3GPP TSG CN Plenary Meeting #14 **NP-010622**
Kyoto, JAPAN, 12th -14th December 2001

Source: TSG CN WG4

Title: CRs on Rel-4 Security Enhancement

Agenda item: 8.10

Document for: APPROVAL

Introduction:

This document contains a CR on Rel-4 Work Item "SEC1", that have been agreed by TSG CN WG4, and are forwarded to TSG CN Plenary meeting #14 for approval.

Spec	CR	Rev	Doc-2nd-Level	Phase	Subject	Cat	Ver_C
29.002	360	1	N4-011423	Rel-4	Aligning the security header elements with TS33.200	F	4.5.0

3GPP TSG CN WG4 Meeting #11 ***N4-011423***
Cancun, Mexico, 26th - 30th November 2001

CR-Form-v5

CHANGE REQUEST

⌘ **29.002** **CR** **360** ⌘ **rev** **1** ⌘ Current version: **4.5.0** ⌘

*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:	⌘	Aligning the security header elements with TS33.200
Source:	⌘	CN4
Work item code:	⌘	TEI-4
Date:	⌘	28-11-2001
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:	⌘	To align 29.002 with TS 33.200. Changes in SA3 have been made to remove redundancy in the security header.
Summary of change:	⌘	Security header elements are modified to remove two existing elements (Initialisation Vector and Sending PLMN Identity) and add three optional elements (TVP, NE-Id, Prop). These new elements contain similar information to the Initialisation Vector.
Consequences if not approved:	⌘	Specifications are not aligned and interoperability may be affected.

Clauses affected:	⌘	7.6.12.1, 17.7.8, 17.7.14
Other specs affected:	⌘	☒ Other core specifications ⌘ TS33.200 ☐ Test specifications ☐ O&M Specifications
Other comments:	⌘	

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://ftp.3gpp.org/specs/ For the latest version, look for the directory name with the latest date e.g. 2001-03 contains the specifications resulting from the March 2001 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.

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 for the use of these parameters.

Table 7.6.12/1: Components of the Security Header

Component name	Presence requirement	Description
~~Initialisation vector~~	~~M~~	~~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.~~
~~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.
TVP	O	A parameter based on time that is used to ensure the current message is fresh. This is only present if required for the current Protection Mode.
NE-Id	O	The identity of the Network Element sending the message. This is only present if required for the current Protection Mode.
Prop	O	Bytes used to ensure the IV is unique for a given TVP and NE-Id. This is only present if required for the current Protection Mode.

****** NEXT MODIFIED SECTION ******

17.7.8 Common data types

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

DEFINITIONS

IMPLICIT TAGS

::=

BEGIN

EXPORTS

   -- general data types and values
   AddressString,
   ISDN-AddressString,
   maxISDN-AddressLength,
   FTN-AddressString,
   ISDN-SubaddressString,
```

```
   ExternalSignalInfo,
   Ext-ExternalSignalInfo,
   AccessNetworkSignalInfo,
   SignalInfo,
   maxSignalInfoLength,
   AlertingPattern,

   -- data types for numbering and identification
   IMSI,
   TMSI,
   Identity,
   SubscriberId,
   IMEI,
   HLR-List,
   LMSI,
   GlobalCellId,
   NetworkResource,
   NAEA-PreferredCI,
   NAEA-CIC,
   ASCI-CallReference,
   SubscriberIdentity,
   PLMN-Id,

   -- data types for CAMEL
   CellGlobalIdOrServiceAreaIdOrLAI,

   -- data types for subscriber management
   BasicServiceCode,
   Ext-BasicServiceCode,
   EMLPP-Info,
   EMLPP-Priority,
   MC-SS-Info,
   MaxMC-Bearers,
   MC-Bearers,
   Ext-SS-Status,

   -- data types for geographic location
   AgeOfLocationInformation,
   LCSClientExternalID,
   LCSClientInternalID
;


…
Unmodified ASN.1
…
```

```
LCSClientInternalID ::= ENUMERATED {
     broadcastService                    (0),
     o-andM-HPLMN                        (1),
     o-andM-VPLMN                        (2),
     anonymousLocation                   (3),
     targetMSsubscribedService           (4),
     ... }
-- for a CAMEL phase 3 PLMN operator client, the value targetMSsubscribedService shall be used
```

```
PLMN-Id ::= TBCD-STRING (SIZE (3))
     -- digits of MCC, MNC, are concatenated in this order.

-- data types for CAMEL
```

****** 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 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 to the encoding of the result of the securely
     -- transported operation
```

```
SecurityHeader ::= SEQUENCE {
     initialisationVector                    InitialisationVector,
     sendingPLMN-Id                          PLMN-Id,
     securityParametersIndex                 SecurityParametersIndex,
     originalComponentIdentifier             OriginalComponentIdentifier,
     initialisationVector                    InitialisationVector            OPTIONAL,
     ...}
```

```
ProtectedPayload ::= OCTET STRING(SIZE(1.. 3438))
     -- 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
          --  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 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 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 the transfer syntax value of the SecurityHeader,
          -- and the encrypted transfer syntax value of the component parameter.
     -- See 33.200.
     -- The length of the protectedPayload is adjusted according to the capabilities of
     -- the lower protocol layers
```

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

```
InitialisationVector ::= OCTET STRING (SIZE(4...14))
     -- 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 100 milliseconds
     --                 elapsed since 1st January 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'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
```