71: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Serving Mobile Location Centre - Base Station System (SMLC - BSS) interface Layer 3 specification".

[50] GSM 09.01: "Digital cellular telecommunications system (Phase 2+); General network interworking scenarios".

[51] 3G TS 29.002: "Mobile Application Part (MAP) specification".

[52] GSM 09.03: "Digital cellular telecommunications system (Phase 2+); Signalling requirements on interworking between the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN) and the Public Land Mobile Network (PLMN)".

[53] GSM 09.04: "Digital cellular telecommunications system (Phase 2+); Interworking between the Public Land Mobile Network (PLMN) and the Circuit Switched Public Data Network (CSPDN)".

[54] GSM 09.05: "Digital cellular telecommunications system (Phase 2+); Interworking between the Public Land Mobile Network (PLMN) and the Packet Switched Public Data Network (PSPDN) for Packet Assembly/Disassembly facility (PAD) access".

[55] 3G TS 29.006: "Interworking between a Public Land Mobile Network (PLMN) and a Packet Switched Public Data Network/Integrated Services Digital Network (PSPDN/ISDN) for the support of Packet Switched data transmission services".

[56] 3G TS 29.007: "Digital cellular telecommunications system (Phase 2+); General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)".

[57] GSM 09.08: "Digital cellular telecommunications system (Phase 2+); Application of the Base Station System Application Part (BSSAP) on the E-interface".

[58] 3G TS 29.010: "Information element mapping between Mobile Station - Base Station System and BSS - Mobile-services Switching Centre (MS - BSS - MSC) Signalling procedures and the Mobile Application Part (MAP)".

[59] 3G TS 29.011: "Signalling interworking for Supplementary Services".

[59a] GSM 09.31: "Digital cellular telecommunications system (Phase 2+); Location Services (LCS); Base Station System Application Part LCS Extension (BSSAP-LE)".

[60] GSM 09.90: "Digital cellular telecommunications system (Phase 2+); Interworking between Phase 1 infrastructure and Phase 2 Mobile Stations (MS)".

[61] GSM 12.08: "Digital cellular telecommunications system (Phase 2); Subscriber and Equipment Trace".

[62] ETS 300 102-1 (1990): "Integrated Services Digital Network (ISDN); User-network interface layer 3 specifications for basic call control".

[63] ETS 300 136 (1992): "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service description".

[64] ETS 300 138 (1992): "Integrated Services Digital Network (ISDN); Closed User Group (CUG) supplementary service Digital Subscriber Signalling System No.one (DSS1) protocol".

[65] ETS 300 287: "Integrated Services Digital Network (ISDN); Signalling System No.7; Transaction Capabilities (TC) version 2".

[66] ETR 060: "Signalling Protocols and Switching (SPS); Guide-lines for using Abstract Syntax Notation One (ASN.1) in telecommunication application protocols".

[67] ITU-T Recommendation E.164: "Numbering plan for the ISDN era".

[68] ITU-T Recommendation E.212: "Identification plan for land mobile stations".

[69] ITU-T Recommendation E.213: "Telephone and ISDN numbering plan for land mobile stations".

[70] ITU-T Recommendation E.214: "Structuring of the land mobile global title for the signalling connection control part".

[71] CCITT Recommendation Q.699: "Interworking between the Digital Subscriber Signalling System Layer 3 protocol and the Signalling System No.7 ISDN User part".

[72] ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Functional description of the Signalling Connection Control Part".

[73] ITU-T Recommendation Q.712: "Definition and function of SCCP messages".

[74] ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; SCCP formats and codes".

[75] ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling Connection Control Part procedures".

[76] ITU-T Recommendation Q.716: "Specifications of Signalling System No.7; Signalling connection control part (SCCP) performances".

[77] ITU-T Recommendation Q.721 (1988): "Specifications of Signalling System No.7; Functional description of the Signalling System No.7 Telephone user part".

[78] ITU-T Recommendation Q.722 (1988): "Specifications of Signalling System No.7; General function of Telephone messages and signals".

[79] ITU-T Recommendation Q.723 (1988): "Specifications of Signalling System No.7; Formats and codes".

[80] ITU-T Recommendation Q.724 (1988): "Specifications of Signalling System No.7; Signalling procedures".

[81] ITU-T Recommendation Q.725 (1988): "Specifications of Signalling System No.7; Signalling performance in the telephone application".

[82] ITU-T Recommendation Q.761 (1988): "Specifications of Signalling System No.7; Functional description of the ISDN user part of Signalling System No.7".

[83] ITU-T Recommendation Q.762 (1988): "Specifications of Signalling System No.7; General function of messages and signals".

[84] ITU-T Recommendation Q.763 (1988): "Specifications of Signalling System No.7; Formats and codes".

[85] ITU-T Recommendation Q.764 (1988): "Specifications of Signalling System No.7; Signalling procedures".

[86] ITU-T Recommendation Q.767: "Specifications of Signalling System No.7; Application of the ISDN user part of CCITT signalling System No.7 for international ISDN interconnections".

[87] ITU-T Recommendation Q.771: "Specifications of Signalling System No.7; Functional description of transaction capabilities".

[88] ITU-T Recommendation Q.772: "Specifications of Signalling System No.7; Transaction capabilities information element definitions".

[89] ITU-T Recommendation Q.773: "Specifications of Signalling System No.7; Transaction capabilities formats and encoding".

[90] ITU-T Recommendation Q.774: "Specifications of Signalling System No.7; Transaction capabilities procedures".

[91] ITU-T Recommendation Q.775: "Specifications of Signalling System No.7; Guide-lines for using transaction capabilities".

[92] ITU-T Recommendation X.200: "Reference Model of Open systems interconnection for CCITT Applications".

[93] ITU-T Recommendation X.208 (1988): "Specification of Abstract Syntax Notation One (ASN.1)".

[94] ITU-T Recommendation X.209 (1988): "Specification of basic encoding rules for Abstract Syntax Notation One (ASN.1)".

[95] ITU-T Recommendation X.210: "Open systems interconnection layer service definition conventions".

[97] 3G TS 23.018: "Basic Call Handling".

[98] 3G TS 23.078: "Customised Applications for Mobile network Enhanced Logic (CAMEL) Phase 3 - Stage 2".

[99] 3G TS 23.079: "Support of Optimal Routeing (SOR) - Stage 2".

[100] GSM 03.68: "Digital cellular telecommunications system (Phase 2+); - Stage 2".

[101] GSM 03.69: "Digital cellular telecommunications system (Phase 2+); - Stage 2".

[102] ANSI T1.113: "Signaling System No. 7 (SS7) - ISDN User Part".

[103] 3G TS 23.054 "Shared Inter Working Function (SIWF) - Stage 2".

[104] 3G TS 23.060: "General Packet Radio Service (GPRS) Description; Stage 2".

[105] 3G TS 29.060: "General Packet Radio Service (GPRS); GPRS Tunnelling Protocol (GTP) across the Gn and Gp Interface".

[106] 3G TS 29.018: "General Packet Radio Service (GPRS); Serving GPRS Support Node (SGSN) - Visitors Location Register (VLR); Gs interface layer 3 specification".

[107] 3G TS 23.093: "Technical Realization of Completion of Calls to Busy Subscriber (CCBS); Stage 2".

[108] 3G TS 23.066: "Support of Mobile Number Portability (MNP); Technical Realisation Stage 2".

[109] ANSI T1.112 (1996): "Telecommunication – Signalling No. 7 - Signaling Connection Control Part (SCCP)".

[110] 3G TS 23.116: "Super-Charger Technical Realisation; Stage 2."

[111] ITU-T Recommendation Q.711: "Specifications of Signalling System No.7; Signalling System No. 7 – Functional Description of the Signalling Connection Control Part".

[112] ITU-T Recommendation Q.712: "Specifications of Signalling System No.7; Signalling System No. 7 – Definition and Function of SCCP Messages".

[113] ITU-T Recommendation Q.713: "Specifications of Signalling System No.7; Signalling System No. 7 – SCCP formats and codes".

[114] ITU-T Recommendation Q.714: "Specifications of Signalling System No.7; Signalling System No. 7 – Signalling Connection Control Part Procedures".

[115] ITU-T Recommendation Q.716: "Specifications of Signalling System No.7; Signalling System No. 7 – Signalling Connection Control Part (SCCP) Performance".

[116] ITU-T Q.850, May 1998: "Usage of cause and location in the Digital Subscriber Signalling System No. 1 and the Signalling System No. 7 ISDN User Part".

[117] 3G TS 22.135: "Multicall; Service description; Stage 1".

[118] 3G TS 23.135: "Multicall supplementary service; Stage 2".

[119] 3G TS 24.135: "Multicall supplementary service; Stage 3".

[120] 3G TS 25.413: "UTRAN Iu Interface RANAP Signalling".

**** Next modified section ****

7.6.12 Secure Transport Parameters

7.6.12.1 Security Header

This parameter carries the security header information which is required by a receiving entity in order to extract the protected information from a securely transported MAP message. The components of the security header are shown in table 7.6.12/1.

See 3GPP TS 33.200~~102~~ for the use of these parameters.

Table 7.6.12/1: Components of the Security Header

Component name	Presence requirement	Description
~~Sending PLMN identity~~	~~M~~	~~The Mobile Country Code and the Mobile Network Code of the PLMN which sent the secure MAP message.~~
~~Protection mode~~	~~M~~	~~The protection mode required for the message – one of:~~ ~~- No protection;~~ ~~- Integrity & Authenticity;~~ ~~- Integrity, Authenticity & Confidentiality.~~
~~Encryption algorithm identifier~~	~~C~~	~~Identifies the encryption algorithm to be used for confidentiality protection. Shall be present if Protection mode indicates 'Integrity, Authenticity & Confidentiality"; otherwise shall be absent.~~
~~Mode of operation~~	~~C~~	~~The mode of operation for confidentiality protection – one of:~~ ~~- ECB;~~ ~~- CBC;~~ ~~- CFB;~~ ~~- OFB.~~ ~~Modes of operation are defined in ISO/IEC 10116 (1991). Shall be present if Encryption algorithm identifier is present; otherwise shall be absent.~~
~~Key version number for Encryption algorithm key~~	~~C~~	~~The version number of the protection key to be used. Shall be present if Encryption algorithm identifier is present; otherwise shall be absent.~~
~~Hash algorithm identifier~~	~~C~~	~~Identifies the hash algorithm to be used for integrity protection. Shall be present if Protection mode is not 'No protection'; otherwise shall be absent.~~
~~Key version number for Hash algorithm key~~	~~C~~	~~The version number for the key used for the Hash algorithm. Shall be present if Hash algorithm identifier is present; otherwise shall be absent.~~
Initialisation vector	M~~C~~	An initialisation vector for the message protection function. The TVP part of the IV is mandatory. The other parts shall be present if required for the current Protection Mode.~~Shall be present if the Mode of operation is CBC, CFB or OFB, otherwise shall be absent.~~
Sending PLMN identity	M	The Mobile Country Code and the Mobile Network Code of the PLMN which sent the secure MAP message.
Security Parameters Index	M	Identifies the Security Association for the component.
Original component identifier	M	Identifies the type of component to be securely transported – one of: - Operation, identified by the operation code; - Error, defined by the error code; - User information.

.....

**** Next modified section ****

17.7.14 Secure transport data types

```
MAP-ST-DataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-ST-DataTypes (27) version7 (7)}

DEFINITIONS
IMPLICIT TAGS
::=
BEGIN

EXPORTS
        SecureTransportArg,
        SecureTransportRes,
        SecurityHeader,
        ProtectedPayload
;

IMPORTS
        IMSI,
        PLMN-Id

FROM MAP-CommonDataTypes {
   ccitt identified-organization (4) etsi (0) mobileDomain (0)
   gsm-Network (1) modules (3) map-CommonDataTypes (18) version7 (7)}
;
```

```
SecureTransportArg ::= SEQUENCE {
     securityHeader                           SecurityHeader,
     protectedPayload                         ProtectedPayload             OPTIONAL
     }
     -- The protectedPayload carries the result of applying the security function
     -- defined in 3G TS 33.200~~102~~ to the encoding of the argument of the securely
     -- transported operation
```

```
SecureTransportRes ::= SEQUENCE {
     securityHeader                           SecurityHeader,
     protectedPayload                         ProtectedPayload             OPTIONAL
     }
     -- The protectedPayload carries the result of applying the security function
     -- defined in 3G TS 33.200~~102~~ to the encoding of the result of the securely
     -- transported operation
```

```
SecurityHeader ::= SEQUENCE {
     initialisationVector                InitialisationVector,
     sendingPLMN-Id                      PLMN-Id,
     securityParametersIndex             SecurityParametersIndex,
     originalComponentIdentifier         OriginalComponentIdentifier,
     ~~sendingPLMN-Id                      PLMN-Id,~~
     ~~protectionMode                      [0] ProtectionMode                OPTIONAL,~~
     ~~encryptionAlgorithmIdentifier       [1] EncryptionAlgorithmIdentifier OPTIONAL,~~
     ~~modeOfOperation                     [2] ModeOfOperation               OPTIONAL,~~
     ~~encryptionKeyVersionNumber          [3] EncryptionKeyVersionNumber    OPTIONAL,~~
     ~~initialisationVector                [4] InitialisationVector          OPTIONAL,~~
     ~~hashAlgorithmIdentifier             [5] HashAlgorithmIdentifier       OPTIONAL,~~
     ~~hashKeyVersionNumber                [6] HashKeyVersionNumber          OPTIONAL,~~
     ...}
```

```
ProtectedPayload ::= OCTET STRING(SIZE(1..3438~~1000~~))
     -- In protection mode 0 (noProtection) the ProtectedPayload carries the transfer
          -- syntax value of the component parameter identified by the
          -- originalComponentIdentifier.
     -- In protection mode 1 (integrityAuthenticity) the protectedPayload carries ~~4~~
          -- ~~octets TVP, followed by~~ the transfer syntax value of the component
          -- parameter identified by the originalComponentIdentifier, followed by
          -- the 32 bit integrity check value.
          -- The integrity check value is the result of applying the hash algorithm
          -- to the concatenation of ~~TVP,~~the transfer syntax value of the SecurityHeader,
          -- and the transfer syntax value of the component parameter.
     -- In protection mode 2 (confidentialityIntegrityAuthenticity) the protected
          -- payload carries ~~4 octets TVP, followed by~~ the encrypted transfer syntax
          -- value of the component parameter identified by the
          -- originalComponentIdentifier, followed by the 32 bit integrity check value.
          -- The integrity check value is the result of applying the hash algorithm
          -- to the concatenation of ~~TVP,~~the transfer syntax value of the SecurityHeader,
          -- and the encrypted transfer syntax value of the component parameter.
     -- See 33.200~~102~~.
     -- The length of the protectedPayload is adjusted according to the capabilities of
     -- the lower protocol layers
```

```
~~ProtectionMode ::= ENUMERATED {~~
~~     noProtection                         (0),~~
~~     integrityAuthenticity                (1),~~
~~     confidentialityIntegrityAuthenticity (2)}~~
```

```
~~EncryptionAlgorithmIdentifier ::= INTEGER (1..127)~~
~~     -- The encryption algorithm corresponding to each value of the Encryption~~
~~     -- Algorithm Identifier type is defined in TS 33.102~~
```

```
~~HashAlgorithmIdentifier ::= INTEGER (1..127)~~
~~     -- The encryption algorithm corresponding to each value of the Hash Algorithm~~
~~     -- Identifier type is defined in TS 33.102~~
```

```
~~ModeOfOperation ::= ENUMERATED {~~
~~     ecb                                  (0),~~
~~     cbc                                  (1),~~
~~     cfb                                  (2),~~
~~     ofb                                  (3),~~
~~     ...}~~
~~     -- Modes of operation are defined in ISO/IEC 10116 (1991)~~
```

```
~~EncryptionKeyVersionNumber ::= INTEGER (0..127)~~
```

```
~~HashKeyVersionNumber ::= INTEGER (0..127)~~
```

```
SecurityParametersIndex ::= OCTET STRING (SIZE(4))
```

```
InitialisationVector ::= OCTET STRING (SIZE(4..14~~8~~))
     -- the internal structure is defined as follows:
     -- Octets 1 to 4 : TVP. The TVP is a 32 bit time stamp. Its value is binary coded
     --                    and indicates the number of intervals of ~~1/~~100 ~~of ~~milliseconds
     --                    ela~~p~~psed since
     ~~--~~                  1st January ~~1st,~~2002, 0:00:00 UTC
     -- Octets 5 to 10: NE-Id. The NE-Id uniquely identifies the sending network entity
     --                    within the PLMN. It is the entity~~ie~~'s E.164 number without CC
and
     --                    NDC. It is TBCD-coded, padded with zeros.
     -- Octets 11 to 14: PROP. This 32 bit value is used to make the
     --                    InitialisationVector unique within the same TVP period.
     --                    The content is not standardized.
```

```
OriginalComponentIdentifier ::= CHOICE {
     operationCode                        [0] OperationCode,
     errorCode                            [1] ErrorCode,
     userInfo                             [2] NULL}
```

```
OperationCode ::= CHOICE {
     localValue                           INTEGER,
     globalValue                          OBJECT IDENTIFIER}
```

```
ErrorCode ::= CHOICE {
     localValue                           INTEGER,
     globalValue                          OBJECT IDENTIFIER}
```

END

3GPP TSG-CN WG4 ad hoc on MAP security
Telephone conference, 6 – 7 June 2001

Tdoc N4-010790
(Revision of N4-010777)

CR-Form-v4

CHANGE REQUEST

⌘ **29.002 CR 289** ⌘ rev **2** ⌘ Current version: **4.3.0** ⌘

*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:	⌘	Component level granularity of protection		
Source:	⌘	Vodafone		
Work item code:	⌘	SEC1	***Date:*** ⌘	6 June 2001
Category:	⌘	**F**	***Release:*** ⌘	REL-4

Use one 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 one 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:	⌘	3GPP TS 33.200 specifies the possibility of different protection levels for different components of the same operation. The currect text in the MAP specification does not correctly reflect this possibility
Summary of change:	⌘	Clarify the way in which the entities involved in a MAP dialogue decide whether to use secured or unsecured transport
Consequences if not approved:	⌘	Misalignment between stage 2 & stage 3 specifications; inter-operation problems because of different interpretations by different manufacturers

Clauses affected:	⌘	15.2.1; 15.5.4 (editorial correction); 15.6 (editorial correction)	
Other specs affected:	⌘	□ Other core specifications □ Test specifications □ O&M Specifications	⌘
Other comments:	⌘	If 3GPP TS 33.200 is not approved by SA#12, this change request falls	

How to create CRs using this form:

Comprehensive information and tips about how to create CRs can be found at: http://www.3gpp.org/3G_Specs/CRs.htm. Below is a brief summary:

1) Fill out the above form. The symbols above marked ⌘ contain pop-up help information about the field that they are closest to.

2) Obtain the latest version for the release of the specification to which the change is proposed. Use the MS Word "revision marks" feature (also known as "track changes") when making the changes. All 3GPP specifications can be downloaded from the 3GPP server under ftp://www.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2000-09 contains the specifications resulting from the September 2000 TSG meetings.

3) With "track changes" disabled, paste the entire CR form (use CTRL-A to select it) into the specification just in front of the clause containing the first piece of changed text. Delete those parts of the specification which are not relevant to the change request.

15.2 Dialogue establishment

The establishment of a MAP dialogue involves two MAP-service-users: the dialogue-initiator and the dialogue-responder.

This procedure is driven by the following signals:

- a MAP-OPEN request primitive from the dialogue-initiator;
- a TC-BEGIN indication primitive occurring at the responding side;
- a MAP-OPEN response primitive from the dialogue-responder;
- the first TC-CONTINUE indication primitive occurring at the initiating side;

and under specific conditions:

- a TC-END indication primitive occurring at the initiating side;
- a TC-U-ABORT indication primitive occurring at the initiating side;
- a TC-P-ABORT indication primitive occurring at the initiating side.

One instance of the MAP dialogue state machine runs at the initiating side, and one at the responding side.

15.2.1 Behaviour at the initiating side

The behaviour of the MAP dialogue state machine at the initiating side is defined in sheets 1 – 9 of the process Secure_MAP_DSM.

Sheet 1: The MAP protocol machine decides according to the application context name received in the MAP-OPEN request and the identity of the responder whether secure transport of the MAP dialogue is required, and if so what level of protection is required. This decision is based on bilateral agreements between the operators of the network entities concerned; it requires the dialogue initiating entity to store configuration information on which the decision is based. Secure transport of a MAP dialogue is required if any of the operation components (invoke, result or error) used in the application context for the dialogue requires secure transport, as shown in 3GPP TS 33.200. If a dialogue uses secure transport then MAP secure transport services shall be used with a protection mode of "No protection" to produce the same functional effect as unsecured transport for those components which do not need protection. If secure transport is required, the MAP protocol machine builds a protected dialogue portion (including the AC name and any user information received in the MAP-OPEN request, encoded as user information for the TC-BEGIN) for the TC-BEGIN; otherwise it builds a normal dialogue portion using the application context name and any user data included in the MAP-OPEN request.

...

**** Next modified section ****

15.5 Procedures for MAP specific services

...

15.5.4 Service invocation receipt for ~~un~~secured dialogues

The behaviour of the performing SSMs which handle a service for a secured dialogue is defined by the SDL for the processes Secure_Performing_MAP_SSM and Performing_MAP_SSM. The secure performing SSM receives a TC-INVOKE component containing a secure MAP transport service from TCAP via the MAP dialogue state machine and unpacks the MAP service indication from it. It then creates an instance of the performing SSM and sends the MAP service indication to it. The performing SSM forwards the MAP service indication to the MAP-Service User. When the MAP dialogue state machine receives a MAP service response from the MAP-Service User it forwards it to the secure performing SSM. The secure performing SSM constructs a MAP secure transport service response and sends it to the performing SSM, which forwards a TC-RESULT or TC-U-ERROR component to TCAP.

**** Next modified section ****

15.6 SDL descriptions

The following SDL specification describes a system which includes three blocks: MAP-user, MAP-provider and TC.

Such a system resides in each network component supporting MAP and communicates with its peers via the lower layers of the signalling network which are part of the environment.

Only the MAP-provider is fully described in this subclause. The various types of processes which form the MAP-User block and the TC block are described respectively in clauses 18 to 25 of the present document and in CCITT Recommendation Q.774.

The MAP-Provider block communicates with the MAP_USER via two channels U1 and U2. Via U1 the MAP-provider receives the MAP request and response primitives. Via U2 it sends the MAP indication and confirm primitives.

The MAP-Provider block communicates with TC via two channels P1 and P2. Via P1 the MAP-Provider sends all the TC request primitives. Via P2 it receives all the TC indication primitives.

The MAP-Provider block is composed of the six following types of process:

a) Secure_MAP_DSM: This type of process handles a dialogue for both secured and unsecured transport of MAP messages. There exists one process instance per MAP dialogue.

b) Load_Ctrl: This type of process is in charge of load control. There is only one instance of this process in each system.

c) Requesting_MAP_SSM: This type of process handles a MAP service requested during a dialogue. For unsecured transport of MAP messages, an instance of this process is created by the instance of the Secure_MAP_DSM process for each requested MAP_-service. For secured transport of MAP messages, an instance of this process is created by the instance of the Secure_Requesting_MAP_SSM process for each requested MAP-Secure-Transport-service.

d) Secure_ Requesting_MAP_SSM: This type of process handles a MAP service requested during a dialogue for secured transport of MAP messages. An instance of this process is created by the Secure_MAP_DSM process for each requested MAP_-service.

e) Performing_MAP_SSM: This type of process handles a MAP service performed during a dialogue. For unsecured transport of MAP messages, an instance of this process is created by the instance of the Secure_MAP_DSM process for each MAP_-service to be performed. For secured transport of MAP messages, an instance of this process is created by the instance of the Secure_Performing_MAP_SSM process for each MAP-Secure-Transport-service to be performed.

f) Secure_Performing_MAP_SSM: This type of process handles a MAP service performed during a dialogue for secured transport of MAP messages. An instance of this process is created by the Secure_MAP_DSM process for each MAP_-service to be performed.

...