3GPP S3#12 meeting
Stockholm, Sweden 11 – 14 April, 2000.

S3-000297

Agenda Item: 12.1

Source: Ericsson

Title: Proposal on authentication vector generation algorithm for conformance testing

Contact: David Castellanos Zamora
e-mail: david.castellanos-zamora@ece.ericsson.se
Phone: +34 91 339 2485

Document for: Discussion

1 Abstract

The definition of a test algorithm for UMTS authentication is under the scope of 3GPP TS 34.108, "Common Test environments for UE conformance Testing" (section 6.11.1.2). The algorithm currently proposed in the latest version of this specification (v1.0.1) is not valid for testing UMTS authentication and key agreement since it is copied from the one used in GSM (as defined in GSM TS 11.10, Annex A4.1.2.). This specification belongs to T1 and it is not under change control yet. The date for approval of such TS is June 00.

This document defines one possible test algorithm for authentication and proposes its consideration for inclusion in TS 34.108.

S3 members are kindly requested to consider this proposal and to provide comments until next S3#13 meeting.

2 Abbreviations

AMF: Authentication Management Field
AK: Anonimity Key
CDOUT: Output from concatenation of **SQN** and **AMF**
CK: Ciphering Key
IK: Integrity Key
MAC: Message Authentication Code
SQN: Sequence Number
XDOUT: Output from bit wise modulo 2 addition of **RAND** and **Ki**
XRES: Expected Response

3 Introduction

GSM has a standardised test algorithm, based on bit wise modulo 2 addition ("XOR") operations, in order to make the testing of the whole authentication and key agreement procedure easier from AUC to SIM card in the mobile terminal. The same principle should apply for UMTS.

The TS 34.108 "Common Test environments for UE conformance Testing" specifies a test algorithm that is the one specified for GSM. In GSM, triplets are used for authentication. For UMTS, quintets will be used and thus the algorithm needs to be modified accordingly.

In order to be able to easily test the UMTS authentication and key agreement procedure along the whole system, the availability of a test set of functions based on bit wise modulo 2 addition ("XOR") operations should be considered.

4 Text proposal for 6.11.1.2 of TS 34.108

6.11.1.2 Definition of the test algorithm for authentication

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

The following convention applies:

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.

Step 1:

XOR to the challenge **RAND**, a predefined number **Ki** (in which at least one bit is not zero), 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:

XRES, **CK, IK** and **AK** are extracted from **XDOUT** this way:

XRES[bits 0,1, . . .n-1,n] = **XDOUT**[bits 0,1, . . .n-1,n] (with 30 < n < 128)

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

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

AK[bits 0,1, . . . 62,63] = **XDOUT**[bits 24,25, . . .86,87]

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]

Step 4:

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

MAC[bits 0,1, . . .62, 63] = **XDOUT**[bits 0,1. . .62,63] XOR **CDOUT**[bits 0,1,. . .62,63]

5 Other impacts due to the implementation of UMTS test algorithm

The test algorithm must be implemented both in the AUC (real or simulated) and in the test USIM cards.

The test authentication vectors calculated with this test algorithm should be handled by all the involved elements in the system, in the same way as for non test ones.

6 Conclusions

As a result of this analysis, it is concluded that the algorithm for generation of authentication test vectors as currently stated in TS 34.108 needs to be updated. The algorithm defined in this document is presented to be considered for this purpose.