3GPP TSG-T (Terminals) Meeting #11
Palm Springs, USA, 14 - 16 March, 2001

Tdoc TP-010008

3GPP TSG T WG1 #10
Copenhagen, Denmark, 8-9 February 2001

T1-010105

Title: LS on authentication test algorithm to be implemented in test USIM

Source: **TSG-T WG1**

TO: **TSG-T3**

Cc: **TSG-T, TSG-SA3**

Contact Person: **Leif Mattisson** (mailto:leif.mattisson@ecs.ericsson.se)

Document: **For approval**

Date: **8 February 2001**

TSG T1 would like to inform TSG T3 that TSG T1 has endorsed a CR to [1] 3GPP TS 34.108 V3.2.0 regarding authentication test algorithm. The CR is intended to be submitted for approval at the TSG T#11 meeting in Palm Springs, US 14-16 March.

As the authentication test algorithm has impact on implementation of test USIM and test USIM simulators TSG T1 would like to have TSG T3 to review and agree the CR at the next TSG T3#18 meeting in Sophia Antipolis, 1-2 March.

The CR can be found in [3] T1-010082 that is attached to this LS.

Background information:

The authentication test algorithm that is to be implemented both in test USIM and System Simulator (SS) is needed to be able to test the UE behaviour regarding authentication key agreement procedure and SQN re-synchronisation procedure. The authentication test cases can be found in [2] 3GPP TS 34.123-1 V3.2.0 in subclause 9.2.

When drafting the authentication test cases it was found that the current definition of the test algorithm did not include the necessary details to be able specify the authentication test cases. The purpose of the CR [3] is to introduce these details.

References

[1] 3GPP TS 34.108 V3.2.0
Common Test Environments for User Equipment (UE) Conformance Testing

[2] 3GPP TS 34.123-1 V3.2.0
User Equipment (UE) conformance specification; Part 1: Protocol conformance specification

[3] T1-010082 Update of authentication test algorithm (CR to TS 34.108 V3.2.0)

3GPP TSG-T1 Meeting #10
Copenhagen, Denmark, 8-9 February, 2001

Tdoc T1-010082

3GPP TSG-T1/SIG Meeting #15
Copenhagen, Denmark, 5-7 Feb. 2001

Tdoc T1S-010018r1

CR-Form-v3

CHANGE REQUEST

⌘ **34.108** **CR** **CR-Num** ⌘ rev **-** ⌘ Current version: **3.2.0** ⌘

*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 [X] ME/UE [ ] Radio Access Network [ ] Core Network [ ]

Title:	⌘	Update of autentication test algorithm.
Source:	⌘	Ericsson
Work item code:	⌘	***Date:*** ⌘ 6 Feb 2001
Category:	⌘ **C**	***Release:*** ⌘ R99

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 be able to test UE behaviour for UE authentication reject and re-synchronisation scenarios the authentication test algorithm, that is to be implemented in test USIM, need to be further detailed.
Summary of change:	⌘	Added references to referenced 31 and 33 series specifications. Split autentication test algorithm between normal case (authentication and key agreement procedure) and the USIM re-synchronisation procedure case. Introduction of definition of the test algorithm functions f1, f2, f3, f4, f5 and the corresponding functions for re-synchronization f1* and f5*. Add new section describing how the tes algorithm is used for testing of UE authentication behaviour.
Consequences if not approved:	⌘	Not possible to test UE authentication reject nor authentication re-synchronisation scenarios.

Clauses affected:	⌘	2, 8.1.2 and 8.2
Other specs affected:	⌘	[ ] Other core specifications ⌘ [ ] 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://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.

<Start of modified section>

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] 3GPP TS 34.123-1: "Mobile Station (MS) conformance specification; Part 1: Protocol conformance specification".

[2] 3GPP TS 34.121: "Radio transmission and reception (FDD)".

[3] 3GPP TS 34.123-2: "User Equipment (UE) conformance specification; Part 2: Implementation Conformance Statement (ICS) proforma specification".

[4] 3GPP TS 34.124: "Electromagnetic compatibility (EMC) requirements for Mobile terminals and ancillary equipment".

[5] 3GPP TS 34.122: "Terminal Conformance Specification; Radio transmission and reception (TDD)".

[6] 3GPP TS 34.109: "Logical Test Interface (FDD) Special conformance testing functions".

[8] 3GPP TS 25.214: "Physical layer procedures (FDD)".

[7] 3GPP TS 25.301 Services Provided by the physical layer

[9] 3GPP TR 21.905: "Vocabulary for 3GPP Specifications".

[10] 3GPP TR 25.990: "Vocabulary".

[11] 3GPP TS 25.101: "UE Transmission and Reception (FDD)".

[12] 3GPP TS 25.102: "UE Transmission and Reception (TDD)".

[13] 3GPP TS 25.211: "Physical Channels and mapping of Transport Channels onto Physical channels (FDD)".

[14] 3GPP TS 25.212 Multiplexing and Channel Coding (FDD)

[15] 3GPP TS 23.107 QoS concept and Architecture

[16] 3GPP TS 26.110 Codec for Circuit Switched Multimedia Telephony Service; General Description

[17] 3GPP TS 29.007 General requirements on interworking between the Public Land Mobile Network (PLMN) and the Integrated Services Digital Network (ISDN) or Public Switched Telephone Network (PSTN)

[18] 3GPP TR 23.910 Circuit Switched Data Bearer Service

[19] GSMA-ISG: Typical Radio Parameter Sets, version 1.1, IS Doc 049/00, 20 March 2000

[20] 3GPP TS 25.104 UTRA (BS)-FDD Radio Transmission and Reception

[21] 3GPP TS 25.105 UTRA (BS)-TDD Radio Transmission and Reception

[22] 3GPP TS 31.101 UICC-Terminal Interface; Physical and Logical Characteristics

[23] 3GPP TS 31.102 Characteristics of the USIM Application

[24] 3GPP TS 33.102 Security Architecture

[25] 3GPP TS 33.103 Integration Guidelines

[26] 3GPP TS 33.105 Cryptographic Algorithm Requirements

<End of modified section>

<Start of modified section>

8. Test USIM Parameters

8.1 Introduction

This clause defines default parameters for programming the elementary files of the test USIM. The requirements of this clause do not apply to the USIM/ME tests of TS34.123-1.

8.1.1 Definitions

"Test USIM card":

A USIM card supporting the test algorithm for authentication, programmed with the parameters defined in this clause. The electrical, mechanical and environmental requirements of the test USIM card are specified in TS31.101 and TS31.102.

"Test USIM":

Either a test USIM card or the USIM simulator programmed with the parameters defined in this clause.

8.1.2 Definition of the test algorithm for authentication

In order to be able to easily test the UMTS authentication and key agreement procedure as specified in [24] TS 33.102 and [26] TS 33.105 along the whole system, the availability of a test algorithm for generation of authentication vector based on quintets is needed (in GSM triplets was used). Additionally, calculation of the parameters for re-synchronisation requests is needed. The definition of the test algorithm are the functions f1, f2, f3, f4, f5 and the corresponding functions for re-synchronization are f1* and f5*.

The test algorithm defined in the present clause shall be implemented in test USIM cards as well in test USIM simulators and SS. The test algorithm may also, for test purposes, be implemented in AUC.

The following procedure employs bit wise modulo 2 addition ("XOR").

The following convention applies:

All data variables in the specification of this test algorithm are presented with the most significant substring on the left hand side and the least significant substring on the right hand side. A substring may be a bit, byte or other arbitrary length bitstring. Where a variable is broken down into a number of substrings, the leftmost (most significant) substring is numbered 0, the next most significant is numbered 1, and so on through to the least significant.

~~In all data transfer the most significant byte is the first byte to be sent; data is represented so that the left most bit is the most significant bit of the most significant byte.~~

8.1.2.1 Authentication and key derivation in the test USIM and SS

The following steps describe sequence of operations for the functions f1, f2, f3, f4 and f5 to perform in the test USIM and SS, in order to obtain the XMAC/MAC, RES/XRES, CK, IK and AK respectively, to be used in the authentication and key agreement procedure.

Step 1:

XOR to the challenge **RAND**, a predefined number **Ki** (in which at least one bit is not zero, see 8.2), having the same bit length (128 bits) as **RAND**.

The result **XDOUT** of this is:

XDOUT[bits 0,1, . . .126,127] = **Ki**[bits 0,1, . . .126,127] XOR **RAND**[bits 0,1, . . .126,127]

Step 2:

RES (test USIM), **XRES** (SS), **CK, IK** and **AK** are extracted from **XDOUT** this way:

~~X~~**RES**[bits 0,1, . . .n-1,n] = **f2(XDOUT**,n) = **XDOUT**[bits 0,1, . . .n-1,n] (with 30 < n < 128)

NOTE: Suggested length for RES is 128 bits (i.e. n = 127).
In SS and AUC, the XRES calculation is identical to RES.

CK[bits 0,1, . . .126,127] = **f3(XDOUT)** = **XDOUT**[bits 8,9, . . .126,127,0,1, . . .6,7]

IK[bits 0,1, . . . 126,127] = **f4(XDOUT)** = **XDOUT**[bits 16,17, . . .126,127,0,1, . . .14,15]

AK[bits 0,1, . . . 46,47] = **f4(XDOUT)** = **XDOUT**[bits 24,25, . . .70,71]

Step 3:

Concatenate **SQN** with **AMF** to obtain **CDOUT** like this:

CDOUT[bits 0,1,. . .62,63] = **SQN**[bits 0,1,. . .46,47] || **AMF**[bits 0,1,. . .14,15]

NOTE: For test USIM the **SQN** = $\mathbf{SQN_{MS}}$ = $\mathbf{SQN_{SS}}$[bits 0,1,. . .46,47] = **AUTN**[bits 0,1,. . .46,47] XOR **AK**[bits 0,1, . . . 46,47] where AUTN is the received authentication token.

Step 4:

XMAC (test USIM) and **MAC~~S~~** (SS) are calculated from **XDOUT** and **CDOUT** this way:

XMAC[bits 0,1, . . .62, 63] = **f1(XDOUT, CDOUT)** = ~~**MACS**[bits 0,1, . . .62, 63] =~~ **XDOUT**[bits 0,1. . .62,63] XOR **CDOUT**[bits 0,1,. . .62,63]

NOTE: In SS and AUC, the MAC calculation is identical to XMAC

~~.~~Step 5:

The SS calculates the authentication token **AUTN**:

AUTN[bits 0,1,..126,127] = **SQN** ⊕ **AK**[bits 0,1,. . .46,47] || **AMF**[bits 0,1,. . .14,15] || **MAC**[bits 0,1, . . .62, 63]

Where **SQN** ⊕ **AK**[bits 0,1,. . .46,47] = **SQN**[bits 0,1,. . .46,47] XOR **AK**[bits 0,1, . . . 46,47]

8.1.2.2 Generation of re-synchronisation parameters in the USIM

For SS to be able to initiate an authentication re-synchronisation procedure a specific AMF value has been defined.

$AMF_{RESYNCH}$ = AMF[bits 0,1,..14,15] = "1111 1111 1111 1111"

When the test USIM receives an authentication token (AUTN) having the value of AMF field equal to the $AMF_{RESYNCH}$ value then the test USIM shall initiate the re-synchronisation procedure.

When the test USIM starts the re-synchronisation procedure, the MAC-S and AK have to be calculated using the functions f1* and f5*, which in the test algorithm are ~~considered in this description~~ identical to f1 and f5, respectively.

Step 1:

XOR to the challenge **RAND**, a predefined number **K** (in which at least one bit is not zero, see 8.2), having the same bit length (128 bits) as **RAND**.

The result **XDOUT** of this is:

XDOUT[bits 0,1, . . .126,127] = **K**[bits 0,1, . . .126,127] XOR **RAND**[bits 0,1, . . .126,127]

Step 2:

AK is extracted from **XDOUT** this way:

AK[bits 0,1, . . . 46,47] = **f5***(**XDOUT**) = **XDOUT**[bits 24,25, . . .70,71]

Step 3:

Concatenate $\mathbf{SQN_{MS}}$ with **AMF*** to obtain **CDOUT** like this:

CDOUT[bits 0,1,. . .62,63] = $\mathbf{SQN_{MS}}$[bits 0,1,. . .46,47] || **AMF***[bits 0,1,. . .14,15]

Where **AMF*** assumes a dummy value of all zeros

NOTE: For test USIM the $\mathbf{SQN_{MS}} = \mathbf{SQN_{SS}}$[bits 0,1,. . .46,47] = **AUTN**[bits 0,1,. . .46,47] XOR **AK**[bits 0,1, . . . 46,47] where AUTN is the received authentication token.

For SS and AUC the $\mathbf{SQN_{MS}}$ = **AUTS**[bits 0,1,. . .46,47] XOR **AK**[bits 0,1, . . . 46,47] where AUTS is the received re-synchronisation parameter.

Step 4:

MAC-S is calculated from **XDOUT** and **CDOUT** this way:

MAC-S[bits 0,1, . . .62, 63] = **f1***(**XDOUT, CDOUT**) = **XDOUT**[bits 0,1. . .62,63] XOR **CDOUT**[bits 0,1,. . .62,63]

NOTE: In SS and AUC, the XMAC-S calculation is identical to MAC-S.

Step 5:

The test USIM calculates the re-synchronisation parameter **AUTS**:

AUTS[bits 0,1,..110,111] = $\mathbf{SQN_{MS}} \oplus$ **AK**[bits 0,1,. . .46,47] || **MAC-S**[bits 0,1, . . .62, 63]

Where $\mathbf{SQN_{MS}} \oplus$ **AK**[bits 0,1,. . .46,47] = $\mathbf{SQN_{MS}}$ [bits 0,1,. . .46,47] XOR **AK**[bits 0,1, . . . 46,47]

8.1.2.3 Using the authentication test algorithm for UE conformance testing

8.1.2.3.1 Authentication accept case

The authentication accept case is illustrated in figure 8.1.2.3.1.

The SS calculates the authentication token AUTN according to the test algorithm as specified in subclause 8.1.2.1 (step 1 to 5) using an AMF value different from the $AMF_{RESYNCH}$ value.

The SS sends an authentication request, including RAND and AUTN parameters, to the ME/USIM.

Based on the received RAND parameter the test USIM calculates the RES, CK IK and XMAC parameters according to subclause 8.1.2.1 (step 1 to 4). The test USIM extracts the $SQN_{MS} = SQN_{SS}$, AMF and MAC parameters from the received authentication token AUTN.

The test USIM checks that XMAC = MAC and then return the RES, CK and IK parameters to the ME.

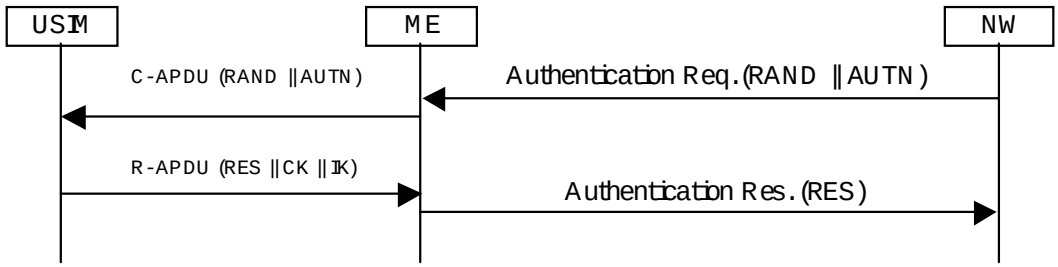

Figure 8.1.2.3.1: Network accepted by UE

8.1.2.3.2 MAC failure case

The MAC failure case is illustrated in figure 8.1.2.3.2.

The SS calculates the authentication token AUTN according to the test algorithm as specified in subclause 8.1.2.1 (step 1 to 5) using an AMF value different from the $AMF_{RESYNCH}$ value and a MAC value different from what is calculated in subclause 8.1.2.1 step 4.

The SS sends an authentication request, including RAND and AUTN parameters, to the ME/USIM.

Based on the received RAND parameter The test USIM calculates the RES, CK, IK and XMAC parameters according to subclause 8.1.2.1 (step 1 to 4).

Based on the received RAND parameter the test USIM calculates the RES, CK IK and XMAC parameters according to subclause 8.1.2.1 (step 1 to 4). The test USIM extracts the $SQN_{MS} = SQN_{SS}$, AMF and MAC parameters from the received authentication token AUTN.

When the test USIM identifies that the calculated XMAC value is different from the MAC value received in AUTN then the USIM notifies the ME of the MAC failure and the ME sends an AUTENTICATION FAILURE message to the SS (cause “MAC failure”).

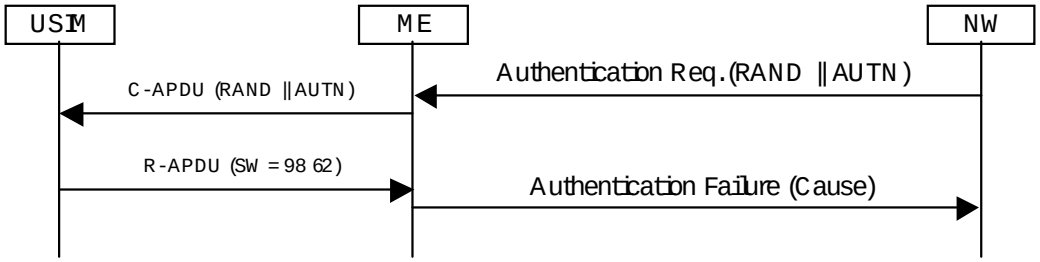

Figure 8.1.2.3.2: MAC failure cases

8.1.2.3.3 SQN failure case

The SQN failure case is illustrated in figure 8.1.2.3.3.

The SS calculates the authentication token AUTN according to the test algorithm as specified in subclause 8.1.2.1 (step 1 to 5) using an AMF value equal to $AMF_{RESYNCH}$.

The SS sends an authentication request, including RAND and AUTN parameters, to the UE/USIM.

The test USIM extracts the $SQN_{MS} = SQN_{SS}$, AMF and MAC parameters from the received authentication token AUTN.

When the test USIM identifies that the AMF field is equal to the $AMF_{RESYNCH}$ value it calculates the re-synchronisation parameter AUTS as specified in subclause 8.1.2.2 (step 1 to 5) and forward it to the ME.

The ME sends an AUTHENTICATION FAILURE message to the SS including the AUTS parameter.

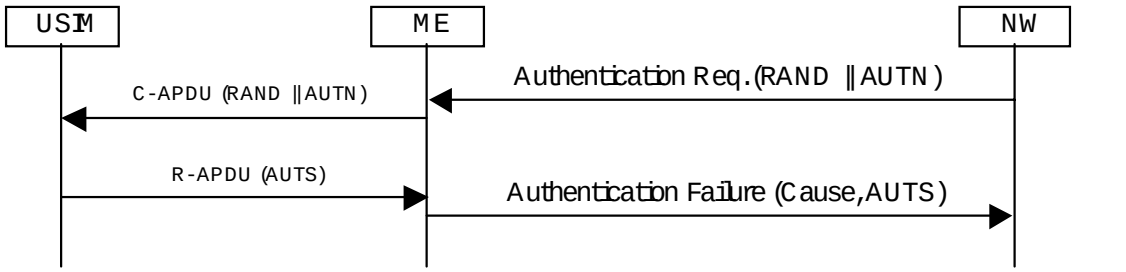

Figure 8.1.2.3.3: SQN failure case

8.2 Default Parameters for the test USIM

Ki:

The authentication key "Ki" will be chosen by the test house and will be non zero. The "Ki" value used by the SS will align with this value.

PIN Disabling:

The PIN enabled / disabled flag will be set to "PIN Disabled". This ensures that when the Test USIM is inserted into a UE the user will not be prompted for PIN entry.

<End of modified section>