3GPP TSG SA WG3 Security — S3#19

4-6 July, 2001

Newbury, England

Source:	**Secretary SA WG3 (Maurice Pope)**
Title:	**Draft Report of SA WG3 Meeting #19, version 0.0.2**
Document for:	**Comment**

Newbury Races - Venue of the SA WG3#19 social event

---

1 Opening of the meeting

The SA WG3 Chairman, Prof. M. Walker opened the meeting, and welcomed delegates to Newbury on behalf of the host, Vodafone.

2 Meeting objectives and approval of the agenda

TD S3-010300 contained the draft agenda for the meeting. The Chairman outlined the objectives for the meeting, including the actions resulting from TSG SA meeting #12, and the progression of work items which needed to be completed for delivery at TSG SA meeting #13, September 2001. A presentation by CN WG1 had been scheduled, and it was hoped that this would help clarify the understanding in the two WGs, and lead to good progress on the IM Security related work. A joint meeting on UE functionality split had been held on 3 July 2001, and the results of this were scheduled for presentation and elaboration under agenda item 7.5.

The draft agenda was then approved.

IPR Declaration: The Chairman reminded delegates of the 3GPP IPR policy and their obligation to declare essential IPRs to their respective Partner Organisations (SDOs).

3 Assignment of input documents

The available documents were assigned to their respective agenda items. Some of the documents had been dealt with at the joint meeting on UE functionality split, and were dealt with in the report of that meeting under agenda item 7.5.

4 Approval of reports from 3GPP SA3 meetings

4.1 S3#18, 21-24 May, Phoenix

TD S3-010301 Draft report of meeting #18. The report of the previous meeting was considered, and some minor modifications were made. The report was then approved and the Secretary undertook to put the updated version 1.0.0 on the FTP server under the meeting #18 directory.

5 Reports and liaisons from other groups

5.1 3GPP SA3 lawful interception sub-group

The written report was not available during the meeting, and would be provided after the meeting in TD S3-010365. delegates were asked to read this for information when available on the FTP server. Mr. Berthold Wilhelm provided a verbal report of the progress in the SA WG3 Lawful Interception (LI) group. Mr. Bernie McKibben (Motorola) had resigned from the Chairmanship of the group due to changes in his workload, and Mr. Rolf Schnitzler (Mannesmann Mobilfunk) had been elected as the new Chairman of the SWG for 1 year. The group had progressed TS 33.107 for Release 1999, with proposed CRs provided in TDs S3-010360 to S3-010363.

TD S3-010364 3GPP TS 33.108, version 0.0.2: This was provided by the LI group for information, and included the Lawful Interception Handover Interface, Stage 3. It was reported that the work was expected for completion by the end of 2001 / beginning of 2002. There was some surprise at the lateness of this document for Release 1999, which had been functionally frozen in March 2000. **It was recognised that the introduction of this functionality into Release 1999 would be problematic, and the LI group were asked to re-consider this work for Rel-5**. The document was then noted.

TD S3-010359 WI description: 3GPP Handover Interface for Lawful Interception (33.108). This proposed a new WI description for the LI Handover Interface work, currently in draft TS 33.108. It was suggested that this specification was already in the scope of the general LI work, and the LI group were asked to update the main LI WI description to include the Handover Interface work. This proposed WI description was therefore rejected.

TD S3-010360 CR to 33.107 v 3.2.0: Missing location related information in Packet Data Event Records. This CR was approved (33.107 CR005).

TD S3-010361 CR to 33.107 v 3.2.0: Correct the MO-SMS and MT-SMS events. This CR was discussed and it was considered that the CR needs to be checked by SA WG3 to determine the practicality of the requirements. The CR was therefore not accepted (33.107 CR006). The LI group were asked to reconsider the text and clarify the requirements.

TD S3-010371 CR to 33.107 v 3.2.0: Reporting of Secondary PDP context (revision of TD S3-010362). This CR was approved (33.107 CR007R1).

TD S3-010363 CR to 33.107 v4.0.0: Reporting of Secondary PDP context. The relevance of this change for Release 1999 was questioned. It was recognised that these changes should be a Category A CR, the Release 1999 changes having been approved in TD S3-010371 and the additional modifications in this CR were already included in the Rel-4 version of the TS. The CR was therefore updated as appropriate in TD S3-010372 which was approved (33.107 CR008R1).

5.2 3GPP SA plenary

The SA WG3 Chairman provided a verbal report on the issues raised at TSG SA Meeting #12. He reported that TS 33.200 (MAP Security) had been approved. TSG SA had asked for the removal of the editors comments as soon as possible and for the production of a guidelines document, with examples of Manual Key Management schemes, for presentation at TSG SA meeting #13 (September 2001).

TSG CN had asked for early visibility of the SA WG3 draft documents in their appropriate working groups. The document rapporteurs were asked to provide the latest drafts of their documents to MCC (Maurice Pope) in order that they be placed in the latest drafts area of the FTP server. Mr. Pope would then send notification of these documents to the TSG and WG Chairmen (i.e. the TSG Leaders e-mail list).

TSG SA asked for the allowed USIM/SIM AKA scenarios for 2G/3G networks to be clarified, to prevent any misunderstanding in other groups of which scenarios are allowed. Peter Howard had been asked to produce an input document on this, but he was absent from the meeting due to illness. The SA WG3 Chairman undertook to ask him to send this to the SA WG3 e-mail list when it was available.

The SA WG3 agreed WI description on analysis of MExE Security had been rejected, as this work was already covered by a T WG2 WI description, and SA WG3 delegates were asked to ensure that the security aspects were covered by attending T WG2 MExE Security sessions.

The SA WG3 Chairman had asked for advice on working with IETF documents, and a presentation had been given by the 3GPP liaison officer to IETF, asking for close collaboration of 3GPP Members in the relevant work in the IETF in order to ensure that the 3GPP requirements were taken into account. The next IETF meeting was scheduled for 5-10 August, and attendance from SA WG3 was requested to present the work of SA WG3, which impacted or was impacted by, the IETF security work. Peter Howard had been asked to provide a presentation, which will be sent to the SA WG3 e-mail list when available, for comment, before presentation to the IETF.

The SA WG3 Chairman also reported that China were proposing to produce their own specific encryption algorithm for their 3GPP system. It was agreed that SA WG3 should track this work, and identify any potential impacts on interoperability of 3GPP systems.

5.3 3GPP working groups

TD S3-010305 Reply from GERAN to LS S3-010290 on integrity protection at RLC/MAC level. This was presented by Nokia, and confirmed that GERAN could not cipher all messages with 32-bit MAC, due to the lack of available bits for this, and consequential performance impacts. GERAN confirmed their intention to cipher the RLC/MAC control messages. A response LS to TSG GERAN, acknowledging this, was provided in TD S3-010373 which was approved.

TD S3-010306 Authentication between "GERAN" MS and 3G CN. This LS from GERAN informed SA WG3 and CN WG1 that the 3GPP CN authentication mechanisms are expected to be fully applicable

and re-used in GERAN. Confirmation of this was provided an LS to TSG GERAN in TD S3-010374 which was approved.

TD S3-010307 LS reply to SA WG1 LS "regarding User Profile", from SA WG5. This was provided to SA WG3 for information, and suggested a cross-WG ad-hoc should be set up. SA WG3 had dealt with this in meeting #18 (TD S3-010293, which was not addressed to SA WG5), and concluded that some SA WG3 involvement would be useful. It was reported that no security implications had been identified at present. The LS was then noted.

TD S3-010308 LS from SA WG5 in reply to three related User Equipment Management liaisons. This was related to terminal core software downloading (MExE) terminal management. A reply LS asking for visibility of the SA WG5 work in this area, in order that SA WG3 could analyse the security impacts, was provided in TD S3-010375 which was approved.

TD S3-010309 LS from SA WG5: IMT2000 Management Co-operation. This was provided to SA WG3 for information. There was some confusion over the use by SA WG5 of the X-interfaces, which are already used for Lawful Interception interfaces. The SA WG3 Chairman undertook to write a LS back to SA WG5 to inform them of this, which was provided in TD S3-010376 which was approved.

TD S3-010310 LS from SA WG5: Reply to N1-010890 "Liaison Statement on the IM Call Transfer service". This had been copied to SA WG3 for information, and it was noted that a response had been provided on this subject at SA WG3 meeting #18 (TD S3-010292). The LS was then noted.

TD S3-010311 Liaison Statement from SA WG4 in Regards to Digital Rights Management. This LS discussed 3 options for DRM. It was agreed that this needed further consideration and contributions were invited to discuss whether DRM should be standardised in 3GPP, and if so, what actions SA WG3 need to perform. The LS was then noted.

The SA WG3 Chairman agreed to draft a LS after the meeting, informing SA WG4 that SA WG3 will consider this at their meeting #20, and confirming that there is a need for standardisation work in this area.

TD S3-010312 Reply from SA WG4 to "LS on Extended Streaming Service" and "LS regarding User Profile". The impacts on security for SA WG3 were unclear. The LS was noted, and the SA WG3 Chairman provided a reply LS in TD S3-010377 asking SA WG4 to keep SA WG3 informed on the progress in order that SA WG3 could analyse the security impacts, which was approved.

TD S3-010313 SA WG2 WI on the End-to-End QoS Architecture for Release 5. The status of the proposed WI description at TSG SA meeting #12 was checked and it was noted that the WI description had been approved. The LS and WI description were noted, and the SA WG3 Chairman provided a reply LS in TD S3-010378 asking SA WG4 to keep SA WG3 informed on the progress in order that SA WG3 could analyse the security impacts, which was approved.

TD S3-010314 Response to LS (GAHW-010109, R3-010890 and S2-010383) on Optimised IP speech and header removal support in GERAN. This had been provided to SA WG3 by SA WG2, copied from the LS they received from RAN WG2. The LS was noted and a response giving details of the use of IPsec by SA WG3 for SIP signalling only (not for speech) was provided in an LS to RAN WG2, copied to TSG GERAN, RAN WG3 and SA WG2, in TD S3-010379 which was approved.

TD S3-010321 Response to LS on "Clarification of UMTS-AKA for GSM R'99 Mobiles" & support of UMTS AKA for GSM only R4 MEs. This LS had been postponed at the previous meeting, and was covered by the request of TSG SA to provide clarification on the allowed 2G/3G SIM/USIM AKA scenarios. The LS was then noted.

5.4 ETSI SAGE

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

TR-45:

TD S3-010318 News from TR45.AHAG. Mr. Greg Rose reported that he had been appointed by

TR-45 as the liaison from TR-45 AHAG to SA WG3 (complimentary to Mr. Michael Marcovici being the liaison from SA WG3 to TR-45).

There had been a proposal for 3GPP2 to form a security group, similar to SA WG3, under 3GPP2 TSG-S WG4, with TR-45 AHAG concentrating on algorithm work, similar to ETSI SAGE. The possible implications of this change in structure on the AKA joint control agreement would need to be checked, as the agreement was at present between SA WG3 and TR-45 AHAG.

GSMA:
Mr. Charles Brookson verbally reported that there had been no meetings of the GSMA SG since the last SA WG3 meeting. The progress on A5/3 was reported as being close to finalisation, and the negotiations were now mainly on who will fund the work (i.e. GSMA or 3GPP Partners).

6 Technical specifications and reports

6.1 Security architecture (TS 33.102)

TD S3-010353 Comments to doc: Support of certificates in 3GPP security architecture. This contribution had first been provided at SA WG3 meeting #16, and had been postponed until this meeting. The contribution was presented by Nokia, and was an exploration paper on the potential support for a WI on standardising certificates in 3GPP. Companies (in particular operators) were asked to consider this and provide contribution and indication of support for such a WI. Support was provided at the meeting by Telenor, Motorola, Qualcomm, Nokia and Orange. These companies were asked to provide a WI description proposal with clear scope and justification at the next meeting (SA WG3 meeting #20).

TD S3-010319 Proposed CR to 33.102 (Rel-4): Adding PS-domain specific access type codes to authentication failure report. This was revised in TD S3-010394 in order to remove the need to update the specification every time a new access was added in TS 29.002, which was approved (33.102 CR155R1).

6.2 Integration guidelines (TS 33.103)

TD S3-010384 (revision of TD S3-010366) CR to 33.103 v3.6.0: Correction of USIM data elements for AKA. This was introduced by Motorola. Some modifications were made and the CR revised in TD S3-010395 which was approved (33.103 CR016R2).

TD S3-010396 CR to 33.103 v4.1.0: Correction of USIM data elements for AKA. This was the corresponding Rel-4 CR to 33.103 CR016R2: This was approved (33.103 CR017).

6.3 Algorithm requirements (TS 33.105)

There were no contributions on this agenda item.

7 Work items

7.1 MAP security (TS 33.200, draft TR 33.800)

Due to lack of time in the meeting to deal with the MAP security contributions, they were postponed to the ad-hoc meeting on MAP security - 13 September 2001. Therefore the following TDs would be input to the meeting: S3-010302, S3-010322, S3-010325, S3-010327, S3-010333, S3-010335, S3-010338, S3-010349, S3-010350, S3-010351, S3-010352, S3-010354, S3-010368.

The rapporteur (Mr. Geir Koien) reported that he was unable to continue in the temporary rapporteurship of TS 33.200, and a new Rapporteur was needed. Mr. Adrian Escott agreed to check whether he would be available for this position, and would report to SA WG3 meeting #20 (or the MAP security ad-hoc meeting).

7.2 IP network layer security (draft TS 33.210)

TD S3-010303 Draft of 33.210, version 0.5.5. This was presented by the Rapporteur, Mr. Geir Koien. The subject of SA bundles was raised, and a contribution was provided by Alcatel in TD S3-010348. Delegates were asked to review the document and provide contribution towards its completion.

TD S3-010348 TS 33.210 V0.5.5: Network Domain Security; IP network layer security (Release 5). This was provided by Alcatel and provided questions and comments on the draft TS. The issue of SEG addressing was discussed, and it was agreed that an off-line discussion on this issue should be held in order that the Rapporteur could clarify the addressing mechanism in the next draft. It was also agreed that protection profiles were not really needed in NDS-IP and the Rapporteur was asked to clarify this for the next draft of the TS.

TD S3-010304 Evolution of NDS/IP - NE authentication using PKI. This was briefly introduced by Telenor and was offered for information to SA WG3, suggesting that this issue is revisited at SA3#20. The document was noted and delegates were asked to consider the document and it's attachments. Contribution on this topic was invited to SA WG3 meeting #20.

7.3 IP multimedia subsystem security (draft TS 33.203)

TD S3-010340 TS 24.228 V1.1.0: Signalling flows for the IP multimedia call control based on SIP and SDP (Release 5). This was provided by CN WG1 for information and was used as reference material for discussions and noted.

TD S3-010339 IM CN SS (Security) - CN WG1 perspective. The work of CN WG1 on IM Core Network Signalling security was presented by Mr. John O'Hara (Motorola). The main discussion points are reported below.

ISC interface: Slide 11 provided details of this interface. The SIP interfaces were assumed to be within a single network, whereas OSAAPI would be between different service providers. SA WG3 need to study the security implications of the ISC interface.

Private/Public Identity issues: It was expected that the operator would allocate one private identity and at least one public identity to each subscriber. It was noted that TS 23.228 may need some clarification on this.

Authentication had not been considered by CN WG1, and information was requested from SA WG3 in order to include this in the specification. A contribution on this was provided by Siemens in TD S3-010355 (see below).

TD S3-010355 Information flows for IMS authentication and key agreement. This was provided by Siemens and discusses the possibilities for optimisation of message flows. After some discussion, it was agreed that a LS to CN WG1, SA WG2 and CN WG4 should be created on the options for optimisation that had been identified by SA WG3, as this has no impact on security. This LS was provided in TD S3-010387 which was approved. TD S3-010355 will be attached to this LS.

Security related categories: Slide 18 listed the security categories assumed by CN WG1 and SA WG3 were asked to confirm this:

- Authentication
- Encryption
- Hiding (Network Configuration)
- Session (Call) Transfer
- Security Mode Set up

SA WG3 confirmed that all categories had been, or were being added to their work programme.

There had been a liaison provided at SA WG3 meeting #18 (TD S3-010291), which provided additional information to the responses to the questions in slide 19. Points discussed are reported below:

- "Via and Record Route Header Hiding by I-CSCF":
  A new work item on hiding mechanisms has been created by SA WG3 at SA WG3 meeting #18, which was approved at TSG SA meeting #12. The SA WG3 work on this new work item is expected to be completed by July 2001?
  This would be worked on by SA WG3 at meeting #19 (this meeting).

- "Usage of the User Private Identity"
  SA WG3 sees no security problem with the current working assumption by SA WG2 and CN WG1 "that the Registration flow is definitely the only time the Private User Identity is sent to the network in SIP signalling messages".
- "Authentication of Invite and other SIP session signalling messages"
  It is the current working assumption of SA WG3 that authentication is only required for registration and re-registration.
  The current assumption was to perform authentication on registration and re-registration only. Other triggers for authentication need further study by SA WG3.

- "Integrity protection of SIP signalling messages (especially the first message that is sent)"
  The mechanism for integrity protection of SIP signalling messages between the UE and the P-CSCF is still under study by SA WG3, the mechanism for integrity protection of SIP signalling messages between other IMS entities is IPsec (ESP). The first message that is sent (REGISTER) cannot be integrity protected as no integrity key establishment has yet taken place. However, when REGISTER is sent a second time it can be integrity-protected. The precise mechanism for this is still under discussion in SA WG3.
  Contributions had been provided to this meeting.

- "Requirement for SIP signalling to support Key exchange for encryption of bearer"
  SA WG3 understands that “encryption of bearer” refers to end-to-end encryption of user data. SA WG3 would like to inform CN WG1 and SA WG2 that a SA WG3 work item relating to end-to-end security in UMTS exists. SA WG3 can confirm that SIP signalling messages will be required to support key exchange for IMS end-to-end encryption. However, no solutions are currently available.
  Contributions had been provided to this meeting on end-to-end encryption. However, the SA WG3 Work Item on end-to-end encryption did not receive adequate supporting companies, and will be removed from the SA WG3 work plan.

A LS was drafted to clarify the issues and information provided by TD S3-010291, which was provided in TD S3-010381 which was modified slightly and provided in TD S3-010391 which was approved. **Note: this was replaced again due a mistake in saving the document, and reproduced by the Secretary in TD S3-010404.**

Authentication: It was noted that the message flows did not contain authentication messages. It was reported that these had not yet been added and SA WG3 were asked for advice on the mechanisms to be used. There was not adequate support in SA WG3 to authenticate for anything more than registration and re-registration. CN WG1 also have work on Network Authentication, and companies were asked to contribute to SA WG3 meetings in order to develop the requirements for this.

It was reported that SA WG2 had changed the architecture recently to allow the S-CSCF handling re-registration to be different than the S-CSCF which performed the original registration. This was not possible in the current authentication model, as only the original S-CSCF holds the required data for authentication. A LS to SA WG2 to clarify this was provided in TD S3-010382 which was approved. (SA WG3 will continue with their original assumptions on the authentication model).

A typographic error was noted in slide 20: The final bullet should read
"**Network initiated re-registrations and de-registrations**".

Slide 21 asked some questions of SA WG3:

Signalling: Assuming hop-by-hop, at what layer does encryption take place?
- It was clarified that in Release 1999, encryption (if ON) terminates at the RNC. The Rel-5 for IMS, the use of SIP is under discussion, with other hops being protected by IPsec, to be detailed in draft TS 33.210.

Bearer: Is end-to end encryption to be assumed? and *Are keys to be transported in SDP information?*
- end-to-end encryption WI in SA WG3 had been removed from the work plan due to lack of company support.

Slide 22: Network hiding requirements: A contribution on hiding of host/domain name and hiding of the number of S-CSCFs in an operators network had been provided in TD S3-010323. The key distribution issues had not yet been considered by SA WG3.

Hiding of callers Public ID: SA WG3 had not identified this as a requirement. It was reported that the IETF had included a mechanism to do this in SIP, and if it is identified as a requirement, contribution should be made to SA WG3 and the possible mechanisms for Public identity privacy will be studied.

Slide 23: Hiding of the callers IP address (anonymity). SA WG3 need to do a security threat analysis to determine whether there is a need to hide the callers IP address.

Slide 24: Session call transfer: This requirement was outside the scope of SA WG3 work, as it is a fraud issue. The GSMA were asked to study the Session Call Transfer issues in a LS provided in TD S3-010383, which was approved.

Lawful Interception of the transferring network: This is not possible, as lawful interception does not apply in cross-border situations. SA WG3 LI group were asked to analyse this scenario from a lawful interception legal and technical viewpoint.

Limiting the number of parallel calls that can be transferred. Again, the GSMA were asked to study this and check the mechanisms available to do this, included in TD S3-010383.

Termination of transferred calls if the transferring party's credit expires. SA WG5 were asked to analyse the billing/charging model for call transfer in IMS, and SA WG3 will consider this when a model is made available. It was agreed to include this in the LS in TD S3-010381 (later revised to TD S3-010404, see above).

Slide 27: A joint meeting between CN WG1 and SA WG3 was requested. The timing of such a meeting would depend upon the stability of TS 33.203, and a suggestion was made for this to be after the October meeting of SA WG3. In the meantime, CN WG1 would be kept aware of progress on the issues by e-mail. It was also suggested that the issues and resolutions are maintained in draft TS 33.203 as an annex (which will be removed before TSG approval). The rapporteur, Mr. Krister Boman, agreed to do this.

TD S3-010358 aSIP-Access Security for IP-Based Services: Activities and the new time plan. This presentation was provided by the rapporteur for TS 33.203, Mr. Krister Boman. (It had also been presented to the Joint meeting on 3 July 2001). A new functional entity had been created "IM-SIM, or ISIM". This was introduced to distinguish between the USIM functionality from the IM functionality, included on the UICC.

The use of cookies, or SIP header extensions was raised. Siemens provided details of a mechanism for optimisation of the signalling in TD S3-010355, outlining a method to reduce the CxPUT CxPULL and CxQUERY messages. SA WG3 agreed to add the results of discussions on this contribution to the LS to SA WG2, CN WG1 and CN WG4 (TD S3-010403, see agenda item 7.1).

After some questions for clarification, the presentation was noted.

TD S3-010385 (revision of TD S3-010370): aSIP-Access Security for IP-Based Services - Activities and time plan. Mr. Krister Boman presented the results of the aSIP ad-hoc meeting. The time plan for stage 3 work was proposed to change from December 2001 to March 2002, which was thought to be more realistic, with an agreed freeze date of June 2002.

Slide 5: Contributions were provided to this meeting for Protection mechanisms, error cases and Security Mode Set-up. The new version 0.4.0 of draft TS 33.203 was also provided for presentation to SA WG3. The principles for handling Security Associations (SAs) between UE and the P-CSCF needed to be determined.

Due to the need to make fast progress on the document, an ad-hoc meeting was proposed to be arranged for around Mid-September 2001, if found to be necessary (see meeting schedule in agenda item 9).

Open issues:
SIP confidentiality protection: It was suggested to propose a NULL algorithm for Rel-5, in order to have the mechanism available for when the algorithm is chosen/developed for this. This would be optional for implementation and it was agreed that SA WG3 need to analyse whether SIP message confidentiality is really required.

Replay protection: If SIP message confidentiality is required, then the replay protection requirements would also need to be analysed.

Authentication trigger: It was clarified that the SA WG3 assumption is to perform authentication on registration and re-registration only. Delegates were asked to carefully consider this, in order to ensure that this is adequate.

Visibility and configurability: This issue needs to be further considered and contribution was requested from SA WG3 members.

UE functional split issues: This issue was discussed under agenda item 7.5.

TD S3-010324 Draft TS 33.203 version 0.4.0. This was presented by the rapporteur, Mr. Krister Boman. It was agreed that T WG3 need to be informed of the proposal and concept of the ISIM logical entity introduced into the document. Mr. Valtterri Niemi agreed to produce a LS to T WG3 related to both the ISIM and UE functional split issues (see TD S3-010400, agenda item 7.5). It was recognised that the Z-interfaces used in figure 2 need to be verified.

TD S3-010330 EAP Extensions - status report. This was introduced by Ericsson. an input to the IETF of a draft HTTPEAP will be contributed by Ericsson and Nokia. It was reported that DIAMETER EAP extensions were stable (DIAMACC). Siemens mentioned that the inclusion of EAP should be the responsibility of CN Wg4, the specification in CN WG1 and that SA WG3 should provide advice. This was further discussed under agenda item 6.1 (see TD S3-010324). CN WG1 and CN WG4 should be asked for feedback on the impact of EAP on their 3GPP specifications, 24.228/24.229 and 29.228/29.229. It was also clarified that the EAP message formats are used, not the full EAP protocol (see also agenda item 6.1).

TD S3-010367 On registering several public identities in IM CN SS. This was provided by Ericsson and provided some options for handling authentication of Public identities. It was noted that network initiated re-authentication would greatly reduce the complexity and that one SA would then be sufficient, providing flexibility to operators to define their own authentication policies. It was agreed to inform SA WG2 of the implications of using different S-CSCFs for different Public IDs, and this was provided in TD S3-010388. This was modified and provided in TD S3-010402 which was approved. (TD S3-010367 will be attached to this LS).

TD S3-010328 Validation of public user identity in registration. This contribution had been presented to SA WG2, who saw security issues and had asked Ericsson to bring it to SA WG3. The need for checking at certain points in the flow was discussed and it was concluded that this required further study in SA WG3. The proposal to download a list of valid Public IDs to the S-CSCF in order to allow the S-CSCF to perform validity checks on them was included in the LS in TD S3-010388 to SA WG1.

TD S3-010326 Security mode set up for the IMS registration. This contribution was provided jointly by Ericsson, Nokia and Nortel, and was presented by Nokia. It was stated that the examples given did not reflect any standpoint of the contributing companies, and were only for illustrative purposes.

Integrity protection on failure messages: It was argued that failure messages need not be integrity protected. It was generally agreed that such protection of these messages from Denial of Service (DoS) attacks would complicate the system and bring no real advantage, as many other DoS attack scenarios cannot be easily protected against. The principles of the contribution were accepted, and some issues were identified, which require resolution. The rapporteur agreed to take this contribution into account in TS 33.203.

SIP Integrity protection. Contributions: TD S3-010347 Integrity protection for SIP signalling (Ericsson); TD S3-010356 Integrity protection between UE and P-CSCF (Siemens AG); and TD S3-010357 Integrity protection mechanism of SIP (Nokia), were presented in order for a joint discussion:

The following was agreed:

- The solutions presented all provided similar header sizes, and this was left out of considerations, as the issue would be solved, whichever scheme is chosen.
- The CMS (Ericsson) proposal required IETF standardisation work, although it was noted that SA WG3 delegates would need to do work in the IETF anyway.
- It was recognised that the IETF should be asked to start CMS work, as it would be too late if decisions are delayed.
- The IPsec solution would need further analysis to determine its full suitability.

Ericsson agreed to check the realistic timescales of the work in the IETF. This then would be used to make a decision in the IMS ad-hoc meeting, 14 September 2001.

TD S3-010389 Use of NDS for SIP. This was presented by Nortel. Protection of GTP-U needs complete User Plane protection, as the IMS control messages cannot be separated out. This proposal recommended the creation of a new GTP-IC, of IMS control plane messages, which can then be protected separately from the User Plane data. This would require separate port numbers for GTP-U and GTP-IC in order to distinguish them. It was agreed to produce an LS to SA WG2, CN WG1 and CN WG4, explaining the problem and asking if they can do the necessary work for IMS Rel-5, and asking for advice and comments on the proposed scheme, and possible alternative solutions. The LS was provided in TD S3-010393 (revised in TD S3-010403, see below).

TD S3-010393 LS to SA WG2, CN WG1 and CN WG4 on creation of GTP-IC plane. This LS explained the problem of protecting IMS GTP signalling. The need for protection and whether protection of all the GTP-U was really unfeasible was discussed. No conclusion was reached and it was agreed that this should be input to SA WG3 meeting #20. In parallel, SA WG2 were asked for the implications of the options 2 and 3 via a LS, which was provided by Mr. Greg Rose in TD S3-010399. This was modified slightly and provided in TD S3-010403 which was approved.

7.4 GERAN security

7.5 Security aspects of UE functionality split 342

TD S3-010392 Draft report of joint meeting S1/S3/T2/T3 about security implications of UE functional split 3rd July 2001 - version 0.0.2. This report of the joint meeting was introduced by the Chairman of the joint meeting, Mr. Valtterri Niemi. Due to lack of time, it was agreed to keep this item as a standing item on the SA WG3 agenda, until a solution and response is produced. The report was then noted.

It was agreed to input this report, in order to have a list of the cases to be considered, to SA WG3 meeting #20, and contributions were requested.

TD S3-010386 LS to T3 on ISIM / UE Functionality Split. This was presented and accepted in principle. Clarification was necessary on the SIM/USIM and 2G/3G network possibilities, and Mr. Niemi agreed to provide a document to be agreed by the meeting. This was produced in TD S3-010400 which was approved. The report of the joint meeting on UE functionality split (TD S3-010392) will be attached to this LS.

7.6 Security aspects of network configuration hiding

TD S3-010323 Network Configuration Independence Mechanism (Network Hiding). This was introduced by AT&T Wireless. It was agreed that this would be optional for implementation and the functionality could be included in draft TS 33.203, instead of sending a proposed CR to SA WG2. The proposal was then revised in TD S3-010398 (see below).

TD S3-010398 Network Configuration Independence Mechanism. This liaison to SA WG2 and CN WG1 on network hiding issues was introduced by AT&T Wireless. It clarified that the Network

Hiding WI had been approved at SA WG3 meeting #18 and was now included in the SA WG3 work plan. The LS was then approved.

7.7 Visibility and configurability of security

TD S3-010369 Proposed CR to 33.102 Rel-4: Configurability of cipher use. This CR was introduced by Telia and proposed as a Category F CR to Rel-4. The changes included were considered as potential functional changes (mandatory requirements replacing optional ones), in which case it would be unacceptable for Rel-4. It was also identified that impacted groups should be informed of this and it was agreed that the CR should be sent to them for comment, as a potential Rel-5 CR. The CR was therefore rejected as it stood, and Telia were asked to re-draft it as appropriate and contribute it to other impacted groups. A LS was provided in TD S3-010397, but due to lack of time to adequately consider the LS and attached CR, it was decided to postpone this to SA WG3 meeting #20.

TS 29.198-03: It was reported that this specification had been approved at TSG SA meeting #12 and that SA WG3 had not seen this CN WG5 specification before, and it was noted to contain some incorrect information on algorithms. **The SA WG3 Chairman agreed to raise this with the CN WG5 Chairman**.

7.8 MExE security

No specific inputs were received for this agenda item. See the report from the TSG SA Meeting #12, under agenda item 5.2 and TDs S3-010308 and S3-010375 under agenda item 5.3.

7.9 OSA security

TD S3-010317 Review of OSA Security - some issues for SA3 to consider. This was provided by BT and outlined some issues related to Key management which need to be considered in SA WG3. Delegates were asked to consider these issues and provide contribution.

7.10 End-to-end security

TD S3-010329 Updated Work Item Description for Network based end-to-end security. This was introduced by Ericsson, and support was requested for the WI. As not enough support to accept the WI was received, the WI was rejected. (The WI can be raised again when enough support is gained).

TD S3-010346 Work Item Description for "End-to-End VoIP Privacy". This was introduced by Lucent and proposed a codec-based end-to-end encryption method. Support was requested for the WI and as there not enough support to accept the WI, it was rejected. (The WI can be raised again when enough support is gained).

It was agreed to remove end-to-end security from the SA WG3 work plan, which would be updated after the meeting, off-line.

TD S3-010331 "Hybrid sync-frame/sync-free E2E Encryption" and the associated presentation TD S3-010332 from Lucent were not considered at the meeting, due to the removal of end-to-end encryption from the SA WG3 work plan. Lucent were invited to re-contribute these documents if end-to-end encryption is re-introduced into the work plan in the future.

7.11 FIGS/IST

There were no contributions on this agenda item.

8 Review and update of work programme

It was reported that Mr. Peter Howard and Mr. Maurice Pope will update the work plan, in order to bring it up to date with decisions made and revised timescales, and send to the SA WG3 e-mail list for comment.

A request was made for Mr. Pope (MCC) to maintain an area on the SA WG3 FTP site, containing the agreed WI description sheets, as they were difficult to find. **Mr. Pope agreed to do this after the meeting**.

9 Future meeting dates and venues

Note change of dates:

Meeting	Date	Location	Host
S3-MAP Sec	13 September 2001	Sophia Antipolis, France	ETSI
S3-IMS Sec	14 September 2001	Sophia Antipolis, France	ETSI
S3#20	16 – 19 October 2001	Sydney, Australia	Qualcomm Int.
S3#21	27 - 30 November 2001	Sophia Antipolis, France	ETSI
S3#22	26 Feb - 1 March 2002	Bristol, UK	Orange
S3#23 + AHAG	14 - 17 May 2002	Vancouver, Canada / Seattle, USA	AT&T Wireless
S3#24	9 - 12 July 2002	Helsinki, Finland (TBC)	Nokia
S3#25	15 - 18 October 2002	Munich, Germany (TBC)	Siemens (TBC)

10 Any other business

A number of documents were not dealt with at this meeting, and will be considered in either the MAP security ad-hoc meeting, the IMS ad-hoc meeting or at SA WG3 meeting #20.

11 Close of meeting

The SA WG3 Chairman thanked delegates for their hard work, and considered that good progress had been made at this meeting, even though not all documents could be dealt with in the allocated time. He then closed the meeting.

Annex A: List of attendees at the SA WG3#19 meeting

Name	Company	e-mail	3GPP ORG	
Mr. Nigel Barnes	MOTOROLA Ltd	Nigel.Barnes@motorola.com	ETSI	GB
Dr. Stephen Billington	Hutchison 3G UK Limited	stephen.billington@hutchison3g.com	ETSI	GB
Mr. Colin Blanchard	BT	colin.blanchard@bt.com	ETSI	GB
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.atea.be	ETSI	BE
Mr. Krister Boman	ERICSSON L.M.	krister.boman@emw.ericsson.se	ETSI	SE
Mr. Charles Brookson	DTI	cbrookson@iee.org	ETSI	GB
Mr. David Castellanos	ERICSSON L.M.	david.castellanos-zamon@ece.ericsson.se	ETSI	SE
Ms. Lily Chen	T1 Standards Committee	lchen1@email.mot.com	T1	US
Mr. Takeshi Chikazawa	Mitsubishi Electric Co.	chika@isl.melco.co.jp	ARIB	JP
Mr. Per Christoffersson	TELIA AB	per.e.christoffersson@telia.se	ETSI	SE
Dr. Adrian Escott	Hutchison 3G UK Limited	adrian.escott@hutchison3G.com	ETSI	GB
Mr. Louis Finkelstein	Motorola Inc.	louisf@labs.mot.com	T1	US
Mr. Anders Hansmats	TELIA AB	anders.o.hansmats@telia.se	ETSI	SE
Mr. Guenther Horn	SIEMENS AG	guenther.horn@mchp.siemens.de	ETSI	DE
Mr. Kazuhiko Ishii	NTT DoCoMo Inc.	ishii@mml.yrp.nttdocomo.co.jp	ARIB	JP
Mr. Geir Koien	TELENOR AS	geir-myrdahl.koien@telenor.com	ETSI	NO
Mrs. Tiina Koskinen	NOKIA Corporation	tiina.s.koskinen@nokia.com	ETSI	FI
Mr. Alexander Leadbeater	BT	alex.leadbeater@bt.com	ETSI	GB
Mrs. Geneviève Mange	ALCATEL S.A.	g.mange@alcatel.de	ETSI	FR
Mr. Michael Marcovici	Lucent Technologies	marcovici@lucent.com	T1	US
Mr. Duncan Mills	VODAFONE Group Plc	duncan.mills@vf.vodafone.co.uk	ETSI	GB
Mr. Sebastien Nguyen Ngoc	France Telecom	sebastien.nguyenngoc@rd.francetelecom.com	ETSI	FR
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com	ETSI	FI
Mr. Petri Nyberg	SONERA Corporation	petri.nyberg@sonera.com	ETSI	FI
Mr. Bradley Owen	Lucent Technologies N. S. UK	bvowen@lucent.com	ETSI	GB
Mr. Olivier Paridaens	ALCATEL S.A.	Olivier.Paridaens@ALCATEL.BE	ETSI	FR
Mr. Maurice Pope	ETSI Secretariat	maurice.pope@etsi.fr	ETSI	FR
Dr. Stefan Pütz	Deutsche Telekom MobilNet	stefan.puetz@t-mobil.de	ETSI	DE
Mr. Gert Roelofsen	KPN	g.roelofsen@kpn.com	ETSI	NL
Mr. Greg Rose	QUALCOMM EUROPE S.A.R.L.	ggr@qualcomm.com	ETSI	FR
Mr. Teruharu Serada	NEC Corporation	serada@aj.jp.nec.com	ARIB	JP
Mr. Hugh Shieh	AT&T Wireless Services, Inc.	hugh.shieh@attws.com	T1	US
Mr. Al Thomas	Cingular Wireless LLC		T1	US
Mr. Lee Valerius	NORTEL NETWORKS (EUROPE)		ETSI	GB
Prof. Michael Walker	VODAFONE Group Plc	mike.walker@vf.vodafone.co.uk	ETSI	GB
Mr. Stuart Ward	ORANGE PCS LTD	stuart.ward@orange.co.uk	ETSI	GB
Berthold Wilhelm	Reg TP	berthold.wilhelm@regtp.de	ETSI	DE

<Other Annexes to be added>

Annex B: List of documents

<Annex to be added>

Annex C: Status of specifications under SA WG3 responsibility

<Annex to be added>

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

<Annex to be added>

Annex E: List of Liaisons

E.1 Liaisons to the meeting

SA WG3 TD Number	Title	Source	Comment	Original WG TD number
S3-010305	Reply to LS S3-010290 on integrity protection at RLC/MAC level	GERAN	Response in TD373	GP-011368
S3-010306	Authentication between "GERAN" MS and 3G CN	GERAN	Noted	GP-011452
S3-010307	LS reply to SA1 LS “regarding User Profile”	SA WG5	Noted	S5-010312
S3-010308	LS in reply to three related User Equipment Management liaisons	SA WG5	Response in TD375	S5-010313
S3-010309	IMT2000 Management Co-operation	SA WG5	Response in TD376	S5-010323
S3-010310	Reply to N1-010890 “Liaison Statement on the IM Call Transfer service”	SA WG5	Response in TD292 (meeting #18)	S5-010324
S3-010311	Liaison Statement in Regards to Digital Rights Management	SA WG4	Noted	S4-010429
S3-010312	Reply to “LS on Extended Streaming Service” and “LS regarding User Profile"	SA WG4	Noted. Response in TD377	S4-010431
S3-010313	WI on the End-to-End QoS Architecture for Release 5	SA WG2	Response in TD378	S2-011098
S3-010314	Response to LS (GAHW-010109, R3-010890 and S2-010383) on Optimised IP speech and header removal support in GERAN	SA WG2 (RAN WG2)	Response in TD379	S2-011393 R2-010978
S3-010315	LS Concerning Reviews of UE Functionality Split	T WG2	Noted (Joint meeting)	T2-010426
S3-010320	WITHDRAWN - LS from CN WG4 on MAP security	CN WG4	WITHDRAWN. Dealt with at NDS ad-hoc (TD228)	N4-010669
S3-010321	Response to LS on “Clarification of UMTS-AKA for GSM R’99 Mobiles” & support of UMTS AKA for GSM only R4 Mes	SA WG1	Noted	S1-000867 S3-010734 S3-010098

E.2 Liaisons from the meeting

TD Number	Title	Status	To CC
S3-010373	Reply to LS on integrity protection at RLC/MAC level, from GERAN (TD S3-010305)	Approved	**GERAN**
S3-010374	Reply LS to GERAN GP 011368 on integrity protection at RLC/MAC level (TD S3-010306)	Approved	**GERAN** **CN WG1**
S3-010375	Reply LS to SA WG5: WID on User Equipment (UE) Management (Feature) (TD S3-010308)	Approved	**SA WG5**
S3-010376	LS to SA WG5: IMT 2000 Management Co-operation (TD S3-010309)	Approved	**SA WG5**
S3-010377	Reply to Liaison Statement to SA WG4 “LS on Extended Streaming Service” and “LS regarding User Profile" (TD S3-010312)	Approved	**SA WG4**
S3-010378	Reply LS to SA WG2: “WI on the End-to-End QoS Architecture for Release 5” (TD S3-010313)	Approved	**SA WG2**
S3-010379	Response to LS (R2-010978) on Optimised IP speech and header removal support in GERAN (TD S3-010314)	Approved	**RAN WG2** **GERAN,** **RAN WG3,** **SA WG2**
S3-010382	LS to SA WG2, CN1, CN4: Flows related to Authenticated Registrations and Re-Registrations	Approved	**SA WG2** **CN WG1** **CN WG4**
S3-010383	LS to GSMA SG and Fraud Forum: Matters arising about the potential fraud scenarios in 3GPP	Approved	**GSMA SG,** **Fraud Forum**
S3-010387	LS to CN WG1, CN WG4 and SA WG2: Stage 2 information flows for authenticated registration and re-registration in the IMS	Approved - attach TD355	**SA WG2** **CN WG1** **CN WG4**
S3-010398	LS to SA WG2, CN WG1: Network Configuration Independence Mechanism	Approved. Contains proposed CR to 23.228 to SA WG2	**SA WG2** **CN WG1**
S3-010400	LS to SA WG1, T WG2 and T WG3: IMS access security and the UE split	Approved. - attach TD392	**SA WG1** **T WG2** **T WG3**
S3-010401	Reply LS to SA WG4 (TD S3-010311) (SA WG3 Chairman to provide)	**For e-mail approval**	**SA WG4**
S3-010402	LS to SA WG2, CN WG4, CC: SA WG1, CN WG1: Requirements related to private and public identities in IMS	Approved - attach TD 328 and TD 367	**SA WG2** **CN WG4** **SA WG1** **CN WG1**
S3-010403	LS to SA WG2, CN WG1 and CN WG4: the use of Network Domain Security for protection of SIP signalling messages	Approved	**SA WG2** **CN WG1** **CN WG4**
S3-010404	Liaison Statement to CN WG1, CC: SA WG2, SA WG5, CN WG4, CN WG5: "Progressing the work in SA3 and CN1 on the IP Multimedia core network subsystem"	Approved (Replacement of TD391, which was erroneously saved)	**CN WG1** **SA WG2** **SA WG5** **CN WG4** **CN WG5**