3GPP TSG SA WG3 Security — S3#17bis **S3z010050**
23rd April – 24th April
Madrid, Spain

3GPP TSG SA WG3 Security — S3#17 **S3-010105**
27 February - 02 March, 2001
Gothenburg, Sweden

Draft 01

Minutes of the S2/S3 joint meeting

27th of February and 1st of March 2001
Gothenburg, Sweden

Chairman: Teuvo Järvelä, Nokia
Meeting Support: Alain Sultan, ETSI

Table of Content

S2/S3 joint meeting
27 February + 1 March 2001
Minutes Draft 01

Note: for the hyperlinks to work, the tdocs have to be stored zipped individually in the sub-folder "\tdocs".

This joint meeting between 3GPP TSG SA WG2 and WG3 took place on 27th of February afternoon and 1st of March 7.15 a.m. to 10 a.m. 2001. It was hosted by Ericsson, in Gothenburg, Sweden.
The meeting was chaired by Mr Teuvo Järvelä from Nokia and supported by Mr Alain Sultan, MCC.

1. Approval of the agenda

S3-010084 from S3 chairman: *Draft agenda for the joint SA WG2/SA WG3 meeting*
The agenda was approved without modification.

2. S2 presentations

S2-010722 from Nokia: *Presentation to S2/S3*
Mr. M. Puuskala from Nokia, just elected as new S2 chairman, gave an overall presentation of the latest development on S2 activities on the IM subsystem.
Conclusion: Noted. The presentation was highly appreciated by S3 delegates.

3. S3 presentations

S3-010082 from Ericsson: *aSIP-Access Security for IP-based services*
Mr. K. Boman from Ericsson gave a presentation on aSIP-Access Security for IP-based services. This consists in defining the new security functions related to the introduction of the IM subsystem. This item has to be completed on time for Rel5 (Dec. 2001).
Discussion: AT&T wondered how there can be a secured relationship directly between UE and S-CSCF knowing that it was decided at S2 that the Proxy can modify the information (e.g. SDP part or URL translation). This point was further discussed later on.
"encryption" is meant for both the user plane and the SIP signalling plane.
Motorola stressed that S3's work should be continued in close cooperation with N1.
Possible interactions with IETF have also to be investigated.
The "security gateway" is to protect the traffic different networks: it is thought that it will not distribute keys between networks but will rather receive the flows, encrypt them if needed and send them to other network.
Conclusion: Noted. The presentation was highly appreciated by S2 delegates.

4. IM subsystem security – Open Discussion

4.1. General issues

S3-010028 from Motorola: *Trust Models for IM Domain Security*
This tdoc proposes to consider a public key method for IM domain security rather than a symmetric key method, which has intrinsic limitations.
Discussion: This topic was judged as only security related: some S2 delegates (like Ericsson) complained that there is no direct S2 involvement in the subject.
Vodafone and Alcatel remarked that the arguments apply mainly to end-to-end security, meaning that public key infrastructure domain and the asymmetric key are OK to guarantee that A is indeed talking to B. It was not clear if the same arguments can be used for security between end-user and network element.
Conclusion: Noted. This should be solved at S3.

S3-010076 from Siemens: *An analysis of 3G TS 23.228 v170 "IP Multimedia Subsystem - Stage 2" from a security point of view*
This document analyses the security implications of some IMS procedures:
The Codec negotiation during initial session establishment leads to the fact that P-CSCF is able to modify SIP messages (e.g. to eliminate the codecs that it does not support).
In the Mobile terminal initiated session release procedure, the P-CSCF releases in 4 the local resources before the home network is contacted, meaning that the P-CSCF should be able to check the integrity of release messages (otherwise anybody can terminate a call of anybody else).
Another main conclusion is that there is a need for network domain security between GGSN and P-CSCF and between P-CSCF and S-CSCF.
Discussion: Alcatel reminded that the P-CSCF can also modify the SIP or E-164 number e.g. for the translation of local numbering to standard numbering.
A possible solution is that S2 clarify which fields might be modified by the P-CSCF, so there are not covered by integrity protection.
A key question is for S3 to know more precisely what roles are playing the P-CSCF and the S-CSCF.
It was noted that the end point for authentication might be different than the end point for integrity.
Conclusion: Noted.

S3-010077 from Siemens: *Considerations on trust and risk*
This contribution makes a threat and risk quick analysis and concludes that a certain degree of trust in the P-CSCF is unavoidable, and it doubts that there is some benefits in having the security functions performed by the home control.
Discussion: The case of Sweden, where different network operators share part of a same infrastructure, has also to be considered, according to Vodafone.
Conclusion: Noted.

S3-010078 from Siemens: *Summary of arguments*
This paper further comments that confidentiality function shall be located in the P-CSCF, it shall terminate integrity protection, and shall also perform final authentication check. None of these functions shall be shared with S-CSCF to simplify the specification.
Discussion: "Confidentiality" means here encryption of the SIP messages between the end-user and the network.
AT&T asked S3 if there are some specific security implications in the compression between UE and the proxy-CSCF: S3 has not studied the issue yet.
Conclusion: Noted.

S3-010080 from Siemens: *Overview of alternative information flows for IMS authentication and key agreement*
This presentation introduces Siemens and Ericsson views on how to do authentication in IMS at registration.
Discussion: Alcatel wondered why, in the Ericsson proposal (slides 4 and 5), the IK is communicated to the S-CSCF only at the end of the procedure, implying the HSS to provide the security information "slide by slide".
S3 has no clear answer on this point which needs further studies.
Conclusion: Noted.

S3-010079 from Siemens: *Open issues beyond location of security functions*
Siemens remind a set of uncorrelated open points for security in IMS, e.g. which entity initiates re-authentication during calls, user IMS identity in REGISTER procedure needs to be protected, etc.
Discussion: It was clarified that ciphering is indeed needed, on top of GPRS ciphering mechanisms.
On the question to introduce or not a TMSI-like identity, Alcatel and Lucent's opinions are that it is not needed: the interest of TMSI is that it avoids sending the IMSI in clear when the mobile is paged, but here the NAI is not used for paging.
Vodafone reminded that encryption has a cost, and it should be avoided if not really needed: encryption is already provided on the radio link. If some countries do not allow encrypting on the radio, it is very probable that they will not allow encryption in the network neither.

In slide 5, Alcatel explains that bullet 2 is answered in 23.221 and bullet 4 has not been considered so far (handover between IM domain and other domain).
The initiation of authentication at call set-up by the UE mentioned in slide 2 are explained to take place e.g. in cases where the keys have a limited time validity.
Conclusion: Noted.

S3-010081 from Ericsson, Nokia, Lucent and Orange: *Authentication and protection mechanism in the IMS*
By opposition to Siemens' point of view, it is argued here that authentication shall be performed by the home network, and integrity protection shall terminate in the home too. The main argument is that S3 should follow the same reasons which have lead S2 to replace the "hybrid" model of service control by having all the service control being performed in the Home.
Discussion: The same arguments as the ones presented in the contributions were repeated.
Conclusion: No conclusion on this item, which was further discussed at S2 on 28th of February (see S3-010100 presented bellow).

S2-010656 from Siemens: *Correction to Caller-ID Call Flow in TS23.228*
To reflect the current status of S3's work and to avoid duplication, it is proposed to remove the Registration part of the flow, the corresponding descriptive text, and the references to the S-CSCF performing user authentication in chapter 5.12.4.1.
Discussion: An editor's note is missing in this section.
There is already a section on registration flows, so there should not be included here but a reference should be made instead.
Conclusion: Editorially revised to S2-010724.

> **S2-010724** from Siemens: *Correction to Caller-ID Call Flow in TS23.228*
> Revision of S2-010656.
> ***Conclusion:*** Approved.

4.2. CSCF related issues

S2-010512 from AT&T: *CSCF Security requirements*
This contribution addresses the security needs of P-, S- and I-CSCFs: they shall mainly maintain IPSec security associations.
Discussion: The proposed solution is adding some information in the header between UE and P-CSCF to support the IPsec data, but this was explained to be applicable to signalling and not to user data, so it might not be repeated on each packet.
The author clarified that this view is that, IPsec is intended to be used not only between I-CSCF (or S-CSCF) and other CSCF, but towards any other IMS node, as HSS.
Vodafone stressed that there is already encryption on the radio link and does not see the clear need to add another encryption mechanism as IPsec proposed here.
The discussions went then to disparate directions.
On 1st of March, the discussions were resumed at this point: AT&T clarified that their proposal can be broken in two parts: the need for security associations between the different IMS elements, and the use of IPsec to cope with this security.
Conclusion: See S3-010100.

S3-010100 from S3 Chairman: *Proposal on IM domain access security*
This one-page document makes a set of assumptions on security between the IMS nodes, taken on 28th of February by S3 in light of the discussions which took place on the first day of the joint S2/S3 meeting:
There should be a security association between UE and P-CSCF.
Between the P-CSCF and the S-CSCF, the security associations are not user specific here and are established via the Network Domain Security mechanisms.
The authentication is performed in the home network.
This contribution does not address neither the use of IPsec nor the security association between other nodes (which are said to be ffs).
Discussion: There was no disagreement on these assumptions, apart from the title "Proposal on IM domain access security" which is not clear. It was explained that this refers to the security between the "IM user" and the IM CN Subsystem. This document can be sent by S3 to the CN groups.

For the security associations between P- and S-CSCF, "when needed by operational conditions" shall however be added in the final document, as these associations are not necessarily needed (this has to be clarified in the final text, maybe in 23.200). It was however judged useless to repeat this statement in 23.228.
Conclusion: This document is taken as a basic assumption.
Back on S2-010512: on P-CSCF: it was temporary agreed to replace the sentence "maintain an IPSec Security Association between itself and each UE, and between itself and each next-hop address for each registered UE." by "maintain a Security Association between itself and each UE and maintain security association between itself and S-CSCF as defined in the Network Domain Security mechanisms." The text on I- and S-CSCF should also be aligned to what is stated in S3-010100 and shall not state anything more.
References to Access Security (TS 33.2xx) and to Network Domain Security (TS 33.200) should also be added in 23.228 . S2-010755 clearly reflects these changes.

> **S2-010755** from AT&T: *CSCF Security requirements*
> Revision of S2-010512 taking into account the discussions on S2-010512 and S3-010100.
> ***Conclusion:*** Approved.

4.3. Public and private identities

S2-010660 from N1-010275: *LS on "IM User Identities"*
N1/S2 SIP drafting asks some questions to S2 and S3 with respect to the private identity, i.e. they want the full intended use of the Private Identity including mandatory and optional uses to be clarified.
Discussion: S2-010701 is related to the issue.
Conclusion: Proposed answer in S2-010701.

> **S2-010701** from Motorola: *Usage of Public and Private Identities of IM users*
> Motorola propose to have clear definitions of Public and Private Identity and their use.
> ***Discussion:*** After some confusion on 14, it was concluded that this is in line with GSM, where the Public identity (MSISDN) is also stored on the SIM.
> On multiple registrations, Alcatel noticed that it's perfectly feasible to have e.g. 10 identities stored on the USIM, but it won't be realistic to register all of them each time a registration is performed.
> It was then preferred to have the registration made only on the unique Private identity and another mechanism to be used to link the public ones to the private one: e.g. the S-CSCF may retrieve from the HSS all the public ones based on the private one. It should be enough if only the S-CSCF (and potentially some application servers) knows all the Public Identities, but if the Access Network, the P- and I-CSCF handle only the Private one.
> It was mentioned that there could be some security problems if the private identity is sent un-encrypted at registration.
> It was discussed if Rel5 can be limited in having only one Public identities, but Alcatel stressed that there will be at least two, namely the E.164 number and the SIP/IP URL, so an efficient mechanism for multiple registrations has to be found right from the beginning.
> Lucent proposed to register any of the public identities and then ENUM is used for the binding of all the identities.
> As no clear conclusion was reached on the registration, this point was deleted from the proposal (point 5).
> Nokia appreciated the idea of collecting all the information on Public and Private identities, but mentioned that some further refinements are needed, e.g. on the charging records.
> A review bullet by bullet was finally performed:
> 2: problem for Ericsson to have the private identity passed only at Registration. "this is the only time it should be sent in SIP messages" is a better wording. It could not be agreed. So 2 is deleted.
> 3 postponed: an LS from T2 is expected,
> 6 is deleted (implementation issue)
> 7 has to be combined with 5 (5 and 7 cover the same issue)
> 8: second sentence is deleted (S5 issue)
> 11: to be re-worded to be non-restrictive
> 12: the second sentence has to be deleted (not agreed)
> 14: postponed: needs T3 input
> 15: deleted (on registration of public identities)
> 17: postponed: needs T3 input

18: rewording needed.
No comment on bullets 1, 4, 5, 9, 10, 13, 16.
Conclusion: Revised to S2-010756. The corresponding LS is in S2-010757.

S2-010756 from Motorola: *Usage of Public and Private Identities of IM users*
Revision of S2-010701.
Conclusion: To be discussed at S2.

S2-010757 from Motorola: *LS on Usage of Public and Private Identities of IM users*
Proposed LS to N1 related to S2-010701.
Conclusion: To be discussed at S2.

4.4. Other issues

S2-010606 from Lucent: *Use of AAA with CSCF*
The paper proposes to use Diameter for user authentication.
Discussion: AT&T was strongly against the idea to have AAA mechanisms on top of the existing mechanisms. Lucent explained that AAA security will apply to IMS, not precluding the existing mechanisms to be used for the existing purposes.
S3 mentioned that the choice of the protocol is not a matter for S2, but Lucent answered that in this case, as for the selection of SIP, there might be some architectural impacts, so S2 might be involved.
It was agreed that this is a critical issue that cannot be decided quickly at this meeting.
Conclusion: Noted. An LS will be provided to S3 in S2-010758 to ask some recommendations on the protocol to be used. Siemens thought it was too early to send an LS because the charging architecture is not stable. Nokia mentioned that it was curious to send an LS to S3 from a joint S2/S3 meeting. However, the LS has to be written and S2 will decide whether to send it or o not.

S2-010758 from Lucent:
LS coming from discussions on S2-010606.
Conclusion: To be discussed at S2.

5. Future joint meeting(s) and coordination

Due to lack of time, all the tdocs could not be handled, in particular all the ones related to network hiding were not addressed.
S3 will propose a way forward to handle the remaining documents.

6. Closing of the meeting

The Chairman thanked the hosts for the organisation. He also thanked the delegates for their positive attitudes and the MCC support.

Annexes

Participant list

There is no specific list for this meeting. Refer to S2 and S3 participant lists.

Tdocs list

S2-010507	Lucent Technologies	Connection re-establishment on forward handover without Iur	23.060	209r2	F	R99
S2-010758	Lucent	- title not provided -				
S2-010757	Motorola	- title not provided -				
S2-010756	Motorola	- title not provided -				
S2-010755	AT&T	CSCF Security requirements				
S2-010724	Siemens	Correction to Caller-ID Call Flow in TS23.228				

S2-010722	Nokia	Presentation to S2/S3				
S2-010718	Nortel	Network hiding mechanism update to 23.228				
S2-010716	Ericsson	- title not provided -				
S2-010701	Motorola	Usage of Public and Private Identities of IM users				
S2-010660	N1-010275	LS on "IM User Identities"	LS in			
S2-010659	N1-010268	LS on Security implications of supporting "hiding"	LS in			
S2-010656	Siemens	Correction to Caller-ID Call Flow in TS23.228				
S2-010625	S3-000758	LS for "IM Subsystem Address Storage on USIM "	LS in			
S2-010618	S1-010166	LS on UE functionality split	LS in			
S2-010606	Lucent	Use of AAA with CSCF				
S2-010602	Ericsson	- title not provided -				
S2-010539	S3 Chairman	Joint S2/S3 meeting agenda				
S2-010513	AT&T	Providing Secure Caller-identification				
S2-010512	AT&T	CSCF Security requirements				
S2-010511	AT&T	Network hiding mechanism				
S3-010100	S3 Chairman	Proposal on IM domain access security				
S3-010084	S3 chairman	Draft agenda for the joint SA WG2/SA WG3 meeting				
S3-010083	Ericsson	Providing the S-CSCF name to the P-CSCF				
S3-010082	Ericsson	aSIP-Access Security for IP-based services				
S3-010081	Ericsson, Nokia, Lucent and Orange	Authentication and protection mechanism in the IMS				
S3-010080	Siemens	Overview of alternative information flows for IMS authentication and key agreement				
S3-010079	Siemens	Open issues beyond location of security functions				
S3-010078	Siemens	Summary of arguments				
S3-010077	Siemens	Considerations on trust and risk				
S3-010076	Siemens	An analysis of 3G TS 23.228 v170 “IP Multimedia Subsystem - Stage 2” from a security point of view				
S3-010028	Motorola	Trust Models for IM Domain Security				

Tdocs not handled

Tdoc #	**Source**	**Title**	**Spec**	**CR #**	**cat**	**Rel**
S2-010507	Lucent Technologies	Connection re-establishment on forward handover without Iur	23.060	209 r2	F	R99
S2-010511	AT&T	Network hiding mechanism				
S2-010513	AT&T	Providing Secure Caller-identification				
S2-010602	Ericsson	- title not provided -				
S2-010618	S1-010166	LS on UE functionality split	LS in			
S2-010625	S3-000758	LS for "IM Subsystem Address Storage on USIM "	LS in			
S2-010659	N1-010268	LS on Security implications of supporting "hiding"	LS in			
S2-010716	Ericsson	- title not provided -				
S2-010718	Nortel	Network hiding mechanism update to 23.228				
S3-010083ı	Ericsson	Providing the S-CSCF name to the P-CSCF				
S2-010539	S3 Chairman	Joint S2/S3 meeting agenda				