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

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

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

Document for: **Information**

---

1 Opening of the meeting

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

2 Approval of the agenda and objectives of the meeting

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

3 Allocation of documents to agenda items

The available documents were allocated to their respective agenda items.

4 Liaisons from other groups

There were no inputs under this agenda item.

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

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

6 aSIP technical issues

6.1 Termination of authentication/signalling flows

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

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

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

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

Session establishment and Authentication of INVITE:

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

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

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

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

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

The location of the authentication comparison:

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

Nokia analysis (from contribution)

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

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

Ericsson stated that the difference in the impact on the HSS of the two approaches was only in the comparison of the RES and XRES, as the security parameters were retrieved or calculated by the HSS in any case. Siemens argued that in the HSS solution a significant number of extra parameters needed to be stored, which would increase the data storage requirements of the HSS significantly, given the large number of users it had to cater for compared to the S-CSCF, and that it opened up a risk to DoS attacks. Ericsson pointed out that ~~that~~ the S-CSCF solution also required the storing of most of the same parameters in the HSS.

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

Denial of service discussion:

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

After some discussion the following working assumption was agreed:

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

Re-authentication:

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

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

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

6.2 Protection mechanisms

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

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

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

This part of the presentation was noted.

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

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

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

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

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

It was proposed that confidentiality of SIP signalling is optional.

The following working assumption was agreed:

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

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

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

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

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

This part of the contribution was then noted.

6.3 Security mode setup

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

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

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

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

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

7 Other technical issues

7.1 Hiding requirements

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

7.2 Public vs Private identities

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

8 S2 issues

8.1 Questions from S3

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

9 Review of output documents

9.1 For joint session with S2, 26th April

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

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

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

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

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

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

9.2 For S3 plenary, 21-24 May

<TEXT NEEDED FOR THIS>

10 AoB

There was no other business signalled.

11 Closing of the meeting

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

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

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