3GPP TSG SA WG3 Security — S3#16 S3-000697
28-30 November, 2000
Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#16 S3-000697
28-30 November, 2000
Sophia Antipolis, France

3GPP TSG SA WG3 Security — S3#15bis ad-hoc

Ad-Hoc meeting 08-09 November, 2000

Munich, Germany

Source: Secretary 3GPP TSG-SA WG3

Title: Draft report version 0.0.3

Document for: Approval

Contents

1 Opening of the meeting 2
2 Meeting objectives 2
3 Approval of the agenda 2
4 Registration and assignment of input documents 2
4.1 General Discussion (Limited to 1 hr Wednesday) 2
4.2 IM subsystem security 2
4.3 Network Domain Security 4
5 IM subsystem security (Rapporteur Krister Boman) 6
6 Network Domain Security (Rapporteur Geir Koien) 6
7 Any other business 6
8 Close of meeting 6
Annex A: List of documents and their status at the meeting: 7
Annex B: List of Participants 9

1 Opening of the meeting

The Chairman, Michael Michovici, welcomed delegates to the SA WG3 ad hoc meeting, in Munich, Germany, hosted by Siemens. Mr. G. Horn (Siemens) welcomed delegates to Munich and provided the domestic arrangements for the meeting.

2 Meeting objectives

The Chairman outlined the objectives, which were to discuss IM Subsystem Security, network domain security and some critical Release 2000 items (limited in time to 1 hour), including GPRS work.

3 Approval of the agenda

The draft agenda, provided in TD S3z000003 was approved without changes.

4 Registration and assignment of input documents

The available documents were allocated to their respective agenda items.

4.1 General Discussion (Limited to 1 hr Wednesday)

TD S3z000011: Draft LS on Integrity Protection in GERAN. This LS from GERAN on options for integrity protection of signalling messages was presented by P. Howard, and the proposed response in TD S3z000024 was considered.

TD S3z000024: Proposed Reply LS on GERAN integrity protection. This proposed reponse to GERAN recommended that the reduction of MAC length to <32 bits was not in line with the recommendations from ETSI SAGE, and that 32 bits was considered the minimum protection needed. It also did not recommend the ability to switch on and off the protection due to the potential delay to the GERAN work in developing a secure mechanism to do this. Thirdly, it stated that the protection in GERAN should be at least equivalent to that in UTRAN and therefore the MAC protection was required. The proposal was modified slightly and agreed in TD S3z000032.

TD S3z000012: Integrity-protection for GERAN-signalling. This proposal for the protection of GERAN messages using a MAC which could be varied in length depending upon the space left in the message for the MAC bits was considered. It was commented and generally agreed that reduction in security requirements should only be made on explicit request for technical reasons, and not proposed by SA WG3, and that GERAN should be asked to identify exactly which messages would need a reduced MAC length for reasons of efficiency, so that SA WG3 could consider mechanisms. This information was included in the LS to GERAN in TD S3z000032.

TD S3z000030: Proposed Reply LS to "Protection of GTP Messages using IPSec". This liaison was considered along with TD S3z000004: LS from CN WG4 on Protection of GTP Messages using IPSec, and was discussed and agreed (with minor modifications) in TD S3z000033. (TD S3z000004 was noted).

TD S3z0000026: Liaison Statementfrom GERAN regarding ciphering of RRLP messages between the SMLC and MS in GPRS. This LS on LCS was not discussed in the meeting, but was forwarded to the SA WG3 meeting #16 for consideration.

4.2 IM subsystem security

TD S3z000028 and TD S3z000029. These contributions contained TS 23.228 version 1.0.0, with and without revision marks, and were provided for information for the discussions below and were noted. It was also noted that version 1.2.0 now exists.

TD S3z000010: Authentication and protection mechanisms for IM CN SS. This was presented by Ericsson, followed by the presentation of TD S3z000022: IMS authentication and integrity/confidentiality protection, by Siemens, using the slides provided in TD S3z000035. The Ericsson contribution proposed a method of providing Integrity and Confidentiality mechanisms in different Network Elements. The Siemens presentation suggested some disadvantages of this method and proposed a method where the mechanisms are co-located in a single NE, avoiding the disadvantages of the Ericsson proposal.

A discussion of both contributions followed and the different approaches were identified as being due to different interpretations of SA WG2 TS 23.228 definition of the proxy CSCF funtionality. It was agreed that a liaison to SA WG2 was needed on this for clarification and further discussion in SA WG3. The Ericsson contribution also pointed out the need for liaison to SA WG2 on the use of IMSI for user identity. It was agreed that this should be done for approval at SA WG3 meeting #16.

ACTION AH01: **Ericsson to draft an LS to SA WG2 on clarification of the proxy CSCF function and to consider the need for a LS on the use of IMSI for user identity, for discussion and approval at SA WG3 meeting #16.**

The need to specify the requirements for “Trust“ for the visited network, etc. was also identified, before any of the detail of the mechanisms could be discussed. AT&T Wireless agreed to send relevant draft RFCs on Trust Management to SA WG3 for information, and to contribute these to the SA WG3 meeting #16, along with a short presentation on Trust Management (15 minutes).

ACTION AH02: **AT&T Wireless to provide RFCs on Trust Mamagement to SA WG3 and provide a short presentation at SA WG3 meeting #16.**

TD S3z000027: S-CSCF issues and security in IM CN SS. This contribution suggested that SA WG3 should urgently look at the SA WG2 security architecture work, which has developed with little involvement of SA WG3. It was agreed that SA WG3 delegates should analyse the architecture work and provide contribution to SA WG3 meeting #16 in order to provide an agreed position to SA WG2 on any identified problems.

TD S3z000037: Some notes on 3GPP TSG CN1 SIP #1 meeting. This contribution requested that SA WG3 views are provided to CN WG1 and SA WG2 on many issues identified at the meeting. It was agreed that these issues should be the subject to contribution to SA WG3 meeting #16. The following general principles were agreed, for contributions:

- Minimise the trust needed between 2 parties.
- Minimise the number of entities which have trust
- Scalability of trust
- Trust models in the new architecture
- Degrees of trust
- Whether the home network can devolve trust
- Regulate “transitivity“ of trust
- Formulate trust in terms of risk assessment
- Performance issues
- Lawful Interception issues
- Access independence issues
- “Fate sharing“ – each entity has most to lose by exposing its’ own secret information.

ACTION AH03: **C Brookson to e-mail a list of trust issues for discussion before SA WG3 meeting #16.**

TD S3z000008. TR 33.8xx v0.2.0: Principles of Access security for IP-based services. This was provided by Telenor for information and was noted. This draft TR will be updated by the editor taking into account the results of discussions at this meeting.

TD S3z000009. TS 33.xxx v0.1.0: Access security for IP-based services. This was a skeleton (ToC) awaiting inclusion of some agreed material from TR 33.8xx (TD S3z000008). It was provided for information and noted.

TD S3z000023. Comments on 3G TR 33.8xx and 3G TR 33.800. These comments were discussed and the editor agreed to include comments in the drafts. It was noted that these documents are Release 5, but early completion is desirable in order to allow the stage 3 to be developed in good time.

4.3 Network Domain Security

TD S3z000007: TR 33.800 v0.2.4: Principles for Network Domain Security. This TR was provided for information. And noted. It will be updated by the Rapporteur (Mr. G. Koien) with the agreed contributions from this meeting and presented to SA WG3 #16 (see below).

TD S3z000013. General Structure of Secure MAP Operations. This contribution was introduced by Ericsson and discussed. It was questioned whether the Protection Mode 0 is still relevant, when it provides no security enhancement, and the newly proposed Security Protection Profiles (PPs) – see TD S3z000014. Some concerns were expressed over the order of the messages to be protected by the MAC functions. It was agreed that these concerns should be further investigated and a cross check with TS 29.002 should be performed, and contributions made to SA WG3 meeting #16. CN WG4 also needed to be asked about the policy on message protection in the Core Network and the value of the implementation of Protection Mode 0, with respect to signalling load.

Ericsson agreed to draft a liaison statement to CN WG4 for discussion and approval by the SA WG3 meeting #16.

TD S3z000014: Protection Profiles for MAP Security. This contribution proposed the introduction of a set of Protection Profiles, and provided some example profiles showing which mesages to be protected under different PPs. The examples were based upon the MAP messages to be protected as identified by SA WG3 previously. It was considered that further analysis of the message protection requirements was needed. Comments to this contribution were also provided in TD S3z000031.

TD S3z000031: Comment to S3z000014. This included an embedded document showing proposed revisions to TD S3z000014 and suggests that “Fallback“ should be against the Protection Profile, and not the Security Association. It was also considered that negotiation mechanism would need to be defined to deal with changing PPs until an acceptable PP is agreed, which could endanger the timescales for Rel4 MAP Security.

TD S3z000015: Structure of Security Header. Some discussion over the inclusion of the original Component Identifier occurred, as this could be more properly included in the SPI, as it is not a Security item. It was agreed that this should be questioned on a contribution basis to SA WG3 and CN WG4.

TD S3z000016: Refinement of MAP Security Association. This contribution was introduced and discussed. It was commented that the definition of the SA lifetime should be made more precise, and described as an expiry time rather than a duration. It was also commented that the MAP Protection Profiles would be agreed in general between Operators, rather than sent as SA parameters. It was finally agreed to include this in the TR, and contributions were invited for the SA WG3 meeting #16.

TD S3z000017. Replay Protection for MAP Security. It was suggested that slowly-changing IVs could be a security weakness. This was discussed, and it was requested that a paper with supporting information on this suggestion should be contributed to the next SA WG3 meeting #16 for consideration.

TD S3z000018: MAP Security Domain of Interpretation for ISAKMP. This IETF draft RFC was provided for information. Delegates were asked to consider the document and provide detailed comments to the IETF. The document was then noted.

TD S3z000021: SA negotiation protocol for the ZA interface. This contribution was introduced using presentation slides, provided in TD S3z000034. It detailed suggested problems with the use of IKE for SA negotiation using KACs. After some discussion and explanation, it was considered that this requires serious consideration, and urgent contributions should be made to SA WG3 meeting #16 to come to a decision on the use of IKE for this.

TD S3z000019: Introduction of MAP security. This contribution requested the mandatory support of MAP Security after a cut-off date to be specified. This would cause much debate for operators and manufacturers to comply with the cut-off date and after discussion it was agreed that Operators and Manufacturers should be consulted. Mr. C. Brookson undertook to contribute this to the GSMA to get their reaction and to look for a suitable cut-off date which can be complied with.

ACTION AH01: C. Brookson to take the question of a cut-off date for Mandatory Support of MAP Security to the GSM Association at their next meeting and report back to SA WG3.

TD S3z000020: Modification of MAP security header. This contribution outlined the request from CN WG4 for clarification from SA WG3 on the definition of the MAP Security header. Ericsson agreed to produce a proposed liaison statement to CN WG4 for consideration at SA WG3 meeting #16. (Other items were later included in this draft LS).

ACTION AH02: Ericsson to produce a draft LS to CN WG4 for consideration at SA WG3 meeting #16. LS to include MAP Security Header information (S3z000020),

TD S3z000007: TR 33.800 v0.2.4: Principles for Network Domain Security. The open issues detailed in this TR were introduced by the Editor, as background for discussion of TDs S3z000023, S3z000002 and S3z000025.

In addition, it was noted that Lawful Interception part had no material. It was requested that the SA WG3 LI group consider appropriate input under this item. Mr. B. Wilhelm agreed to ask SA WG3 LI group for this at their next meeting.

ACTION AH03: B. Wilhelm to ask SA WG3 LI group for input to TR 33.800 on relevant LI issues at their November 2000 meeting.

It was also noted that the Definitions, abbreviations should be contributed to the 3GPP Vocabulary document (TR 21.905). It was agreed to replace the content of Clause 4 with references to the relevant information, instead of duplicating the text in the TR. It was further noted that the Ga interface (charging information) had not been standardised so that the feasibility of protecting this interface in a standardised way would need to be investigated. Contribution on this was required if any progress is to be made.

The Iu/Iur interfaces were also in need of contribution for final decision on the inclusion of security work on these interfaces at the SA WG3 meeting #16.

Delegates were asked to consider all the open issues provided in the TR and to make comments to SA WG3 meeting #16 in order to finalise the document for provision to SA meeting #10 in December 2000 for information.

TD S3z000023: Comments on 3G TR 33.8xx and 3G TR 33.800. This provided comments to TR 33.800 (TD S3z000007). The main concern was the inclusion of much of the material in the TR into the companion TS. The Editor undertook to try to make a identify and mark within the TR, what is expected to be included in the TS.

The editor, Mr. G. Koien agreed to update the TR with all comments received at this meeting and distribute as soon as possible for consideration at SA WG3 meeting #16.

Mr. Koien also indicated that he would be preparing a contribution to SA WG3 meeting #16 suggesting that tunnel-mode was used everywhere to simplify the security. Delegates were asked to consider the pros and cons of the suggestion for contribution to SA WG3 meeting #16.

TD S3z000002: Network Domain Security: 3G TS 33.1de V0.0.1. No contribution had been received for this document and input was requested. The editor, G. Koien agreed to include the parts of TR 33.800 that he considered relevant for this TS for distribution and input to SA WG3 meeting #16 in order to stabilise it for presentation at SA meeting #10 for information. Contribution on this was therefore urgently requested for the SA WG3 meeting #16.

TD S3z000025: Security Services using Public Key Cryptography. This contribution was introduced by Motorola and argued that symmetric key schemes were adequate for the one to many environment, but that the many-to-many environment envisaged for IP-based networks required an asymmetric key system. It suggested that a WI be defined in SA WG3 to include this for Rel4, or to include it within a suitable existing Rel4 WI for MM Access. Mr. Brookson reported that PKI had been evaluated for GSM, but rejected on the grounds of signalling load and smart-card capacity limitations, when using PKI in the wireless environment. These constraints would need re-evaluation for 3GPP systems. It was also stated that the use of PKI in the wireless environment had already been discussed and rejected by SA WG3, following the joint CN/SA WG3 meeting.

It was also questioned whether MultiMedia security was to be covered in the wireless environment, and this would need further discussion in SA WG3 meeting #16. Contributions on this subject were invited.

TD S3z000005: Inter-PLMN Backbone Guidelines. This contribution was provided for information, and noted.

5 IM subsystem security (Rapporteur Krister Boman)

This was dealt with under agenda item 4.1.

6 Network Domain Security (Rapporteur Geir Koien)

This was dealt with under agenda item 4.3.

7 Any other business

There was no contribution under this agenda item. It was noted that Emergency Call issues would need to be handled at SA WG3 meeting #16 and contributions were requested in advance in order to progress towards a solution.

8 Close of meeting

The Chairman thanked the hosts for providing the facilities, and the delegates for their hard work and closed the meeting.

Annex A: List of documents and their status at the meeting:

NUMBER	TITLE	SOURCE	AGENDA ITEM	Document For	REPLACED BY
S3z000001	Principles of Newtork Domain Security: TR	Telenor	4.3		S3z000007
S3z000002	Network Domain Security: 3G TS 33.1de V0.0.1	Telenor	4.3		
S3z000003	Draft agenda for the ad-hoc meeting	Chairman	2		
S3z000004	LS on Protection of GTP Messages using IPSec	CN WG4	4.1		
S3z000005	Inter-PLMN Backbone Guidelines	Telenor (original: GSMA)	4.3	Information	
S3z000006	Proposed Reply LS to CN WG4: "Protection of GTP Messages using IPSec"	Telenor	4.1	Discussion	S3z000030
S3z000007	TR 33.800 v0.2.4: Principles for Network Domain Security	Rapporteur (Telenor)	4.3	Information	
S3z000008	TR 33.8xx v0.2.0: (Principles of) Access security for IP-based services	Rapporteur (Telenor)	4.2	Information	
S3z000009	TS 33.xxx v0.1.0: Access security for IP-based services	Rapporteur (Telenor)	4.2	Information	
S3z000010	Authentication and protection mechanisms for IM CN SS	Ericsson	4.2	Discussion / Decision	
S3z000011	Draft LS on Integrity Protection in GERAN	TSG GERAN	4.1	Discussion	
S3z000012	Integrity-protection for GERAN-signalling	Siemens	4.1	Discussion	
S3z000013	General Structure of Secure MAP Operations	Ericsson	4.3		
S3z000014	Protection Profiles for MAP Security	Ericsson	4.3		
S3z000015	Structure of Security Header	Ericsson	4.3		
S3z000016	Refinement of MAP Security Association	Ericsson	4.3		
S3z000017	Replay Protection for MAP Security	Ericsson	4.3		
S3z000018	MAP Security Domain of Interpretation for ISAKMP	Ericsson	4.3		
S3z000019	Introduction of MAP security	Siemens	4.3	Discussion/ Decision	
S3z000020	Modification of MAP security header	Siemens	4.3		
S3z000021	SA negotiation protocol for the ZA interface	Siemens	4.3		
S3z000022	IMS authentication and integrity/confidentiality protection	Siemens	4.2		
S3z000023	Comments on 3G TR 33.8xx and 3G TR 33.800	Siemens	4.3		
S3z000024	Proposed Reply LS on GERAN integrity protection	S3_15bis_Adhoc	4.1	Approval	
S3z000025	Security Services using Public Key Cryptography	Motorola	4.3	Discussion	
S3z000026	Liaison Statement to SA WG3 regarding ciphering of RRLP messages between the SMLC and MS in GPRS	TSG GERAN	4.1	Discussion	
S3z000027	S-CSCF issues and security in IM CN SS	BT	4.2	Discussion	
S3z000028	3G TS 23.228 V1.0.0 (with revision marks)	BT	4.2	Information	
S3z000029	3G TS 23.228 V1.0.0 (revision marks accepted)	BT	4.2	Information	
S3z000030	Proposed Reply LS to "Protection of GTP Messages using IPSec"	Telenor/Motorola	4.1	Discussion	
S3z000031	Comment to S3z000014	Siemens	4.3		
S3z000032	Reply LS on GERAN integrity protection		4.1		
S3z000033	Reply LS to "Protection of GTP Messages using IPSec"		4.1		

NUMBER	TITLE	SOURCE	AGENDA ITEM	Document For	REPLACED BY
S3z000034	SA negotiation protocol for the ZA interface (presentation slides)	Siemens	4.3		
S3z000035	IMS authentication and integrity/confidentiality protection (Presentation slides)	Siemens	4.2	Information	
S3z000036	SOME NOTES ON 3GPP TSG CN1 SIP #1 MEETING 17TH – 19TH OCTOBER 2000, SOPHIA ANTIPOLIS, FRANCE	BT	4.2	Information	S3z000037
S3z000037	SOME NOTES ON 3GPP TSG CN1 SIP #1 MEETING 17TH – 19TH OCTOBER 2000, SOPHIA ANTIPOLIS, FRANCE	BT	4.2	Information	

Annex B:
List of Participants

Name	Firma
Günther Horn	Siemens AG
Dirk Kröselberg	Siemens AG
Klaus Müller	Siemens AG
Marc Blommaert	Siemens ATEA
Michael Marcovici	Lucent
Uri Blumenthal	Lucent
Maurice Pope	ETSI
Takeshi Chikazawa	Mitsubishi
Peter Howard	Vodafone
Sebastien Nguyen Ngoc	France Telecom
Geir M. Køien	Telenor R&D
Per Christoffersson	Telia
Dan Brown	Motorola
Lily Chen	Motorola
Stephen Billington	Motorola
Krister Boman	Ericsson
Anders Liljekvist	Ericsson
David Castellano	Ericsson
Valtteri Niemi	Nokia
Berthold Wilhelm	RegTP
Charles Brookson	Department of Trade and Industry, U.K.
Roland Schmitz	T-Nova
Peter Windirsch	T-Nova
Patrick Johnson	Nortel Networks
J. Ioannidis	AT&T Wireless
Benno Tietz	d2mannesmann
Colin Blanchard	BT