Technical Specification Group Services and System Aspects   ***TSGS#6(99)514***
Meeting #6, Nice, France, 15-17 December 1999

Source:	**TIA - Engineering Committee TR45**
Title:	**TR45 Comittee Correspondence in response to Liaison from SA WG3 (S3-99460)**
Document for:	**Information**
Agenda Item:	**5.3.2**

The attached Correspondence was received by the TSG SA Chairman.

TELECOMMUNICATIONS

TIA

INDUSTRY ASSOCIATION

COMMITTEE CORRESPONDENCE

Please reply to:

John A. Marinho
Chair, TR45 Engineering
Committee
c/o Lucent Technologies,
Room 3A-301
67 Whippany Road
Whippany, NJ   07981, U.S.A.

e-mail: jmarinho@lucent.com

December 7, 1999

Niels Andersen
Chair, 3GPP SA Plenary
c/o Motorola
Midtager 20
DK-2605
Broendby, Denmark
e-mail: NielsPeter_Andersen@Europe30.mot.com

Maurice Pope
Secretary, 3GPP SA Plenary
3GPP Support
ETSI Mobile Competence Centre
F-06921 Sophia Antipolis Cedex, France
e-mail: maurice.pope@etsi.fr

Mike Walker
Chair, 3GPP S3 and Chair, ETSI SMG10
c/o Vodafone-Airtouch
The Courtyard, 2-4 London Road
Newbury, Berkshire, RG14 1JX
e-mail: mike.walker@vf.vodafone.co.uk

Ansgar Bergmann
Secretary, 3GPP S3 and Secretary, ETSI SMG10
ETSI Mobile Competence Centre
F-06921 Sophia Antipolis Cedex, France
e-mail: ansgar.bergmann@etsi.fr

Christopher Carroll
Chair, TIA TR45 AHAG
c/o GTE Laboratories
40 Sylvan Road
Watham, MA 02254
email: ccarroll@gte.com

Cheryl Blum
Chair TR45.2
c/o Lucent Technologies
263 Shuman Boulevard
Naperville, IL 60566
email: cjblum@lucent.com

Timothy Wright
c/o Vodafone-Airtouch
The Courtyard, 2-4 London Road
 Newbury, Bershire, Rg14 1JX
email: timothy.wright@vf.vodafone.co.uk

Bart Vinck
c/o Seimens Atea
Atealaan 34
B-2200 Herentals, Belgium
email: Bart.Vinck@seimens.atea.be

Dear Standards Colleagues:

This correspondence is to apprise you that at the TR45 Engineering Committee meeting held on December 1-2, 1999 in Koloa, Hawaii, U.S.A., a decision on Enhanced Security Algorithm(s) (ESA) standards was addressed. In response to the recommendations contained in contributions TR45/99.12.01.41 and TR45/99.12.01.43 (please see Attachments), it was agreed that correspondence from TR45 to the Chairs and Secretaries of ETSI SMG10, 3GPP S3, and 3GPP SA plenary, as well as to the originators of the contributions would contain the following text.

Committee TR45 thanks S3 for its liaison statement (S3-99460) containing a suggested way forward for global 3G roaming. TR45 has adopted the 3GPP AKA proposal as presented in TR45.2./99.11.08.09 (Stage 2 authentication flows for the 3GPP AKA) as the basis of its ESA solution provided that it can be modified as required to meet all TR45 requirements, including global roaming. In the event that 3GPP AKA cannot be appropriately modified, this decision will be re-evaluated at the March 8-9, 2000 TR45 meeting. TR45.2 and the AHAG have been directed to evaluate the 3GPP AKA against the TR45 requirements and recommend changes as required by the end of February 2000. TR45 may decide that some of these changes should also be made to 3GPP AKA for optimal global roaming. The proposals to S3 that AHAG and TR45.2 will generate will be presented to the TR-45 plenary in March 2000 and can therefore be discussed at the joint S3/AHAG meeting in April 2000. TR45 is pleased to see confirmation of this joint meeting. TR45 hopes that this will be part of further fruitful co-operation between TR45 and 3GPP on security matters.

If there are any comments or questions regarding the above statement, please feel free to contact me. In addition, it is requested that replies be copied to the TR45 Secretary, Jane Brownley at jbrownley@lucent.com.

Regards,

< original signed >

John A. Marinho
Chairman
Engineering Committee TR45

Attachments:

(1) Ad Hoc Authentication Group Meeting Summary (Addendum) for September, 1999 – November, 1999 (TR45/99.12.01.41)
(2) Liaison statement from 3GPP S3 and ETSI SMG10 (security groups of 3GPP and ETSI respectively) to TR45 AHAG, TR45, TR45.2, TR45.3 and TR45.5 (TR45/99.12.01.43)

Copy to w/attachments:

Dan Bart, TIA Vice President
Susan Hoyler, TIA Director
Frank Quick, Vice-Chair, TR45 AHAG
Secretary and Chairs, TR45 Subcommittees

Title:

Ad Hoc Authentication Group Meeting Summary (Addendum)

for September, 1999 - November, 1999

Source:

Frank Quick, TR45.AHAG Vice Chair

QUALCOMM Incorporated

5775 Morehouse Drive

San Diego, CA 92121

Phone: 858-658-3608

Fax: 858-658-5006

email: fquick@qualcomm.com

This addendum to the TR-45 AHAG report covers the AHAG meeting held November 29-30 at the Sheraton Kauai Resort, Poipu, Kauai, HI.

1. Revision D of "Common Cryptographic Algorithms" was approved for transmittal to TIA in connection with the ballot of SP-4027. This revision adds support for enhanced voice, data and message encryption for the TDMA air interface. Procedures that were in Revision C are not changed.

2. 3GPP SA3 has agreed to hold a joint meeting with AHAG in April 2000.

3. AHAG continued its discussion of Enhanced Subscriber Authentication (ESA).   AHAG's recommendation to TR-45 is as follows:

AHAG requests that TR-45 affirm that support for global roaming is a requirement for ESA.

If global roaming support is not required, then TR-45 should select one of the two remaining ESA proposals (LESA and 3GPP AKA), and should direct the subcommittees to begin standardization of the selected proposal.

If, on the other hand, global roaming support is required, then TR-45 should take note of the following observations:

a. Global roaming requires that the ESA standard be interoperable with 3GPP AKA, since 3GPP has adopted this approach and did not adopt LESA.

b. LESA appears to meet all TR-45 requirements as developed by AHAG and TR-45.2. The 3GPP AKA scheme may meet all TR-45 requirements, though further study is needed.

Two general approaches have been identified to provide global roaming support while meeting all TR-45 requirements:

a. A dual-mode strategy, in which some or all network elements support both LESA and 3GPP AKA.

b. A 3GPP-based strategy, in which modifications or enhancements may be made, if needed, to the 3GPP baseline or its usage in order to meet TR-45 requirements.

AHAG recommends that TR-45 select one of these two approaches. It is noted that either approach may require the cooperation of 3GPP if modifications or enhancements are necessary to meet TR-45 requirements. AHAG therefore proposes that TR-45 determine the need for such changes. AHAG would present these findings to 3GPP at the joint meeting in April.

AHAG further recommends that TR-45 send correspondence to 3GPP advising them of this plan, and making them aware that changes to their procedures may be requested.

TITLE

Liaison statement from 3GPP S3 and ETSI SMG10 (security groups of 3GPP and ETSI respectively) to TR45 AHAG, TR45, TR45.2, TR45.3 and TR45.5

SOURCE

ETSI SMG10 and 3GPP S3

Contacts: Timothy Wright   Bart Vinck
                 Vodafone-Airtouch   Siemens Atea
                 +44 1635 676456   +32 14 252592
                 timothy.wright@vf.vodafone.co.uk
             Bart.Vinck@siemens.atea.be

ABSTRACT

Support of the 3GPP AKA as a minimum by all 3G systems, to provide global 3G roaming, is recommended. If 3G family members require additional mechanisms within their family system, they may devise and specify such mechanisms for use within their family system.

RECOMMENDATIONS

Consider and agree a response to the proposal. Commission AHAG to begin any necessary work.

Notice

Tdoc S3-99460

TSG-SA WG3 (Security) meeting #8

Sophia Antipolis, 16-19 November, 1999

Source: ETSI SMG10 / 3GPP TSG-SA WG3

To: TIA TR-45.AHAG

Cc: TIA TR-45, TR-45.2, TR-45.3, TR-45.5

Title: Principles concerning the development of a common authentication mechanism to support global roaming

To aid global roaming across all 3G systems, S3 would like to propose that the following principles are adopted by TR-45.AHAG:

- All 3G family member systems support the 3GPP AKA mechanism as a minimum.

- If other features not provided by the 3GPP AKA mechanism are required by particular 3G family systems then additional mechanisms must be developed for, and supported by, that particular system providing that the ability to support global roaming is not impaired.

These principles would allow features required by particular family member systems to be made available to users of that system. Users of other family member systems may not be able to support such features when roaming to the affected system. However, it is argued that the inability to support these features for some roaming users will have negligible impact on the overall system performance.

One example feature which would fall into this category would be support for authentication based on a global challenge in 3G ANSI-41 systems. In this case it is proposed that such a feature is not provided when users from other 3G systems roam to 3G ANSI-41 networks.