3GPP TSG SA WG3 NDS ad hoc
Madrid, Spain
23-24 April 2001 **Tdoc S3z010030**

3GPP TSG CN4 Meeting #6
Beijing, 15th January - 19th January 2001 ***Document*** ***N4-010030***

CHANGE REQUEST

29.002	**CR**	**168r1**	Current Version: 4.1.0

For submission to:	CN#10	for approval	☒	strategic	□
		for information	□	non-strategic	□

Form: CR cover sheet, version 2 for 3GPP and SMG The latest version of this form is available from: ftp://ftp.3gpp.org/Information/CR-Form-v2.doc

Proposed change affects: (U)SIM □ ME □ UTRAN / Radio □ Core Network ☒
(at least one should be marked with an X)

Source:	Siemens	**Date:**	12st December 2000
Subject:	Security Header modification		
Work item:	Security		

Category:

Category:	F	Correction	□	**Release:**	Phase 2	□
	A	Corresponds to a correction in an earlier release	□		Release 96	□
	B	Addition of feature	□		Release 97	□
	C	Functional modification of feature	☒		Release 98	□
	D	Editorial modification	□		Release 99	□
					Release 00	☒

Reason for change: SA3 have decided to remove security parameters from the security header and replace them with a Security Parameter Index which (together with the sending and receiving PLMN-Id) identifies the Security Association.

Clauses affected: 7.6.12.1, 17.7.14

Other specs affected:	Other 3G core specifications	□	→ List of CRs:	
	Other GSM core specifications	□	→ List of CRs:	
	MS test specifications	□	→ List of CRs:	
	BSS test specifications	□	→ List of CRs:	
	O&M specifications	□	→ List of CRs:	

Other comments:

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 3G TR~~S~~ 33.800~~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	C	An initialisation vector for the message protection function. Shall be present if required by the Security Association~~the Mode of operation is CBC, CFB or OFB~~, otherwise shall be absent.
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.
Security Parameters Index	M	Identifies the Security Association for the component.

.....

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 TR~~S~~ 33.800~~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 TR~~S~~ 33.800~~102~~ to the encoding of the result of the securely
     -- transported operation
```

```
SecurityHeader ::= SEQUENCE {
     originalComponentIdentifier         OriginalComponentIdentifier,
     sendingPLMN-Id                      PLMN-Id,
     securityParametersIndex             SecurityParametersIndex,
~~     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 integrity check value.
          -- The integrity check value is the result of applying the hash algorithm
          -- to the concatenation of TVP, transfer syntax value of the SecurityHeader,
          -- 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 integrity check value.
          -- The integrity check value is the result of applying the hash algorithm
          -- to the concatenation of TVP, transfer syntax value of the SecurityHeader,
          -- encrypted transfer syntax value of the component parameter.
     -- See 33.800~~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(2~~8~~..32))
```

```
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
```