3GPP TSG SA WG3 Security / TIA TR-45 AHAG Draft Report V 0.0.2

Joint Meeting: 12 April, 2000, Stockholm, Sweden

Source: **3GPP TSG-SA WG3 Secretary**

Title: **Draft report of the joint session with TIA TR-45 AHAG on 3GPP/3GPP2 security harmonisation**

Document for: **Comment**

Contents

1 Opening of the meeting

The document numbers given in this report refer to the SA WG3 documents, which are available on the 3GPP FTP server at : ftp://ftp.3gpp.org/TSG_SA/SA_WG3_Security/TSGS3_12_Stockholm/Docs

The SA WG3 Vice Chairman, Mr S. Pütz, opened the meeting, welcomed delegates and presented the draft agenda, given in TD S3-000232. The draft agenda was approved without change.

2 Introduction to 3GPP standards Stefan Pütz (S3 vice chair, T-Mobil)

TD S3-000273: Overview of 3GPP. Mr. S. Pütz presented the history, structure and achievements of 3GPP. The main specifications of SA WG3 were also listed (Slide 20). It was clarified that the publication of the algorithms on the ETSI Web site is awaiting Partners' agreement, and they should be available soon (Slide 17).

3 3GPP AKA development/requirements Bart Vinck (Siemens)

TD S3-000275: 3GPP Security/AKA - Requirements and development. Mr. B. Vinck, Siemens Atea, presented the requirements and development of the AKA.

4 Introduction to TR-45, TR-45.2, TR-45 AHAG and 3GPP2 standards Chris Carroll (AHAG chair)

TD S3-000274: TIA TR-45 and 3GPP2 Security. Mr. C Carroll, Chairman of TR-45 AHAG Presented the structure of TIA, TR-45 and the 3GPP2 Project and the Security work of TR-45 AHAG. It was explained that AHAG are formal security consultants to 3GPP2 and support the Core Sub-committees.

5 TR-45 ESA development/requirements Frank Quick (AHAG vice chair)

TD S3-000276: The ESA Process. Mr. F Quick, Qualcomm Inc. presented the Enhanced Subscriber Authentication being developed in AHAG. The ESA will provide stronger mutual authentication and key generation algorithms, with 128 bit key length, which will provide compatibility with 3GPP.

6 3GPP AKA issues

6.1 Joint control of 3GPP AKA specifications

It was necessary to elaborate a procedure for the joint control of the 3GPP AKA specification. There was an exchange of requirements from SA WG3 and AHAG to facilitate this.

AHAG feel that the control of the algorithm should be with SA WG3, but that there should be some liaison with AHAG in order to allow formal input to the development and review process for the AKA. The general concern was to have input to the change process to ensure that the AKA remains applicable to the 3GPP2 system. SA WG3 should therefore ensure that AHAG are provided with CRs to the AKA in order to make comments if considered necessary. A liaison to TR-45 should be created in order to record an agreed mechanism. It was suggested that the mechanism and identification of the parts of the specification which are affected by the agreement could be recorded as an Annex to TS 33.102.

The affected parts of TS 33.102 will need to be identified and agreed between AHAG and SA WG3. The contents of AKA messages need to be subject to joint control. (This information may be contained in the Security Guidelines document, TR 33.900).

ACTION 1: SA WG3 to provide AHAG with a list of relevant SA WG3 documents which have an impact on AKA (First draft - Bart Vinck).

ACTION 2: SA WG3 to provide a list of areas where joint control with AHAG over AKA related sections of documents will be needed (Bart Vinck).

The timing of changes was discussed, as SA Plenary is often fairly soon after an SA WG3 meeting, which would not give time for AHAG to review and comment on the CRs. It was considered that major changes to the AKA are unlikely, but in case of a change, then it should generally wait for agreement of both sides before submitting to SA Plenary for approval. In the case that urgent approval is needed, then a joint meeting with AHAG could be arranged to gain approval of both groups together. It was considered that time pressures for SA WG3 would only occur just before a release freezing date, i.e. once per year. Suitable dates for 2000 was considered around the November SA WG3 meeting. AHAG and SA WG3 will exchange meeting schedules in order to find a suitable solution.

This was changed to the beginning of September at the end of the meeting, because November would be very difficult due to already existing meeting dates and public holidays.

ACTION 3: AHAG and SA WG3 to exchange meeting schedules to find a suitable time for a joint meeting in early September 2000.

It was clarified that both AHAG and SA WG3 will need to get approval of their parent bodies for agreements reached at this meeting.

6.2 Inter-operation with IS-41

There are separate MAPs for IS-41 and 3GPP networks, so a AKA mechanism alone will not guarantee Global Roaming.

The Operators Harmonisation Group (OHG) are concerned with Inter-Operation between 3G Networks, and it was suggested that a liaison is sent to the OHG to explain the steps taken towards Global roaming by use of the common AKA. This liaison should also be transmitted to the Core Network groups.

ACTION 4: Tim Wright: To investigate what is being done and what work is needed on the NNI for harmonisation.

6.3 General 3GPP/3GPP2 security harmonisation issues

IN order to have cross-information between the groups, it was suggested that some form of liaison officers were made available. As this could be difficult to achieve with the frequency of meetings, it was then suggested to exchange official (approved) reports of the groups on the e-mail lists. This was considered a useful idea, and TR-45 approval to do this would be requested by AHAG.

The status of the AHAG Enhanced Subscriber Privacy (ESP) programme was reported: there were 5 candidates being evaluated. One of the 5 candidates will be selected for each of the 3 interfaces, based on performance.

AHAG would like to see the KASUMI algorithm published by 3GPP, as they have a preference for publicly available algorithms. It was considered by SA WG3 that a single ciphering algorithm would also be useful for harmonisation, and it was asked that if KASUMI was made publicly available, if it would still be possible to include it in the TR-45 selection process. The answer to this was not known at the time.

6.4 Other issues

TD S3-000243: Cipher and Integrity key update. The decision on whether to remove the key lifetime was considered as internal SA WG3 matter, and was left to be discussed in the main SA WG3 meeting.

7 TR-45 ESA issues

TD S3-000233: TR-45 AHAG AKA Issues. The contribution was introduced by Mr. C Carroll. The contribution covered points under the following agenda items.

7.1 Home control of AKA

AHAG recommended:

1 that 3GPP add signalling to allow the HLR to revoke the current Authentication Vector (AV) and thereby causing an AV update and that that this ability be independent of the ability to revoke a registration.
2 that the Home System have a mechanism to control the duration of the Security Association (SA).
3 that the Serving Network (SN) report the failure of any authentication and, at the HLR's option, the success of the 3GPP AKA procedure.

The justifications for adding this mechanism were described in the Global challenge (see Agenda Item 7.2). The benefits of implementing this system needed clarification. The benefits are mainly centred in North America (i.e. for TR-45 systems), where different levels of trust exist between operators, and it is an operational/business requirement. There may be no direct advantage in some other countries, but would be required for harmonisation of the systems. The home serving system will retain control over the duration of the Mobiles Security Association.

After some discussion, the Chairman summarised that there are three things to concentrate upon:

a) 3GPP think this is a useful mechanism to be included in the AKA. In this case it should be standardised in 3GPP.
b) 3GPP think that some operators may not want to implement this (e.g. if they do not wish to interwork with 3GPP2 networks and do not wish to have global roaming). In this case, it could still be standardised in 3GPP, and left as optional for implementation.
c) 3GPP do not see the need for this mechanism. In this case it should not be standardised in 3GPP.

Taking into account that TR-45 have asked AHAG to request their requirements are included in the AKA.

It was suggested that separate contexts could be maintained in a mobile, and use the 3GPP context and keys in 3GPP systems, and 3GPP2 context and keys in 3GPP2 systems.

It was suggested that 3GPP would be more likely to agree to changes which affect the HLR, rather than the VLR, for an optional functionality. Therefore, if HLRs who wish to use the functionality implement the Revoke Authentication Vector (AV) command, this could be used instead of mandating that all VLRs keep timers to revoke the AVs after the period of time specified by the HLR. (i.e. implement requirement 2 by the use of requirement 1).

It was decided that the AV revoke mechanism should be considered as a mandatory requirement in 3GPP with consultation with 3GPP TSG CN.

ACTION 5: Home control of AKA: 3GPP TSG CN WGs to be consulted over this requirement to ensure there are no problems for Release 2000. A Liaison to CN WG4 to be drafted (Mr. G. Køien) on implementation of 1 and 2. CN WG4 also to be asked to consider the implications of recommendation 3 and provide feedback to SA WG3.

The need for requirement 3 was then discussed, given that key pairs will be renewed when moving between 3GPP and 3GPP2 networks. It was suggested that the mechanism may be useful to allow the 3GPP2 network to use the report as an SSD update command acknowledgement.

It was proposed by AHAG members that they take the results of the discussion back to TR-45 for consideration and decide whether the recommendation 3 is still required in the context of the suggested implementation of requirements 1 and 2. This was agreed.

ACTION 6: Home control of AKA: AHAG to determine the consequences of the proposed implementation of recommendations 1 and 2 with respect to recommendation 3.

7.2 Global (broadcast) challenge

7.2.1 Local authentication

TR-45 had decided that Broadcast Challenge is mandatory within all air interfaces standardised by TR-45 for local authentication, and therefore will be mandatory for all mobiles/UIMs operating in air interfaces standardised by TR-45.

There were no issues for 3GPP identified with this decision and SA WG3 noted the decision of TR-45.

7.2.2 Initial registration

TR-45 were currently debating the issue of using Global Challenge on initial registrations to speed up the access process and minimise system loading on TR-45 traffic channels. For this reason, TR-45 was considering the use of 3GPP AKA for Enhanced Subscriber Authentication (ESA), either with minimal changes, as a secondary key (SSD) update procedure, or both.

TD S3-000272 Global Challenge for Initial Registration. This contribution describes the background of the discussions and ideas for Global Challenge and Enhanced Subscriber Authentication ongoing in AHAG and was provided for information. The main principle is to authenticate users at the same time as obtaining subscriber information from the Home Network in order to speed up initial registration as a service improvement. Impact upon performance and radio network capacity were being investigated by AHAG. It was added that subsequent authentication failure would cause the ongoing (or completed) call set-up to terminate.

This work was noted by SA WG3 and further results of the ongoing studies will be forwarded to SA WG3 by AHAG.

7.3 R-UIM security (protection of privacy and authentication information)

TR-45 was concerned with the potential vulnerability of passing privacy and authentication information (IK and CK) from the UIM to a potentially rogue “MS-Shell”. AHAG recommends that SA WG3 and AHAG explore whether the privacy and authentication information need protection, or how the vulnerability to a rogue “MS-shell” may be minimised.

Related topics have been explored by SA WG3 in the past. It was considered that CK and IK passed to the mobile should be deleted from the mobile when the IC Card is removed or the mobile switched off. CK and IK shall only be passed to the mobile after successful 3G authentication has been performed. If Authentication is performed for every call set-up then this threat is reduced. In GSM partial call timers were introduced to allow operators to reset mobiles which have kept CK and IK. Protection by means of embedding the vulnerable data in the UIM is technically difficult due to ME-UIM interface bandwidth requirements etc. and was not considered feasible.

7.4 SHA-1 for 3GPP AKA

TR-45 had agreed to adopt SHA-1 as the local authentication algorithm for 3GPP AKA within TR-45 networks. Additionally, TR-45 strongly recommend the use of SHA-1 for 3GPP AKA key agreement within TR-45 networks. TR-45 proposed that 3GPP consider adopting SHA-1 as the default key agreement algorithm for 3GPP networks.

It was reported that the status of GPP authentication algorithm was that a default algorithm would be developed by ETSI SAGE, pending funding confirmation. It has not yet been decided what the

algorithm will be. SA WG3 agreed to forward the proposal to use SHA-1 for 3GPP default authentication algorithm to ETSI SAGE if formally requested by AHAG.

In any case, as the algorithm is the default, to be used if operators do not wish to develop their own, the final choice should not cause any impact on interworking between 3GPP and 3GPP2 systems.

7.5 Other issues

None.

8 Close of meeting

The Chairman thanked delegates for their co-operation and AHAG also thanked SA WG3 for the opportunity for this exchange of views and ideas. The Chairman then closed the meeting.

Annex A: List of Actions from the Joint meeting

ACTION 1: **SA WG3 to provide AHAG with a list of relevant SA WG3 documents which have an impact on AKA (First draft - Bart Vinck).**

ACTION 2: **SA WG3 to provide a list of areas where joint control with AHAG over AKA related sections of documents will be needed (Bart Vinck).**

ACTION 3: **AHAG and SA WG3 to exchange meeting schedules to find a suitable time for a joint meeting in early September 2000.**

ACTION 4: **Tim Wright: To investigate what is being done and what work is needed on the NNI for harmonisation.**

ACTION 5: **Home control of AKA: 3GPP TSG CN WGs to be consulted over this requirement to ensure there are no problems for Release 2000. A Liaison to CN WG4 to be drafted (Mr. G. Køien) on implementation of 1 and 2. CN WG4 also to be asked to consider the implications of recommendation 3 and provide feedback to SA WG3.**

ACTION 6: **Home control of AKA: AHAG to determine the consequences of the proposed implementation of recommendations 1 and 2 with respect to recommendation 3.**