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