3GPP TSG CN Plenary Meeting #12 **Tdoc NP-010295**
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 1 CR on Rel-4 Work Item "Security Enhancement", 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	267	3	N4-010785	Rel-4	Additional Parameters in Authentication Failure Report	C	4.3.0

3GPP TSG-CN4 Meeting #8 ***Tdoc N4-010785***
Rio Grande, Puerto Rico, 14th May – 18th May 2001

CR-Form-v3

CHANGE REQUEST

⌘ **29.002** **CR** **267** ⌘ rev **3** ⌘ 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:	⌘	Additional Parameters in Authentication Failure Report
Source:	⌘	CN4
Work item code:	⌘	SEC1 - EHCS
Date:	⌘	2001-02-27
Category:	⌘	C
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 provide additional information to HE to detect fraud conditions, as requested by SA3 (N4-010514-S3-010131)
Summary of change:	⌘	Add new information elements, access type, authentication re-attempt, VLR/SGSN address and identitication of the AV that failed, to the authentication failure report service and protocol definitions.
Consequences if not approved:	⌘	

Clauses affected:	⌘	7.6.7, 8.5.3, 17.7.1		
Other specs Affected:	⌘	☐ Other core specifications ☐ Test specifications ☐ O&M Specifications	⌘	CR 33.102-139 (S3-010104)
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://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.

7.6.7 Authentication parameters

7.6.7.1 Authentication set list

This parameter represents a list of sets of authentication parameters for a given subscriber.

The list either contains Authentication Triplets (Rand, Sres, Kc) or Authentication Quintuplets (Rand, Xres, Ck, Ik, Autn). If the list contains Authentication Quintuplets, the order of sequence in this list is chronological, the first quintuplet in the list is the oldest one.

7.6.7.2 Rand

This parameter represents a random number used for authentication.

7.6.7.3 Sres

This parameter represents the response to an authentication request.

7.6.7.4 Kc

This parameter refers to a key used for ciphering purposes.

7.6.7.5 Xres

This parameter represents the response to an UMTS authentication request.

7.6.7.5A Ck

This parameter refers to a key used for UMTS ciphering purposes.

7.6.7.5B Ik

This parameter refers to the Integrity Key.

7.6.7.5C Autn

This parameter refers to the Authentication Token.

7.6.7.6 Cksn

This parameter refers to a ciphering key sequence number.

7.6.7.6A Ksi

This parameter refers to a key set identifier.

7.6.7.6B Auts

This parameter refers to the resynchronisation token.

7.6.7.7 Ciphering mode

This parameter refers to the ciphering mode which is associated with a radio channel. It may take values as follows:

- no encryption;
- identification of specific ciphering algorithm.

7.6.7.8 Current Security Context

This parameter represents a list of security context parameters for a given subscriber.

The list either contains GSM Security Context data (Kc, Cksn) or UMTS Security Context Data (Ck, Ik, Ksi).

7.6.7.9 Failure cause

This parameter refers to an authentication failure which has occurred. It may take values as follows:

- wrong user response;
- wrong network signature.

7.6.7.10 Re-attempt

It indicates whether the failure ocurred in a normal authentication attempt or in an authentication reattempt (there was a previous unsuccessful authentication).

7.6.7.11 Access Type

It indicates whether the authentication procedure was initiated due to a call, an emergency call, a location updating, a supplementary service procedure or a short message transfer.

8.5.3 MAP_AUTHENTICATION_FAILURE_REPORT service

8.5.3.1 Definition

This service is used between the VLR and the HLR or between the SGSN or HLR for reporting of authentication failures.

8.5.3.2 Service primitives

The service primitives are shown in table 8.5/3.

Table 8.5/3: MAP_AUTHENTICATION_FAILURE_REPORT parameters

Parameter name	Request	Indication	Response	Confirm
Invoke id	M	M(=)	M(=)	M(=)
IMSI	M	M(=)		
Failure cause	M	M(=)		
Re-attempt	M	M(=)		
Access Type	M	M(=)		
Rand	M	M(=)		
VLR number	C	C(=)		
SGSN number	C	C(=)		
User error			C	C(=)
Provider error				O

8.5.3.3 Parameter use

Invoke id

See subclause 7.6.1 for the use of this parameter.

IMSI

See subclause 7.6.2 for the use of this parameter.

Failure Cause

See subclause 7.6.7 for use of this parameter.

Re-attempt

See subclause 7.6.7 for use of this parameter.

Access Type

See subclause 7.6.7 for use of this parameter.

Rand

This parameter identifies the specific AV that failed authentication.

See subclause 7.6.7 for use of this parameter.

VLR number

Shall be present if the sender is VLR. See definition in subclause 7.6.2.

SGSN number

Shall be present if the sender is SGSN. See definition in subclause 7.6.2.

User error

This parameter is sent by the responder upon unsuccessful outcome of the service, and then takes one of the following values defined in subclause 7.6.1:

- Unknown Subscriber;
- System Failure;
- Unexpected Data Value.

Provider error

These are defined in subclause 7.6.

17.7.1 Mobile Service data types

...

```
AuthenticationFailureReportArg ::= SEQUENCE {
    imsi                                IMSI,
    failureCause                        FailureCause,
    extensionContainer                  ExtensionContainer              OPTIONAL,
    ...,
    re-attempt                          BOOLEAN,                        OPTIONAL,
    accessType                          AccessType,                     OPTIONAL,
    rand                                RAND,                           OPTIONAL,
    vlr-Number                          [0] ISDN-AddressString          OPTIONAL,
    sgsn-Number                         [1] ISDN-AddressString          OPTIONAL }
```

```
AccessType ::= ENUMERATED {
    call (0),
    emergencyCall (1),
    locationUpdating (2),
    supplementaryService (3),
    shortMessage (4),
    ...}
    -- exception handling:
    -- received values greater than 4 shall be ignored.
```

...