Technical Specification Group Services and System Aspects **TSGS#12(01)0348**
Meeting #12, Stockholm, Sweden, 18-21 June 2001

Source: **SA WG3.**

Title: **Reports of SA WG3 ad-hoc and joint meetings since SA#11**

Document for: **Information**

Agenda Item: **7.3.2**

Meetings of SA WG3 since TSG SA#11:

- SA WG3 meeting #17bis, Madrid, 23-27 April 2001
  - NDS ad hoc (2 days)
  - IMS security ad hoc (1 day)
  - SA3/SA2 IMS security joint meeting (1 day)
  - SA3/GERAN joint meeting (1 day)
- T3 ad hoc meeting #37 (joint with SA3), Munich, 3 May 2001
- SA WG3 meeting #18, Phoenix, 21-24 May 2001
  (Including joint meeting with TIA TR-45 AHAG)

The reports of these meetings are attached to this contribution for information, except for the T3 ad hoc report which is not available at this time.

3GPP TSG SA WG3 NDS ad hoc **version 0.0.4**
Madrid, Spain
23-24 April 2001

Source: **Secretary (Maurice Pope, MCC)**

Title: **Draft report version 0.0.4**

Document for: **INFORMATION (an updated version will be provided for comment)**

---

1 Opening of the meeting

The Chairman, Mr. Geir Koien opened the meeting and welcomed delegates. Mr. D. Castellanos, representing the host, Ericsson, welcomed delegates to Madrid and provided domestic arrangements and wished everyone a successful meeting.

2 Approval of the agenda and objectives of the meeting

The agenda, provided in TD S3z010001 was agreed. The objectives, proposed by the SA WG3 Chairman, were discussed - the proposed primary objectives of the meeting were agreed with the addition of agreements of Local Key Distribution, based on contributions that had been provided for the ad-hoc meeting. It was noted that the recommendations made at the meeting were for e-mail approval by SA WG3 before the CN WG4 meeting on 14 May 2001, e-mail approval deadline was suggested as 4 May 2001, and was later agreed as 8 May 2001).

3 Allocation of documents to agenda items

The available documents, relevant to the NDS ad-hoc meeting, were assigned to appropriate agenda items.

4 Liaisons from other groups

It was noted that TD S3z010011 did not contain a CR from CN WG4, and this was provided in TD S3z010030.

5 Summary of events since S3#17

Peter Howard, Vodafone, provided a short summary of the events that had occurred in the SA WG3 reporting to SA Plenary meeting #11: The SA WG3 Chairman asked TSG SA to grant SA WG3 an extended deadline for submission for approval of the MAP Security requirements, as the NDS ad-hoc had been set up in order to finalise this document (TS 33.200): It was agreed that SA WG3 should submit a draft for information after their May 2001 meeting #18 by e-mail, and a version for approval at SA#12 in June 2001. This process would mean that TSG CN would not need to remove the already completed material from their Release 4 specifications (an e-mail had been sent to the SA WG3 list informing them of this).

6 Status of draft network domain security specification, TS 33.200 (Rel-4)

TD S3z010004 New version of TS 33.200. This TD was introduced by the editor, and contained an introduction to the NDS document, information of the updates made to the specification and a new version with and without revision marks.

Introduction part: This proposed a split of the document into MAP security part and an IP Security part, as the MAP Security part was expected to be completed and no further modification was expected, whereas the

IP Security parts were expected to be updated as the IP requirements develop. This received general support as it would help the MAP Security work to be completed and frozen without the need to further modify the document for IP Security requirements. It was noted that some contributions for update of the draft TS were to be discussed during the meeting before final a version could be agreed. **It was agreed to recommend this to SA WG3**.

It was noted that Ericsson had provided a contribution for inclusion of automated Key Management along with the MAP Security. Whether this can be included in Rel-4 was for further discussion.

Update information: The editor asked whether the KAC <--> MAP-NE interface should be IP-based. Delegates were asked to consider this.

Version 0.3.2 to 0.3.5 Changes: It was reported that the Iu/Iur interface section had been removed due to lack of contribution, as it is not a MAP interface. The other changes were mainly the removal of IP parts and the addition of placeholders for Rel-5 material.

Version 0.3.5 to 0.4.0: It was noted that TD S3z010024 provides editorial comments to version 0.4.0.

Review of version 0.4.0 (with revision marks): Ericsson stated that they had expected automatic key management to be included in the approved Release for MAP Security. There was some discussion and it was suggested that the WIs should be consulted on this point. It was not considered feasible for the first phase of MAP Security which could be included in time for Rel-4 (extended to June 2001). The update information document provided some discussion on this and it was agreed that the intention for the additional MAP Security material in Rel-5 should be made apparent in the Rel-4 document, it was proposed that this should be done by including the expected Rel-5 MAP Security items in an informative annex, rather than in notes as done in version 0.4.0. This proposal was generally agreed.

It was also noted that the MAP Security SA needs to be defined in the document.

The editor was asked about the progress on completion on the associated TR 33.800. It was reported that the document was in an immature condition and that it was unlikely to be worth publishing the material by June 2001. He suggested that the TR should be removed from the SA WG3 work programme, as it would not provide any useful, accurate information over the specification itself. **It was agreed to recommend the deletion of this document to SA WG3.**

Guidance on Security Parameters to CN WG4 would be needed when representatives arrived for a joint session. It was decided that these should be provided as part of LSs considered in the meeting. It was agreed that the ad-hoc should provide guidance on the content, but that the coding aspects should be left to CN WG4 for inclusion in their specifications.

7 MAP security technical issues

7.1 Security Level (i.e. component, operation or Application Context (AC))

The "discussion" parts of TD S3z010011 and TD S3z010013 were taken together:

TD S3z010011 Protection Profiles for MAP Security. This was introduced by Ericsson and proposed an agreement on the choice between 3 Protection Profiles (PPs):

- MAP Application Context level;
- MAP Operation level;
- MAP Operation Component level.

The contribution discussed the pros and cons of each level of PP and proposed that the Operation level for MAP PP structure as the best compromise between granularity of protection and complexity, while fulfilling the security requirements. Operators were asked to express their wishes on this proposal.

TD S3z010013 Protection Profiles for MAP Security. This was introduced by Siemens as an alternative proposal to the Ericsson document (TD S3z010011). Siemens proposed to have 4 Component level PPs,

where the operator would negotiate the PPs supported from the defined profiles, and suggested that it provides the best granularity and can reduce loading on the network.

Discussion of Ericsson and Siemens contributions:

Vodafone commented that handover was not included in the Siemens PP1, but that it was protected in the Ericsson contribution. It was reported that this had not been an issue in the risk analysis, but it was agreed that this should be considered for protection, and could be added to the Siemens proposal as an additional PP to be included in negotiations. It was clarified that in the Siemens scheme, the operators would negotiate a ***list*** of PPs to be used, rather than negotiating a single PP, which had been the assumption for the development of the Ericsson contribution. Ericsson requested some time to consider the implications of this mechanism.

It was generally agreed that the most sensitive messages need to be protected in Rel-4. It was also suggested that a PP to protect all protectable parameters should be included in a Rel-4 scheme, to be used in case of problems (however, it was also recognised that this would probably cause severe loading/efficiency problems).

It was agreed that in order to make progress on this matter, the DoI discussions should also be taken into account (see agenda item 7.3) and the matter discussed in an evening session.

During the evening discussions, it was concluded that the reolution of the matter depended on whether the PPs are defined on the Operation or Component level, and CN WG4 should be asked to decide on this matter, as the arguments were not security related ones. A LS to CN WG4 was drafted by P. Howard, in TD S3z010033. **<RETURN>**

Fallback indicators: The “fallback to unprotected mode indicator” is mainly to allow stepwise deployment of MAPSec (some nodes are upgraded while others aren't), so either a node will be able to apply a MAP-PP or not at all. There were some minor differences in the detail of the management and scenarios for the fallback indicator between the Ericsson and Siemens contributions, and it was agreed to discuss this in an off-line evening session in order to reach some consensus on the basic set of operations that need to be protected (including the need to protect handover authentication). **<RETURN>**

TD S3z010011 (CN WG4 LS part): Structure of the Security Header. CN WG4 asked whether a single Initialisation Vector (IV) would be sufficient to be used, e.g. in protection mode 2, if both the Encryption Algorithm and the Integrity/Authenticity Algorithm require an IV. Potential problems were raised with this when encrypting the MAC and using the same IV for integrity protection, as these should be independently generated for best security protection. This was discussed in the evening off-line group and TD S3z010031 produced, which shows the agreements for the MAPSec mode. This showed a scenario where the same IV is used for both the MAC and the integrity protection, as a practical solution, although it was noted that there was a theoretical risk in doing this. Using stream cipher for the encryption would reduce the need for padding, as may occur if block ciphering were used (the AES has a 16-byte lock size, which means that up to 16 bytes of padding may be necessary in some cases). The diagram showed the IV as being made up from a 24 or 16 bit Node ID, a 32 bit TVP and an 8 bit Clock extension. For replay protection, the Global clock synchronisation would need to be specified as small (e.g. 1 second), in order to prevent two identical IVs being generated (there is a requirement for unique IVs). It was noted that the CN specification currently reserve 18 bytes for an IV, which could be reduced, allowing compensation for padding bits.

It was agreed that a response would be created by Ericsson and included in the LS to CN WG4 (TD S3z010033, produced by P. Howard).

SA WG3 were also asked to determine the refine their algorithm selection by determining:

- the block length which is to be mandatorily supported,
- the key length which is to be mandatorily supported,
- the mode of operation for AES which is to be mandatorily supported,
- the mode of operation for AES-MAC which is to be mandatorily supported,
- the length of the Integrity Check Value which is to be mandatorily supported

in a way which minimises the overhead as far as possible while ensuring an acceptable level of security.

It was decided to discuss this in an evening session in order to provide some answers to CN WG4 in the joint session. **<RETURN>**

TD S3z010008 Comments on MAP DoI. This was presented by Siemens and suggested a number of changes:

A) Deletion of some MAPsec DoI text from the MAP DoI draft which reproduce information in the IETF IPSec DoI document and using references instead, but leaving the items which need to be maintained by 3GPP in the document (e.g Key derivation procedures).
B) KACs between two NEs is not an SA WG3 working assumption, and this should be clarified in the document. It was discussed whether KAC needs to be in the MAPsec DoI document, and it was agreed that the text should be removed, replacing it with a small introduction about the purpose of the mechanism.
C) The IETF draft MAPsec DoI RFC parts should be included in 3GPP specifications for maintenance and easier referencing reasons. The editor was asked to list the items to be added to the 3GPP MAP DoI document and those which should reference the IETF RFC document.
D) KINK should not be used, due to its immaturity compared to IKE. The editor agreed to remove this option.
E) PPs were discussed. The proposal for a 16 bit fixed-length field, to provide for adequate number of PPs to be selected was noted.
F) This suggested that there is no need for asynchronous negotiation of the SA-pairs. IKE cannot handle asynchronous negotiation and would need modification. It was agreed that this should be removed.
G) The SA duration had been agreed in SA WG3 as an absolute time value. The editor reported that this was an error in the document and that absolute time would be inserted.
H) This proposed allowing additional provision for AES-CBC (192 or 256 bit key lengths) for future use. It was noted that only 128 bit is mandatory for Rel-5. This was agreed.
I) The MAP SA payload requires specification. This was not considered appropriate for DoI, but the inclusion of SA specification and transport of the SA to the NE in SA WG3 specifications should be considered. Contributions were requested on this for SA WG3 meeting #18.

The editor agreed to provide an update of the MAPSec DoI document to SA WG3 meeting #18, taking the agreements at this ad-hoc into account. Contributions are requested on SA specification and transport. The editor thanked Siemens for their comprehensive review of the document and requested other companies to review the document and provide contributions.

7.2 ASN.1 descriptions within TS 33.200 or in TS 29.002

There were no contributions on this agenda item. It was agreed that the ASN.1 descriptions should be included in 29.002, and SA WG3 would specify the semantics for this in 33.200. This information was included in the LS to CN WG4.

7.3 MAPsec DOI

TD S3z010010: MAP DOI Status (Powerpoint presentation part). This was presented by Ericsson. There were some questions for clarification. It was recognised that the group would need to decide what will be left in the IETF Information document on MAP-DoI RFC and what should be put into 3GPP specifications for maintenance considerations.

TD S3z010012 IPsec and IKE profile for network domain security. The presentation was given by Ericsson. IKE profiling was suggested to limit cost, complexity and to improve interoperability. It was suggested that this did not limit vendors in providing additional functionality, nor 3GPP in requiring further functionality in the future.

The mandatory use of IPv6 was questioned, as this had not been a decision of SA WG3. It was decided that an LS should be written to relevant groups on this.

MAP DoI IKE profiling:

- Only phase 1 of IKE is used: The rest is MAP DoI. This was agreed.
- Only IPv6 is mandatory: This needs to be checked via an LS to SA WG2 and other relevant groups. There was no preference from the Security point of view, but there were interoperability concerns (IPv6 versus IPv4).

- Perfect Forward Secrecy (PFS) optional: This was acceptable for speed in Phase 2.
- Aggressive and Main Mode use: It was agreed that only Main Mode would be mandated (it was noted that Main Mode provides better protection against DoS attacks than Aggressive Mode, although Agressive Mode would provide better performance).
- FQDN, Only Fully Qualified Domain Names to be mandated for identities: This was agreed.
- Use of AES and SHA-1: It was agreed that AES should be used for encryption and SHA-1 for the MAC. It was reported that AES is useable and has an RFC number allocated already, so it could become an RFC if requested to the IETF. AES / SHA-1 for the MAC was agreed, with a note to say that AES-CBC-MAC is expected to be the preferred MAC solution for the future. **The Working Assumption that AES can be used both for encryption and MAC in IKE was agreed**. The problem with AES-CBC-MAC is the assignment of IETF number and the NIST publication of the AES modes (including AES-CBC-MAC), and the DoI editor was asked to try to expediate this and to send the draft to SA WG3, before meeting #18, for information.
- SA lifetime notification not allowed: **This was taken as a working assumption**. Input is expected at SA WG3 #18 meeting if any problems are discovered with this.
- SA deletion between KACs not allowed: This would allow the Pull mode to be easily implemented, but will make it difficult to inform other nodes of any compromise of keys. This proposal should be studied further, as the deletion function may be required in emergency/exceptional cases, limiting to use of Pull mode may cause problems in the future. It was suggested that removing deletion would necessitate a reduction on SA lifetimes to days or hours. It was also suggested that revoking SAs should be possible, perhaps using manual management action. **After some off-line discussion it was agreed that a working assumption was that SA deletion between KACs should be possible.** Delegates were asked to check the implications and report any problems by contribution to SA WG3 meeting #18.

7.4 Other general issues regarding the protection mechanism

TD S3z010006 "CR" to 33.200: Cleanup of MAPsec structure of protected operations. These proposed changes were presented in CR style on the request of the editor. The changes were reviewed and the editor asked to take them into account for the revised version of 33.200, MAPSec document and the IPSec document to be extracted from it.

7.5 Security association establishment

TD S3z010005 MAP-SA Negotiation and Distribution Procedures. This was introduced by Ericsson which set a solid and consistent basis for the specification of MAP-SA negotiation and distribution mechanisms.

From contribution summary:

S3 members are asked to consider this proposal in order to be able to reach the following agreements:

1. *Agreement on the general overview of the MAP-SA negotiation and distribution mechanisms (chapters 3.1 and 3.2).*
2. *Agreement on the principles of the "RequestSA" procedure (chapter 3.3).*
3. *Agreement on requesting CN4 to select and further develop/refine the actual protocol to be used at Ze interface (chapter 3.4) according to the requirements provided in this proposal. If this is agreed, a LS informing CN4 of such request shall be submitted as soon as possible.*
4. *Agreement on the basic functionality at the KAC and MAP-NEs in relation to MAP Security and Key Management (chapter 4.1. and 4.2).*

If these agreements can be reached, the information in this proposal could be included in TS 33.200.

Discussion:

The use of "towards" and "from" were clarified as relating to SA information, which is asymmetric. Security Policy databases are synchronised via roaming aggreements, rather than dynamically. If a NE tries to send a secure message and an indication "not allowed" is returned, the Policy database is checked to verify if fallback is allowed, before changing the SA.

A failure scenario was not included and some text on this was considered to be advantageous. Error scenarios need development and fallback scenarios were also considered as needed. There was a request for a test procedure, to be applied before implementing an upgrade to roaming agreement security policies, in order to prevent failure on live traffic when the new SA is applied.

This contribution was generally considered as a very useful start, and it was recognised that more detail was required.

Ericsson requested that this procedure should be included in the same Release as MAPSec (which was targetted for Rel-4 at this ad-hoc meeting), but this could only be done if both Stage 2 and Stage 3 specifications are completed in time for the extended finalisation date of June 2001 and it was thought unlikely that the Stage 3 would be completed by CN in time. Ericsson questioned whether the Rel-4 MAPSec would be used in practice without the inclusion of automatic Key management procedures.

The principles of the contribution were agreed, and it was noted that local Key distribution needs also to be managed in a secure way.

TD S3z010027 Proposed changes to 33.200 about KAC. This was presented by Nokia and proposed text to 33.200 to clarify that there may be several KACs in order to provide redundancy in case of failure, with one logical KAC visible at the interface. It was noted that this would require database synchronisation.

It was generally agreed that redundancy was expected to be provided in systems, but that this was an implementation issue, rather than a standardisation issue. After some off-line discussion, some complications were identified on the receiving network node side (addressing may be an issue for calling nodes) and the proposal should be further considered at the SA WG3 meeting #18 and contributions were invited.

8 Other network domain security technical issues

8.1 GTP security

This was deferred to SA WG3 meeting #18 due to lack of time at the ad-hoc meeting.

9 N4 issues

9.1 Questions from S3

The LS in TD S3z0100xx covered the questions that SA Wg3 ad-hoc addressed to CN WG4.

Local SA distribution is a much needed part of the architecture, but SA WG3 cannot provide full details at present and lack recovery procedures, so it was considered premature to ask CN WG4 to develop the protocol yet. It was thought that even if SA WG3 can agree on the outstanding issues, there may not be enough time for CN WG4 to complete their work and the Rel-5 details missing from the Rel-4 would be outlined in an informative annex. It was agreed that it would not be possible to have automatic local Key management procedures in time for Rel-4, manual local Key management would need to be implemented.

Question to CN WG4: Should MAPSec Transport be included in Rel-4 (the primary objective of this ad-hoc) without automatic Local Key management ?

BT stated that guidance on manual Key management would be required in any case if MAPSec Transport is included.

Vodafone stated that the specification of SA is needed in order to have manual Key management in Rel-4.

It was noted that the primary objective of the ad-hoc was only to attempt to complete the MAPsec transport security (Zf-interface). A Rel-4 version of TS 33.200 could therefore be completed even without the Local SA distribution (Ze-interface). It was noted that it was essential that CN4 receive answers to their LS (see TD S3z010011) in time for their meeting 14-17 May in order to achieve this. In the end it was therefore decided that S3 should for now only respond to the questions that CN4 asked in their LS (see TD S3z010011). Questions related to Local SA distribution would have to wait for Rel-5. It was further acknowledged that there was still a number of open issues for S3 to decide in order to complete the MAPsec transport security specification and that these issues would have to be addressed by S3#18 is a Rel-4 version of TS 33.200 was to be achieved.

9.2 Clarification on output documents required for N4 plenary, 14-17 May

An evening session was held to provide the results of the discussions to CN WG4 and produced a draft which was discussed and edited on-line in the meeting. The draft was modified and agreed in TD S3z010033 (see agenda item 10.1).

It was recognised that contribution for SA WG3 meeting #18 was needed in order to update 33.200 on these issues.

10 Review of output documents

10.1 For N4 plenary, 14-17 May

TD S3z010033 LS to CN WG4 on MAP security. This was produced after discussion of the results of the evening session group to provide information to CN WG4. The contribution provided the agreements and open issues on the following topics:

- MAP protection profiles
- Structure of security header
- Algorithm mode selection for MAP security

Additionally it informs CN WG4 that the coding of MAP security elements should be contained as ASN.1 in TS 29.002 based on stage 2 specifications to be included in TS 33.200.

This LS was agreed for forwarding to CN WG4.

10.2 For S3 plenary, 21-24 May

The following list was developed on-line for reporting to SA WG3 on progress and outstanding issues:

- **Format and length of IV needs to be determined**

  An input paper from Rolf Blom and Valterri Niemi suggested that one IV of 8 octets could be sufficient if it was cleverly composed. They suggested to let the IV be composed of TVP (4 octets), a unique node identifier (3 octets) and a local clock (1 octet). The definition of the local clock needs to specified.

- **Format and construction of TVP (4 octets assumed) must be resolved**

  The exact format of the TVP, including bit ordering etc, would need to be defined. This would include defining the clock resolution (1 second suggested) and to defined a clock reference point. (it had previously been been decided to use absolute time in the TVP)
  It would also be necessary to define a clock window size.
  The meeting also decided to recommend to move the TVP from the payload to the MAPsec header. Updates to the TS to reflect this would have to be produced.

- **The Node-Id identifier must be precisely defined**

  It was suggested to let the Node-Identifier be 3 octets long and that it would be constructed by means of a hash over the E.164 Global Title for the MAP-NE. All details of the Node-Id, including the definition of the hash function, would need to be specified.

- **Specification of cryptographic algorithms to be used**

  All details regarding the choice of cryptographic algorithms (both confidentiality and integrity) needs to be defined. In addition to the specifying the algorithm identifiers (4 bits for each algorithms was suggested to be sufficient), the standard algorithms would have to be precisely specified. This would include specification of the mode to be used as well as a specification for the algorithm interface. Decisions about whether to use stream- or blockciphering would have to be made and it was noted that a streamcipher would not require padding. This may be an issue since it was questioned whether CN4 could afford padding. Valterri Niemi mentioned that according CN4 calculations it was not clear that the MAP SendAuthenticationInfo containing a

single AV could be sent without segmentation with the current security overhead requirements. This would provide a strong incentive to reduce the need for padding.

- **The integrity check value (ICV) would need to be defined.**

  In particular the length of the ICV need to be defined. It was assumed to 64 bits would be sufficient, but that 32 bits might be accepted should it be the case that this would avoid segmentation.

- **MAPsec SA defintion**

  All aspects of the SA would need to be defined This would include defining the SA liftetime, the integrity key, the confidentiality key, the algorithm identifiers, the security domain identity (=PLMN identity), SPI.

- **Protection Profiles**

  The protection profiles encoding must be specified. It was agreed that 16 bits should be used for this information element.

- **MAPsec local SA distribution procedures needs to be refined/completed**

  Although Ericsson had produced a good starting point, the need for recovery procedures as well as the need for revocation mechanisms needs to be studied further.

11 Evaluation of progress

Independent of whether SA WG3 would be able to produce a Rel-4 of 33.200 it was agreed to recommend to S3#18 that TS 33.200 should be split into two TSs (one containing MAP/SS7 material and one containing GTP/IP material). The rapporteur agreed to produce a new version of TS 33.200 with only MAPsec/SS7 material and to provide an initial draft for a new TS to cover GTP/IP security based on the GTP/IP material as found in TS 33.200 v035.

The ad-hoc had reached agreement to attempt to include MAPSec transport protocol in Rel-4.

- Peter Howard will complete the reply LS to CN WG4 based on the agreements at the ad-hoc and lead an e-mail agreement procedure for the reply LS. The e-mail agreement process will be concluded 8 May 2001 1600 CET.
- TS 33.200: Those items which cannot go into Rel-4 will go into an informative Annex of the Rel-4 document (if there is one).
- Guidelines for manual SA handling need to be included in the Rel-4 specification at SA WG3 meeting #18.
- It was concluded that a number of open items have been identified and a clearer view obtained of what is left to be done for completion of MAPSec. (see list in 10.2). Contributions on these issues are required for S3#18.

It was agreed that the SA WG3 Chairman should be consulted about these conclusions, as the situation would need to be explained by the SA WG3 Chairman at SA Plenary.

12 Closing of the meeting

The Convenor thanked the delegates for their contributions and hard work and co-operation at the meeting and the Host for the meeting facilities, and closed the meeting.

Meeting objectives:

- The primary objective is to make technical progress on MAP security with the aim of ensuring that the necessary specifications for Rel-4 can be agreed at the N4 plenary meeting, 14-17 May, and at the S3 plenary, 21-24 May. Particular issues to resolve include the granularity of protection required (component, operation or application context) and where to specify the coding of the security parameters (directly in TS 29.002 in ASN.1 or in TS 33.200).

- A secondary objective is to make technical progress on other aspects of network domain security, especially GTP security.

- A further objective is to make technical progress on automatic security association (SA) establishment for MAP security.

A session *at the end* of the meeting (agenda item 11) shall evaluate progress and agree a recommendation to S3 plenary (cc N4) which will state which network domain security features should be presented to the June TSG plenary meetings for inclusion in Rel-4. The recommendation of the S3 ad hoc meeting shall be considered for email approval by S3 plenary prior to the N4 meeting on 14th May. The deadline for email approval shall be Friday 4th May.

Annex A: List of attendees at the SA WG3 NDS ad-hoc meeting

Name			Company	e-mail	3GPP Member	
Mr.	Shinichiro	Aikawa	Fujitsu Limited	aikawa@ss.ts.fujitsu.co.jp	TTC	x
Mr.	Jari	Arkko	Telefon AB LM Ericsson	jarkko@piuha.net	ETSI	x
Mr.	Stephen	Billington	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Colin	Blanchard	BT	colin.blanchard@bt.com	ETSI	x
Mr.	Rolf	Blom	Telefon AB LM Ericsson	rolf.blom@era.ericsson.se	ETSI	x
Mr.	Marc	Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	x
Ing.	Krister	Boman	Telefon AB LM Ericsson	krister.boman@emw.ericsson.se	ETSI	x
Mr.	Daniel	Brown	Motorola Inc.	adb002@email.mot.com	T1	x
Mr.	David	Castellanos	Telefon AB LM Ericsson	david.castellanos@ece.ericsson.se	ETSI	x
Ms.	Lily	Chen	Motorola Inc.	Lily.chen@motorola.com	T1	x
Dr.	Adrian	Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Louis	Finkelstein	Motorola Inc.	louisf@labs.mot.com	T1	x
Mr.	Peter	Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	x
Mr.	Jari	Jansson	Nokia	jari.jansson@nokia.com	ETSI	x
Mr.	Geir	Koien	Telenor AS	geir-myrdahl.koien@telenor.com	ETSI	x
Mrs.	Tiina	Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI	x
Mr.	Dirk	Kroeselberg	SIEMENS AG	dirk.kroeselberg@mchp.siemens.de	ETSI	x
Mr.	Vineet	Kumar	Intel Sweden AB	vineet.kumar@intel.com	ETSI	x
Mr.	Carlos	Lazaro	TELEFONICA DE ESPAÑA SA	lazaro_c@tsm.es	ETSI	x
Mrs.	Geneviève	Mange	ALCATEL S.A.	g.mange@alcatel.de	ETSI	x
Mr.	Michael	Marcovici	Lucent	marcovici@lucent.com	T1	x
Mr.	Tomi	Mikkonen	SSH Communications Security Corp	tomi.mikkonen@ssh.com	ETSI	x
Mr.	Valtteri	Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	x
Mrs.	Susana	Ochoa	AIRTEL Movil SA	sochoag@airtel.es	ETSI	x
Mr.	Bradley	Owen	Lucent Technologies Network Systems UK	bvowen@lucent.com	ETSI	x
Mr.	Olivier	Paridaens	ALCATEL S.A.	olivier.paridaens@alcatel.be	ETSI	x
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	x
Mr.	Hugh	Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	x
Mr.	Toshiyuka	Tamura	NEC	tamurato@aj.jp.nec.com	ARIB	x
Mr.	Lee	Valerius	NORTEL NETWORKS (EUROPE)		ETSI	x
Dr.	Peter	Windirsch	T-Nova Deutsche Telekom	Peter.Windirsch@t-systems.de	ETSI	x

3GPP TSG SA WG3 aSIP ad hoc **version 0.0.1**
Madrid, Spain
25th April 2001

Source: **SA WG3 Secretary (Maurice Pope, MCC)**

Title: **Draft Report of aSIP ad-hoc meeting version 0.0.1**

Document for: **Information**

---

1 Opening of the meeting

The Chairman, Mr. Krister Boman, opened the meeting and welcomed delegates. Mr. D. Castellanos, representing the host, Ericsson, welcomed delegates to Madrid and provided domestic arrangements and wished everyone a successful meeting.

2 Approval of the agenda and objectives of the meeting

TD S3z010020 contained the agenda and objectives for the meeting, the objectives were also provided in presentation slides in TD S3z010039. The objective of location of confidentiality protection was clarified on to determine whether extra protection is needed and Public versus Private identities (agenda item 7) was also considered an important objective for this meeting. Agenda Items 6.2. and 6.3 were still open and additional input to these items was needed to progress this. It was stated that for agenda item 6.1, we need to agree on the termination point of authentication (HSS or S-CSCF). With these comments, the agenda was then approved.

3 Allocation of documents to agenda items

The available documents were allocated to their respective agenda items.

4 Liaisons from other groups

There were no inputs under this agenda item.

5 Status of draft access Security for IP-based services (aSIP) specification (Rel-5)

TD S3z010041: Draft 33.203 v 0.2.1 status. The editor introduced the draft, which showed the changes made from the Draft 0.2.0 which had been distributed by e-mail mid-March. The draft was reviewed and noted as a basis for further update.

6 aSIP technical issues

6.1 Termination of authentication/signalling flows

TD S3z010023: Use of AAA from SIP servers in the IP Multimedia CN Subsystem. This was presented by Lucent and proposed that the DIAMETER AAA architecture described in the contribution be incorporated into 33.8xx and the requirements forwarded to SA WG2 for update of 23.228 and/or 23.002 as necessary. Ericsson reported that the DIAMETER AAA is currently in the architecture, but that the Broker AAA was out of the scope at present. Vodafone commented that the validity of the trust relationship models for use of a Broker AAA is missing from the contribution and this would make it difficult to evaluate. Lucent clarified that the configuration was proposed as optional. It was considered that the requirement for inclusion of such options needed to be determined. SA WG3 were asked whether they saw any security implications to the use of this scheme. The decision had been made at SA WG3 meeting #17 that Authentication would be performed in the Home Network, and this proposal allows the Visited Network to perform the authentication.

It was also noted that the contribution assumed UE authentication in the S-CSCF, which was a subject for discussion at this ad-hoc meeting and had not yet been agreed by SA WG3, and there was also a proposal for UE authentication in the HSS.

The proposal was therefore noted. It was agreed that the use of DIAMETER for the Cxs interface was acceptable from the security point of view, but that this was not an issue for SA WG3 decision.

It was noted that the note beneath figure 3 did not align with the flows provided in the figure, Lucent clarified that the figure was the correct intention.

Session establishment and Authentication of INVITE:

Authentication of session establishment: Reauthentication should be possible by a trigger mechanism, controlled by the operator, so that it is not just done on session establishment, as this could be a risk.

TD S3z010003: Alternatives for terminating authentication in the home domain of the IM Subsystem. This was presented by Siemens and propovided an analysis of the advantages and disadvantages of termination of authentication in the HSS and S-CSCF.

Siemens reported that in order to solve the S-CSCF addressing issue, an IETF header extension mechanism for distributed state information could be employed, which would eliminate the need for storage of state information in the I-CSCF, which would be undesirable. BT reported that the internet draft which included this mechanism did not provide for protection of the information. Siemens considered that the impact of this would depend upon whether this information was already integrity protected, and on whether it would therefore be necessary. It was suggested that SA WG2 should be consulted on the viability of this mechanism. Another mechanism was later suggested by AT&T, to retrieve this information from the HSS database, instead of using the header extension scheme, which was considered as a more acceptable proposal by Siemens. Siemens asked that this solution be taken into account when comparing the two proposals. Siemens later agreed to update their proposal to include this. **<TD not yet provided?>**

TD S3z010040 An analysis on where to perform the authentication of an IMS subscriber (presentation slides). This was presented by Ericsson and was based on the proposals provided in detail in TD S3z010025. It proposed the termination of authentication in the HSS and provided pros and cons to the two proposals (S-CSCF and HSS termination).

TD S3z010029 Open issues in IMS security. This was provided by Nokia and discussed the open issues on the solutions provided by Ericsson and Siemens:

The location of the authentication comparison:

It was noted that the additional Pros cited for S-CSCF authentication, were in error, and were Pros for HSS authentication.

Nokia analysis (from contribution)

> *At first sight it may seem that the first pro and the con balance each other. However, as the INVITEs are integrity protected between UE and P-CSCF there is no big need to authenticate the INVITEs by the home network. The refreshing of keys can as well be done during re-registrations. On the other hand, registrations must be authenticated because integrity protection is not available yet.*
>
> *As a conclusion, the additional points listed here seem to turn the balance into the direction of performing authentication comparison in the HSS.*

AT&T reported that the idea of placing extra processing functions into the HSS was against the SA WG2 intention which was to have a "dumb" database, which only serves data to received requests and therefore the S-CSCF solution was their preference. Clarification was requested on where this is stated in 23.228, and AT&T responded that the specification had been carefully drafted in order to reduce the processing in the HSS to a minimum.

Ericsson stated that the difference in the impact on the HSS of the two approaches was only in the comparison of the RES and XRES, as the security parameters were retrieved or calculated by the HSS in any case. Siemens argued that in the HSS solution a significant number of extra parameters needed to be

stored, which would increase the data storage requirements of the HSS significantly, given the large number of users it had to cater for compared to the S-CSCF, and that it opened up a risk to DoS attacks. Ericsson pointed out that ~~that~~ the S-CSCF solution also required the storing of most of the same parameters in the HSS.

Nokia pointed out that the AuC functionality was usually an integral part of the implementation of the HSS, and that this should not be taken as a seperate functional entity for the purposes of the comparison of the two approaches.

Denial of service discussion:

It was pointed out that the UE is already authenticated so that there should no be any risk of DoS attacks from authenticated UEs. However, it was agreed that this could not be the situation in all cases when considering the requirement for Access Independence, and non-UMTS accesses need to be supported and could not always be trusted.

After some discussion the following working assumption was agreed:

> Session establishment
> It is the working assumption of the aSIP ad hoc group that the hop-by-hop integrity protection of session establishment (INVITEs) and the option to authenticate the user during re-registrations and the ability of the Network to force re-registration, provide adequate protection for session establishment. The re-registration timer can be reset to a new value when forcing a re-registration.

Re-authentication:

It was agreed that a mechanism to force re-authentication is required, but that this need not necessarily be triggered by INVITE. It was reported that SIP does not provide a mechanism for network-triggered re-authentication, but some form of event-triggered re-registration would be desirable for operators, so that they only generate signalling traffic for this when, e.g., a chargeable event occurs (i.e., not while the UE is idle). Operators would also require flexibility in their triggering policies. It was agreed that SA WG3 should send a LS to SA WG1 to receive verification whether step-by-step integrity protection of INVITEs would cover operator requirements and that no further authentication would be needed.

It was generally agreed as a working assumption that hop-by-hop integrity protection would be enough.

Any justified arguments against this assumption should be forwarded to SA WG3 meeting #18.

6.2 Protection mechanisms

TD S3z010036 - part 1: Open issues for aSIP - Authentication Protocol details. This was presented by Ericsson and discussed the factors affecting the choices and the preliminary working assumptions for the issues of protocol details for authentication, protection mechanisms for future messages (third party requirements) and Security mode set-up. Proposals on definition on how to use SASL in SIP and how to use AKA in SASL, as it will not always be possible to assume direct AKA support. If this support is considered useful, then further detail will need to be provided. Proposals were therefore requested for contribution to SA WG3 meeting #18.

It was reported that SASL is stable and that the use of SASL for HTTP was under development. The competing proposals to HTTP were questioned for clarification, but this was not available at the time, but should be available from the IETF documentation.

Message size was reported as a strong concern of CN WG1, and some of the messages could be large for third party authentication schemes. It was clarified that this had been provided as an example of why the authentication scheme needed to be made future-proof and served as an example of how the authentication procedures may need to develop in the future, which would require update of the affected network nodes.

This part of the presentation was noted.

TD S3z010029 - Part 2: Open issues in IMS security - Protection of SIP signaling between UE and P-CSCF. Nokia presented this part of their contribution, which analysed the use of IPSec on the IP layer in order to protect upper layer communications:

Pros: The mechanism is already specified; Security associations may be derived from AKA generated Keys.

Cons: The protection is tied to the IP address and not directly to SIP identity - Distinction of users needs to be done (i.e. seperate SPIs); The receiving end needs to check that the used SA in IPSec corresponds to the correct SIP identity.

Nokia proposed the use of S/MIME for integrity protection and assumed the radio interface confidentiality protection is acceptable.

It was noted that the use of Temporary PUIs should be discussed, as it was not available in current standards.

It was proposed that confidentiality of SIP signalling is optional.

The following working assumption was agreed:

> Confidentiality Protection of SIP signalling
> It is the working assumption of the aSIP ad hoc group that the confidentiality of SIP signalling between the UE and P-CSCF is optional for implementation. Confidentiality of SIP signalling can rely on existing mechanisms, or mechanisms which will be provided by NDS.

Nokia were thanked for their contribution to the ad-hoc meeting, which helped focus the discussions on these difficult issues.

TD S3z010036 - Part 2: Open issues for aSIP - Protection Mechanisms for future messages. This was presented by Ericsson and proposed that 3GPP should not develop a new scheme, but should choose from subsets of available schemes: IPSec, S/MIME or CMS, PGP, etc. An analysis of some choices had been done by Ericsson and concluded that S/MIME seemed to be a good choice, due to re-useability, but that Profiling would need some work. The use of the same scheme for both hop-by-hop and end-to-end SAs needs to be considered.

It was proposed that more detailed contributions could be input to SA WG3 meeting #18 for discussion and determination of time scales for such work. Profiling is needed to remove unwanted parts (PKI, certificates, etc.). It was clarified that existing IETF mechanisms, integrated into SIP would be used for the application level, which would require co-operation with the IETF work and time scales.

It was agreed to re-assess the issues at SA WG3 meeting #18. Delegates were urged to consider this and contribute to the meeting.

This part of the contribution was then noted.

6.3 Security mode setup

TD S3z010036 - Part 3: Open issues for aSIP - Security Mode set-up. This was presented by Ericsson and proposed a principle to avoid delay by using a fixed-position security mode set-up scheme and by the use of piggybacking, e.g.:

- Algorithm proposals piggybacked to the first message sent to the server;
- Server responds with selected alforithm;
- Next message from the client is always protected.

It was clarified that the radio interface would already be protected when this procedure is started.

It was considered that more detailed proposals and flows were needed to make a decision on this, and an evaluation of threats that can be protected against should be done, aiming for a similar protection to that for the UTRAN.

Ericsson offered to provide an example information flow, which was provided in TD S3z0100XX **<To be provided>** . P. Howard (Vodafone) was asked to develop some initial requirements for e-mail discussion, in order to produce a contribution in good time before SA WG3 meeting #18. The evening session discussion group was asked to consider this **<RETURN>**.

7 Other technical issues

7.1 Hiding requirements

This subject was postponed for the joint meeting with SA WG2. **<RETURN>**

7.2 Public vs Private identities

This subject was postponed for the joint meeting with SA WG2. **<RETURN>**

8 S2 issues

8.1 Questions from S3

List to be provided on requirements to 23.228 **<RETURN>**

9 Review of output documents

9.1 For joint session with S2, 26th April

TD S3z010034 Security Relationships of Interogating CSCF (I-CSCF). This document was intended for the joint session with SA WG2, and was presented briefly to the meeting for initial clarification and views by Motorola. The document was noted, and delegates were asked to consider the contribution overnight for comment in the joint SA WG2 session.

TD S3z010035 SIP Headers and Messages for Security in 24.228 Flows. This document was intended for the joint session with SA WG2, and was presented briefly to the meeting for initial clarification and views by Motorola. The main questions from SA WG2 were outlined. SA WG3 were asked to contribute to SA WG2 and CN WG1 on 24.228, when stable information is available.

The stealing of voice traffic for re-authentication/Key exchange was rasied, and an idea of the expected frequency of the procedure was requested. It was clarified that SA WG3 would not specify the frequency of such procedures, but only the mechanism to use, leaving the frequency as a value settable by the operator. A figure of hours could typically be expected, rather than minutes, or days.

Requirements for Key exchange mechanisms for encryption of media streams during session initialisation were urgently needed by SA WG2 and CN WG1. It was indicated that SA WG3 have a new Work Item on Network-based end-to-end encryptio, targetted for Rel-5.

The document was noted, and delegates were asked to consider the contribution overnight for comment in the joint SA WG2 session.

The working assumptions achieved by the ad-hoc meeting were provided for the SA WG2 joint session in TD S3z0100YY **<TO PROVIDE>**.

9.2 For S3 plenary, 21-24 May

<TEXT NEEDED FOR THIS>

10 AoB

There was no other business signalled.

11 Closing of the meeting

The Convenor thanked the delegates for their contributions and hard work and co-operation at the meeting and the Host for the meeting facilities. He announced that an evening session would be held after the close of the meeting for discussion of the outstanding issues and closed the meeting.

Annex A: List of attendees at the SA WG3 aSIP ad-hoc meeting

Name			Company	e-mail	3GPP Member	
Mr.	Shinichiro	Aikawa	Fujitsu Limited	aikawa@ss.ts.fujitsu.co.jp	TTC	x
Mr.	Jari	Arkko	Telefon AB LM Ericsson	jari.arkko@ericsson.fi	ETSI	x
Mr.	Stephen	Billington	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Colin	Blanchard	BT	colin.blanchard@bt.com	ETSI	x
Mr.	Rolf	Blom	Telefon AB LM Ericsson	rolf.blom@era.ericsson.se	ETSI	x
Mr.	Marc	Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	x
Ing.	Krister	Boman	Telefon AB LM Ericsson	krister.boman@emw.ericsson.se	ETSI	x
Mr.	Daniel	Brown	Motorola Inc.	adb002@email.mot.com	T1	x
Ms.	Tao	Bu	Nokia	tao.bu@nokia.com	ETSI	x
Mr.	David	Castellanos	Telefon AB LM Ericsson	david.castellanos@ece.ericsson.se	ETSI	x
Ms.	Lily	Chen	Motorola Inc.	Lily.chen@motorola.com	T1	x
Dr.	Adrian	Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Louis	Finkelstein	Motorola Inc.	louisf@labs.mot.com	T1	x
Mr.	Guenther	Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	x
Mr.	Peter	Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	x
Mr.	Geir	Koien	Telenor AS	geir-myrdahl.koien@telenor.com	ETSI	x
Mrs.	Tiina	Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI	x
Mr.	Dirk	Kroeselberg	SIEMENS AG	dirk.kroeselberg@mchp.siemens.de	ETSI	x
Mr.	Vineet	Kumar	Intel Sweden AB	vineet.kumar@intel.com	ETSI	x
Mr.	Carlos	Lazaro	TELEFONICA DE ESPAÑA SA	lazaro_c@tsm.es	ETSI	x
Mrs.	Geneviève	Mange	ALCATEL S.A.	g.mange@alcatel.de	ETSI	x
Mr.	Bill	Marshall	AT&T Wireless Services, Inc.	wtm@research.att.com	T1	x
Mr.	Michael	Marcovici	Lucent	marcovici@lucent.com	T1	x
Mr.	Tomi	Mikkonen	SSH Communications Security Corp	tomi.mikkonen@ssh.com	ETSI	x
Mr.	Valtteri	Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	x
Mrs.	Susana	Ochoa	AIRTEL Movil SA	sochoag@airtel.es	ETSI	x
Mr.	Bradley	Owen	Lucent Technologies Network Systems UK	bvowen@lucent.com	ETSI	x
Mr.	Olivier	Paridaens	ALCATEL S.A.	olivier.paridaens@alcatel.be	ETSI	x
Mr.	Miika	Poikselka	NOKIA Corporation	miikka.poikselka@nokia.com	ETSI	x
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	x
Mr.	Hugh	Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	x
Mr.	Toshiyuka	Tamura	NEC	tamurato@aj.jp.nec.com	ARIB	x
Mr.	Lee	Valerius	NORTEL NETWORKS (EUROPE)		ETSI	x
Dr.	Peter	Windirsch	T-Nova Deutsche Telekom	Peter.Windirsch@t-systems.de	ETSI	x

SA WG3 / SA WG2 joint ad hoc **version 0.0.1**
Madrid, Spain
26 April 2001

Source: **Secretary (Maurice Pope, MCC)**

Title: **Draft report version 0.0.1**

Document for: **Information (NOT FOR COMMENT AT THIS TIME)**

---

1 Opening of the meeting

The SA WG3 Chairman, Mr. Michael Walker, opened the meeting and welcomed delegates to the meeting and outlined the domestic arrangements for the day.

2 Approval of the agenda and objectives of the meeting

The agenda, provided in TD S3z010021 was modified to include Agenda Item 7.3 "General Issues" and Item 7/1 "AoB", for discussion of IPv6. With these changes, the agenda was approved. The objectives were outlined: the joint ad-hoc meeting had been requested by the SA WG2 Chairman after the joint meeting held with SA WG3 meeting #17, to cover the issues relating to security which were not completed at that joint meeting. The objectives were agreed.

3 Allocation of documents to agenda items

The available documents were allocated to their respective agenda items.

4 Liaisons from other groups

There were no documents assigned to this agenda item, the liaisons to SA WG3 were dealt with under other agenda items, with specific topics.

5 Status of WI IP Multimedia (IM) Subsystem

A short verbal report on progress in SA WG2 was provided by Avelina Paido, Ericsson, on the IMS work. **<Mike: Maybe you can add a short summary of points she mentioned - I was doing the doc list etc.>**

6 Status report from S3 on access Security for IP based services (aSIP)

6.1 Termination of authentication/signalling flows

TD S3z010053: Alternatives for terminating authentication in the home domain of the IM Subsystem. This was a revision of TD S3z010003, which has been discussed at the aSIP ad-hoc meeting, removing the need to make the I-CSCF stateful. The information flows of the scheme were presented using TD S3z010054.

SA WG2 were asked for input to the termination of authentication issue, given the arguments from Siemens and Ericsson (TD S3z010040), from an architectural point of view. The issues that had been raised in the aSIP ad-hoc meeting were provided in TD S3z010047 which was presented by the aSIP ad-hoc Convenor.

SA WG2 representatives were asked for a set of issues they considered in addition to this and the following were proposed:

- More information stored in the HSS
- Failure of Authentication causes extra signalling
- VLR functionality in the HSS and S-CSCF
- S-CSCF validity in HSS
- Access independence
- Inter-vendor issue of transfer of data between nodes
- HSS solution gives the I-CSCF the role of "Registrar"

Working assumptions which had been reached at the aSIP ad-hoc were:

> Session establishment
> It is the working assumption of the aSIP ad hoc group that the hop-by-hop integrity protection of session establishment (INVITEs) and the option to authenticate the user during re-registrations and the ability of the Network to force re-registration, provide adequate protection for session establishment. The re-registration timer can be reset to a new value when forcing a re-registration.
>
> Confidentiality Protection of SIP signalling
> It is the working assumption of the aSIP ad hoc group that the confidentiality of SIP signalling between the UE and P-CSCF is optional for implementation. Confidentiality of SIP signalling can rely on existing mechanisms, or mechanisms which will be provided by NDS.

The SA WG3 Chairman asked companies to provide an indication of the solution which they preferred from the two, in order to get an idea of the balance. Some companies made an indication, which showed that there was no strong majority for either solution.

AT&T asked that any Working Assumptions that could be reached at this meeting be liased to SA WG2 for discussion and reaction.

The SA WG3 Chairman stressed that a solution should be strived for on this issue in order to allow work to progress, and companies were asked to be flexible in order to allow a solution to be chosen.

The issues that were identified in the aSIP ad-hoc meeting were also reviewed and integrated with those mentioned by SA WG2 delegates.

"Dumb" database

One issue proposed in the aSIP ad-hoc was that the HSS had been designed in 23.228 to be a "dumb" database entity and should not have the functionality of checking authentication Vectors. Ericsson asked for verification of this from SA WG2 delegates present. It was stated that this discussion had been raised many times in SA WG2, where some delegates asked for signalling for signalling functionality and others asking for Store-Retrieve functionality only. Siemens stated that the Release 1999 HLR performs data handling only and session functionality is in the VLR, with the AuC considered as a "black box" which provides the Authentication vectors. After some discussion, it was agreed that the HSS does generate authentication vectors as part of it's functionality, so that the "dumb database" argument was removed from the discussion. It was stated that the AuC function was a VLR function in Release 1999.

It was concluded that the issue was really security session related data handling, rather than IP session related.

HSS performs functionality per user authentication (HSS proposal):

Nokia stated that this is new functionality in the Home network anyway, as this is performed by the Visited network in Release 1999, and is now performed by the Home network. Siemens responded that the HSS is a precious, centralised resource and the functionality should be distributed among the S-CSCFs in the network. Ericsson pointed out that the new Siemens proposal also contacted the HSS in order to get S-CSCF routing information and that this also required higher dynamic storage in the HSS, which was included as an argument against the HSS solution.

It was finally noted that this resource issue was not a security concern, but an SA WG2 issue.

DoS attack risk:

AT&T proposed that DoS attack protection functionality is already included in S-CSCF and would need to be duplicated in the HSS for the HSS solution. It was argued that both solutions are susceptible to DoS attacks to some extent. It was also stated that the HSS would need to have protection against other potential types of DoS attacks anyway.

After some discussion, the SA WG3 Chairman summarised that the main issue for DoS is the flooding of the AuC with requests, and as such, the S-CSCF solution appeared to provide a filter function against this at the S-CSCF. Therefore there seemed to be some justification for the increased DoS threat with the HSS solution.

HSS/I-CSCF acting as Registrar role:

Motorola suggested that the S-CSCF includes the functionality to act as Registrar, and that in the HSS solution the I CSCF performs this role. Ericsson argued that this functionality was already in the I CSCF. After some discussion, it was concluded that this was not a security issue, but an archtectural one, and such decisions should be held by SA WG2.

Early allocation of I-CSCF resources and many messages in case of Authentication Failure:

Ericsson pointed out that the S-CSCF solution allocates many resources before authentication is performed, and that in case of authentication failure, many more messages are exchanged than in the HSS proposal, which provided potential risk for DoS attacks, which would normally be authentication failure cases. Siemens stated that the S-CSCF solution would have the advantage of less accesses to HSS for re-registration, if the S-CSCF can be provided to the I-CSCF in the Register message (which would require further modification to the scheme to transport the S-CSCF ID in the messages).

Conclusion:

The SA WG3 Chairman concluded that no compelling Security argument had emerged from the discussions in either the aSIP ad-hoc or this joint ad-hoc. He asked Ericsson and Siemens to try to come to an agreement on a single solution, which would be taken to be the agreed solution unless some serious security problem emerges in the future. SA WG2 were also asked to consider whether there is a compelling architectural reason to favour one solution over the other and to advise the SA WG3 Chairman. If no solution can be reached in this way, then the SA WG3 Chairman will make a selection at SA WG3 meeting #18. Ericsson and Siemens both accepted this proposal.

The SA WG3 Chairman agreed to write a letter to the SA WG2 Chairman advising him of this.

6.2 Protection mechanisms

TD S3z010047 Working assumptions and HSS/S-CSCF concerns. This was produced by the aSIP ad-hoc meeting and the ***Confidentiality protection of SIP signalling*** issue was reviewed:

Problems had been identified with the integrity protection methodology, IETF time scales for SIP and that IPsec had potential security problems. It was agreed that this should be further discussed in SA WG3. The placing of the integrity checking mechanism needs to be resolved at SA WG3 meeting #18.

6.3 Security mode set-up

TD S3z010056 R Release 99 Security Mode Set-up and “Fixed” SIP Security Mode Set-up. This was presented by Ericsson and outlined how signalling could work, while not requiring additional SIP signalling. It was recognised that this proposal would require analysis to ensure that it is a viable solution. It was also recognised that any solution which is chosen would require some form of SIP extension and that the choice of solution may have an impact on the final time scales for finalisation in the IETF, although it was also thought that the two solutions provided would probably have a similar impact.

It was agreed that where there is a choice of equally viable solutions, the solution requiring the minimum changes to SIP will be chosen by SA WG3.

6.4 Other issues from the S3 ad hoc session

It was reported that in off-line discussions it was questioned whether the Security Gateway should be included in the SA WG2 architecture descriptions, for signalling flows. It was reported that this is included in the draft NDS document 33.200 and is specified on the IP layer and did not need to be repeated in the architecture flows. SA WG3 delegates should check this. It was suggested that any information that is identified for the architecture should be contributed to SA WG2 for inclusion in 23.002.

It was reported that the SA WG3 ad-hoc discussions had considered the statements in 23.228 about where the authentication takes place, and the correctness of this text was questioned. Depending on the outcome of discussions to contribution TD S3z010034, SA WG2 may be asked to verify and update this text (see agenda item 7.4).

7 Open issues from the S2/S3 joint meeting in Gothenburg

7.1 Hiding requirements

TD S3z010052: Network hiding mechanism. AT&T presented this contribution, which addressed security needs of configuration independence (network hiding), including a mechanism needed to route SIP requests and responses to hide the S-CSCF information from unauthorised entities. It proposed that SA WG3 endorse the detailed changes to Section 5.2.2.3 of TS 23.228, as a method of implementing the network configuration independence requirement. It was clarified that the changes were internal to the S-CSCF, but that SA WG3 were requested to check the proposals from a security viewpoint. There was an argument for standardisation of the encryption mechanism due to a potential multi-vendor environment between S-CSCFs. SA WG3 delegates were asked to consider this.

TD S3z010048: LS from CN WG1/SA WG2-SIP ad-hoc on Security implications of supporting "hiding". This was considered at SA WG2 and was postponed to this joint ad-hoc meeting, as there was no time to deal with this at the SA WG3 meeting #17 joint session with SA WG2. A request that some standardisation is needed from a practical point of view, so that manufactures can limit the number of algorithms that will be required by different operators, even though it could be possible to leave this to proprietary solutions. Interested companies (in particular the supporting companies for any WI on this) were asked to provide a WI description and contributions to SA WG3 in order that SA WG3 can do the work. It was agreed that SA WG3 would keep SA WG2 informed on any progress of this work. Peter Howard agreed to draft a LS to SA WG2 on this topic.

TD S3z010055 This document was withdrawn.

TD S3z010035: SIP Headers and Messages for Security in 24.228 Flows. This was presented by Motorola and informs SA WG3 that SA WG2 would like information on the frequency of periodic authentication to be used, due to concerns in GERAN on speech quality degradation on "optimised voice" channels during re-authentication data transmission. After some consideration it was reported that authentication would only be needed at registration.

7.2 Public vs private identities

TD S3z010049: LS on "IM User Identities". This had been postponed from SA WG3 meeting #17 and was re-submitted by Motorola. A proposed reply was provided in TD S3z010057.

The security of the binding of Public and Private IDs was recognised as needing further study in SA WG3. From a security point of view, mapping Public to Private IDs is inherently insecure, and would probably not be implemented as only Private IDs can be securely authenticated in the architecture.

A potential solution was introduced to send the Private ID for the first registration to establish a secure authentication, and a Public ID for subsequent authentications, where the session would already be integrity protected. SA WG3 would need to verify this scheme, and would consider contributions on this at SA WG3 meetings.

TD S3z010057: Proposed Reply LS from SA WG2 for " IM User Identities". It was clarified that it had been agreed that (multiple) Public and Private identities can be stored on the USIM. It was noted that the Public ID is not authenticated, therefore it is not associated with any authenticated ID. The only ID which is authenticated is the Private ID and SA WG2 were asked to note this. It was agreed that this information should be included in 24.228.

7.3 General Issues

TD S3z010035: SIP Headers and Messages for Security in 24.228 Flows. This was provided by Motorola and proposed that the joint meeting consider the above issues for discussion and make a decision on the following points:

1. SIP level flows and parameters related to security should be included in TS 24.228 based on the work conducted by SA3.
2. The identification of SIP headers, responses and mechanisms required for AKA authentication and encryption of SIP messages, should be pursued by SA3 as a high priority item since this information is needed by SA2 and CN1.
3. The identification of SIP and/or SDP headers, and mechanisms required for key exchanges needed for encryption of media streams, (bearer) during Session Initiation, should be pursued by SA3 as a high priority item since this information is needed by SA2 and CN1.

The Chairman stated that SA WG3 can only assign priorities based on contribution it receives. Therefore SA WG2 and CN WG1 should ensure that delegates urge their security colleagues to make contribution to SA WG3 on subjects that they consider important.

It was agreed that SA WG3 could define the requirements as far as possible, but that bit-level knowledge was not in their expertise, so when ready, a joint meeting could be arranged to sort out the details together. SA WG3 agreed that a joint meeting would be arranged with CN WG1 on this subject.

TD S3z010034: Security Relationships of Interrogating CSCF (I-CSCF). This was introduced by Motorola. Although some security relationships had been agreed in the SA WG3/SA WG2 joint session during the SA WG3 meeting #17, there were some errors identified in 22.228, which SA WG2 would like the help of SA WG3 for early resolution to progress the document.

The proposals for changes to 22.228 provided in the contribution were reviewed and modifications agreed. The changes were re-drafted on-line and an updated version produced in TD S3z010059, which was further edited to clean up the result, and provided in TD S3z010060, which was **endorsed** by the meeting for contribution to SA WG2 (to be contributed by Motorola in the form of a CR).

Security Gateway:

SA WG3 were asked whether security elements should be defined in the reference architecture. The principle from SA WG3 was that security elements are only defined where there are defined interfaces.

It was reported that there was an interface in SA WG2 documentation between the HSS and the AuC, describing the interaction, and should the Security Gateway therefore be included. It was concluded that 23.002 did not need to include the Security Gateway at the moment and that SA WG3 will further consider whether this is needed.

7/1 AoB

- IPv6

TD S3z010058: LS to SA WG2: Request to Study IP Version Selection for Security Nodes. This LS was considered. It was agreed that this should be re-written after consultation of 23.221, but that there was not enough time at this meeting. This will be added to the agenda for SA WG3 meeting #18.

Closing of the meeting

The Chairman thanked the host, Ericsson, for the meeting arrangements, and the delegates from SA WG2 and SA WG3 for supporting the meeting to progress the Security issues and closed the meeting.

Annex A: List of attendees at the SA WG3/SA WG2 joint ad-hoc meeting

Name			Company	e-mail	3GPP Member	
Mr.	Andrew	Allen	MOTOROLA Ltd	caa019@email.mot.com	ETSI	x
Mr.	Stephen	Billington	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Colin	Blanchard	BT	colin.blanchard@bt.com	ETSI	x
Mr.	Marc	Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	x
Ing.	Krister	Boman	Telefon AB LM Ericsson	krister.boman@emw.ericsson.se	ETSI	x
Mr.	Daniel	Brown	Motorola Inc.	adb002@email.mot.com	T1	x
Miss	Tao	Bu	NOKIA Corporation	tao.bu@nokia.com	ETSI	x
Mr.	David	Castellanos	Telefon AB LM Ericsson	david.castellanos@ece.ericsson.se	ETSI	x
Ms.	Lily	Chen	Motorola Inc.	Lily.chen@motorola.com	T1	x
Dr.	Adrian	Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Louis	Finkelstein	Motorola Inc.	louisf@labs.mot.com	T1	x
Mr.	Guenther	Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	x
Mr.	Peter	Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	x
Mr.	Geir	Koien	Telenor AS	geir-myrdahl.koien@telenor.com	ETSI	x
Mrs.	Tiina	Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI	x
Mr.	Dirk	Kroeselberg	SIEMENS AG	dirk.kroeselberg@mchp.siemens.de	ETSI	x
Mr.	Vineet	Kumar	Intel Sweden AB	vineet.kumar@intel.com	ETSI	x
Mr.	Carlos	Lazaro	TELEFONICA DE ESPAÑA SA	lazaro_c@tsm.es	ETSI	x
Mrs.	Geneviève	Mange	ALCATEL S.A.	g.mange@alcatel.de	ETSI	x
Mr.	Bill	Marshall	AT&T Wireless Services, Inc.	wtm@research.att.com	T1	x
Mr.	Michael	Marcovici	Lucent	marcovici@lucent.com	T1	x
Mr.	Tomi	Mikkonen	SSH Communications Security Corp	tomi.mikkonen@ssh.com	ETSI	x
Mr.	Valtteri	Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	x
Mr.	Bradley	Owen	Lucent Technologies Network Systems UK	bvowen@lucent.com	ETSI	x
Ms.	AVELINA	PARDO	Telefon AB LM Ericsson	avelina.pardo-blazquez@ece.ericsson.se	ETSI	x
Mr.	Olivier	Paridaens	ALCATEL S.A.	olivier.paridaens@alcatel.be	ETSI	x
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	x
Mr.	Hugh	Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	x
Miss	Shabnam	Sultana	Telefon AB LM Ericsson	shabnam.sultana@era.ericsson.se	ETSI	x
Mr.	Nacho	Uzquiano	TELEFONICA DE ESPAÑA SA	uzquiano_ji@tsm.es	ETSI	x
Prof.	Michael	Walker	VODAFONE Group Plc	michael.walker@vf.vodafone.co.uk	ETSI	x
Dr.	Peter	Windirsch	T-Nova Deutsche Telekom	Peter.Windirsch@t-systems.de	ETSI	x

registered but not signed in as attending:

Mr.	Shinichiro	Aikawa	Fujitsu Limited	aikawa@ss.ts.fujitsu.co.jp	TTC
Mr.	Jari	Arkko	Telefon AB LM Ericsson	jarkko@piuha.net	ETSI
Mr.	Rolf	Blom	Telefon AB LM Ericsson	rolf.blom@era.ericsson.se	ETSI
Mr.	Sebastien	Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@rd.francetelecom.fr	ETSI
Mrs.	Susana	Ochoa	AIRTEL Movil SA	sochoag@airtel.es	ETSI
Mr.	Magnus	Olsson	Telefon AB LM Ericsson	magnus.olsson@era.ericsson.se	ETSI
Mr.	Miika	Poikselka	NOKIA Corporation	Miikka.Poikselka@NOKIA.COM	ETSI
Mr.	Lee	Valerius	NORTEL NETWORKS (EUROPE)		ETSI

3GPP TSG GERAN/SA WG3 ad hoc **version 0.0.1**
Madrid, Spain
27 April 2001

Source: **Secretary (Maurice Pope, MCC)**

Title: **Draft report version 0.0.1**

Document for: **Information (NOT FOR COMMENT AT THIS TIME)**

---

1 Opening of the meeting

The Chairman, Marc Blommaert, opened the meeting, welcomed delegates and provided the domestic arrangements.

2 Approval of the agenda, organisation and objective of the meeting

TD S3z010014 provided that agenda for the meeting which was approved.

The documents were allocated to their appropriate agenda items.

The Chairman outlined that this was a GERAN meeting and output to SA WG3 would need to be done formally by LS.

The objectives of the meeting were:

- To conclude the specification of ciphering in GERAN 'Iu' mode. (proposed CR)
- To progress the stage 2 work on integrity protection in GERAN 'Iu' mode. (set of working assumptions).
- To study/progress/solve other security related problems affecting GERAN (e.g. use of the Iur-g interface)

3 Letters from other groups

The LSs from other groups were considered with other related contributions under their appropriate agenda item.

4 Status of the Work Item

TD S3z010042 GERAN security ~ WI status (presentation slides). This was presented by Vodafone and provided the status, open issues and the expectations from the meeting. Release 5 integrity protection had been worked on for a few months, but problems arose and SA WG3 were asked for this joint meeting to help progress the work.

Problems include, that there were vague requirements, the ciphering has not progressed over last meetings; although it was thought to be near completion. Open issues included ciphering and integrity protection. Other open issues were LCS and use of the Iur-g interface.

GERAN would like to obtain from this meeting: Clarification of requirements; Completion of ciphering, i.e. production of CR to stage 2; Progress integrity protection, providing a set of working assumptions. Also, if possible to progress other issues, e.g. LCS and use of the Iur-g

A request for advice from SA WG3 on the use of IMSI and TMSI was received, when IMSI can be used and when TMSI is used. It was clarified that the TMSI should always be used, and it was also suggested the solution as used in UTRAN should also be considered.

Requirements on integrity protection: GERAN are working on the assumption that S3 want to align GERAN and UTRAN security. SA WG3 have only said this in LSs and do not cover GERAN security in the specifications. It is the wish that GRRAN Security should be aligned as closely as possible to the UTRAN Security. It was explained that the approach for UTRAN is to integrity protect the Control Plane and not the user Plane, in order to protect against attacks on the signalling over the air. This is done to protect against more sophisticated attacks, which may be possible in the future, in order to try to avoid continuous patching up of the system, which would be expensive.

It was clarified that ciphering is not mandatory for UTRAN, but integrity protection is. Integrity protection should also be mandatory in GERAN, also recommended that ciphering is optional, unless there are no restrictions in areas where GERAN will be used.

It was stated that there are problems in integrity protecting all messages in GERAN as the architecture is not the same as UTRAN, and clarification of which messages are necessary to protect was requested. It was clarified that at least the same messages as must be protected in UTRAN should be considered. This was discussed further based on other contributions.

The presentation was then noted. The agreed working assumptions were provided in TD S3z010065.

TD S3z010043: Current status of stage 2. This was presented by Vodafone, and requested conclusions are aimed for at this meeting:

1 A decision be made at this meeting as to where the stage 2 description of the GERAN security should be, along whit the scope if it is to be split between different specifications.
2 SA3 confirm the validity of the working assumptions regarding ciphering; the remaining open points should be closed at this meeting.
3 The sub-clause in the stage 2 is enhanced so that other issues regarding GERAN security are dealt with; these at least include integrity protection.
4 The scenarios where the Iur-g interface is used are studied from the security point of view so that security matters can be considered by GERAN during the ongoing work on this interface.

It was recommended that the stage 2 description of GERAN Security is keep it in 43.051 at present, and to include a reference to 43.051 in 33.102, until the GERAN Stage 2 work is stable enough for a decision to be made to move the architectural aspects of GERAN Security into 33.102. There were no objections to this, and it was taken as a **working assumption** of the joint meeting (see TD S3z010065 for agreed text).

Other items (ciphering, integrity protection, Iur-g) were dealt with as the subject of other contributions.

TD S3z010046 SA WG3 LS to GERAN: Reply to LS on integrity protection for GERAN. This was considered during the discussions of TD S3z010016 and noted.

TD S3z010045: GERAN LS to SA WG3: LS on integrity protection for GERAN. - this was included in text of TD S3z010046 and noted.

TD S3z010015: LS on LCS message security from SA WG3 drafting group. This was not handled at the meeting due to lack of time.

5 Technical discussion

5.1 Requirements

5.2 Ciphering

5.3 Integrity protection (General, RRC, RLC/MAC)

TD S3z010044: On integrity protection and the effects of additional segmentation. This was introduced by Vodafone and the SA WG3 details were highlighted. It had been suggested that adding integrity protection to GERAN messages may cause segmentation, which can give performance problems. This provided the

results of a study that Vodafone made and concluded that the benefits of integrity protection outweigh the side effects of possible (additional) segmentation and it is requested that the use of integrity protection in GERAN be adopted as the working assumption, unless other significant impacts are found. Further study is felt to be needed before this is ratified for the case of RLC/MAC control messages.

The document was noted (see TD S3z010065 for agreed working assumptions).

TD S3z010037: GERAN RRC Messages and Integrity Protection. This was introduced by Nokia and lists the RRC messages and the applicability of and criticality of integrity protecting each message.

There was some discussion on the messages that were not protected, e.g. IMMEDIATE_ASSIGNMENT messages, which were protected in UTRAN. These messages could not be protected as the user was not known at the time. For immediate assignment, however, there is no further interaction after this. This was considered a significant threat by SA WG3.

It was noted that the question of protection of Immediate assignment procedures should be provided by GERAN to SA WG3 for analysis of the threat scenarios and possible solutions. GERAN need to clearly describe the scenario in order that SA WG3 can understand the problem. The immediate assignment set up procedure was outlined and discussed, where messages are exchanged before the integrity checking is done and the user either provided with service or rejected. This was the same set-up procedure as for the UTRAN set-up. The radio bearers are established after authentication, and this is integrity protected. The problem is for non- RT services when the Radio bearer is established but there are no physical resources allocated, so that the UE sends the service request, which does not include the ID. The UE sends the ID it has received from the GERAN (8-11 bits), which could be guessed by an attacker (there are only 256 possible IDs).

Exceptions to the list in table 9.1 were accepted as a current assumed status, except for the IMMEDIATE-ASSIGNMENT messages which need to be checked against the methods used in UTRAN.

Note 3 was considered as FFS, and replaced by the working assumption below.

The following **working assumption** on RRC message integrity protection was established and agreed and included in TD S3z010065.

<Add Working Assumption here?>

It was asked whether the draft CR to 25.331 could be updated to include the results of the discussions with the endorsement of the joint meeting - with the knowledge that the draft CR would be available for comment by SA WG3. There was no opinion on this, as draft CRs can be produced by companies, and their correctness can be discussed in relevant WGs before approval.

TD S3z010038: Simulation results on RLC/MAC signalling. This was presented by Ericsson and discusses some of the issues raised in GERAN on integrity protection for RLC/MAC signalling. It provides simulation results on the impact of integrity protection and reports that difficult to conclude on the frequency of RLC/MAC messages and the real impact of integrity protection, but it is clear that the introduction of delayed TBF release will reduce the amount RLC/MAC signalling and therefore also the impact of integrity protection on the system performance.

It was concluded that more work was needed in order to identify whether there will be any security questions to SA WG3. However, it was also agreed that the issue needs to be addressed as it will not be possible to produce simulation results for all possible cases. The contribution was then noted.

TD S3z010016: Integrity Protection at RLC/MAC. This was introduced by Nokia and analyses the impact of integrity protection on the segmentation mechanism in GERAN.

The paper addressed the extreme cases for the different messages (maximum size), but did not address the cases where the authentication code for integrity protection causes segmentation (i.e. segments one into two radio blocks). The status of Packet Cell Change Order was left open, however was thought that a variable size MAC-I with a minimum guaranteed size can be introduced. The same would apply to Immediate Assignment for TBF establishment.

The contribution concluded that for the scenarios analysed, no major redesign of the RLC/MAC protocols is needed for supporting integrity protection of RR flavoured RLC/MAC control messages, as the existing segmentation mechanism is enough. A variable sized, with guaranteed minimum, MAC-I was suggested to be introduced, with the introduction on a 32-bit MAC-I, if the segmentation overhead is acceptable (this needs to be studied).

Note: SA WG3 recommended the use of variable MAC-I, with a minimum MAC-I length of 8-bits in TD S3z010046.

It was reported that variable-length MAC-I also has an overhead implication to signal it's length, alternatively, the MAC-I could be set to exactly fit the length of the message and then the length be derived.

A **working assumption** was agreed that a that GERAN should specify a variable length MAC-I, with length indicator, where the maximum number of MAC-I bits would be used in messages (up to 32 bits), with a minimum size of 8 bits in order to avoid segmentation where possible. SA WG3 were asked to specify the mechanisms for dealing with truncated MAC-I (see TD S3z010065 for agreed text).

The RLC/MAC messages in this contribution were agreed as a **working assumption**. RLC/MAC messages will have a fixed MAC-I of 32 bits. (see TD S3z010065 for agreed text).

<MARC - I think I have reversed RRC and RLC/MAC discussions here - PLEASE CHECK>

There was some discussion over the validity of using a variable length field, as the overall security level of the system will be down to the weakest link - i.e. 8 bit MAC-I in this case. This concern over the added complexity was noted.

TD S3z010063: Some GERAN-specific security issues. This was presented by Alcatel, The issues not covered already by agreements were discussed:

Ciphering of layer 2 signalling

There is no possibility for the source BSS to control the integrity protection when the user is in a drift BSS. It was suggested that when moving from a BSS, a Cell update is performed, triggering update location. During this procedure the assignment messages are not protected. This is seen by Alcatel as a security void, even though it is limited.

The conclusion of discussions on this topic were covered by the working assumption on integrity protection (TD S3z010065).

Integrity protection of RLC/MAC control messages.

The user plane is used in UTRAN but this is not possible in GERAN. As this was an open issue within GERAN, the proposals here should be further discussed in GERAN.

The document was then noted.

5.4 Other

TD S3z010062: Iur-g related security issues. This was presented by Siemens. It reports that assuming a GRA exceeding the BSC area and a MS in RRC_GRA_PCH state, then an MS can move within the GRA without performing location management procedures (except e.g. periodic location updates). There were 2 open issues:

- to identify the earliest possible instant for triggering the Relocation procedure taking into account that CN procedures shall not be changed and security requirements are fulfilled.
- a CN initiated paging (triggered from the CS domain) might be lost. A possible solution for the identified CN initiated paging problem can be found in GAHW-010134. The following discussion is based on this proposal with some changes with the main focus on security issues:

  Security-related assumptions made in the contribution were:

- MSC1 may execute the Authentication and Key Agreement procedure to be able to check, whether the TMSI (received in the NAS-Paging response) belongs to the correct subscriber. This requires NAS signalling between MSC1 and the MS, and is currently performed in UTRAN using dedicated resources on Iur.
- MSC1 has to send the RANAP Security Mode Command to the Serving BSC before a Relocation procedure is allowed.
- The RRC CELL_UPDATE_CONFIRM message has to be protected because security parameters can be delivered with this message. This message has to be transmitted to terminate the Cell Update procedure.

SA WG3 were asked whether the NAS-Paging response to be ciphered and integrity protected. If so, further analyses are needed to identify a solution, how to transport a ciphered message towards Serving BSC without having security related information within Controlling BSC.

In summary, the contribution lists some security related issues (besides general ones) which are related to the intra GERAN Iur-g interface as well as to the inter-RAN Iur-like interface. No concrete solution is provided, but some of the issues listed in section 2 have to be discussed / answered. It is proposed that the Joint GERAN / SA3 Ad hoc meeting agrees on the security related assumptions listed above and discusses the issues raised.

It was considered to be an architecture-related problem, which SA WG3 would look at when there are stable architectural solutions available.

There was some discussion between GERAN delegates on these issues, but the SA WG3 delegates needed time to study the issues in order to understand the problem and provide advice. It was agreed that this should be further discussed in GERAN and provided as a LS to SA WG3. This was added to the list of open issues in TD SP-01065.

The document was therefore noted in this meeting.

6 Output of the meeting

6.1 Preparation of the results

The results, agreements and working assumptions from the meeting were captured in a document which was reviewed and modified on-line, the final text was provided in TD S3z010065 which was agreed.

6.2 Letters to other groups

It was agreed that TD S3z010065 (see agenda item 6.1) would be used for input to SA WG3 and GERAN.

7 Closing of the meeting

The Chairman thanked delegates for their co-operation and hard work during the meeting and the Host (Ericsson) for the meeting facilities and closed the meeting.

Annex A: List of attendees at the SA WG3/GERAN joint ad-hoc meeting

Name			Company	e-mail	3GPP Member	
Mr.	Stephen	Billington	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Marc	Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	x
Ing.	Krister	Boman	Telefon AB LM Ericsson	krister.boman@emwericsson.se	ETSI	x
Mr.	Daniel	Brown	Motorola Inc.	adb002@email.mot.com	T1	x
Ms.	Tao	Bu	NOKIA Corporation	tao.bu@nokia.com	ETSI	x
Mr.	David	Castellanos	Telefon AB LM Ericsson	david.castellanos@ece.ericsson.se	ETSI	x
Ms.	Chen	Lily	Motorola Inc.	Lily.chen@motorola.com	T1	x
Dr.	Adrian	Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	x
Mr.	Louis	Finkelstein	Motorola Inc.	louisf@labs.mot.com	T1	x
Mr.	Guenther	Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	x
Mr.	Peter	Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	x
Mr.	Mathias	Johansson	Telefon AB LM Ericsson	mathias.p.johansson@era.ericsson.se	ETSI	x
Mr.	Michael	Marcovici	Lucent	marcovici@lucent.com	T1	x
Mr.	Vincent	Muniere	ALCATEL S.A.	Vincent.Muniere@alcatel.fr	ETSI	x
Mr.	Valtteri	Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	x
Mr.	Bradley	Owen	Lucent Technologies Network Systems UK	bvowen@lucent.com	ETSI	x
Mr.	Olivier	Paridaens	ALCATEL S.A.	olivier.paridaens@alcatel.be	ETSI	x
Mr.	Maurice	Pope	ETSI	maurice.pope@etsi.fr	ETSI	x
Mr.	Guillaume	Sebire	NOKIA Corporation	guillaume.sebire@nokia.com	ETSI	x
Mr.	Hugh	Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	x
Mr.	Jean-Michael	Traynard	Siemens AG	jean-michael.traynard@icn.siemens.de	ETSI	x

registered but not signed in as attending:

Mr.	José Luis	Carrizo Martínez	VODAFONE Group Plc	jose-luis.carrizo@vodafone.co.uk	ETSI	
Mr.	Vineet	Kumar	Intel Sweden AB	vineet.kumar@intel.com	ETSI	
Mr.	Tomi	Mikkonen	SSH Communications Security Corp	tomi.mikkonen@ssh.com	ETSI	
Mrs.	Susana	Ochoa	AIRTEL Movil SA	sochoag@airtel.es	ETSI	
Mr.	Lee	Valerius	NORTEL NETWORKS (EUROPE)		ETSI	

3GPP TSG SA WG3 Security — S3#18

21-24 May, 2001

Phoenix, USA

Source: **Secretary, SA WG3 (Maurice Pope, MCC)**

Title: **Draft Report of Meeting #18**

Version: **0.0.3**

The hiking pioneers at 100°F: South Mountain

---

1 Opening of the meeting

The Chairman, Prof. Michael Walker welcomed delegates to the 18th meeting of SA WG3. Mr. Dan Brown, Motorola Inc., welcomed delegates to Phoenix, and provided the domestic arrangements and wished SA WG3 a successful meeting.

2 Meeting objectives and approval of the agenda

The Chairman provided the objectives for the meeting:

- Election of SA WG3 Chairman and 2 Vice Chairmen (Tuesday a.m.)
- Completion of Rel-4 NDS documents for presentation to TSG SA for approval in June 2001 (and for information by e-mail after this meeting)
- Completion of the GERAN Integrity Protection for approval in the June 2001 TSG meeting
- UE Split to be completed
- Network Security to be progressed
- IMS Security to be progressed, as it needs to be provided to TSG SA in June 2001 for information - the ad-hoc IMS meeting had discussed the positioning of the authentication checking and SA WG2 were asked for advice from an architecture viewpoint. Ericsson had since withdrawn their proposals
- Changes for Release 1999 in order to align and corrections to UTRAN - SIM access specifications

The agenda, provided in TD S3-010140, was updated to include some extra items: 8.2, 8.3 and 9.9 was updated to the title "UE Split". The agenda was then approved.

3 Assignment of input documents

The available documents were assigned to their appropriate agenda items.

4 Approval of reports from 3GPP SA3 meetings

4.1 S3#17, 27 February – 1 March, Gothenburg

TD S3-010141 Draft report of meeting #17 version 0.0.4: This was modified editorially and approved. The updated version 1.0.0 will made available on the ftp server.

4.2 S3#17bis, 23-27 April, Madrid

TD S3-010143 Draft report of NDS ad-hoc, April 23-24 April 2001: This report was approved. The approved version will made available on the ftp server.

TD S3-010144 Draft report of aSIP ad-hoc, April 25 2001: This report was approved. The approved version will made available on the ftp server.

TD S3-010145 Draft report of SA WG3/SAWG1 IMS joint session, April 26 2001: This report was approved with minor changes. The approved version will made available on the ftp server.

TD S3-010146 Draft report of SA WG3/GERAN joint meeting, April 27 2001: This report was approved with minor changes. The approved version will made available on the ftp server.

4.3 Joint S3/T3 meeting, 3 May, Munich

TD S3-010224 Report of the TSG-T3 Ad Hoc Meeting #37 (Joint with TSG-S3): This report was presented by N. Barnes, Motorola, and the conclusions were taken into account in the discussion of other relevant topics during the meeting. The report was then noted.

5 Reports and liaisons from other groups

5.1 3GPP SA3 lawful interception sub-group

TD S3-010229 Report of the 3GPP TSG SA WG3-LI (S3-LI) meeting #2/01 on lawful interception. The SA WG3 – LI Chairman presented the report of the Clearwater meeting, the agreed output of which were summarised in Annex C of the report. The report was noted and Bernie McKibben, having earlier announced his resignation, was thanked by SA WG3 for all his hard work in the LI group, and wished him success in his future work.

5.2 3GPP SA plenary

TD S3-010213 Report to SA3 on SA#11. This was presented by the SA WG3 Chairman, and had been distributed by e-mail before the meeting. The main points were the importance of distribution of Security algorithm documents very quickly after approval in order to reduce criticism of the algorithms, as the evaluation reports usually provide answers to the alleged "threats" that may be reported. The Liaison of SA WG3 to other groups was also criticised in the SA Plenary, with no specific examples of problems, but it was noted that the LS procedure needed to be improved. Mr. Pope agreed to try to improve the MCC side of the liaison process, as some LSs that SA WG3 had approved in previous meetings had taken a long time to be delivered to the relevant groups. The report was then noted.

5.3 3GPP WGs

5.3.1 SA

TD S3-010159 LS from SA WG1 regarding User Profile: The contribution on User Profiles from Ericsson, which was presented at the SA WG1 ad-hoc meeting was provided in TD S3-010172, and was noted. TD S3-010159 was considered and discussed, but SA WG3 did not identify any specific security contribution that could be made to the user profile description. The liaison was noted, and a response to SA WG1 and SA WG4 was included in TD S3-010225, replaced by TD S3-010281 "Reply LS on streaming and user profile" which was again updated in TD S3-010293 and approved.

TD S3-010160 Reply LS from SA WG2 for "IM User Identities": The LS was considered, but there was some confusion over the meaning of the LS, and delegates were asked to consider it overnight and contact their SA WG2 collegues. This was returned to under agenda item 9.3.

TD S3-010161 Proposed Liaison to S3 on use of Diameter. SA WG2 had considered the adoption of the IETF AAA architecture as the architecture to be used for Authentication and Authorization in the IP Multimedia CN subsystem, and asked SA WG3 for their reaction. This had been handled at the April 2001 ad-hoc meeting, ~~and~~ which concluded that SA WG3 did not favour this approach. The LS was then noted.

TD S3-010168 LS from SA WG5 in reply to T WG2 LS on MExE and User Equipment Management (T2-000756): This was copied to SA WG3 for information, and noted. The MExE Rapporteur was asked to provide a LS back to SA WG5, informing them that SA WG3 will consider this as part of the MExE Security work. This was provided in TD S3-010226 and an updated WI description was provided in TD S3-010227. This was modified in TD S3-010288 to add SA WG5 as a secondary responsible group which was approved. The WI description sheet was attached for information to TD S3-010226.

TD S3-010142 Response to LS (S1-010144) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT: This LS was noted as the LS from T WG3 in TD S3-010166 " Response to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT (T3-010323)" reported no security work was required at this stage.

TD S3-010156 LS from SA WG1 on basic and advanced services examples (S1-010271): This LS was noted. SA WG3 will inform SA WG1 if any security definition is needed for these services when they have been agreed and further elaborated by SA WG1.

TD S3-010157 LS from SA WG1 on Extended Streaming Service (S1-010501): This was provided to SA WG3 for information, and a response from SA WG4 had been provided in TD S3-010174. A response LS was drafted by P. Howard in TD S3-010293 to inform SA WG1 that SA WG3 have a WI on end-to-end encryption, and asking whether SA WG3 should also produce a WI on Digital Rights Management to support this work (see above).

TD S3-010267 Response LS to S1 LS Regarding User Profiles. A joint meeting was suggested, an invitation provided in TD S3-010278. A LS to SA WG1 had been produced, informing SA WG1 that there were no security impacts identified, included in TD S3-010225, which was updated to include this in TD S3-010281 (later updated further in TD S3-010293).

5.3.2 CN

TD S3-010151 LS from CN WG1 on Re-transmission of authentication requests: This included a CR to 24.008. SA WG3 had submitted and had approved CR134 on this at SA#11. A response to inform CN WG1 of this was drafted in TD S3-010230 which was approved.

TD S3-010152 LS from SA WG2 / CN WG1 Joint SIP Adhoc on "Security for IM SIP session Signalling": This requests SA WG3 to send representatives to CN WG1 to present the SIP signalling status and to discuss the identified issues. CN WG1 also offered to provide input to SA WG3, which was welcomed by SA WG3. Günther Horn agreed to draft a reply LS to deal with the questions to be elaborated at the meeting, in TD S3-010231, which was updated in TD S3-010291 and approved.

TD S3-010234 Liaison Statement from CN WG1 on THRESHOLD check at RRC connection establishment: A corresponding LS from RAN WG2 in TD S3-010153 is covered under agenda item 5.3.4. A reply was sent in TD S3-010273 (see agenda item 9.1).

5.3.3 T

TD S3-010162 Reply LS from T WG3 to T WG1 on authentication test algorithm to be implemented in test USIMs. This was copied to SA WG3 for information and was noted.

TD S3-010163 LS from T WG3 on Rejection of 2G Authentication and Key Agreement by 3G ME with USIM in UTRAN: SA WG3 considered this liaison and agreed that this should be made a clear requirement. The situation would only arise due to incorrect implementation of the standards. It is a requirement that issuers of 3G USIMs support 3G authentication in their Authentication Centres. A reply LS was drafted to T WG3, TSG T and TSG SA on this in TD S3-010232, which was approved (copied to the GSMA-SG for information).

TD S3-010164 LS from T WG3 for "IM Subsystem Address Storage on USIM": This was a response to SA WG2, and was provided to SA WG3 for information, and was noted.

TD S3-010166 Response from T WG3 to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT: No activity was considered necessary by T WG3 at the moment in SA WG3, and they will inform SA WG3 when action is needed.The LS was therefore noted.

TD S3-010167 LS from T WG3 to T WG1 on authentication test algorithm to be implemented in test USIM. SA WG3 noted that using f1 = f1* was acceptable for a test USIM to test MEs. It was also agreed that these test USIMs could not be used for testing towards the AuC, as a real USIM would be needed for this. The LS was then noted (see also TD S3-010193).

TD S3-010193 Response from T WG1 to T WG3 LS on authentication test algorithm in test USIM: This was covered in the discussion of TD S3-010167. A response LS was produced to inform T WG1 and T WG3 that the proposals were acceptable in order to prevent delay of the work, if the test USIMs are used only for testing of MEs, and to inform them that this would not test that f1 and f1* are different for real USIMs in TD S3-010233, which was approved.

TD S3-010194 LS from T WG3 on New feature for SAT originated SMS. This was copied to SA WG3 for information, and was noted. SA WG3 will consdier this further after SA WG1 provide firm service requirements for such a feature.

TD S3-010253 T WG2 Reply to T WG3 LS on New feature for SAT originated SMS. This LS was a response to the T WG3 LS in TD S3-010194 (see above) and was copied to SA WG3 for information and was noted.

5.3.4 RAN

TD S3-010153 LS from RAN WG2 on THRESHOLD check at RRC connection establishment. This was presented by Ericsson, and a corresponding CR was provided in TD S3-010196 (see agenda item 9.1). A corresponding LS from CN WG1 was provided in TD S3-010234. A draft reply LS was provided in TD S3-010237. This LS was updated to remove "Draft" in S3-010273 and approved. This was sent immediately to the RAN WG2 Chairman with the approved CRs in TD S3-010271 and TD S3-010272 attached (see agenda item 9.1), in the hope that they would be able to receive it during their meeting the same week.

TD S3-010154 LS from RAN WG2 on Wrap around of the calculated START value: This was presented by Ericsson, and Ericsson proposed to keep the START at its maximum value (option 1), rather than wrapping it around (option 2), in order to better limit the possibility of ~~repeqting~~ repeating of the Key string. After some discussion, and consideration of corresponding CRs in TD S3-010195 (see agenda item 9.1), Option 1 was chosen as the best method. A LS to RAN WG2 was provided in TD S3-010235, which was updated in TD S3-010268 and approved. This was sent immediately to the RAN WG2 Chairman with the approved CRs in TD S3-010269 and TD S3-010270 attached (see agenda item 9.1), in the hope that they would be able to receive it during their meeting the same week.

TD S3-010155 Response from RAN WG3 to SA WG2 and TSG GERAN to LSs related to optimised IP speech and header removal support in GERAN: This was copied to SA WG3 for information and was noted.

TD S3-010173 LS from RAN WG3 to SA WG3 on security in IP-transport based UTRAN: RAN WG3 asked SA WG3 to check the security issues for their IP transport in UTRAN Work Task, and to provide any comments. This document was noted.

5.3.5 GERAN

TD S3-010150 LS from GERAN ad-hoc #5: Revised working assumptions made at the joint TSG GERAN / SA WG3. This output from the joint GERAN/SA WG3 ad-hoc meeting had been sent to SA WG3 for further agreement. It was noted that SA WG3 would need to add a reference to GERAN TS 43.051 in TS 33.102. This CR was created in TD S3-010236, which was approved. SA WG3 did not consider the allowance of an 8-bit MAC as reasonable from a security point of view, as it would provide a false sense of security, and it would be preferable not to protect the message, than to let operators wrongly think that the messages were adequately secured. This was further discussed under agenda item 9.4.

5.4 ETSI SAGE

TD S3-010259 LS from GSMA on Development of new A5/3. This was presented by Charles Brookson, and provided information on the status in the development of A5/3. A reply was provided in TD S3-010260, which informed SAGE that SA WG3 endorsed the work plan provided in TD S3-010261. TD S3-010261 was considered and it was noted that it did not include the design of GEA3, and the reply LS was updated in TD S3-010282 to include a request for a similar work plan for GEA3. **<CHECK IF APPROVED>**

A5/3:

Mr. C. Brookson provided a verbal report on the status of A5/3: He reported that the ETSI and GSMA lawyers still had not reached agreement on the distribution and ownership of the algorithm, which is expected to be similar to the handling of the KASUMI algorithm. When agreement has been made, the 3GPP Partners will be consulted and then ETSI SAGE will be able to start the design work.

It was clarified that the algorithm will be available from 3GPP SDOs and the GSMA, so that membership of the GSMA will not be required in order to obtain the A5/3 licence, i.e. membership of one of the SDOs or GSMA will not be a pre-requisite~~necessary~~. The algorithm was expected to be ready for the end of 2001.

It was reported that the work should not take much time for ETSI SAGE, as it mainly consists of extracting only 64 bits from the output of the KASUMI kernel. Some time for public scrutiny had been included in the end of 2001 estimation for completion.

5.5 Others (e.g. ETSI MSG, GSMA, TIA TR-45)

GSMA:

Mr. C. Brookson provided a verbal report on the activities of the GSM Association, Security work. The group meet four times a year. Operators are welcomed to join the group.

IMEI:

It was reported that the Terminal Strategies Working Group had agreed that IMEIs are to be included in terminals and that the ITU-T have shown interest in this. The IMEI may therefore become globally mandatory, i.e. all handset manufacturers will be required to include an IMEI in their equipment, in order to gain type approval.

A5/1 key length:

It was reported that tests had been done and that a 64-bit Key will work for A5/1. Many changes to the GSM specifications would be needed, however, for the use of 128-bit Key for GSM, and this was not considered practical.

Security accreditation scheme:

Audits had been performed on some SMART card manufacturers, which had produced some improvements. AuC manufacturers and GRX Network Providers were also scheduled for auditing. The scheme encourages equipment manufacturers to improve their output.

GPRS Risks and Guidelines group:

The group hold 4 meeting per year and will provide guidelines to operators on the risks and avoidance of them. Operators are welcomed to join the group.

6 Joint meeting with TIA TR-45 AHAG

6.1 Joint AKA control procedure

TD S3-010206 TR-45 / 3GPP Joint AKA Control. This was presented by TR-45 AHAG and had been approved by TR-45 in March 2001. The agreement was discussed and approved by SA WG3. The SA WG3 Chairman agreed to forward this agreement to TSG SA informing them of the status, for endorsement.

6.2 Positive authentication reporting

TD S3-010255 3GPP S3 Request for Clarification on Positive Authentication Reporting. This contribution, presented by AHAG was in response to TD S3-010131 (SA WG3 meeting #17), and confirmed that Positive Authentication Reporting is a 3GPP2 requirement for all successful Authentication and Key Agreement (AKA) procedures associated with a location update (i.e. registration). The reporting needs to include User ID, and the RAND used for the AKA procedure. It was clarified that the inclusion of an Information Element in the Location Update Information Element to include RAND would be enough to satisfy the AHAG request. SA WG3 needed to check whether the RAND would always be available for transmission. SA WG3 reported that this would be progressed when the Rel-5 work had been progressed, due to priority in SA WG3 on this work. The contribution was then noted.

6.3 Other issues

TD S3-010256 UIM Authentication Method. This contribution reported that TR-45 has recognized that the use of AKA in conjunction with Removable UIM (R-UIM) creates vulnerability in a form of “rogue shell” attack. The contribution proposes a possible solution and concludes that this proposal would provide adequate protection from the attack, and can be economically implemented on a R-UIM.

The contribution was considered, and it was reported that this would not be necessary for interworking between 3GPP and 3GPP2, but that if 3GPP wished to implement such a solution, it would be more efficient to implement it early, rather than later, for future interoperability. The contribution was then noted and would be considered in future SA WG3 work.

There were no other contributions for the joint session and the meeting was closed.

7 Work programme management

7.1 New work items

TD S3-010212 aSIP-Access Security for IP-Based Services - Activities and a new timeplan: These slides were presented by Ericsson and was accompanied by an updated WI description for Access security for IP-based services. The updated WI clarified that the Stage 3 is not the same as the Stage 2 document (i.e. 33.203). The timescales were reviewed and updated in TD S3-010239 which delayed the work to March 2002: This was further updated to more realistic date in TD S3-010283 and approved.

TD S3-010246 - update to WID FIGS - updates the time schedule. Ericsson reported that they did not support this WI, BT considered that there would be difficulty progressing the IMSS FIGS work, due to lack of contribution, e.g. to Immediate Service Termination (IST). The WID was **not approved**, and companies interested in the work were asked to discuss the future of this work off-line.

TD S3-010264 WID on Network Hiding: SA WG2 asked SA WG2 to provide recommendations and CRs on the security requirements of the new WI for SA WG2. The timescales were not included but it was reported that the work in SA WG2 was expected to be rapid (2-3 meetings) - completion date July 2001 for SA WG3 in order to forward any CRs to SA WG2 in August 2001. Updated in TD S3-010284 and approved.

TD S3-010275 Update to Network Domain Security WIs - NDS-MAP. The automated key distribution was due for completion in December 2001, which was considered an aggressive timescale. The support by T-Mobil also needed to be verified and Mr. Koien agreed to continue the rapporteurship until S3#19 meeting. The completion date was thought unrealistic and was extended to March 2002 completion. The WID was updated and provided in TD S3-010285 which was approved. Contributions were needed in July 2001 in order to prepare the CRs to produce Rel-5.

TD S3-010276 Update to Network Domain Security WIs - IP. This was updated in TD S3-010286 and approved.

TD S3-010222 End-to-end security WI: See agenda item 9.5.

8 Release 99 and earlier

8.1 3G security architecture (TS 33.102) (2G/3G interoperation etc.)

TD S3-010179 Proposed R99 CR to 33.102: Correction to periodic local authentication: Siemens reported that TD S3-000726 had not been fully implemented in the R99 version of 33.102, but that changes approved by RAN#11 had required another update to the text to align it. This CR therefore aligned the text and covered the changes in the mis-implemented CR to 33.102. M. Pope agreed that the CR database would need to track the mistake in implementation, along with the new CR which corrected this and aligned with the RAN specifications. The CR was then approved as **Category F**.

TD S3-010180 Proposed Rel-4 CR to 33.102: Correction to periodic local authentication: This was the Rel-4 equivalent of the R99 CR in TD S3-010179 and was approved as **Category A**.

TD S3-010181 Proposed R99 CR to 33.102: Correction to COUNT-C description: Siemens introduced the CR which aligned the Stage 2 with the Stage 3. The CR was approved as **Category F**.

TD S3-010182 Proposed Rel-4 CR to 33.102: Correction to COUNT-C description: This was the Rel-4 equivalent of the R99 CR in TD S3-010181 and was approved as **Category A**.

TD S3-010183 Proposed R99 CR to 33.102: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted: Nokia introduced this CR, some modifications were made to remove the changes to section F.3 and the updated CR was provided in TD S3-010240, which was approved as **Category F**.

TD S3-010184 Proposed R99 CR to 33.102: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted: This was the Rel-4 equivalent of the R99 CR in TD S3-010183 and was modified to remove the changes to section F.3 and updated in TD S3-010241 which was approved as **Category A**.

TD S3-010195 Proposed R99 and Rel-4 CRs to 33.102: Calculation and Wrap-around of START value: These CRs were introduced by Ericsson. There was a lot of discussion on the meaning of the text, and it was decided to have an off-line discussion on this to clarify the CR. See discussion of TD S3-010154, under agenda item 5.3.4). These CRs were updated in TD S3-010269 and TD S3-010270 which were approved. A corresponding LS to RAN WG2 was produced in TD S3-010268, which was approved, informing them of the decision of SA WG3, with the CRs attached (see agenda item 5.3.4).

S3-010196 Proposed R99 and Rel-4 CRs to 33.102 on THRESHOLD Check at RRC connection establishment. These CRs were presented by Ericsson. See discussion of TD S3-010153, under agenda item 5.3.4. The classification of the R99 CR was agreed as Category F, and the Rel-4 CR as Category A. The CRs were updated accordingly in TD S3-010238 and then separately in TD S3-010271 and TD S3-010272 which were approved. The CRs were attached to related LS in TD S3-010273 which was approved (see agenda item 5.3.4).

8.2 33.103 changes (Integration doc)

TD S3-010185 Proposed R99 CR to 33.103: The multiplicity of Data integrity symbols: This CR was introduced by Nokia and improved the consistency of the document. It was decided that COUNT-I_{UP} and COUNT-I_{DOWN} needed to be further checked. The CR was later checked as OK and was approved as **Category F**.

TD S3-010186 Proposed Rel-4 CR to 33.103: The multiplicity of Data integrity symbols: This was the Rel-4 equivalent of the R99 CR in TD S3-010185 and was approved as **Category A**.

8.3 33.105 Changes (Algorithms doc)

TD S3-010187 Proposed R99 CR to 33.105: Deletion of the maximum size of a RRC message: This CR was introduced by Nokia, and corrected some inconsistencies in the specification. The CR was presented as Category B, but was approved as **Category F**.

TD S3-010188 Proposed Rel-4 CR to 33.105: Deletion of the maximum size of a RRC message: This was the Rel-4 equivalent of the R99 CR in TD S3-010187 and was approved as **Category A**.

9 Work items

TD S3-010147 Status report for NDS: An additional SA WG3 plenary meeting was suggested to develop the IP Part of NDS for early delivery, between SA WG3 meeting #19 and TSG SA Meeting #13.

It was reported that the NDS ad-hoc meeting had agreed to propose a split of TS 33.200 into two documents, one dealing with NDS-MAP, and a second with NDS-IP. SA WG3 agreed to try to finalise the MAP part for approval in TSG SA#12 as Rel-4, and the IP part for Rel-5 (to be sent for information early to TSG SA). A new TS number was requested for the IP part, which was later confirmed as TS 33.210. A Rapporteur was required for TS 33.210, and delegates were asked to consider taking this responsibility during the meeting. Mr. Geir Koien agreed that he was willing to take this if nobody else volunteered. The report was then noted.

9.1 MAP security (draft TS 33.200)

TD S3-010149 Update information - TS 33.200 and TS 33.200 version 0.5.0: The update information was noted and the draft TS was considered section by section, moving on to any contributions related to each section:

> TD S3-010228 LS from CN WG4 on MAP security: CN WG4 asked SA WG3 to change the granularity of the protection profile assumption, reached at the NDS ad-hoc meeting, to the component level. CN WG4 also prepared CRs to remove the MAP Security work from their Rel-4 specifications, which they intended to present to TSG CN #12 if the issues are not resolved by SA WG3 and the NDS-MAP document not finalised in time for TSG SA #12 approval.
>
> There was a comment that the Rel-5 material in Annexes A and B should be removed and included in a TR, as it could be mis-interpreted as being a part of Rel-4 implementation. It was agreed to move Annex A to TR 33.800 which will be continued for the time being, in order to hold information moved out of the Rel-4 specification. In order to facilitate stabilisation of 33.200 for Rel-4, it was agreed that TR 33.800 will not be progressed and will be moved to Rel-5.
>
> There was discussion on the removal of Annex B, for Manual Key Management, as no agreement could be reached on the completeness of this ~~part~~Annex. It was agreed that at least some guidance was required on Manual Key Management. Contributions on Annex B were therefore requested to be provided during the meeting in order that the specification can be completed with a basic Manual Key Management system included.

For the remaining contributions on this subject, the contributions of major issues were concentrated upon.

TD S3-010189 Comments on TS 33.200 v050. This was presented by Siemens and proposes to:

Remove all Rel5 material from the normative sections. This was agreed.

Clean section 5.3 from the MAPsec DoI parts and rename it. This was agreed.

Review and clean-up the Annexes, Annex B was recognised as an open issue. It was agreed to move Annexes A and C to TR 33.800.

Review the MAP SA definition of annex A.3.4 and complete MAP SA definition in section 5.3.2. Contributions were requested for this at the meeting.

Provide a definition for both the integrity algorithm and the encryption algorithm. Contributions were requested for this at the meeting.

Evaluate MAP protection Profiles and Protection Groups. This was done by consideration of the CN WG4 recommendations in TD S3-010192.

Clarify definitions: e.g. Local key distribution, UMTS network Domain, manual Interdomain SA. This was done in the editing sessions.

Clarify whether the interfaces table 2 is normative or informative. This was done in the editing sessions.

Include fallback to Unprotected Mode Indicator, and MAP SA handling. Contributions were requested for this at the meeting.

TD S3-010218 33.200 (MAP) v0.5.0. Comments provided by Alcatel: These comments were covered by other contributions and the proposals used in the editing sessions.

TD S3-010214 Proposed changes to 33.200v0.5.0: This was provided by Vodafone. It proposed that MAP DoI should be removed and included in a self-contained document. For the MAPsec encryption algorithm, the choice of Block or Stream cipher mode was an open issue. It was agreed that stream cipher should be chosen as it is available now, and the block cipher could be added later, when available and if required, as an option.

TD S3-010197 Use of Combined TVP/IV parameter. This was presented by Ericsson and provided the structure for IV as agreed at the NDS ad-hoc meeting. This was used in conjunction with TD S3-010190.

TD S3-010190 Structure of Initialisation Vector in MAPsec: This was presented by Siemens. It was agreed that the NE-Id numbering should be standardised, in order to ensure uniqueness of IVs, this should be considered by delegates for further contribution. The IV padding rule also requires standardisation and consideration. The possibility to reduce the length of the TVP transmitted by utilisation of the node synchronisation should also be considered. The length of the TVP had been defined as 4 bytes, but other lengths should be considered for definition.

The proposal of TD S3-010197, modified by those in TD S3-010190 were discussed and the significant points taken as a basis for the editing sessions.

TD S3-010192 Protection Profiles for MAP Security: This was presented by Siemens and assumed that single operators will have a single PLMN ID for both their GSM networks and UMTS Networks. In this ID could be used as a Network Domain ID. This was agreed as the assumption that SA WG3 would work on.

It was clarified that MAPsec applies only to MAP version 3, and not to MAPv2 or MAPv1, and therefore the Security context needs to be defined for MAPv3. The proposal of the contribution was agreed as an acceptable basis for the Protection Profiles part of 33.200, and it was noted that the Protection Profiles need to be completed.

The rapporteur for TS 33.200 agreed to take into account the following contributions in an editing session with the help of concerned parties: TD S3-010197, TD S3-010190, TD S3-010192, TD S3-010214, TD S3-010216.

Several editing sessions were held to progress the document for network aspects and algorithm aspects (to study which ISO algorithms to refer to) in parallel in order to progress faster. Interim versions of the specification were provided in TD S3-010149, TD S3-010257, TD S3-010258 and TD S3-010277. The results of both sets of sessions presented to the full SA WG3 group in TD S3-010294 and TD S3-010295 and presented to the full SA WG3 group for approval. It was noted that message flows were intended to be added and other editors notes may remain for improvement later. The document was then approved by SA WG3.

M. Pope will receive the final version from G. Koein and produce version 1.0.0 to send to TSG SA list by e-mail for information, and update again to version 2.0.0 for presentation to TSG SA for approval at TSG SA meeting #12 (June 2001).

9.2 IP network layer security (draft TS 33.210)

TD S3-010147 (NDS/IP Parts) - Rapporteur for TS 33.xxx: Geir Koien, Telenor volunteered to keep rapporteurship for this new document and this was welcomed by SA WG3. It was planned to present the TS to TSG SA for information in September, if it is to be approved and under change control in December 2001. This was considered a little over-ambitious given the other work that SA WG3 need to deal with for Rel-5 and recent slow progress of this work. Some contributions had been provided to the meeting which should help with progress. It was agreed that the final date should be updated to March 2002, and the WI descriptions for all NDS WIDs were updated and presented in TD S3-010275 and TD S3-010276 which were updated in TD S3-010285 and TD S3-010286 (see agenda item 7.1).

TD S3-010148 Introduced by the NDS Rapporteur, and relevant contributions were taken as the document was reviewed. Contributions were invited to help finalise the document in good time.

> TD S3-010203 Proposed changes to 33.xxx NDS IP Security about interfaces. This was introduced by Nokia, and proposes the addition of Mw and Mm interfaces for SIP support. Other interfaces may be affected but this required further study. This proposal was agreed.
>
> TD S3-010176 NDS architecture for IP-Based protocols. This was introduced by Motorola and proposes a centralised inter-domain SA negotiation. The proposed modifications to the draft were provided in TD S3-010178. There was some discussion over this proposal, and the claim of improved efficiency required verification. A related contribution in TD S3-010198 was also considered:
>
> > TD S3-010198 GTP security issue. This was presented by France Telecom and proposed that the protection of the signaling messages between the SGSN and GGSN is done end to end when roaming in order to guarantee the security of operators' networks for Rel-5, guarding against hackers breaking into Border Gateways and sending valid messages over the protected link between networks.
>
> The Chairman remarked that he was reluctant to change anything in the established architecture, as this would cause delays on this work, which is already delayed to March 2002, and with a lot of work to complete. It was agreed to leave this for the time being and move on to other contributions.
>
> TD S3-010191 Mandate 3DES for use of ESP with GTP-C. This proposes to use 3DES instead of AES for GTP-C confidentiality, in order to re-use existing products. It was argued that AES could be very common by the time Rel-5 is implemented and this proposal may lose the advantages of using it. It was considered premature to mandate the use of 3DES when AES is expected to be chosen as a replacement by the IETF. In view of the delay added to the target for the NDS/IP document, this may no longer be necessary and it was agreed that this should not be considered at the moment.
>
> TD S3-010201 Proposed changes to 33.200 about Za, Zb, Zc interfaces. This was introduced by Nokia and provided changes to the document to include the multiple SEG description to avoid a single point of failure. It was agreed that the description about multiple physical SEGs was not relevant to the stage 2 and this should not be included. Some minor modifications for the text on implementation of the Zb interface and clarifications were suggested (e.g. note 2 should remain until the document is near finalised), and the updated proposals were accepted. The overall security with the allowed implementation options should be considered during the editing of the document. It was agreed that Za (inter domain interface) is mandated and to consider the status of the Zb and Zc interfaces for further contribution.

TD S3-010204 Proposed changes to 33.xxx about protecting user plane traffic. This was presented by Nokia and mainly proposes to allow security domain operators to use NDS procedures to protect GTP-U. There was argument that the protection of the user-plane data would produce a large overhead and therefore had been forbidden. It was agreed that this should be considered at a later date in order to focus on signalling plane data protection.

TD S3-010202 Proposed changes to 33.200 about firewalls. This was presented by Nokia and proposes including some simple filtering on the input to the SEG to reject e.g. non-operator addressed traffic. This principle was accepted, although the text should be softened.

The editor was then asked to update the document off-line.

9.3 IM subsystem security (draft TS 33.203)

TD S3-010199 Integrity protection for SIP signalling. This was presented by Ericsson. The concern raised by Nokia on e.g. Multiple SIP clients on a laptop computer and the MS having the same IP address, causing packets to be~~ing~~ mixed up, was reported not to be a problem, as in the IP model, MSs need to have different IP addresses and Port numbers. The assumption that ESP would be appropriate and that security associations could be bound to port numbers needs to be studied.

It was reported that IPsec does not work well with Network Address Translators (NATs), and a solution which can cope with IPv4 should be sought in case of problems.

Cryptographic Message Syntax (CMS) was considered to be high on overhead and contains many features that are not needed by the 3GPP system. A solution to select only the required parts of CMS in order to develop a protocol with smaller overhead should also be investigated. It was noted that syntax is normally outside the SA WG3 scope, and was also a CN WG1 issue, so that the SA WG3 and the CN WG1 points should be separated for discussion in relevant groups. The contribution was then noted.

TD S3-010200 Proposal to use a generic authentication scheme for SIP. This was presented by Ericsson, and an AKA draft was attached. The contribution compares SIP AKA, SIP EAP and SIP SASL approaches for authentication and concluded that EAP and SASL were good candidates, but that all need some standardisation work to be done in the IETF.

Ericsson agreed to provide an updated contribution including the agreements reached, which would require an extension in the IETF. The stability of the RFC was questioned and it was considered that due to the increasing use (e.g. in wireless LAN networks) the RFC is likely to remain in the future.

It was recognised that the IETF would have to be informed that the proposed requirements would be used for 3GPP Security and therefore they should seriously consider the mechanism for inclusion.

The dependency of the SA WG3 specifications on the IETF documents which are under development would need to be considered, as late changes or future modification by the IETF could cause problems with the 3GPP implementations. **The Chairman agreed to take this to TSG SA as an issue for advice on how this problem should be handled in general within 3GPP**.

An updated version of TD S3-010200 containing the current assumptions agreed by SA WG3 was created by Ericsson in TD SP-010263 which was presented and agreed as an input to 33.203. A related LS in TD S3-010262 to CN WG1 and CN WG4 (and also copied to SA WG2) was presented. This was discussed and updated in TD S3-010287 and approved. The Chairman agreed to provide a LS to SA WG2 confirming the decision to terminate the authentication check in the S-CSCF.
<Secretary Note: HAS THIS BEEN PRODUCED? - WHICH TD NUMBER ?>

TD S3-010211 33.203v0.3.0 - Access security for IP-based services (Rel-5). This provided the changes since the previous version taking into account changes agreements at the IMS ad-hoc meeting in April 2001. The document was reviewed and relevant contributions discussed when relevant:

TD S3-010205 Authentication aspects in IM. This was introduced by BT, and concludes that the ability to authenticate at any time would give the operator the same flexibility as 3G Release 1999 and that this flexibility should be available within the IM in the Rel-5 timeframe.

It was reported by AT&T that SA WG2 had discussed the re-registration on IM sessions, and had concluded that it was not a user-friendly procedure, and long session times are foreseen for IMS. It was explained that re-registration frequency would be an operator value, and the

mechanisms for this were currently being discussed.

TD S3-010203 Proposed changes to 33.xxx NDS IP Security about interfaces. This was introduced by Nokia, and proposes the addition of Mw and Mm interfaces for SIP support. Other interfaces may be affected but this required further study. This was reconsidered under agenda item 9.2.

It was reported that Ericsson had withdrawn their proposals for termination of authentication in the HSS. The SA WG3 Chairman had written a letter to SA WG2 Chairman stating that he had instructed the group as follows:

Ericsson and Siemens to try to find a mutually acceptable solution, if no agreement is reached, then SA WG2 were asked to look for compelling architectural reason to favour one proposal over the other. If no compelling reason is found, then the SA WG3 Chairman would make a decision at S3#18 meeting.

TD S3-010209 LS from SA WG2 on the termination of authentication in the IMS (S2-011528). This LS informed SA WG3 that SA WG2 had discussed the termination of authentication and concluded that it should terminate in the S-CSCF. Ericsson pointed out that this was not based on a compelling architectural reason, although they did not contest the decision to terminate in the S-CSCF as they had come to agreementnet with Siemens in order to progress the IMS work. Siemens agreed that some information flows were still required. The LS was then noted.

TD S3-010208 The CR in S2-011524 was noted, and a document number for the references to the IP-based access security document would be provided was provided in a response LS, in TD S3-010265 which was approved.

TD S3-010249 Liaison Statement from CN WG1on the IM Call Transfer service. This was introduced by BT and it requesteds SA WG3 to review the IM Call transfer service message flows with a view to potential fraud problems and to respond to CN WG1 by their meeting, 10 July 2001. The flows in the attachment were considered briefly, but it was considered better to receive an explaination of the flows from a CN WG1 expert. A LS requesting this at SA WG3 meeting #19 was produced in TD S3-010266, which was updated in TD S3-010292 and approved. **This LS will be sent to the CN WG1 Chairman**.

TD S3-010219 Integrity protection mechanism between UE and P-CSCF. This was presented by Nokia and proposes a method to provide integrity protection by a method similar to the one used in UTRAN and the message authentication code function can be defined to be the Kasumi f9. This was discussed and it was recognised that this could be used in conjunction with other contributions in order to obtain a good basis for further work. It was agreed that the whole SIP message will be protected. ***Interested parties were asked to get together and elaborate a joint proposed solution***.

TD S3-010220 Integrity protection of the IMS registration. This was presented by Nokia and reports on potential lack of integrity protection on certain registration messages and problems with performance aspects for authentication to protect these which need to be studied. After some discussion, Nokia agreed to work with Ericsson and other interested parties in order to complete the details, detail the issues and clarify the security implications for the SA WG3 meeting #19.

TD S3-010160 Proposed Reply LS for " IM User Identities " (S2-010757): This LS had been presented in the joint meeting with SA WG2 in April 2001, and was considered by SA WG3. It was clarified that the "Proposed" in the title was an editorial error, and the reply had been approved at SA WG2. It was agreed to include a response to this in TD S3-010231 which was provided by Siemens and was revised in TD S3-010291 and then approved.

TD S3-010250 Liaison Statement from CN WG1 on " Handling of ICMP messages by 3GPP SIP Implementations". This LS asked SA WG3 whether the 3GPP SIP implementation should handle the ICMP messages as recommended in RFC 2543, or be ignored by the 3GPP SIP implementation. It was agreed that it was never the intention to protect ICMP messages. A response LS was drafted in TD S3-010274 which was approved.

9.4 GERAN security

TD S3-010150 Revised working assumptions made at the joint TSG GERAN / TSG SA WG3. This provided the agreements for working assumptions that were made at the Joint ad-hoc meeting in April 2001. The proposal to use 32-bit MAC protection for messages which this would not cause additional segmentation and therefore not adversely affect the efficiency, and to use a shorter MAC length for other messages was discussed. It was recognised that the RLC/MAC Messages could not be integrity protected, and this was noted as a weakness of the GERAN compared to UTRAN, as protection had not been designed in from the beginning. Some questions were asked of SA WG3 in the document:

Q1	Can a shorter MAC-I be used for RRC messages?
A1	No
Q2	How is ciphering/integrity provided when the Controlling RAN is different from the Serving RAN node?
A2	This is open for further study (Keys need to be provided to both the Controlling and Serving RAN nodes).
Q3	What identity is used to page a MS?
A3	The MS is paged as available in the order: TMSI/PTMSI; IMSI; IMEI.

The SA WG3 Chairman agreed to provide a response LS to GERAN on the length of MAC for message protection and with the answers to the questions, which was provided in TD S3-010247. Delegates were asked to consider this overnight in order to update this Liaison if necessary before approval. The LS in TD S3-010247 was presented and approved.

9.5 End-to-end security

TD S3-010210 Hybrid sync-frame/sync-free E2E Encryption. This was provided by Lucent. The Chairman asked which companies supported the work item, and it was agreed that this should be postponed until the number of supporting companies is enough. These TDs will be input to SA WG3 meeting #19 if enough companies support the work item.

TD S3-010222 Updated Work Item Description for Network based end-to-end security: This was presented by Ericsson and proposes to restrict the scope of end-to-end encryption to IP-based services. BT and Nortel had withdrawn their support, and Motorola had been added, but the status of GemPlus support was not known. There was therefore no Rapporteur for this WI. It was agreed that the required support would be needed before SA WG3 continue with this contribution. Ericsson will check if they support this work, given the withdrawal of the other companies. Support was requested to be confirmed during the meeting in order to progress this WI. **Support is requested for this WI for re-assessment at SA WG3 meeting #19.**

9.6 MExE security

There were no contributions on this agenda item ~~m~~(see also agenda item 7.1).

9.7 OSA security

Contributions for this work item were expected at SA WG3 meeting #19.

9.8 FIGS/IST

There was a proposal to extend FIGS to include the PS domain, but no progress had been made on this so far. Contributions need to be provided to SA WG3 meeting #19. It was agreed that the timescales would need to be reviewed in order to make the deadline more realistic. P. Howard provided a proposal for this update in TD S3-010246. This was presented under agenda item 7.1.

9.9 UE Split

TD S3-010158 Liaison Statement from SA WG1 on UE Functionality Split: This LS points out various scenarios where the basic security was thought to be vulnerable. It was agreed that a joint meeting should be held with SA WG1, T WG2, T WG3, SA WG2 and CN WG1 in order to discuss this, with an early version of the Report for information, as a basis for discussion. A suggested time and venue was made as 3 July 2001, in London, before the SA WG3 meeting #19. A LS to inform the groups of this proposal was provided in TD S3-010289 (approved, see agenda item 9.3).

TD S3-010207 LS from T WG2 concerning reviews of UE Functionality Split: T WG2 informed SA WG1 that they were willing to send delegates to the SA WG1 ad-hoc meeting in the week of 25 June, Dallas, USA. Although SA WG3 delegates would not be able to attend this meeting, it was thought that this could provide useful input to SA WG3 meeting #19. SA WG1 were therefore asked to provide input from this meeting to SA WG3, which would be included in TD S3-010289 (see discussion of TD S3-010158, above).

TD S3-010252 This was a duplication of TD S3-010207, above and was withdrawn.

TD S3-010165 Response from T WG3 to LS (T2-000793) on discussion document on UE functionality split over physical devices: This LS was noted. **M Walker agreed to talk to the SA WG1 Chairman** (K. Holley) to clarify that SA WG3 consider this to be a direct violation of the Security Architecture requirements, which would need a complete redesign to accommodate the proposals, in order to help prevent the WGs doing work which would not be acceptable from a security viewpoint, and thus wasting time.

TD S3-010175 UE Split over several Devices: This contribution was presented by Orange and provided some proposals for a Bridging Function to control access authentication of multiple USIMs. It also raised some of the issues of the proposal. This was discussed, and the Chairman agreed to draft a LS to T WG3, SA WG1 and T WG2 to point out the security concerns and to suggest a joint meeting on 3 July 2001. This was provided in TD S3-010289.

TD S3-010280 Presented by Stewart Ward and Colin Blanchard as a personal contribution. The idea of a bridge module, which would act like a visited network, requesting AVs and authenticating the users in the same way as a Visited Network would, required some consideration. The contribution was noted, and delegates asked to contribute on this at future meetings, before SA WG3 formally endorse it for forwarding to other groups.

TD S3-010279 LS to T WG3 on Security and UE functionality split. This was introduced by the SA WG3 Chairman and discussed. It proposes a joint meeting between SA WG3, SA WG1, T WG3 and T WG2 on 3 July 2001, before SA WG3 meeting #19 in London, UK. This was updated in TD S3-010289 which was approved.

TD S3-010248 This was withdrawn as it was covered by TD S3-010289.

10 Election of S3 chair and vice chairs

The Candidates for Chairman and Vice Chairmen were as follows:

Chairman: Michael Walker (Vodafone, ETSI)

Vice Chairmen: Michael Marcovici (Lucent, T1) and Valtteri Niemi (Nokia, ETSI)

These candidates were therefore appointed to the posts, without the need for a Vote. All were congratulated and welcomed by SA WG3.

10/1 Approval of CRs and LSs from the meeting

See Annexes D and E for a full list of incoming LSs, approved outgoing LSs and approved CRs.

11 Future meeting dates and venues

Meeting	Date	Location	Host
Joint S1, S2, T3, S3 meeting	3 July 2001	London	Vodafone
S3#19	4 - 6 July 2001	London	Vodafone
S3#20	15 or 16 – 18 October 2001	Sydney, Australia	Qualcomm Int.
S3#21	3 - 5 December 2001	Sophia Antipolis, France	ETSI
S3#22	26 - 28 February 2002	Bristol, UK	Orange
S3#23 + AHAG	14 - 16 May 2002	Canada / NW USA	AT&T Wireless
S3#24	9 - 11 July 2002	Helsinki, Finland (TBC)	Nokia
S3#25	15 - 17 October 2002	Munich, Germany (TBC)	Siemens (TBC)

12 Any other business

There were no other topics raised under this agenda item.

The procedure for the approval of 33.200 Rel-4 was agreed as follows:

The Rapporteur will update the document with the agreements reached, amalgamating the two updated documents drafted in parallel sessions and send to M. Pope. Mr. Pope will update the document editorially into correct 3GPP TS format as version 1.0.0 and send to the TSG SA e-mail list for information. The document will then be updated to version 2.0.0 by Mr. Pope for submission to TSG SA#12 Plenary for approval as Rel-4 (assuming no adverse comments are received on the version 1.0.0).

13 Close of meeting

The Chairman thanked the Host, Motorola, for the excellent venue and services for the meeting, the delegates for their very hard work and good co-operation in the difficult task of finalising TS 33.200 for Rel-4, and congratulated the new Vice Chairmen, Valtteri Niemi on his appointment, Michael Marcovici on his re-appointment, and closed the meeting.

Annex A: List of attendees at the SA WG3#18 meeting

Name	Company	e-mail	3GPP ORG
Mr. Hiroshi Aono	NTT DoCoMo Inc.	aono@mml.yrp.nttdocomo.co.jp	ARIB
Mr. Jari Arkko	ERICSSON L.M.	jarkko@piuha.net	ETSI
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	ETSI
Ms. Tao Bu	Nokia Corporation	tao.bu@nokia.com	ETSI
Dr. Stephen Billington	Hutchison 3G UK Limited	stephen.billington@hutchington3g.com	ETSI
Mr. Colin Blanchard	BT	colin.blanchard@bt.com	ETSI
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI
Mr. Krister Boman	ERICSSON L.M.	krister.boman@emw.ericsson.se	ETSI
Mr. Charles Brookson	DTI	cbrookson@iee.org	ETSI
Mr. Daniel Brown	Motorola Inc.	adb002@email.mot.com	T1
Mr. David Castellanos	ERICSSON L.M.	david.castellanos-zarrora@era.ericsson.se	ETSI
Ms. Lily Chen	T1 Standards Committee	lchen1@email.mot.com	T1
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB
Mr. Brian K. Daly	AT&T Wireless Services, Inc.	brian.daly@attws.com	T1
Dr. Adrian Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI
Miss Jessica Gunnarsson	TELIA AB	jessica.l.gunnarsson@telia.se	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI
Miss Janette Huntington	Motorola Inc.	P28213@email.mot.com	T1
Mr. Tom Inklebarger	AT&T Wireless Services, Inc.	tominkle@home.com	T1
Mr. Geir Køien	TELENOR AS	geir-myrdahl.koien@telenor.com	ETSI
Mrs. Tiina Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI
Mr. Alexander Leadbeater	BT	alex.leadbeater@bt.com	ETSI
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com	T1
Mr. Sebastien Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@francetelecom.com	ETSI
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI
Mr. Petri Nyberg	SONERA Corporation	petri.nyberg@sonera.com	ETSI
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com	ETSI
Mr. Olivier Paridaens	ALCATEL S.A.	olivier.paridaens@alcatel.be	ETSI
Mr. Frank Quick	QUALCOMM EUROPE S.A.R.L.	fquick@qualcomm.com	ETSI
Mr. Greg Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	ETSI
Mr. Dewayne Sennett	AT&T Wireless Services, Inc.	dewayne.sennett@attws.com	T1
Mr. Teruharu Serada	NEC Corporation	serada@aj.jp.nec.com	ARIB
Mr. Hugh Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1
Mr. Benno Tietz	MANNESMANN Mobilfunk GmbH	benno.tietz@d2vodafone.de	ETSI
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)	valerius@nortelnetworks.com	ETSI
Prof. Michael Walker	VODAFONE Group Plc	mike.walker@vf.vodafone.co.uk	ETSI
Mr. Stuart Ward	ORANGE PCS LTD	stuart.ward@orange.co.uk	ETSI
Dr. Peter Windirsch	Deutsche Telekom AG	Peter.Windirsch@t-systems.de	ETSI
Dr. Ernest Woodward	Intel Sweden AB	ernest.e.woodward@intel.com	ETSI
Tom Defray ???	PLEASE CHECK AND CORRECT/UPDATE		

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010140	Draft agenda for meeting #18	SA WG3 Chairman	2	Approval		Approved
S3-010141	Draft report of meeting #17	Secretary	4.1	Approval		Approved
S3-010142	Response to LS (S1-010144) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT	SA WG1	5.3.1	Discussion		Noted. TD166 reports no problem.
S3-010143	Draft report of NDS ad-hoc, April 23-24 April 2001	Secretary	4.2	Information		Approved
S3-010144	Draft report of aSIP ad-hoc, April 25 2001	Secretary	4.2	Information		Approved
S3-010145	Draft report of SA WG3/SAWG1 IMS joint session, April 26 2001	Secretary	4.2	Information		Approved
S3-010146	Draft report of SA WG3/GERAN joint meeting, April 27 2001	Secretary	4.2	Information		Approved
S3-010147	Status report for NDS	NDS Rapporteur	9.1	Information and decision		Noted. Used for editing sessions
S3-010148	Update information on TS33xxx (NDS-IP) (from TS33200 v035) and 33.ndsIP v 0.5.0	NDS Rapporteur	9.2	Information and discussion		Checked and contributions provided. Spec to be updated by Rapporteur
S3-010149	Update information –TS 33.200 (NDS-MAPSec) and 33.200 v.0.5.0	NDS Rapporteur	9.1	Information and discussion		Noted. Used for editing sessions
S3-010150	Revised working assumptions made at the joint TSG GERAN / TSG SA WG3 (GAHW-01 0245)	TSG-GERAN Adhoc#5	5.3.5 / 9.4	Discussion		CR in TD236. Response in TD247
S3-010151	Re-transmission of authentication requests	CN WG1	5.3.2	Discussion		Response in TD230
S3-010152	LS on "Security for IM SIP session Signaling" (N1-010588)	CN WG1 Joint SIP ad-hoc	5.3.2	Dicussion		Response in TD291
S3-010153	LS on THRESHOLD check at RRC connection establishment (R2-010981)	RAN WG2	5.3.4 / 5.3.6	Dicussion		Corresponding CR in TD196. Corresponding response from N1 in TD234. Noted.
S3-010154	LS on Wrap around of the calculated START value (R2-010982)	RAN WG2	5.3.4	Discussion		Response in TD278
S3-010155	Response to LSs related to optimised IP speech and header removal support in GERAN (R3-010890)	RAN WG3	5.3.4	Information		Noted.
S3-010156	LS on basic and advanced services examples (S1-010271)	SA WG1	5.3.1	Information		Noted.
S3-010157	LS on Extended Streaming Service (S1-010501)	SA WG1	5.3.1	Information		Response in TD293

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010158	Liaison Statement on UE Functionality Split (S1-010575)	SA WG1	9.9	Discussion		Agreed that a JM is needed. Response LS in TD289
S3-010159	LS regarding User Profile (S1-010591)	SA WG1	5.3.1	Discussion		Noted. Response LS in TD225
S3-010160	Proposed Reply LS for " IM User Identities " (S2-010757)	SA WG2	5.3.1, 9.3	Discussion		Response in TD291
S3-010161	Proposed Liaison to S3 on use of Diameter (S2-010758)	Lucent	5.3.1	Discussion		Noted.
S3-010162	RE : LS on authentication test algorithm to be implemented in test USIMs (T3-010246)	T WG3	5.3.3	Discussion		See also S3-010167. Noted.
S3-010163	Rejection of 2G Authentication and Key Agreement by 3G ME with USIM in UTRAN (T3-010379)	T WG3	5.3.3	Discussion		Agreed. Response in TD232
S3-010164	LS for "IM Subsystem Address Storage on USIM " (T3-010193)	T WG3	5.3.3	Information		Noted.
S3-010165	Response to LS (T2-000793) on discussion document on UE functionality split over physical devices (T3-010250)	T WG3	9.9	Discussion		M Walker to talk to S1 Chairman to prevent time wasted on insecure work
S3-010166	Response to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT (T3-010323)	T WG3	5.3.3	Discussion		Noted.
S3-010167	LS on authentication test algorithm to be implemented in test USIM (T3-010324)	T WG3	5.3.3	Discussion		See also S3-010162. Noted.
S3-010168	LS in reply to LS on MExE and User Equipment Management - T2-000756 (S5-010114)	SA WG5	5.3.1	Information		Noted.Response in TD293. Updated WI in TD226
S3-010169	Canidature for Vice Chairman - Valter Niemi, Nokia	Nokia	10	Information		Elected as VC
S3-010170	Canidature for Vice Chairman - Michael Marcovici, Lucent	Lucent	10	Information		Elected as VC
S3-010171	Canidate for Chairman - Michael Walker - Vodafone	Vodafone	10	Information		Elected as Chairman
S3-010172	User Profiles (S1-010435)	Ericsson LM	5.3.1	Discussion		Attachment to S3-010159. Noted
S3-010173	LS to SA WG3 on security in IP-transport based UTRAN (R3-011081)	RAN WG3	5.3.4	Approval		Noted.
S3-010174	Proposed new SA4 Work Item on Extended Streaming Service (S4-010304 attached)	SA WG4 Chairman	5.3.1	Discussion		Response in TD293
S3-010175	UE split over several devices	Orange	9.9	Discussion		Discussed. LS on security concerns produced in TD289
S3-010176	NDS architecture for IP-Based protocols	Motorola Inc.	9.2	Discussion and decision		Used to update 33.210 draft

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010177	WITHDRAWN - Change Request for "TS33.200 Network Domain Security v032"	Motorola Inc.	9.1	Discussion and decision		Withdrawn due to split of TS 33.200
S3-010178	Change Request for "TS33.xxx Network Domain Security: IP Network Layer Security"	Motorola Inc.	9.2	Discussion and decision		Used to update TS 33.210 draft
S3-010179	Proposed CR to 33.102 v3.8.0: Correction to periodic local authentication	Siemens Atea	8.1	Approval		Approved as Cat F
S3-010180	Proposed CR to 33.102 v4.0.0: Correction to periodic local authentication	Siemens Atea	8.1	Approval		Approved as Cat A
S3-010181	Proposed CR to 33.102 v3.8.0: Correction to COUNT-C description	Siemens Atea	8.1	Approval		Approved as Cat F
S3-010182	Proposed CR to 33.102 v4.0.0: Correction to COUNT-C description	Siemens Atea	8.1	Approval		Approved as Cat A
S3-010183	Proposed CR to 33.102 v3.8.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	Nokia	8.1	Approval	S3-010240	Updated in TD240
S3-010184	Proposed CR to 33.102 v4.0.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	Nokia	8.1	Approval	S3-010241	Updated in TD241
S3-010185	Proposed CR to 33.103 v3.5.0: The multiplicity of Data integrity symbols	Nokia	8.2	Approval		Approved
S3-010186	Proposed CR to 33.103 v4.0.0: The multiplicity of Data integrity symbols	Nokia	8.2	Approval		Approved
S3-010187	Proposed CR to 33.105 v3.7.0: Deletion of the maximum size of a RRC message	Nokia	8.3	Approval		Approved
S3-010188	Proposed CR to 33.105 v4.0.0: Deletion of the maximum size of a RRC message	Nokia	8.3	Approval		Approved
S3-010189	Comments on TS 33.200 v050	Siemens Atea	9.1	Discussion and decision		Discussed and used for editing sessions
S3-010190	Structure of Initialisation Vector in MAPSec	Siemnes AG	9.1	Discussion and decision		Agreed proposal.
S3-010191	Mandate 3DES for use of ESP with GTP-C	Siemnes AG	9.2	Discussion and decision		Not to be considered at present.
S3-010192	Protection Profiles for MAP Security	Siemens Atea	9.1	Discussion and decision		Agreed assumption. Used in editing session.
S3-010193	LS from T WG1: Response to LS on authentication test algorithm in test USIM (T1-010231)	T WG1	5.3.3	Discussion		Covered by TD167, response in TD233
S3-010194	LS from T WG3 on New feature for SAT originated SMS (T3-010443)	T WG3	5.3.3	Discussion		Noted.

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010195	Proposed CRs to 33.102 R99 and Rel-4: Calculation and Wrap-around of START value	Ericsson	8.1	Approval	S3-010269, S3-010270	Updated in TD269, TD270
S3-010196	Proposed CRs to 33.102 R99 and Rel-4: THRESHOLD Check at RRC connection establishment	Ericsson	8.1	Approval	S3-010238	Updated in TD238
S3-010197	Use of Combined TVP/IV parameter	Ericsson	9.1	Discussion and decision		Used in conjuntion with TD190. Used in editing session
S3-010198	GTP security issue	France Telecom	9.2	Discussion and decision		Should be considered for future development
S3-010199	Integrity protection for SIP signaling	Ericsson	9.3	Discussion and decision		Discussed and noted.
S3-010200	Proposal to use a generic authentication scheme for SIP	Ericsson	9.3	Discussion	S3-010263	Chairman to ask SA how to work with IETF
S3-010201	Proposed changes to 33.200 about Za, Zb, Zc interfaces	Nokia	9.2	Discussion and decision		Za agreed. Zb and Zc for future study.
S3-010202	Proposed changes to 33.200 about firewalls	Nokia	9.2	Discussion and decision		Accepted in principle, text should be softened.
S3-010203	Proposed changes to 33.xxx NDS IP Security about interfaces	Nokia	9.3 / 9.2	Discussion and decision		Proposal agreed.
S3-010204	Proposed changes to 33.xxx about protecting user plane traffic	Nokia	9.2	Discussion and decision		User plane protection to be considered at a later date.
S3-010205	Authentication aspects in IM	BT	9.3	Discussion and decision		Discussed and used for input to 33.203
S3-010206	TR-45 / 3GPP Joint AKA Control	TR-45/AHAG	6.1	Discussion		Approved. SA3 Chair to forward to SA for endorsement
S3-010207	LS Concerning Reviews of UE Functionality Split	T WG3	9.9	Discussion		Input requested to S3#19 in LS TD289
S3-010208	LS from SA WG2 on Security Associations for IMS functional elements (S2-011573)	SA WG2	9.3	Discussion / Decision		Provided by Motorola. Response in TD265
S3-010209	LS from SA WG2 on the termination of authentication in the IMS (S2-011528)	SA WG2	9.3	Discussion / Decision		Provided by Motorola. Noted.
S3-010210	Hybrid sync-frame/sync-free E2E Encryption	Lucent	9.5	Discussion		Postponed until enough supporting companies.
S3-010211	33.203 v 0.3.0: Access security for IP-based services (Rel-5)	Rapporteur	9.3	Discussion		Reviewed for update and other contributions discussed as appropriate.
S3-010212	WID: Access security for IP-based services		7.1		S3-010239	Updated in TD239 and then TD283
S3-010213	Report to SA3 on SA#11		5.2			Noted.
S3-010214	Proposed changes to 33.200v0.5.0	Vodafone	9.1			Discussed and used for editing sessions

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010215	The MAP Security Domain of Interpretation for ISAKMP	Ericsson	9.1			
S3-010216	Corrections to 33.200		9.1			Used for editing sessions
S3-010217	WITHDRAWN (dup of TD 210)					
S3-010218	33.200 (MAP) v0.5.0	Alcatel	9.1			Discussed and used for editing sessions
S3-010219	Integrity protection mechanism between UE and P-CSCF	Nokia	9.3			Needs further study
S3-010220	Integrity protection of the IMS registration	Nokia	9.3			Revisit at S3#19. Nokia Ericsson and interested parties to discuss and contribute.
S3-010221	Presentation on MAPSEC DOI Version -02	Ericsson	9.1			
S3-010222	Updated Work Item Description for Network based end-to end- security	Ericsson	9.5	Approval		Support requested at S3#19.
S3-010223	comments on draft-arkko-map-doi-01.txt		9.1			
S3-010224	Report of TSG-T3 Ad Hoc Meeting #37 (Joint with TSG-S3)	T WG3 Secretary	4.3	Information		Noted
S3-010225	LS to SA WG1: Reply LS on streaming and user profile	SA WG3	9.5	Approval	S3-010281	Updated in TD281
S3-010226	Response to LS S5-010114 (S3- 010168) on MExE and User Equipment Management	SA WG3	9.6	Approval		Approved.
S3-010227	Revised MExE Security Analysis Activity WID	SA WG3	7.1	Approval	S3-010288	Updated in TD288
S3-010228	LS from CN WG4 on MAP security (N4-010669)	CN WG4	9.1	Discussion		Noted. Used for editing sessions of NDS.
S3-010229	Report of LI meeting, Clearwater	SA WG3-LI Chairman	5.1			Noted
S3-010230	Reply LS on the handling of retransmitted authentication requests	SA WG3	10.1			Approved.
S3-010231	Reply to the following LSs: LS on "Security for IM SIP session Signaling" (Tdoc N1-010588, received as S3-010152) AND LS on " IM User Identities" (Tdoc S2-010757, received as S3-010160)	SA WG3	10.1		S3-010291	Updated in TD291
S3-010232	Reply to LS on rejection of 2G authentication and key agreement by 3G ME with USIM in UTRAN	SA WG3	10.1	Approval		Approved.
S3-010233	Reply LS on authentication test algorithm to be implemented in test USIM	SA WG3	10.1	Approval		Approved.
S3-010234	[DRAFT] Liaison Statement on THRESHOLD check at RRC connection establishment	CN WG1	5.3.4	Discussion		Noted

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010235	Draft Reply LS to RAN WG2 on Wrap around of the calculated START value	SA WG3	5.3.4	Approval	S3-010278	Updated in TD278
S3-010236	CR to 33.102 : Include reference to TS 43.041 GERAN Stage 2 specification	SA WG3	10.1	Approval		Approved as Cat B
S3-010237	Draft Reply LS on THRESHOLD Check at RRC connection establishment	SA WG3		Approval	S3-010273	Updated in TD273
S3-010238	CRs to 33.102 R99 and Rel-4: THRESHOLD Check at RRC connection establishment	SA WG3	5.3.6	Approval	S3-010272, S3-010271	Updated in TD272, TD271
S3-010239	WID: Access security for IP-based services	SA WG3	7.1	Approval	S3-010283	Updated time scales in TD283
S3-010240	Proposed CR to 33.102 v3.8.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	SA WG3	8.1	Approval		Approved as Cat F
S3-010241	Proposed CR to 33.102 v4.0.0: Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted.	SA WG3	8.1	Approval		Approved as Cat A
S3-010242	WITHDRAWN (not needed)					
S3-010243	WITHDRAWN (not needed)					
S3-010244	WITHDRAWN (not needed)					
S3-010245	WITHDRAWN (not needed)					
S3-010246	Revised FIGS/IST work item description	Vodafone	7.1	Approval		Approved.
S3-010247	Reply to LS on revised working assumptions made at joint GERAN/S3 meeting	SA WG3	10.1	Approval		Approved.
S3-010248	WITHDRAWN (covered by TD289)					
S3-010249	[DRAFT] Liaison Statement from CN WG1on the IM Call Transfer service	CN WG1	9.3	Discussion		Response to CN WG1 Chair in TD292
S3-010250	Liaison Statement from CN WG1 on " Handling of ICMP messages by 3GPP SIP Implementations"	CN WG1	9.3	Discussion		Response in TD274
S3-010251	WITHDRAWN (duplication of TD234)					
S3-010252	WITHDRAWN (duplication of TD207)					
S3-010253	Reply to LS on New feature for SAT originated SMS	T WG2	5.3.3	Discussion		Response to TD194. Noted.
S3-010254	Comments on MAPsec DOI –02 Internet Draft	Alcatel	-	Discussion		Postponed to S3#19
S3-010255	3GPP S3 Request for Clarification on Positive Authentication Reporting	AHAG	6.2	Discussion		Noted. To be progressed when the Rel-5 work has been progressed
S3-010256	UIM Authentication Method	AHAG	6.1	Discussion		Noted.
S3-010257	33.200 version 0.6.0	NDS Drafting group	9.1	Editing		Further edited

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010258	33.200 version 0.6.0 (as edited in morning drafting session)	NDS Drafting group	9.1	Editing		Further edited
S3-010259	LS from GSMA on Development of new A5/3	GSMA SG	5.5	Discussion		Response in TD282, including proposed update to Work Plan (TD261)
S3-010260	Reply to LS on the Development of new A5/3	SA WG3	5.5	Approval	S3-010282	Updated in TD282.
S3-010261	Provisional work plan for the design of the SAGE GSM A5/3 Task Force (SAGE GSM A5/3 TF)	KPN Research	5.5	Information		Noted. Proposed update to timescales in TD282
S3-010262	reserved for LS to CN1,N4,S2 on S3 assumptions for IMS/SIP (Ericsson)	SA WG3	10.1	Approval	S3-010287	Updated in TD287
S3-010263	Proposal to use a generic authentication scheme for SIP (rev of TD200)	Ericsson	9.3	Discussion		Agreed as input to 33.203.
S3-010264	WID Security aspects of requirements for Network Configuration Independence	AWS	7.11	Approval	S3-010284	Updated in TD284
S3-010265	Reserved for response LS to TD208	Peter H	10.1	Approval		Approved
S3-010266	Response to Liaison Statement on the IM Call Transfer Service N1-010890 (S3-010249)	SA WG3	10.1	Approval	S3-010292	Updated in TD292
S3-010267	Response LS to S1 LS Regarding User Profiles	SA WG2	5.3.1	Discussion		Joint Meeting invitation in TD278. Response LS in TD293
S3-010268	Reply LS on Wrap around of the calculated START value	SA WG3	10.1	Approval		Approved. TD269 and 270 attached
S3-010269	CR to 33.102 R99: Calculation and Wrap-around of START value	SA WG3	8.1	Approval		Approved. Attached to TD268
S3-010270	CR to 33.102 Rel-4: Calculation and Wrap-around of START value	SA WG3	8.1	Approval		Approved. Attached to TD268
S3-010271	CR to 33.102 Rel-4: THRESHOLD Check at RRC connection establishment.	SA WG3	8.1	Approval		Approved. Attached to TD273
S3-010272	CR to 33.102 R99: THRESHOLD Check at RRC connection establishment.	SA WG3	8.1	Approval		Approved. Attached to TD273
S3-010273	Reply LS on THRESHOLD Check at RRC connection establishment	SA WG3	8.1	Approval		Approved. TD271 and 272 attached.
S3-010274	Response to TD250 on ICMP protection	SA WG3	10.1	Approval		Approved.
S3-010275	Updated WIDs for NDS/MAP	NDS Rapporteur	7.1	Approval	S3-010285	Updated in TD285
S3-010276	Updated WIDs for NDS/IP	NDS Rapporteur	7.1	Approval	S3-010286	Updated in TD286
S3-010277	NDS-MAP drafting output 33.200v0.7.0	NDS Drafting group	9.1		S3-010294	updated in TD294
S3-010278	Invitation to joint meeting on User Profiles	SA WG1	5.3.1	Information		Response in TD293

TD number	Title	Source	Agenda	Document for	Replaced by	Comment
S3-010279	LS to T WG3 on Security and UE functionality split	SA WG3	10.1	Approval	S3-010289	Updated in TD289
S3-010280	UE Split over several Devices Version 2	S. Ward, C. Blanchard	9.9	Discussion		Noted.
S3-010281	Reply LS on extended streaming service and user profiles	SA WG3	5.3.1	Approval	S3-010293	Updated in TD293
S3-010282	Reply to LS on the Development of new A5/3	SA WG3		Approval		To check if approved?
S3-010283	WID: Access security for IP-based services	SA WG3	7.1	Approval		Approved
S3-010284	WID Security aspects of requirements for Network Configuration Independence	SA WG3		Approval		Approved
S3-010285	Updated WIDs for NDS/MAP	SA WG3		Approval		Approved
S3-010286	Updated WIDs for NDS/IP	SA WG3		Approval		Approved
S3-010287	reserved for LS to CN1,N4,S2 on S3 assumptions for IMS/SIP	SA WG3	10.1	Approval		Approved
S3-010288	Revised MExE Security Analysis Activity WID	SA WG3	7.1	Approval		Approved and attached to TD226
S3-010289	LS to T WG3 on Security and UE functionality split	SA WG3	10.1	Approval		Approved
S3-010290	WITHDRAWN (not needed)					
S3-010291	Reply to the following LSs: LS on "Security for IM SIP session Signaling" (Tdoc N1-010588, received as S3-010152) AND LS on " IM User Identities" (Tdoc S2-010757, received as S3-010160)	SA WG3	10.1	Approval		Approved.
S3-010292	Response to Liaison Statement on the IM Call Transfer Service N1-010890 (S3-010249)	SA WG3	10.1	Approval		Approved. Send toi CN WG1 Chairman
S3-010293	Reply LS on extended streaming service and user profiles	SA WG3	5.3.1	Approval		Approved
S3-010294	NDS-MAP final drafting output 33.200v0.8.0 Geir draft group	NDS Drafting group1		Agreement of update		Rapporteur to update main document for SA information
S3-010295	NDS-MAP final drafting output 33.200v0.8.0 Valtteri draft group	NDS Drafting group2		Agreement of update		Rapporteur to update main document for SA information
S3-010296						
S3-010297						
S3-010298						
S3-010299						

Annex D: List of CRs to specifications under SA WG3 responsibility

Note: SA WG3 agreed CRs to be presented to TSG SA#12 for approval.

Spec	CR	Rev	Phase	Subject	Cat	Cur Vers	WG meeting	WG TD	WG status	Acronym	Remarks
33.102	144		R99	Correction to periodic local authentication	F	3.8.0	S3-18	S3-010179	agreed	SEC1	
33.102	145		Rel-4	Correction to periodic local authentication	A	4.0.0	S3-18	S3-010180	Agreed	SEC1	
33.102	146		R99	Correction to COUNT-C description	F	3.8.0	S3-18	S3-010181	Agreed	SEC1	
33.102	147		Rel-4	Correction to COUNT-C description	A	4.0.0	S3-18	S3-010182	Agreed	SEC1	
33.102	148		Rel-5	Include reference to TS 43.041 GERAN Stage 2 specification	B	4.0.0	S3-18	S3-010236	Agreed	SEC1	Implement to version 4.1.0 when Rel-4 CRs are included
33.102	149		R99	Calculation and Wrap-around of START value	F	3.8.0	S3-18	S3-010269	Agreed	SEC1	
33.102	150		Rel-4	Calculation and Wrap-around of START value	A	4.0.0	S3-18	S3-010270	Agreed	SEC1	
33.102	151		R99	Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted	F	3.8.0	S3-18	S3-010240	Agreed	SEC1	
33.102	152		Rel-4	Correction to integrity protection when the user is attached to a UTRAN with R99+ ME with a SIM inserted	A	4.0.0	S3-18	S3-010241	Agreed	SEC1	
33.102	153		R99	THRESHOLD Check at RRC connection establishment	F	3.8.0	S3-18	S3-010272	Agreed	SEC1	
33.102	154		Rel-4	THRESHOLD Check at RRC connection establishment	A	4.0.0	S3-18	S3-010271	Agreed	SEC1	
33.103	014		R99	The multiplicity of Data integrity symbols	F	3.5.0	S3-18	S3-010185	Agreed	SEC1	
33.103	015		Rel-4	The multiplicity of Data integrity symbols	A	4.0.0	S3-18	S3-010186	Agreed	SEC1	
33.105	019		R99	Deletion of the maximum size of a RRC message	F	3.7.0	S3-18	S3-010187	Agreed	SEC1	
33.105	020		Rel-4	Deletion of the maximum size of a RRC message	A	4.0.0	S3-18	S3-010188	Agreed	SEC1	

Annex E: List of Liaisons

E.1 Liaisons to the meeting

TD Number	Title	Source	Comment
S3-010142	Response to LS (S1-010144) from T3 chairman on the Elaboration of KEY IDENTIFICATION EVENT	SA WG1	Noted. TD166 reports no problem.
S3-010150	Revised working assumptions made at the joint TSG GERAN / TSG SA WG3 (GAHW-01 0245)	TSG-GERAN Adhoc#5	CR in TD236. Response in TD247
S3-010151	Re-transmission of authentication requests	CN WG1	Response in TD230
S3-010152	LS on "Security for IM SIP session Signaling" (N1-010588)	CN WG1 Joint SIP ad-hoc	Response in TD291
S3-010153	LS on THRESHOLD check at RRC connection establishment (R2-010981)	RAN WG2	Corresponding CR in TD196. Corresponding response from N1 in TD234. Noted.
S3-010154	LS on Wrap around of the calculated START value (R2-010982)	RAN WG2	Response in TD278
S3-010155	Response to LSs related to optimised IP speech and header removal support in GERAN (R3-010890)	RAN WG3	Noted.
S3-010156	LS on basic and advanced services examples (S1-010271)	SA WG1	Noted.
S3-010157	LS on Extended Streaming Service (S1-010501)	SA WG1	Response in TD293
S3-010158	Liaison Statement on UE Functionality Split (S1-010575)	SA WG1	Agreed that a JM is needed. Response LS in TD289
S3-010159	LS regarding User Profile (S1-010591)	SA WG1	Noted. Response LS in TD225
S3-010160	Proposed Reply LS for " IM User Identities " (S2-010757)	SA WG2	Response in TD291
S3-010162	RE : LS on authentication test algorithm to be implemented in test USIMs (T3-010246)	T WG3	See also S3-010167. Noted.
S3-010163	Rejection of 2G Authentication and Key Agreement by 3G ME with USIM in UTRAN (T3-010379)	T WG3	Agreed. Response in TD232
S3-010164	LS for "IM Subsystem Address Storage on USIM " (T3-010193)	T WG3	Noted.
S3-010165	Response to LS (T2-000793) on discussion document on UE functionality split over physical devices (T3-010250)	T WG3	M Walker to talk to S1 Chairman to prevent time wasted on insecure work
S3-010166	Response to LS (S3-010128) on the Elaboration of KEY IDENTIFICATION EVENT (T3-010323)	T WG3	Noted.
S3-010167	LS on authentication test algorithm to be implemented in test USIM (T3-010324)	T WG3	See also S3-010162. Noted.
S3-010168	LS in reply to LS on MExE and User Equipment Management - T2-000756 (S5-010114)	SA WG5	Noted.Response in TD293. Updated WI in TD226
S3-010173	LS to SA WG3 on security in IP-transport based UTRAN (R3-011081)	RAN WG3	Noted.
S3-010174	Proposed new SA4 Work Item on Extended Streaming Service (S4-010304 attached)	SA WG4 Chairman	Response in TD293
S3-010193	LS from T WG1: Response to LS on authentication test algorithm in test USIM (T1-010231)	T WG1	Covered by TD167, response in TD233
S3-010194	LS from T WG3 on New feature for SAT originated SMS (T3-010443)	T WG3	Noted.

TD Number	Title	Source	Comment
S3-010208	LS from SA WG2 on Security Associations for IMS functional elements (S2-011573)	SA WG2	Provided by Motorola. Response in TD265
S3-010209	LS from SA WG2 on the termination of authentication in the IMS (S2-011528)	SA WG2	Provided by Motorola. Noted.
S3-010234	[DRAFT] Liaison Statement on THRESHOLD check at RRC connection establishment	CN WG1	Noted
S3-010249	[DRAFT] Liaison Statement from CN WG1on the IM Call Transfer service	CN WG1	Response to CN WG1 Chair in TD292
S3-010250	Liaison Statement from CN WG1 on " Handling of ICMP messages by 3GPP SIP Implementations"	CN WG1	Response in TD274
S3-010253	Reply to LS on New feature for SAT originated SMS	T WG2	Response to TD194. Noted.
S3-010255	3GPP S3 Request for Clarification on Positive Authentication Reporting	AHAG	Noted. To be progressed when the Rel-5 work has been progressed
S3-010256	UIM Authentication Method	AHAG	Noted.
S3-010259	LS from GSMA on Development of new A5/3	GSMA SG	Response in TD282, including proposed update to Work Plan (TD261)
S3-010267	Response LS to S1 LS Regarding User Profiles	SA WG2	Joint Meeting invitation in TD278. Response LS in TD293
S3-010278	Invitation to joint meeting on User Profiles	SA WG1	Response in TD293

E.2 Liaisons from the meeting

TD Number	Title	Status	To CC
S3-010226	Response to LS S5-010114 (S3- 010168) on MExE and User Equipment Management	Approved	**T WG2/MExE** **SA WG5**
S3-010230	Reply LS on the handling of retransmitted authentication requests	Approved	**CN WG1**
S3-010232	Reply to LS on rejection of 2G authentication and key agreement by 3G ME with USIM in UTRAN	Approved	**T WG3,** **SA WG1,** **GSMA-SG** **T WG2,** **CN WG1**
S3-010233	Reply LS on authentication test algorithm to be implemented in test USIM	Approved	**T WG1, T WG3**
S3-010247	Reply to LS on revised working assumptions made at joint GERAN/S3 meeting	Approved	**TSG GERAN**
S3-010265	Reply LS on Security Associations for IMS functional elements	Approved	**SA WG2**
S3-010268	Reply LS on Wrap around of the calculated START value	Approved e-mailed during S3#18 meeting	**RAN WG2**
S3-010273	Reply LS on THRESHOLD Check at RRC connection establishment	Approved e-mailed during S3#18 meeting	**RAN WG2,** **CN WG1**
S3-010274	Reply to LS on "Handling of ICMP messages by 3GPP SIP Implementations"	Approved	**CN WG1**
S3-010287	Using a generic authentication scheme for SIP	Approved	**CN WG1,** **CN WG4** **SA WG2**
S3-010289	Security and UE functionality split	Approved	**SA WG1,** **T WG2, T WG3** **TSG SA,** **TSG T,** **ETSI EP SCP**
S3-010291	Reply to LSs: "Security for IM SIP session Signaling" (Tdoc N1-010588, received as S3-010152) AND “IM User Identities” (Tdoc S2-010757, received as S3-010160)	Approved	**CN WG1,** **SA WG2**
S3-010292	Response to Liaison Statement on the IM Call Transfer Service N1-010890 (S3-010249)	Approved e-mailed during S3#18 meeting	**CN WG1** **CN WG2,** **CN WG3,** **CN WG4,** **SA WG5**
S3-010293	Reply LS on extended streaming service and user profiles	Approved	**SA WG1,** **SA WG4** **SA WG2,** **T WG2**