

3GPP TSG SA WG3 Security — S3#15
12-14 September, 2000
Washington D.C., USA

S3-000501

3GPP TSG SA WG3 Security — S3#14

Draft Report, version 0.0.7

1-4 August, 2000, Oslo

Source: Secretary SA WG3

Title: Draft Report of SA WG3 Meeting #14, version 0.0.7

Document for: Approval



The Wheel of Life Sculpture, Vigeland Park, Oslo

Contents

1	Opening of the meeting.....	4
2	Meeting objectives	4
3	Registration and assignment of input documents.....	4
4	Approval of the agenda.....	4
5	Approval of meeting reports.....	4
5.1	S3#13 (Yokohama).....	4
5.2	CN/S3 joint meeting (Nice).....	5
6	Reports / Liaisons from other 3GPP and SMG groups.....	5
6.1	3GPP and SMG plenary	5
6.2	3GPP WGs and SMG STCs.....	5
6.3	3GPP partners.....	6
6.4	Others (GSMA, GSM2000, T1P1, SAGE, TIA, TR-45)	7
7	R00+ security work items.....	8
7.1	Access security for IP multimedia services	8
7.2	Network based end-to-end security.....	9
7.3	User plane security.....	9
7.4	MAP application layer protection.....	10
7.5	Core network signalling security.....	10
7.6	Key management for core network signalling security.....	11
7.7	OSA/VHE security	11
7.8	MExE security.....	11
7.9	FIGS	12
7.10	Visibility and configurability of security	12
7.11	Evolution of CS algorithms (A5/3 development and deployment).....	12
7.12	Evolution of PS algorithms (GEA2 deployment)	13
7.13	GERAN security	13
7.14	Lawful interception architecture.....	13
7.15	General security enhancements.....	14
8	GSM/GERAN security issues	14
8.1	GPRS (to be dealt with under AI 7.12)	14
8.2	A5/3 (to be dealt with under AI 7.11/7.12).....	14
8.3	GERAN (Wednesday, August 02, 11:00).....	14
9	UMTS security issues	14
9.1	Algorithms.....	14
9.2	Review of other specifications (integrity protection).....	14
9.3	Open R99 security issues (emergency call handling, ...).....	15
9.4	AHAG/S3 Interactions	15
9.5	Separation of terminal functionality	15
10	Review of (draft) S3 specifications/reports	15
10.1	TS 21.133 Threats and requirements.....	15
10.2	TS 22.022 Personalisation of ME	15
10.3	TS 33.102 Security architecture	15
10.4	TS 33.103 Integration guidelines.....	16
10.5	TS 33.105 Algorithm requirements.....	16
10.6	TS 33.106 LI requirements.....	16
10.7	TS 33.107 LI architecture	16
10.8	TR 33.120 Security principles and objectives	16
10.9	TR 33.900 Guide to 3G security.....	16
10.10	TR 33.901 Criteria for algorithm design process.....	17

- 10.11 TR 33.902 Formal analysis..... 17
- 11 Approval of output documents 17
- 12 Future meeting dates and venues 17
- 13 Any other business 18
- 14 Close of meeting 18
- Annex A: List of documents at the meeting..... 19
- Annex B: List of attendees 24
- Annex C: Status of specifications under SA WG3 and SMG 10 responsibility 25
 - C.1 SA WG3 specifications 25
 - C.2 SMG10 Specifications 26
- Annex D: List of CRs to specifications under SA WG3 and SMG 10 responsibility..... 27
 - D.1 SA WG3 CRs at the Meeting 27
 - D.2 SMG10 CRs at the Meeting 27
- Annex E: List of Liaisons 28
 - E.1 Liaisons to the meeting 28
 - E.2 Liaisons from the meeting 29
- Annex F: List of Actions from the meeting 30

1 Opening of the meeting

The meeting was opened by the Vice Chairman Mr. S. Pütz, who welcomed delegates to the meeting, which was kindly hosted by Telenor. Mr. G. Koien, Telenor, provided the domestic arrangements for the meeting and wished all delegates a successful meeting. The Chairman, Professor Michael Walker, chaired the meeting from the second day.

2 Meeting objectives

The objectives of the meeting were outlined at the end of the agenda, in [TD S3-000400](#).

- Decide on way forward with CNSS
- Start and organisation of work on R00+ WI
- Technical issues:
 - Clarification of interoperation and handover with GSM
 - Emergency call handling
 - Integrity protection

These objectives were [agreed](#).

3 Registration and assignment of input documents

The available documents were allocated to their respective agenda items.

4 Approval of the agenda

The draft agenda, provided in [TD S3-000400](#) was [approved](#) with some minor changes to document allocation.

5 Approval of meeting reports

5.1 S3#13 (Yokohama)

[TD S3-000401](#): The draft report of the previous meeting was reviewed. Annex C was identified as needing update to the Rapporteurs. P Howard to provide the update. CR099 to 33.102 (Annex D) was annotated to indicate that the CR would be replaced with an updated version.

Action Points from the meeting:

13/1: Completed.

13/2: Completed.

13/3: Ongoing.

13/4: Ongoing.

13/5: M Pope to complete this ongoing action to transmit approved SA WG3 Meeting Reports to AHAG.

13/6: Completed.

13/7: Completed.

13/8: Completed, all content of the document are now included in the work programme or in WI description sheets.

13/9: The LS was to be reviewed at this meeting.

13/10: The document was updated and sent to SA WG3, but has not yet been sent to T WG3 for review.

13/11: Completed.

13/12: C Blanchard to be asked if this is completed.

13/13: Completed.

The discussion over R99 ME support of UMTS AKA was clarified, as the liaison statement provided in [TD S3-000385](#) from meeting #13 was not addressed to SA WG1 as recorded in the report. It was also suggested that the LS should be addressed to T WG2 and CN WG1. It was decided to produce a new LS on this, addressing all relevant parties. <**Check if TD385 was transmitted to T3/SMG9**>. This is dealt with under agenda item 11 (Approval of output documents).

With the above comments, the report was **approved**.

5.2 CN/S3 joint meeting (Nice)

[TD S3-000415](#): Draft report of the joint meeting. The report was introduced by P. Howard. The Release 2000 Work Plan and work item descriptions were reviewed at the meeting and many schedules modified to align the work of SA WG3 and the CN WGs. The main output of this meeting was the update to the Release 2000 Work Plan, which had been mailed to the SA WG3 e-mail list. The results of this is contained in the Work Plan in [TD S3-000449](#), which was dealt with under agenda item 7. The report was then noted. Any comments to the report should be transmitted to M. Pope. (**Meeting dates need correction**)

6 Reports / Liaisons from other 3GPP and SMG groups

6.1 3GPP and SMG plenary

[TD S3-000414](#) containing the Chairmans' Report from SA#8. The GEA2 requirements for R99 was discussed. It was requested that a reference to the SMG#31bis decision, for implementation of GEA2 in MEs after a certain date, should be included.

The implementation of GEA2 will be mandatory for R99 MEs and Networks. For R98/R97 MEs, implementation is optional, due to backward compatibility for existing R97/R98 MEs. The validity of the SMG#31bis decision for the GEA2 implementation dates was questioned. The Report of SMG#31bis and SA#08 need to be checked for the compatibility of the decisions.

ACTION #14/1: Chairman: Reports of SMG#31bis and SA#08 to be checked for GEA2 decisions and clarification to SA#08 Report to be proposed if necessary.

For the request for SA WG3 to study the security issues with PC-based Multimedia services ([TD SP-000353](#), provided separately in [TD S3-000469](#)) it was decided to handle this under a new agenda item 9.5: Separation of terminal functionality.

6.2 3GPP WGs and SMG STCs

It was reported that SMG had their last meeting at SMG#32. The remaining GSM work will be transferred into 3GPP (mainly in GERAN), "New SMG9" and a new ETSI Body MSG was created for regulatory matters.

The 3GPP FTP server is an open area, and requests for having a restricted area for more sensitive work were made. M. Pope undertook to look into this, and report back on the options. The access restriction requirements and validation of requests needs to be specified.

ACTION #14/2: M. Pope to check on 3GPP FTP site access restrictions and to verify what will happen to the SMG10 FTP area when the transfer is completed. Also to check for e-mail list subscription restriction for SA WG3 and the new LI SWG group.

B. Vinck provided a report on the meeting of RAN WG2, where he represented SA WG3 for integrity protection issues. It was agreed that SA WG3 should ensure that integrity protection is provided on signalling messages. The mechanism to provide this on all signalling, rather than on complete messages needs further study. SA WG3 delegates were invited to the RAN WG2 meetings to co-operate on this. It was identified that a CR to 33.102 was needed to correct the CFN from 7 bits to 8 bits. This was provided in [TD S3-000460](#).

[TD S3-000402](#): LS from CN WG1 on UE triggered authentication and key agreement during connections. This was covered under the security enhancements work item. This LS was then [noted](#).

It was noted that the ICG Security responsible had changed to Mr. Paul Dwyer (Vodafone).

P. Howard was asked to prepare a response LS to CN WG1 outlining the work in SA WG3 on this. This response liaison was provided in [TD S3-000487](#) (see agenda item 11).

[TD S3-000403](#) and [TD S3-000451](#): T WG3 had sent the LS in [TD S3-000403](#) on security issues with ME user input and DTMF tones. ([TD S3-000451](#) is the advice from SA WG1 to T WG3 to consult SA WG3 on this matter). It was agreed that from the security point of view, no key-dependent keypad tones should be emitted when a secret code is entered into any ME. (e.g. no tones or a neutral key-sound for keypad inputs for CHV1 code entry). It was agreed to ask T WG3 to broaden the requirement for hidden text for CHV1 input to include non-identifiable key tones. V. Naimi agreed to write a response LS to T WG3 on this which was produced in [TD S3-000477](#) (see agenda item 11).

[TD S3-000404](#): Response from CN WG1 to LS on hexadecimal IMEI format. The LS was [noted](#), as there is nothing for SA WG3 to do on this matter until studies into the IMEI extension are completed.

[TD S3-000409](#): Liaison statement regarding IMEI format for UMTS. This LS was provided for information and [noted](#).

[TD S3-000411](#): Response to LS (T3-99304) on Parameters to be stored in the USIM. This LS was provided for information and was studied and [noted](#).

ACTION #14/3: C. Blanchard to check [TD S3-000411](#) against [TS 33.103](#).

[TD S3-000436](#): Notes on security related issues from MExE Meeting 27th-29th June 2000. Delegates were asked to read these notes, and the document was considered again under agenda item 7.8.

[TD S3-000450](#): LS from SA WG1: Suggested changes to Vodafone CR on 33.102 (Emergency Call handling). It was decided to consider this LS under agenda item 9.3. (This was taken into account in the LS provided in [TD S3-000483](#))

[TD S3-000452](#): LS from SA WG1: LS on Support of VHE User Profiles. The document was considered again under agenda item 7.8. TS 22.121 version 4.0.0 was not attached (in fact, version 4.0.0 - Release 2000, did not exist), so the latest available Release 1999 version, version 3.3.0, was provided in [TD S3-000462](#).

[TD S3-000454](#): LS from SA WG1: Response to comments on TR22.976 (v1.4.0). This LS was provided for information and [noted](#). Delegates were asked to consider the implications of the statements in this LS.

6.3 3GPP partners

No input on this agenda item. It was reported that the decision for the publication of the KASUMI algorithm is awaiting T1 to agree, as they need to hear the view of the U.S. government. The decision was expected to be known by 15 August 2000.

6.4 Others (GSMA, GSM2000, T1P1, SAGE, TIA, TR-45)

TD S3-000437: Proposed LS from BT to ITU-T SG7, WP3/11, ETSI (for 3GPP), TIA TR-45.7 (for 3GPP2), AND TR45-AHG on IMT-2000 security management. It was decided that this proposed LS requires consideration by SA WG3 delegates in their companies, and that the document would need to be presented at SA WG3 Meeting #15. The document was therefore **noted** at this time.

ACTION #14/4: P. Howard to present more information or the LS in TD S3-000437 at SA WG3 Meeting#15.

SAGE: P. Christoffersson reported the progress in the SAGE-led Task Force on the authentication example algorithm work. The work started the previous week and is scheduled to be finalised by the end of November 2000. Apart from ordinary SAGE members, also Nokia, Gemplus and Mitsubishi take part. The use of a 128 bit size block cipher as the exchangeable kernel and the placing of the Operator Key outside of the kernel is proposed by SAGE. An example of the kernel will be referenced by SAGE, probably taken from the AES work. External evaluation of the proposal was not considered as absolutely necessary by SAGE under these circumstances and considering time pressure, it was proposed that this part is dropped from the work plan.

ACTION #14/5: All delegates to consider whether the external evaluation can be dropped from the work plan.

SAGE have also, to some extent, looked at the AHAG proposal to use SHA-1, and some discussions are ongoing between one of the proposal authors (Lucent) and SAGE.

SAGE were also considering a change to the generation of the AK in AUTS by direct use of RAND (instead of MAC-S) to make the algorithm more efficient. Some discussion ensued, and it was decided that this needs to be evaluated by delegates to see if there are any drawbacks to the proposed technique. This will be revisited at SA WG3 Meeting #15.

The specification of padding for response expectations between different networks was discussed. It was proposed that the response should be specified to be a multiple of 32 bits. It was decided that a CR on this should be produced in order to structure the discussion better and come to a decision. P. Christoffersson also asked whether a 64 bit RES would be sufficient to specify in the example algorithm set. After some discussion it was decided that Operators should check whether a 64 bit RES example would be acceptable.

ACTION #14/6: All Operators to check whether a 64 bit RES is sufficient in the example produced by SAGE.

It was proposed by SAGE that they are not involved in the production of the RAND function (f0) and that this is left to Operators, as the additional complication would take time and a requirement specification focussing on "internal states" and outputs for f0 would be needed from SA WG3. There was some discussion over this proposal, and some concerns against it (e.g. a high quality f0 is required as this is the basis of the authentication processes. It was decided that SAGE were not required to produce a pseudo-random generator, but that SA WG3 should consider how to ensure that the chosen pseudo-random generators are of a high quality.

ACTION #14/7: All delegates to consider how to ensure that high quality pseudo-random generators are used for generation of RAND.

TD S3-000463: Use of Kasumi for A5/3. The report was presented by C. Brookson. It includes an input document from Mitsubishi on the use of KASUMI for A5/3. SA WG3 were asked to approve the use of KASUMI for A5/3 and other GSM purposes such as EDGE and GEA-3. This proposal was **approved** by SA WG3, subject to meeting the technical requirements of SAGE. SAGE has expressed willingness to consider the adequacy of KASUMI for A5 and to do the needed specification work from November 2000 to March 2001. This comprises adjusting of input and output parameters for the different modes, production of test data, etc. An ETSI STF would be organised for this work.

7 R00+ security work items

[TD S3-000416](#): Status of R00+ security work programme. P. Howard introduced the document. The details in the work plan were expected to be updated. Each WI was checked in order to complete the supporting companies and Rapporteur fields where necessary. The updated document was made available in [TD S3-000470](#). Problem items were marked with *Italics* in the table:

Network based end-to-end security: This WI requires at least 2 more supporting companies.

User plane protection: It was noted that the intention of this was user-data integrity protection over the air interface, but the WI description does not capture this clearly. This WI also needs at least 3 more supporting companies.

VHE Security: C Blanchard agreed to create the WI for this at the meeting.

MExE Security: C Blanchard agreed to re-draft the WI to include the VHE work.

FIGS: A solution for PS services is not available in the current GSM-FIGS system. The CS FIGS could be done by transposing the GSM FIGS documents into 3GPP applicability (for CS). This WI also needs at least 2 more supporting companies.

Location Services Security: This work item needs to be drafted.

Enhancements to (U)SIM Toolkit secure messaging: This is a T WG3 WI. P Howard agreed to draft an SA WG3 WI to support the T WG3 activities.

ACTION #14/8: All: To consider all the WIs marked in *Italics* in [TD S3-000470](#) for providing support at SA WG3 meeting #15.

[TD S3-000449](#): Work Plan for Release 2000. This was provided for information and should be updated with the agreements at this meeting and distributed to the SA WG3 list.

ACTION #14/9: M Pope to update the Work Plan and distribute to SA WG3 for comment.

[TD S3-000457](#): WI proposal on UMTS network protection for DoS attacks. This WI was presented by Motorola and aims to address the risk of Denial of Service attacks in UMTS due to the additional threats from the Internet environment and new services possible in UMTS. The WI was proposed for approval at SA WG3 Meeting #15 for completion of relevant CRs (i.e. TSG Approval) by June 2001.

It was asked whether the "Core Network Security - Full system" Work Item may cover some of this work: The proposed WI concentrated on User Plane attacks, rather than the Signalling Plane. Motorola were asked to focus the WI on doing a threat analysis to determine what needs to be standardised, and where guidelines are needed for presentation to the SA WG3 Meeting #15 for approval.

7.1 Access security for IP multimedia services

[TD S3-000446](#): Requirements on access security for IP-based services (Siemens). This contribution discusses essential requirements related to the access security of the IM domain, including both security requirements and system requirements influencing the selection of security mechanism and contains first considerations on the implications of these requirements leading to working assumptions. It was suggested that a similar concept as for MExE could be considered, using different partitions on the USIM for different types of Access Control.

It was suggested that the information in this contribution should be considered for inclusion in the Security Requirements document and create a new section in the Security Architecture document for Security in the IM domain.

It was **agreed** to use this contribution to separate the security requirements out for consideration for the security requirements specification, and to determine which features should be added to the security architecture document.

It was noted that until the network architecture is finalised, the mechanisms for the security in the IM domain could not be fully determined.

TD S3-000458: Security requirements for access to R'00 IM subsystem (Nortel Networks). This contribution identifies security requirement for the IM CN subsystem to minimise the opportunity for fraudulent activity and promote a smooth evolution path. It proposes to include the sections "IM CN Subsystem Security Architecture" & "IM CN Subsystem Security Architecture Requirements" in TS 33.102 to include the specification of the use of firewalls, policing functions and a peer-to-peer security association between the Multimedia client and the IM CN subsystem to reduce fraudulent use.

It was **agreed** that this contribution will be used in combination with the Siemens contribution in **TD S3-000446** as outlined above.

TD S3-000447: Overview of security mechanisms for access security for IP-based services (Siemens). This contribution was presented for information and contains a first overview over candidate security mechanisms. It notes that none of the options listed are suitable for 3 party authentication and key management. It was mentioned that the protection of lower layers provides larger overheads in the Packet Mode, and would have an effect on QoS. The document was **noted** and should be referred to by delegates when considering what mechanisms will be employed/modified for use in 3GPP.

TD S3-000456: UMTS AKA in SIP (Nokia). This contribution considers that as SIP has been selected as the protocol over the UNI (Mt reference point) for UMTS Release 2000 IM CN subsystem, a natural option is to standardise the current UMTS AKA as the authentication mechanism for the UMTS R00 IM CN domain also; but the SIP RFC (RFC 2543) does not define the appropriate messages to perform a UMTS AKA procedure. The contribution suggests 2 ways to carry the necessary UMTS AKA parameters and discusses their relative merits. The document was **noted** and should be used for reference if SIP is chosen for 3GPP and the AKA mechanism is chosen for the authentication mechanism.

It was generally **agreed** that existing IETF protocols and mechanisms should be used as far as possible, rather than defining new mechanisms for 3GPP.

ACTION #14/10: All: The Pros and Cons of mechanisms (e.g. AKA) to use should be discussed (via e-mail) and developed, in order to agree a solution at SA WG3 Meeting #15. V. Niemi to lead the e-mail discussion and produce a document outlining the issues and agreements reached for Meeting #15.

ACTION #14/11: C. Blanchard to provide the definitive SIP documentation and the changes being made to the e-mail list.

It was decided that changes to the security architecture and requirements documents should not be considered immediately, but the text should be collected in separate documents in the 33.8xx series for further consideration on whether to include them in the main documents or to restructure the specifications.

7.2 Network based end-to-end security

No contributions were presented for this agenda item.

7.3 User plane security

No contributions were presented for this agenda item.

7.4 MAP application layer protection

[TD S3-000419](#): Preparing the Use of BEANO as Confidentiality and Integrity Protection Algorithm for 3G Core Network Signalling Security. This suggests that the BEANO algorithm is investigated as suitable for 3GPP core network signalling security encryption algorithm, which, if selected, would require that the algorithm is made Public. It was **agreed** that ETSI should be requested to publish the algorithm to allow evaluation of it's suitability for 3GPP (see [TD S3-000420](#)).

[TD S3-000420](#): Proposed Liaison to ETSI: Request concerning use of the BEANO. This proposed LS asks ETSI to publish the BEANO algorithm and asks for the conditions for acquisition of the algorithm by 3GPP Members. The LS was discussed, modified slightly for clarification and revised in [TD S3-000475](#), which was **approved**.

7.5 Core network signalling security

[TD S3-000412](#): A method to retain the IPsec full security services in the three layer network domain security architecture (Motorola). This contribution was presented by Motorola, which proposes a way of providing Replay protection if IPsec is chosen. This contribution was agreed to be used in the e-mail discussions for [TD S3-000434](#) and [TD S3-000444](#).

[TD S3-000421](#): Protect GTP signalling messages by IPsec (Motorola). This contribution proposes using IPsec to protect GTP-C messages, and optionally also for GTP-U messages. This contribution was agreed to be used in the e-mail discussions for [TD S3-000434](#) and [TD S3-000444](#).

[TD S3-000434](#): Principles for Core Network Security (Ericsson). This contribution was provided in order to stimulate discussion on the basic principles for providing the "Complete Solution" for Core Network security. It was identified that Network-Network protection was preferable to Element-Element protection, and mechanisms to protect the data integrity in the Internet, where many different parties may be involved in the transport of Network information, need to be found. It was noted that Network-Network information transmitted over the Public Internet would be susceptible to Denial of Service attacks. It was clarified that the envisaged networks are more "shared" networks rather than fully Public networks.

Ericsson proposed that the SGW functionality and mechanisms need to be standardised as a minimum.

It was proposed that the term "DMZ" would be better expressed as "ExtraNet" to avoid confusion with Firewalls.

After some discussion on the contribution, it was **agreed** as a working hypothesis for the future work and discussions in SA WG3, depending upon further investigation into the implications of choosing such a mechanism.

ACTION #14/12: All: The Pros and Cons of the architecture proposed in [TD S3-000434](#) should be discussed (via e-mail) and developed, in order to agree a solution at SA WG3 Meeting #15. G Koen to lead the e-mail discussion and produce a document outlining the issues and agreements reached for Meeting #15.

[TD S3-000444](#): Core network security protocols. This contribution describes, and discusses, the advantages and disadvantages of the different approaches to secure core network protocols. It proposes that security for protocols which can be based on both SS7- and IP-transport.

After some discussion on the contribution, it was **agreed** as a working hypothesis for the future work and discussions in SA WG3, depending upon further investigation into the implications of choosing such a mechanism.

ACTION #14/13: All: The Pros and Cons of the core network security protocols proposed in TD S3-000444 should be discussed (via e-mail) and developed, in order to agree a solution at SA WG3 Meeting #15. G Koien to lead the e-mail discussion and produce a document outlining the issues and agreements reached for Meeting #15.

7.6 Key management for core network signalling security

TD S3-000410: Response to LS on Protocol Choice for Layer I of MAP Security. This liaison was **noted**. It was suggested that a Liaison is sent to SA WG5 and CN WG4 reporting the relevant discussions of this meeting. This was produced in **TD S3-000478**, but will not be sent unless the original Liaison in **TD S3-000381** had not been sent (see agenda item 11).

TD S3-000432: Key management for MAPSec(urity). This contribution was presented by Ericsson using presentation slides, provided in **TD S3-000476**. This concludes that key management and distribution can be built on existing protocols, Key management procedures common between MAPSec and IPSec, and that IKE includes needed mechanisms.

TD S3-000433: Security Associations for MAPSec. This contribution was presented by Ericsson.

TD S3-000445: Key management for core network security.

Documents 432 (476), 433 and 445 were presented and discussions held on all 3 contributions.

It was noted that there were many common proposals in the contributions. SA WG3 **agreed** that **MAPSec-IPSec** would be adopted as the key management approach **(with MAPSec used for the encryption)**. It was also **agreed** that it will be recommended that all NEs will have an IPSec interface (from a date to be defined). P. Howard agreed to include this in the Liaison Statement in **TD S3-000478** (see also agenda item 11).

It was agreed to have 2 e-mail discussion groups on Key Management and on Network signalling security to elaborate the issues to be managed by P. Howard and G. Koien.

7.7 OSA/VHE security

TD S3-000438: Work Item Description: Scope of VHE in Release 2000 (N5-000099).

TD S3-000439: Work Item Description: Scope of Open Interface for Service Provision in Release 2000 (N5-000100).

TD S3-000441: 3G TS 22.121 V3.3.0. **Noted**.

TD S3-000442: 3G TS 23.127 V3.1.0. **Noted**.

The content of documents 438, 439, 441 and 442 were presented by C. Blanchard, who had created a summary in **TD S3-000479**. It was agreed that the work would be split into 2 WIs (OSA and VHE). C. Blanchard agreed to progress the work in the relevant groups and SA WG3 would continue the work on these WIs when stable enough to provide the security aspects.

7.8 MExE security

TD S3-000448: MExE Presentation. This was presented by L. Finklestein. The presentation was noted. Questions should be addressed to Mark Cataldo, the author of the presentation.

TD S3-000436: Notes on security related issues from MExE Meeting 27th-29th June 2000. This was covered by the presentation in **TD S3-000448**.

[TD S3-000443](#): 3G TS 23.057 V3.2.0 (MExE specification). This was **noted** for information.

[TD S3-000452](#): LS from SA WG1 on Support of VHE User Profiles.

The attachment was provided in [TD S3-000462](#). It was decided to respond with a LS that SA3 will do the security aspects when the other groups have stabilised their work. M. Walker agreed to include this in the SA WG3 status Report at SA Meeting #9.

7.9 FIGS

No items were provided for discussion.

7.10 Visibility and configurability of security

[TD S3-000418](#): E-mail from T WG2 on Rejection of non-ciphered connections. This was **noted** and taken into account in the discussions of [TD S3-000468](#).

[TD S3-000468](#): Rejection of non ciphered calls. This proposal was presented by France Telecom. This document had been previously sent on the SA WG3 e-mail list and no comments had been received.

The proposed mechanism has a parameter in the SIM/USIM, which can have 2 values:

- 0 (default): reject non-ciphered calls and offer the user the opportunity to change the parameter to 1;
- 1: accept non-ciphered calls. If a ciphered call is received, this parameter automatically reverts to the default (0) value.

It was noted that removal of the SIM/USIM while in a non-ciphering network area will require the user to accept non-ciphered calls again (the parameter reverts to default value).

After some questions and discussion, the proposal was **accepted in principle**, and France Telecom was asked to update the proposal to explain all the scenarios discussed, and the resulting action.

ACTION #14/14: France Telecom to update [TD S3-000468](#) to clarify the mechanism for more scenarios.
Note: [TD S3-000497](#) created, but not discussed.

[TD S3-000459](#): Draft LS on Rejection of non ciphered calls for GPRS. This proposed Liaison was contributed by France Telecom, and will be discussed when the update to [TD S3-000468](#) has been discussed and agreed (see action #14/14 above).

7.11 Evolution of CS algorithms (A5/3 development and deployment)

[TD S3-000466](#): Evolution of GSM circuit switched encryption. This contribution was introduced by Vodafone. It proposes that a new security architecture for GSM CS services is standardised as part of Release 2000 GERAN standards development. The security architecture should include a new encryption mechanism which terminates in the BSC rather than the BTS. The architecture should also include a new integrity mechanism which allows the GERAN security mode to be securely established. Integrity protection is introduced primarily to prevent the suppression of the instruction from the network to turn on GERAN encryption and to guard against “roll back” attacks if multiple GERAN encryption algorithms are deployed in the future. Integrity protection across the GSM radio access network enables dual mode GSM-UMTS terminals to benefit from UMTS integrity protection.

It is further proposed that efforts are concentrated on the development of new encryption and integrity algorithms for GERAN. The requirements for a new BTS-based A5 algorithm or a new SGSN-based GEA algorithm are for further study.

It was decided to add information about the operator requirements to increase security in GSM-EDGE to the liaison statement in [TD S3-000474](#) (see agenda item 7.13).

7.12 Evolution of PS algorithms (GEA2 deployment)

[TD S3-000440](#): Proposed LS on Support of additional GPRS ciphering algorithms. This informs SA WG3 of the rejection by TSG CN of the CR on the GPRS ciphering algorithm. This was covered under agenda item 6.1 and the LS was [noted](#).

[TD S3-000405](#): Reply from CN WG1 to LS on "GPRS ciphering". This was included in [TD S3-000440](#) and was [noted](#).

7.13 GERAN security

[TD S3-000407](#): 10.99 v 0.0.6 - GERAN project schedule. This was introduced using presentation slides by Ericsson using [TD S3-000471](#). SMG2 had now been moved to 3GPP and become TSG GERAN which has 4 WGs and an Ad-Hoc group, which will co-ordinate inputs into the Plenary meetings, to reduce the time spent in Plenary on discussions over contentious issues.

GERAN foresee a problem in the synchronisation with SA WG3, as the SA WG3 plan is to approve the GERAN security architecture in March 2001, before GERAN start writing the Stage 3 specifications. This was considered very late by GERAN, as if the architecture is not aligned with their expectations at that time, they would need to modify their specifications, which could cause a delay in their expected schedule. This was followed by a presentation by Nokia of the technical work of GERAN, provided in [TD S3-000472](#).

After some questions and comments, the two presentations and the GERAN Project schedule were [noted](#).

[TD S3-000408](#): Ciphering for GSM/EDGE RAN. This was covered by the above mentioned presentations and was [noted](#).

[TD S3-000455](#): Ciphering parameters in GERAN. This contribution was introduced by Nokia, and proposes that GERAN ciphering be performed on RLC/MAC layer, using the same algorithm as defined in UTRAN, in order to reach equivalent security level in an acceptable time schedule for GERAN'00. The contribution also provides details on how to set the inputs to the parameters to enable such ciphering. It was proposed that this contribution would be useful for the GERAN ad-hoc meeting being held the following week. The choice for construction of the sequence number was considered, the impact is on the time before repetition of the sequence number on long speech calls. This proposal would increase the time by 64 times. The contribution was [approved](#) as a set of working assumptions on parameters in SA WG3.

It was decided to forward the document to the GERAN ad-hoc group as an SA WG3 approved set of working assumptions. Mr. V. Niemi agreed to produce a liaison to accompany this document and to clarify some of the points discussed on integrity and security requirements, which was provided in [TD S3-000474](#) (see agenda item 11).

It was clarified that the lu interface in GERAN is intended to be the same as for UMTS.

It was [agreed](#) that this needs to be added as a new Clause in the future Release 2000 version of 33.102.

7.14 Lawful interception architecture

[TD S3-000427](#): Progress report on release 2000 LI work item. This was presented for information and [noted](#).

[TD S3-000426](#): SA WG3 LI ad-hoc initial draft meeting report from Saarbruecken, and [TD S3-000425](#): SMG10 WPD report from Mesa meeting, April 2000. These reports of these meetings were presented for information and [noted](#).

7.15 General security enhancements

SA WG3 delegates were urged to consider the Home Control issues (e.g. Home Environment Control over Authentication and Security Association lifetime) for discussion at SA WG3 Meeting #15. It was noted that a response is awaited from CN on the signalling impacts of different mechanisms. SA WG3 need to make a policy decision on the requirement of the features requested by TR-45, and then consider the feasibility/cost of implementation.

ACTION #14/15: P. Howard to collect together the arguments for/against, from the 3GPP perspective, the TR-45 Home Control features, for discussion at joint SA WG3#15/TR-45 AHAG meeting. All: Send arguments to P. Howard.

ACTION #14/16: M Michalvici to collect together the arguments for, from the 3GPP2 perspective, the TR-45 Home Control features, for discussion at joint SA WG3#15/TR-45 AHAG meeting.

It was decided to write another Liaison to CN WG4 to clarify the issue under discussion in SA WG3, to provide early warning of the possible impacts. G. Koien agreed to produce this Liaison, which was provided in [TD S3-000482](#) (see agenda item).

8 GSM/GERAN security issues

8.1 GPRS (to be dealt with under AI 7.12)

This was dealt with under agenda item 7.12.

8.2 A5/3 (to be dealt with under AI 7.11/7.12)

This was dealt with under agenda items 7.11 and 7.12.

8.3 GERAN (Wednesday, August 02, 11:00)

This was dealt with under agenda item 7.13.

9 UMTS security issues

9.1 Algorithms

No contributions were provided under this agenda item.

9.2 Review of other specifications (integrity protection)

[TD S3-000467](#): Review of the integrity protection procedure. P Howard introduced this contribution, which outlines the reasons for supplementing the existing ciphering mechanism and identifies the protection criteria for various RRC messages.

The principle that **all** messages should be integrity protected, unless specifically identified by SA WG3 as not necessary, was **confirmed**. This contribution aimed at identifying all messages that need to be protected and those which do not necessarily need protection, in order to allow RAN WG2 to optimise the overhead on signalling protection.

The contribution was considered a good basis for identifying individual messages encryption needs. *Delegates were asked to consider this document in order to identify which messages do not require protection, and the impact of not protecting them.* The length and frequency of the individual messages should also be considered from the point of view of assessing the cost of providing integrity protection.

9.3 Open R99 security issues (emergency call handling, ...)

[TD S3-000450](#): LS from SA WG1: Suggested changes to Vodafone CR on 33.102. This LS was taken into account in the updated CR provided in [TD S3-000483](#). The document was therefore [noted](#).

[TD S3-000465](#): 33.102 CR095R2: Handling of Emergency Calls. This CR was considered and updated in [TD S3-000483](#), which was [approved](#).

9.4 AHAG/S3 Interactions

[TD S3-000413](#): Guidelines for AHAG/3GPP SA3 Interactions. The guidelines were [noted](#) and a liaison to AHAG, provided in [TD S3-000484](#) was considered.

[TD S3-000484](#): LS to AHAG. This liaison was [approved](#).

9.5 Separation of terminal functionality

[TD S3-000453](#): LS from SA WG1: Applications on external devices (response to Tdoc SP-00353). This was considered, along with SA document SP-000313, which was provided in [TD S3-000313](#). It was agreed that delegates should analyse these documents and to make comments. C. Brookson agreed to collate comments received.

[TD S3-000469](#): LS from TSG SA - security issues with PC-based Multimedia services. This was dealt with at the same time as the related LS in [TD S3-000453](#) and was [noted](#).

10 Review of (draft) S3 specifications/reports

10.1 TS 21.133 Threats and requirements

10.2 TS 22.022 Personalisation of ME

Sebastien Nguyen Ngoc agreed to be the Editor for this document.

10.3 TS 33.102 Security architecture

[TD S3-000435](#): CR to 33.102: Conversion functions for GSM-UMTS interoperation. This proposal aims to complicate decryption of the conversion functions by addition of the IMSI to the Kc to create the conversion functions, instead of repeating Kc. It was argued that the detection of the IMSI was not difficult compared to the decryption of the conversion function itself, and would not act as much of a deterrent. It had not been verified whether the IMSI will always be available. Due to lack of support for this change, the proposed CR was [not approved](#).

[TD S3-000406](#): CR to 33.102: Re-transmission of authentication request using the same quintet. Some suggestions for modification were made. It was decided that the CR should be updated and submitted to SA WG3 Meeting #15.

[TD S3-000417](#): Liaison statement on the modified lengths of parameters AUTN and AUTS. This CR was copied to SA WG3 for information and was [noted](#).

[TD S3-000422](#): Suggested changes to Vodafone CR on 33.102. This was covered when dealing with [TD S3-000483](#) and was [noted](#).

[TD S3-000423](#): CR to 33.102: Clarification on the interworking procedure when a UICC has to support GSM and UMTS AKA. There was some discussion over the use of "UICC" in the CR. An off-line discussion was held to discuss this. It was decided to progress this after information is obtained from T WG3 on SIM / USIM / UICC (see report on [TD S3-000461](#)).

[TD S3-000428](#): Interactions between a user identity module (SIM or USIM) and a phone (ME). (Note that the term "IMSG_{UMTS}" should read "IMSI_{UMTS}" in this contribution). This document was [noted](#). Comments should be sent to D. Rousseau for collation and forwarding to T WG3.

[TD S3-000429](#): CR to 33.102: Clarification on sequence numbers (SQN - SEQ). This proposes to clarify the SEQ terminology to the correct SQN. This CR was updated in [TD S3-000495](#) and **approved** as an editorial CR, Category D, (33102CR106).

[TD S3-000430](#): CR to 33.102: Replace IMUI and TMUI with IMSI and TMSI. This CR was **approved**. (33102CR107)

[TD S3-000431](#): CR to 33.102: Replace Quintuplet by Quintet . This CR was **approved**. (33102CR108)

[TD S3-000461](#): LS to S1, N1 and T2 on Clarification of UMTS-AKA for GSM R'99 Mobiles. This Liaison was discussed, and some modifications made to the text and terminology, and the updated version, provided in [TD S3-000491](#) was **approved**. S. Puetz agreed to draft an LS to T WG3 about the SIM and USIM being resident on a single card for SA WG3 Meeting #15.

[TD S3-000424](#): Clarification on condition on rejecting keys CK and IK. After some discussion, no agreement could be made to move control to the USIM, and S. Puetz agreed to include a request for clarification in the liaison to T WG3 ([TD S3-000492](#)). The CR was **not approved**.

[TD S3-000460](#): 33.102: CR105: Length of CFN. This CR was **approved**.

[TD S3-000464](#): CR to 33.102: Conversion function c2. This CR was **approved**. (33102CR109)

After some discussion on the parameters in 33.102, Gunter agreed to manage an e-mail group to analyse and produce proposals for Annex C of 33.102.

[TD S3-000485](#): CR to 33.102: Terminology regarding VLR/SGSN This CR was **approved** (33102CR110).

10.4 TS 33.103 Integration guidelines

[TD S3-000493](#): Removal of Network wide encryption. This CR was **approved**. (33103CR010).

ACTION #14/17: B Vinck to produce a CR to 33.103 to make it consistent with HFN values in TS 33.102, for presetaion at SA WG3 Meeting #15.

10.5 TS 33.105 Algorithm requirements

[TD S3-000473](#): Deletion of eUIC. This CR was **approved**. (33105CR013)

[TD S3-000486](#): This CR was updated in [TD S3-000494](#), which was **approved**. (33105CR012)

10.6 TS 33.106 LI requirements

No contributions were received for this agenda item.

10.7 TS 33.107 LI architecture

No contributions were received for this agenda item.

10.8 TR 33.120 Security principles and objectives

No contributions were received for this agenda item.

10.9 TR 33.900 Guide to 3G security

This document was not preseted to the meeting, but delegates were asked to chack the document and make comments to C. Brookson, in order to discuss whether it should be approved at the next SA WG3 meeting.

10.10 TR 33.901 Criteria for algorithm design process

No contributions were received for this agenda item.

10.11 TR 33.902 Formal analysis

No contributions were received for this agenda item.

11 Approval of output documents

TD 381, was a liaison approved at Meeting #13, but it was not clear whether it had been sent. It was therefore decided to make potential changes, to be used if the original liaison had not been sent.

ACTION #14/18: M Pope: If S3-000381 was not sent: to send modified version in TD478.

TD S3-000488: WI description for UE triggered authentication during connections. This WI was approved.

TD S3-000487: LS on UE triggered authentication and key agreement during connections. This LS was approved, TD S3-000488 to be attached to this.

TD S3-000489: WI description for P-TMSI signature stage 2 specification. It was decided to update this WI description for consideration for approval at the next meeting. It will stay on the SA WG3 work plan.

TD S3-000490: WI description for enhancing home environment control of security. This WI was approved.

TD S3-000474: Proposed LS on GERAN security issues. This was modified slightly and provided in TD S3-000498, which was approved.

TD S3-000477: Response LS to T3 on keypad tones for CHV1. This Liaison statement was approved.

TD S3-000482: Evaluation of the impact on positive authentication reporting on network performance. The liaison was updated editorially and provided in TD S3-000499, which was approved.

TD S3-000495: Clarification on Sequence Numbers (SQN - SEQ). This CR was approved.

12 Future meeting dates and venues

Note 1: Changes to Meeting #15 schedule.

Note 2: Meeting #16 may be 4 days if an ad-hoc meeting is required on the first day.

Meeting	Date	Location	Host
S3#15	12-14 September 2000	Washington USA	Host TBC
S3 Joint with AHAG	12 September 2000 (afternoon)	Washington USA	Host TBC
S3#16	27 or 28-30 November 2000	Israel (TBC)	Motorola (TBC)
S3#17	27 February - 1 March 2001	-	Host required

ETSI Secretariat to be reserved as a contingency for meeting #16.

13 Any other business

E-mail approval. S. Puetz requested a procedure for e-mail approval, in order to make the system more efficient than experienced before the SA #8.

Discussion of CRs should be done by e-mail before the SA WG3 meeting, for approval at the meeting, rather than sent for approval by e-mail after a meeting.

Delegates were requested to submit documents in good time before meetings, in order to give everyone time to consider the documents before the meeting.

It was **agreed** that any CR for approval at SA WG3 meeting should be made available for discussion at least 1 week before the meeting, otherwise it may not be accepted for approval at the meeting.

It was suggested that for e-mail discussions, a **keyword** should be chosen by the moderator, in order to allow sorting of the e-mail. This idea was **agreed**.

14 Close of meeting

The Chairman thanked the host for the excellent facilities and the excellent social event, the delegates for their hard work and co-operation, which permitted good progress at the meeting. The meeting was then closed.

Annex A: List of documents at the meeting

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000400	Draft Agenda for meeting #14	Chairman	4	Approval		Approved
S3-000401	Draft Report of meeting #13 v0.0.3	Secretary	5.1	Approval		Approved
S3-000402	LS from CN WG1 on UE triggered authentication and key agreement during connections	CN WG1	6.2	Discussion		Noted. P. Howard was asked to prepare a response LS
S3-000403	Security issues with ME user input and DTMF tones	New SMG9	6.2	Discussion		Response LS to T3 in TD477
S3-000404	Response from CN WG1 to LS on hexadecimal IMEI format	CN WG1	6.2	Discussion		Noted.
S3-000405	Reply from CN WG1 to LS on "GPRS ciphering"	CN WG1	7.12	Discussion		Noted.
S3-000406	CR to 33.102: Re-transmission of authentication request using the same quintet	Siemens Atea	10.3	Approval		To be updated and submitted to meeting#15
S3-000407	10.99 v 0.0.6 - GERAN project schedule	Rapporteur	7.13	Information		Noted.
S3-000408	Ciphering for GSM/EDGE RAN	Ericsson, Nokia, Siemens	7.13	Discussion		Noted.
S3-000409	Liaison statement regarding IMEI format for UMTS	GSM Association SG	6.2	Information		SA WG1 Liaison also attached. Noted
S3-000410	Response to LS on Protocol Choice for Layer I of MAP Security	SA WG5	7.6	Discussion		Noted. LS to S3/N4 on discussions at this meeting to be produced?
S3-000411	Response to LS (T3-99304) on Parameters to be stored in the USIM	RAN WG2	6.2	Information		Noted. C Blanchard to check against 33.103
S3-000412	A method to retain the IPsec full security services in the three layer network domain security architecture	Motorola	7.5	Discussion		be used in the e-mail discussions for TD S3-000434 and TD S3-000444
S3-000413	Guidelines for AHAG/3GPP SA3 Interactions	TR-45 AHAG	9.4	Discussion		Noted. LS in TD484 considered.
S3-000414	Report to 3GPP SA3 on 3GPP SA#8	SA WG3 Chairman	6.1	Information		Includes attachments. Noted
S3-000415	Draft report of CN/SA WG3 Joint meeting	CN Secretary	5.2	Information		Noted.
S3-000416	Status of R00+ security work programme	P Howard	7	Information		Work plan attachment updated after discussion in TD480
S3-000417	Liaison statement on the modified lengths of parameters AUTN and AUTS	CN WG4	10.3	Information		Noted.
S3-000418	E-mail on Rejection of non-ciphered connections	T WG2 (K Holley)	7.10.	Discussion		Forwarded to SMG10/SA WG3 by e-mail. M Walker to produce LS (TD 481)
S3-000419	Preparing the Use of BEANO as Confidentiality and Integrity Protection Algorithm for 3G Core Network Signalling Security	T-Mobil	7.4	Discussion		agreed that ETSI should be requested to publish the algorithm

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000420	Proposed Request concerning use of the BEANO encryption algorithm	T-Mobil	7.4	Discussion	S3-000475	Modified and approved in TD475
S3-000421	Protect GTP signalling messages by IPSec	Motorola	7.5	Discussion		be used in the e-mail discussions for TD S3-000434 and TD S3-000444
S3-000422	Suggested changes to Vodafone CR on 33.102	SA WG1	10.3	Discussion		Covered with TD465. Noted.
S3-000423	CR to 33.102: Clarification on the interworking procedure when a UICC has to support GSM and UMTS AKA	T-Mobil	10.3	Approval		Discussed. See TD461
S3-000424	CR to 33.102: Clarification on condition on rejecting keys CK and IK	T-Mobil	10.3	Approval		Not approved. S Puetz to include request for clarification in TD492.
S3-000425	SMG10 WPD report from Mesa meeting, April 2000 (AD00-49R2)	SMG10 WPD	7.14	Information		Noted
S3-000426	SA WG3 LI ad-hoc initial draft meeting report from Saarbruecken (AD00-76)	SMG10 WPD	7.14	Information		Noted
S3-000427	Progress report on release 2000 LI work item (AD00-76)	SMG10 WPD	7.14	Information		Noted
S3-000428	Interactions between a user identity mobile (SIM or USIM) and a phone (ME)	GemPlus	10.3	Information		Noted. Comments to author for sending to T3
S3-000429	CR to 33.102: Clarification on sequence numbers (SQN - SEQ)	Ericsson	10.3	Approval	S3-000495	Modified in TD495
S3-000430	CR to 33.102 Replace IMUI and TMUI with IMSI and TMSI	Ericsson	10.3	Approval		Approved CR107
S3-000431	CR to 33.102 Replace Quintuplet by Quintet	Ericsson	10.3	Approval		Approved CR108
S3-000432	Key management for MAPSec(urity)	Ericsson	7.6	Approval		Presented using TD476. LS in TD478 created
S3-000433	Security Associations for MAPSec	Ericsson	7.6	Approval		LS in TD478 created
S3-000434	Principles for Core Network Security	Ericsson	7.5	Approval		to be discussed via e-mail and developed, for solution at S3#15
S3-000435	CR to 33.102: Conversion functions for GSM-UMTS interoperation	BT	10.3	Approval		Not Approved
S3-000436	Notes on security related issues from MExE Meeting 27th-29th June 2000	BT	6.2/7.8	Information		Covered by TD448
S3-000437	LIASON TO ITU-T SG7 (lead Studygroup for Security), WP3/11(lead for IMT-2000), ETSI, FOR FORWARDING TO 3GPP, AND COMMUNICATIONS TO TIA TR-45.7, FOR FORWARDING TO 3GPP2, AND TR45-AHG ON IMT2000 SECURITY MANAGEMENT	BT	6.4	Discussion		Noted. Requires consideration by S3 delegates
S3-000438	Work Item Description: Scope of VHE in Release 2000 (N5-000099)	BT	7.7	Information		Presented using summary in TD479
S3-000439	Work Item Description: Scope of Open Interface for Service Provision in Release 2000 (N5-000100)	BT	7.7	Information		Presented using summary in TD479
S3-000440	Proposed LS on Support of additional GPRS ciphering algorithms (N5-000366)	BT	7.12	Discussion		Noted
S3-000441	3G TS 22.121 V3.3.0	BT	7.7	Information		Presented using summary in TD479. Noted

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000442	3G TS 23.127 V3.1.0	BT	7.7	Information		Presented using summary in TD479. Noted
S3-000443	3G TS 23.057 V3.2.0	BT	7.8	Information		Noted
S3-000444	Core network security protocols	Siemens AG	7.5	Discussion & Decision		to be discussed via e-mail and developed, for solution at S3#15
S3-000445	Key management for core network security	Siemens AG	7.6	Discussion & Decision		LS in TD478 created
S3-000446	Requirements on access security for IP-based services	Siemens AG	7.1	Discussion & Decision		agreed to separate out security requirements and features
S3-000447	Overview of security mechanisms for access security for IP-based services	Siemens AG	7.1	Discussion		Noted
S3-000448	Presentation on MExE (Mobile Execution Environment)	Motorola	7.8	Information		Noted
S3-000449	3GPP Work Plan (000728)	MCC	7	Discussion		MS Project 98 file & PDF printout. M Pope to update the Work Plan and distribute
S3-000450	LS from SA WG1: Suggested changes to Vodafone CR on 33.102	SA WG1	6.2/9.3	Discussion		Noted. Taken into account in TD465
S3-000451	LS from SA WG1: Reply to LS on Security issues with ME user input and DTMF tones	SA WG1	6.2	Discussion		Noted. Part of TD403
S3-000452	LS from SA WG1: LS on Support of VHE User Profiles	SA WG1	6.2/7.8	Discussion		TD462 to be considered as the attachment. LS provided in TD481
S3-000453	LS from SA WG1: Applications on external devices (response to Tdoc SP-00353)	SA WG1	6.2	Information		All to analyse, C. Brookson to collate comments.
S3-000454	LS from SA WG1: Response to comments on TR22.976 (v1.4.0)	SA WG1	6.2	Information		Noted. Delegates to consider the implications
S3-000455	Ciphering parameters in GERAN	Nokia	7.13	Discussion /Decision		Approved as a set of working assumptions on parameters
S3-000456	UMTS AKA in SIP	Nokia	7.1	Discussion /Decision		The Pros and Cons of mechanisms (e.g. AKA) to use should be discussed via e-mail (V Niemi) for S3#15
S3-000457	WI proposal on UMTS network protection for DoS attacks	Motorola	7	Discussion		Motorola asked to focus WI on threat analysis for S3#15
S3-000458	IM Security requirements	Nortel Networks	7.1	Discussion		will be used in combination with TD446

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000459	Draft LS on Rejection of non ciphered calls for GPRS	SA WG3	7.12	Approval		To be discussed when the update to TD468 has been discussed and agreed
S3-000460	33.102: CR105: Length of CFN	Siemens Atea	10.3	Approval		Approved CR105
S3-000461	LS to S1, N1 and T2 on Clarification of UMTS-AKA for GSM R'99 Mobiles	SA WG3	9.1	Approval	S3-000491	Updated in TD491
S3-000462	TS 22.121 version 3.3.0 (Attachment to TD S3-000452)	SA WG1	7.8	Information		Version 4.0.0 did not exist, so v3.3.0 was provided. LS provided in TD481
S3-000463	Use of Kasumi for A5/3	Chairman GSM2000 SA WG3 and GSMA SG Joint Working Party	6.4			use of KASUMI for A5/3 approved subject to SAGE evaluation
S3-000464	CR109 to 33.102: Conversion function c2	Siemens Atea	10.3	Approval		Approved CR109
S3-000465	draft 33.102 CR095R2: Handling of Emergency Calls	Vodafone	9.3	Approval	S3-000483	Updated in TD483
S3-000466	Evolution of GSM circuit switched encryption	Vodafone	7.11	Decision		Included in LS in TD474
S3-000467	Review of the integrity protection procedure	Vodafone	9.2	Discussion /Decision		Delegates to consider the message protection requirements .
S3-000468	Rejection of non ciphered calls	France Telecom	7.10.	Approval	S3-000497	Accepted in principle. Sebastien updated document with more scenarios in TD497
S3-000469	SP-000353: LS from TSG SA - security issues with PC-based Multimedia services	TSG SA	9.5	Discussion		M Walker to write LS to SA reporting analysis (see TD453)
S3-000470	Updated Status of security work items	SA WG3	7	Information	S3-000480	Replaced by TD480
S3-000471	GERAN Structure and timescales Presentation	Ericsson	7.13	Information /Discussion		Presented and discussed.
S3-000472	GERAN technical Presentation	Nokia	7.13	Information /Discussion		Presented and discussed.
S3-000473	CR 013 to 33.105: Deletion of eUIC	Siemens Atea	10.5	Approval		Approved
S3-000474	Proposed LS to GERAN Ad-hoc on Ciphering and security in GERAN	SA WG3	7.13	Approval	S3-000498	updated in TD498
S3-000475	Request concerning use of the BEANO encryption algorithm (rev of TD 420)	SA WG3	7.4	Approval		Approved
S3-000476	Presentation slides on Key Management for MAP Security	Ericsson	7.2	Presentation		Presented for TD432. LS in TD478 created
S3-000477	Response LS to T3 on keypad tones for CHV1	SA WG3	6.2	Approval		Approved
S3-000478	LS on Key management agreements in SA WG3	SA WG3	7.6	Approval		Approved

Number	Title	Source	Agenda item	Document for	Replaced by Tdoc	Comments Status
S3-000479	VHE/ OSA Summary	C Blanchard				C. Blanchard agreed to progress the work. S3 to continue when stable.
S3-000480	Updated Status of security work items	SA WG3	7	Information		Updated from attachment to TD 416. All to consider all the WIs marked in Italics
S3-000481	LS on MExE	SA WG3	7.8	Approval		M Walker to produce
S3-000482	Evaluation of the impact on positive authentication reporting on network performance	SA WG3	7.15	Approval	S3-000499	Updated in TD499
S3-000483	33.102 CR095R2: Handling of Emergency Calls	SA WG3	9.3	Approval		Approved
S3-000484	LS to AHAG	SA WG3	9.4	Approval		Approved
S3-000485	CR to 33.102: Terminology regarding VLR/SGSN	Ericsson	10.3	Approval		Approved CR110
S3-000486	CR to 33.105: AK in re-synchronisation	Siemens Atea	10.5	Approval	S3-000494	
S3-000487	LS to N1, cc T3, R2 on UE triggered authentication during connections	SA WG3	11	Approval		Approved
S3-000488	WI description for UE triggered authentication during connections	Vodafone	11	Approval		Approved
S3-000489	WI description for P-TMSI signature stage 2 specification	Vodafone	11	Approval		To be updated for approval at meeting #15
S3-000490	WI description for enhancing home environment control of security	Vodafone	11	Approval		Approved
S3-000491	LS to S1, N1 and T2 on Clarification of UMTS-AKA for GSM R'99 Mobiles	SA WG3	10.3	Approval		Approved
S3-000492	Withdrawn					Withdrawn
S3-000493	CR to 33.103: Removal of Network wide encryption					Approved CR010
S3-000494	CR to 33.105: AK in re-synchronisation	Siemens Atea	10.5	Approval		Approved CR012
S3-000495	Clarification on Sequence Numbers (SQN - SEQ)	SA WG3		Approval		Approved CR106
S3-000496	Withdrawn					Withdrawn
S3-000497	Rejection of non ciphered calls (Update of TD468)	France Telecom	7.10.	Approval		Not discussed
S3-000498	Proposed LS to GeRAN Ad-hoc on Ciphering and security in GERAN (update of TD474)	SA WG3	7.13	Approval		Approved
S3-000499	Evaluation of the impact on positive authentication reporting on network performance (update of TD482)	SA WG3	7.15	Approval		Approved

Annex B: List of attendees

Name			Company	e-mail	3GPP Member	
Mr.	Tom Erling	Aamodt	TELENOR AS	tom-erling.aamodt@telenor.com	ETSI	NO
Mr.	Alf. S	Aanonsen	ERICSSON L.M.	etoals@eto.ericsson.se	ETSI	SE
Mr.	Phil	Ames	Intel Sweden AB	phil.h.ames@intel.com	ETSI	SE
Mr.	Stefan	Andersson	ERICSSON L.M.	stefan.x.andersson@ecs.ericsson.se	ETSI	SE
Mr.	Hiroshi	Aono	NTT DoCoMo	aono@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr.	Jose Antonio	Aranda Legazpe	AIRTEL Movil SA	jaranda@airtel.es	ETSI	ES
Mr.	Colin	Blanchard	BT	colin.blanchard@bt.com	ETSI	GB
Mr.	Rolf	Blom	ERICSSON L.M.	rolf.blom@era.ericsson.se	ETSI	SE
Mr.	Krister	Boman	ERICSSON L.M.	Krister.Boman@emw.ericsson.se	ETSI	SE
Mr.	Charles	Brookson	DTI	cbrookson@iee.org	ETSI	GB
Mr.	David	Castellanos	ERICSSON L.M.	david.castellanos@ece.ericsson.se	ETSI	SE
Ms.	Lilly	Chen	Motorola Inc.	lchen1@email.mot.com	T1	US
Mr.	Takeshi	Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB	JP
Mr.	Per	Christoffersson	TELIA AB	per.e.christoffersson@telia.se	ETSI	SE
Mr.	Janos	Csirik	AT&T Corp.	janos@research.att.com	T1	US
Mr.	Louis	Finkelstein	Motorola Inc.	louisf@crl.mot.com	T1	US
Mr.	Guenther	Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	DE
Mr.	Peter	Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	GB
Mr.	Geir	Koien	TELENOR AS	geir-myrdahl.koien@telenor.com	ETSI	NO
Mrs.	Tiina	Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI	FI
Mr.	Anders	Liljekvist	ERICSSON L.M.	anders.liljekvist@era.ericsson.se	ETSI	SE
Mr.	Robert	Lubarsky	Deutsche Telekom AG	robert.lubarsky@t-mobil.de	ETSI	DE
Mr.	Michael	Marcovici	Lucent Technologies	marcovici@lucent.com	T1	US
Mr.	Frank	Mueller	ERICSSON L.M.	frank.muller@era.ericsson.se	ETSI	SE
Mr.	Sebastien	Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@rd.francetelecom.fr	ETSI	FR
Mr.	Valtteri	Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	FI
Mr.	Petri	Nyberg	SONERA Corporation	petri.nyberg@sonera.fi	ETSI	FI
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	FR
Dr.	Stefan	Pütz	Deutsche Telekom MobilNet	stefan.puetz@t-mobil.de	ETSI	DE
Mr.	Greg	Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	ETSI	FR
Mr.	Ludovic	Rousseau	GEMPLUS Card International	ludovic.rousseau@gemplus.com	ETSI	FR
Ms.	Rong	Shi	Motorola Inc.	yongshi1@email.mot.com	T1	US
Mr.	Hamiti	Shkumbin	NOKIA Corporation	shkumbin.hamiti@nokia.com	ETSI	FI
Mr.	Benno	Tietz	MANNESMANN Mobilfunk GmbH	benno.tietz@d2mannesmann.de	ETSI	DE
Mr.	Peter	Trautmann	BMW	peter.trautmann@regtp.de	ETSI	DE
Mr.	Pierre	Truong	Ericsson Inc.	pierre.truong@ericsson.com	T1	US
Mr.	Bart	Vinck	SIEMENS ATEA NV	bart.vinck@icn.siemens.de	ETSI	BE
Prof.	Michael	Walker	VODAFONE Group Plc	mike.walker@vf.vodafone.co.uk	ETSI	GB
Mr.	Berthold	Wilhelm	BMW	berthold.wilhelm@regtp.de	ETSI	DE
Apologies for absence:						
Mr.	Nigel	Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	ETSI	GB

Annex C: Status of specifications under SA WG3 and SMG 10 responsibility

C.1 SA WG3 specifications

Specification			Title		Editor	Rel	Comment
TS	21.133	3.1.0	Security Threats and Requirements	April 99	Christoffersson, Per	R99	
TS	22.022	3.1.0	Personalisation of GSM ME Mobile functionality specification - Stage 1	Oct 99	Nguyen Ngoc, Sebastien	R99	Transfer>TSG#4, CR at TSG#5
TS	33.102	3.5.0	Security Architecture	Mar 00	Vinck, Bart	R99	TSG#7: 3.4.0 TSG#8:3.5.0
TS	33.103	3.3.0	Security Integration Guidelines	Oct 99	Blanchard, Colin	R99	TSG#7: 3.2.0 TSG#8:3.3.0
TS	33.105	3.4.0	Cryptographic Algorithm requirements	Jun 99	Chikazawa, Takeshi	R99	TSG#7: 3.3.0 TSG#8:3.4.0
TS	33.106	3.1.0	Lawful interception requirements	Jun 00	Wilhelm, Berthold	R99	
TS	33.107	3.0.0	Lawful interception architecture and functions	Dec 99	Wilhelm, Berthold	R99	New at TSG#6 approved
TS	33.120	3.0.0	Security Objectives and Principles	April 99	Wright, Tim	R99	
TR	33.900	1.2.0	Guide to 3G security	Mar 00	Brookson, Charles	R99	New at TSG#6
TR	33.901	3.0.0	Criteria for cryptographic Algorithm design process	Jun 99	Blom, Rolf	R99	
TR	33.902	3.1.0	Formal Analysis of the 3G Authentication Protocol	Oct 99	Horn, Günther	R99	
TR	33.908	3.0.0	Security Algorithms Group of Experts (SAGE); General report on the design, specification and evaluation of 3GPP standard confidentiality and integrity algorithms	Mar 00	Walker, Michael	R99	TSG#7: S3-000105=NP-000049
TR	33.909	3.0.0	ETSI SAGE 3GPP Standards Algorithms Task Force: Report on the evaluation of 3GPP standard confidentiality and integrity algorithms	Jun 00	Walker, Michael	R99	TSG#7: Is a reference in 33.908
TS	35.201	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 1: f8 and f9 specifications	Mar 00	Walker, Michael	R99	ex SAGE - not publicly available; supplied by ETSI under licence
TS	35.202	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 2: Kasumi algorithm specification	Mar 00	Walker, Michael	R99	ex SAGE - not publicly available; supplied by ETSI under licence
TS	35.203	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 3: Implementors' test data	Mar 00	Walker, Michael	R99	ex SAGE - not publicly available; supplied by ETSI under licence
TS	35.204	3.1.0	Specification of the 3GPP confidentiality and integrity algorithms; Document 4: Design conformance test data	Mar 00	Walker, Michael	R99	ex SAGE - not publicly available; supplied by ETSI under licence

C.2 SMG10 Specifications

Specification latest version		Title	Release	ETSI Number		ETSI WI ref
01.31	7.0.1	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	Release 1998			RTR/SMG-100131Q7
01.31	8.0.0	Fraud Information Gathering System (FIGS); Service requirements - Stage 0	Release 1999			RTR/SMG-100131Q8
01.33	7.0.0	Lawful Interception requirements for GSM	Release 1998			
01.33	8.0.0	Lawful Interception requirements for GSM	Release 1999			
01.61	8.0.0	General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements	Release 1997	TS	101 106	DTS/SMG-100161Q6
02.09	3.1.0	Security Aspects	Phase 1	GTS	02.09	DGTS/SMG-010209
02.09	4.5.0	Security Aspects	Phase 2	ETS	300 506	RE/SMG-010209PR2
02.09	5.2.0	Security Aspects	Phase 2+	ETS	300 920	RE/SMG-010209QR2
02.09	6.1.0	Security Aspects	Release 1997	EN	300 920	DEN/SMG-010209Q6R1
02.09	7.1.0	Security Aspects	Release 1998	EN	300 920	DEN/SMG-010209Q7R1
02.09	8.0.0	Security Aspects	Release 1999			DEN/SMG-010209Q8
02.31	7.1.1	Fraud Information Gathering System (FIGS) Service description - Stage 1	Release 1998	TS	101 107	RTS/SMG-100231Q7
02.31	8.0.0	Fraud Information Gathering System (FIGS) Service description - Stage 1	Release 1999			RTS/SMG-100231Q8
02.32	7.1.1	Immediate Service Termination (IST); Service description - Stage 1	Release 1998	TS	101 749	DTS/SMG-100232Q7
02.32	8.0.0	Immediate Service Termination (IST); Service description - Stage 1	Release 1999			DTS/SMG-100232Q8
02.33	7.3.0	Lawful Interception - Stage 1	Release 1998	TS	101 507	DTS/SMG-100233Q7
02.33	8.0.0	Lawful Interception - Stage 1	Release 1999			DTS/SMG-100233Q8
03.20	3.0.0	Security-related Network Functions	Phase 1 extension	GTS	03.20-EXT	RGTS/SMG-030320B
03.20	3.3.2	Security-related Network Functions	Phase 1	GTS	03.20	DGTS/SMG-030320
03.20	4.4.1	Security-related Network Functions	Phase 2	ETS	300 534	RE/SMG-030320PR
03.20	5.2.0	Security-related Network Functions	Release 1996			
03.20	6.1.0	Security-related Network Functions	Release 1997	TS	100 929	RTS/SMG-030320Q6R1
03.20	7.3.0	Security-related Network Functions	Release 1998	TS	100 929	RTS/SMG-030320Q7
03.20	8.1.0	Security-related Network Functions	Release 1999			RTS/SMG-030320Q8
03.31	7.0.0	Fraud Information Gathering System (FIGS); Service description - Stage 2	Release 1998			
03.31	8.0.0	Fraud Information Gathering System (FIGS); Service description - Stage 2	Release 1999			
03.33	7.1.0	Lawful Interception - stage 2	Release 1998	TS	101 509	DTS/SMG-100333Q7
03.33	8.0.0	Lawful Interception - stage 2	Release 1999			DTS/SMG-100333Q8
03.35	7.0.0	Immediate Service Termination (IST); Stage 2	Release 1998			DTS/SMG-100335Q7
03.35	8.0.0	Immediate Service Termination (IST); Stage 2	Release 1999			DTS/SMG-100335Q8
10.20	-	Lawful Interception requirements for GSM	Release 1999			DTS/SMG-101020Q8

Annex D: List of CRs to specifications under SA WG3 and SMG 10 responsibility**D.1 SA WG3 CRs at the Meeting**

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	Next Vers	Date	Source	WG	WG meeting	WG TD	WG status	Remarks
33.102	104		R99	Re-transmission of authentication request using the same quintet	C	3.5.0		20/06/2000	S3	S3	S3-14	S3-000406		To be updated and submitted to meeting #15
33.102	105		R99	Length of CFN	F	3.5.0		20/06/2000	S3	S3	S3-14	S3-000460	Agreed	Security
33.102	106		R99	Clarification on Sequence Numbers (SQN - SEQ)	D	3.5.0		03/08/2000	S3	S3	S3-14	S3-000429	Agreed	Security
33.102	107		R99	Replace IMUI and TMUI with IMSI and TMSI	F	3.5.0		03/08/2000	S3	S3	S3-14	S3-000430	Agreed	Security
33.102	108		R99	Replace Quintuplet by Quintet	D	3.5.0		04/08/2000	S3	S3	S3-14	S3-000431	Agreed	Security
33.102	109		R99	Conversion function c2	F	3.5.0		04/08/2000	S3	S3	S3-14	S3-000464	Agreed	Security
33.102	110		R99	Update terminology regarding VLR/SGSN	D	3.5.0		04/08/2000	S3	S3	S3-14	S3-000485	Agreed	Security
33.103	010		R99	Removal of Network Wide Confidentiality for R99 (clause 6)	F	3.3.0		04/08/2000	S3	S3	S3-14	S3-000493	agreed	Security
33.105	012		R99	Calculation of AK in re-synchronisation	D	3.4.0		07/08/2000	S3	S3	S3-14	S3-000494	agreed	Security
33.105	013		R99	Deletion of eUIC	F	3.4.0		07/08/2000	S3	S3	S3-14	S3-000473	agreed	Security

D.2 SMG10 CRs at the Meeting

None.

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-000402	LS from CN WG1 on UE triggered authentication and key agreement during connections	CN WG1	Noted. response LS in TD487
S3-000403	Security issues with ME user input and DTMF tones	New SMG9	Response LS to T3 in TD477
S3-000404	Response from CN WG1 to LS on hexadecimal IMEI format	CN WG1	Noted.
S3-000405	Reply from CN WG1 to LS on "GPRS ciphering"	CN WG1	Noted.
S3-000409	Liaison statement regarding IMEI format for UMTS	GSM Association SG	SA WG1 Liaison also attached. Noted
S3-000410	Response to LS on Protocol Choice for Layer I of MAP Security	SA WG5	Noted. LS to S3/N4 on discussions at this meeting to be produced?
S3-000411	Response to LS (T3-99304) on Parameters to be stored in the USIM	RAN WG2	Noted. C Blanchard to check against 33.103
S3-000413	Guidelines for AHAG/3GPP SA3 Interactions	TR-45 AHAG	Noted. LS in TD484 considered.
S3-000417	Liaison statement on the modified lengths of parameters AUTN and AUTS	CN WG4	Noted.
S3-000418	E-mail on Rejection of non-ciphered connections	T WG2 (K Holley)	Forwarded to SMG10/SA WG3 by e-mail. M Walker to produce LS (TD 481)
S3-000437	LIASON TO ITU-T SG7 (lead Studygroup for Security), WP3/11(lead for IMT-2000), ETSI, FOR FORWARDING TO 3GPP, AND COMMUNICATIONS TO TIA TR-45.7, FOR FORWARDING TO 3GPP2, AND TR45-AHG ON IMT2000 SECURITY MANAGEMENT	BT	Noted. Requires consideration by S3 delegates
S3-000440	Proposed LS on Support of additional GPRS ciphering algorithms (N5-000366)	BT	Noted
S3-000450	LS from SA WG1: Suggested changes to Vodafone CR on 33.102	SA WG1	Noted. Taken into account in TD465
S3-000451	LS from SA WG1: Reply to LS on Security issues with ME user input and DTMF tones	SA WG1	Noted. Part of TD403
S3-000452	LS from SA WG1: LS on Support of VHE User Profiles	SA WG1	TD462 to be considered as the attachment. LS provided in TD481
S3-000453	LS from SA WG1: Applications on external devices (response to Tdoc SP-00353)	SA WG1	All to analyse , C. Brookson to collate comments.
S3-000454	LS from SA WG1: Response to comments on TR22.976 (v1.4.0)	SA WG1	Noted. Delegates to consider the implications
S3-000463	Use of Kasumi for A5/3	Chairman GSM2000 SA WG3 and GSMA SG Joint Working Party	Use of KASUMI for A5/3 approved subject to SAGE evaluation
S3-000469	SP-000353: LS from TSG SA - security issues with PC-based Multimedia services	TSG SA	M Walker to write LS to SA reporting analysis (see TD453)

E.2 Liaisons from the meeting

TD Number	Title	Status	Comment
S3-000459	Draft LS on Rejection of non ciphered calls for GPRS	SA WG3	To be discussed when the update to TD468 has been discussed and agreed
S3-000475	Request concerning use of the BEANO encryption algorithm (rev of TD 420)	Approved	
S3-000477	Response LS to T3 on keypad tones for CHV1	Approved	
S3-000478	LS on Key management agreements in SA WG3	Approved	
S3-000481	LS on MExE	SA WG3	M Walker to produce
S3-000484	LS to AHAG	Approved	
S3-000487	LS to N1, cc T3, R2 on UE triggered authentication during connections	Approved	
S3-000491	LS to S1, N1 and T2 on Clarification of UMTS-AKA for GSM R'99 Mobiles	Approved	
S3-000498	Proposed LS to GERAN Ad-hoc on Ciphering and security in GERAN (update of TD474)	Approved	
S3-000499	Evaluation of the impact on positive authentication reporting on network performance (update of TD482)	Approved	

Annex F: List of Actions from the meeting

- ACTION #14/1:** Chairman: Reports of SMG#31bis and SA#08 to be checked for GEA2 decisions and clarification to SA#08 Report to be proposed if necessary.
- ACTION #14/2:** M. Pope to check on 3GPP FTP site access restrictions and to verify what will happen to the SMG10 FTP area when the transfer is completed. Also to check for e-mail list subscription restriction for SA WG3 and the new LI SWG group.
- ACTION #14/3:** C. Blanchard to check TD S3-000411 against TS 33.103.
- ACTION #14/4:** P. Howard to present more information on the LS in TD S3-000437 at SA WG3 Meeting#15.
- ACTION #14/19:** All delegates to consider whether the external evaluation can be dropped from the work plan.
- ACTION #14/6:** All Operators to check whether an example produced by SAGE is acceptable to use a 64 bit RES.
- ACTION #14/7:** All delegates to consider how to ensure that high quality pseudo-random generators are used for generation of RAND.
- ACTION #14/8:** All: To consider all the WIs marked in *Italics* in TD S3-000470 for providing support at SA WG3 meeting #15.
- ACTION #14/9:** M Pope to update the Work Plan and distribute to SA WG3 for comment.
- ACTION #14/10:** All: The Pros and Cons of mechanisms (e.g. AKA) to use should be discussed (via e-mail) and developed, in order to agree a solution at SA WG3 Meeting #15. V. Niemi to lead the e-mail discussion and produce a document outlining the issues and agreements reached for Meeting #15.
- ACTION #14/11:** C. Blanchard to provide the definitive SIP documentation and the changes being made to the e-mail list.
- ACTION #14/12:** All: The Pros and Cons of the architecture proposed in TD S3-000434 should be discussed (via e-mail) and developed, in order to agree a solution at SA WG3 Meeting #15. G Koiem to lead the e-mail discussion and produce a document outlining the issues and agreements reached for Meeting #15.
- ACTION #14/13:** All: The Pros and Cons of the core network security protocols proposed in TD S3-000444 should be discussed (via e-mail) and developed, in order to agree a solution at SA WG3 Meeting #15. G Koiem to lead the e-mail discussion and produce a document outlining the issues and agreements reached for Meeting #15.
- ACTION #14/14:** France Telecom to update TD S3-000468 to clarify the mechanism for more scenarios.
Note: TD S3-000497 created, but not discussed.
- ACTION #14/15:** P. Howard to collect together the arguments for/against, from the 3GPP perspective, the TR-45 Home Control features, for discussion at joint SA WG3#15/TR-45 AHAG meeting. All: Send arguments to P. Howard.

- ACTION #14/16:** M Michalvici to collect together the arguments for, from the 3GPP2 perspective, the TR-45 Home Control features, for discussion at joint SA WG3#15/TR-45 AHAG meeting.
- ACTION #14/17:** B Vinck to produce a CR to 33.103 to make it consistent with HFN values in TS 33.102, for presentation at SA WG3 Meeting #15.
- ACTION #14/18:** M Pope: If S3-000381 was not sent: to send modified version in TD478.