3GPP TSG SA WG3 ad hoc **Draft Report v0.0.3**

Antwerp, Belgium

3-4 September 2003

Source:	**Vodafone**
Title:	**Draft report from SA WG3 ad hoc meeting, 3-4 September**
Status:	**For Comment**

Contents

1 Opening of the meeting

The Chairman, V. Niemi, opened the meeting and welcomed delegates on behalf of the hosts "Alcatel". Annelies Van Moffaert explained the local arrangements.

2 Agreement of the agenda and meeting objectives

TD S3z030001 Proposed agenda and objectives for the ad hoc meeting on GAA and MBMS. The draft agenda was reviewed.

The primary objectives of the meeting are:

- to reach a common understanding on the way forward in the development of a generic authentication architecture (GAA);
- to reach a common understanding on the key management needed for MBMS;
- to progress the work on other open issues in MBMS

The agenda was then approved.

3 Allocation of documents to agenda items

The documents were assigned to the respective agenda items.

4 Relevant LSs from other groups

TD S3z030004 Liaison statement (from SA WG2) on Generic Authentication Architecture. This was introduced by Nortel Networks. SA WG2 ask SA WG3 to develop guidelines on the criteria which should be used when choosing an authentication solution and to avoid if possible multiple new solutions to this problem, unless there are differing requirements which lead to a need for multiple solutions. The ad hoc agreed that guidelines would be needed especially if GAA is used by other groups outside 3GPP. The guidelines may also be useful internally by 3GPP. The LS was then noted.

TD S3z030030 LS (from T WG3) on potential USIM impact of the MBMS security framework. This was introduced by SchlumbergerSema. It was clarified that the proposal attached to the LS regarding the 3GPP2 mechanism was not endorsed by T WG3. It was also clarified that the proposal does not impose a logical limit on the number of BAKs that can be stored on the USIM. The LS was then noted.

> TD S3z030009 USIM enhancements for MBMS support. This is a duplication of the proposal attached to TD S3z030030.

TD S3z030031. Reply LS (from SA WG1) on clarification of MBMS charging issues. This was introduced by “3”. SA WG1 provides the following answers to SA WG3:

1. SA WG1 does not foresee the need to verify the exact amount of bits received by the user at the MBMS bearer level.
2. SA WG1 does not foresee the need to verify the exact reception duration by the user at the MBMS bearer level.

The LS was noted. This LS does not need to be reconsidered at SA3#30.

5 Generic authentication architecture

5.1 Open issues related to key management of HTTP-based services (results of AP29/09)

TD S3z030003 Generic Authentication Architecture requirements. This was introduced by Siemens and presents the result of AP 29/09 from SA3#29. SA WG3 is asked to endorse the list of GAA requirements identified during email discussion and use them as the basis for future work on a GAA. The list of requirements were reviewed and some modifications were made. The following requirements were then endorsed by SA WG3:

Requirements on GAA:

1. A Generic Authentication Architecture (GAA) shall provide shared secrets to entities for use with 3G security features for Release 6 and future releases. Features already specified for Release 5 and earlier releases shall not be affected by the GAA.
2. This provision of shared secrets shall be based on the 3G AKA infrastructure (bootstrapping from AKA).
3. The GAA should be applicable as widely as possible to 3G security features for Release 6 and future releases, whether they are http-based or not.
4. The co-existence of several bootstrapping procedures in the 3G architecture should be avoided. In particular, the co-existence of a procedure for bootstrapping of HTTP-based services (as in S3-030367 and S3-030371) and a procedure for generic bootstrapping, as described in the context of support for subscriber certificates (S3-030317), should be avoided.
5. Dependencies on external bodies should be minimised. This would still allow to re-use completed external specifications if seen beneficial.
6. The GAA should respect the HSS/HLR-related security architecture guidelines, as documented in S3-030460. If further guidelines and other criteria regarding service provision or the impact on other entities are agreed by SA3 in the future these should be taken into account in the design as well.
7. Traffic bottlenecks should be avoided. (In particular, it should be investigated whether an HTTP authentication proxy could be such a bottleneck.)
8. The GAA should be able to support applications requiring end-to-end security.
9. The usefulness of the cryptographic separation of keys among applications should be further investigated under the aspect of future-proofing the GAA. If found that such a separation may be useful the GAA should be able to support it.
10. The GAA should support scenarios which require mutual authentication between UE and application server, based on the bootstrapped shared secret. This should not preclude the use of the GAA in scenarios where mutual authentication is provided also using other means (e.g. network certificates).
11. The Generic Architecture should be able to allow the application servers and the terminal to acquire (re-)fresh keys for use.
12. It would be desirable for the GAA to be applicable to non-3GPP security features.
13. For Release 6, the GAA should concentrate on home-provided services, i.e.the authentication is always performed by a server in the home network. But the GAA should not prevent future extension to a scenario where the authentication is performed by a server in a visited networks.
14. The GAA should not mandate intervention by the human user.

Some remarks listed at the end of the contribution were also considered:

1. It needs to be clarified whether the use of subscriber certificates for authentication should be within the scope of the GAA, or whether the GAA should be limited to the provision of shared secrets (which may, of course, be used to obtain subscriber certificates, as specified in the draft TS on Support for Subscriber Certificates).
2. A suitable trade-off between the generality of the GAA and potential efficiency gains of customised solutions has to be found (potential inefficiencies: additional protocol runs, use of "heavy" protocols such as TLS when not needed).
3. Potential attacks should be carefully studied (Mitm attacks in tunneled authentication, missing link between identities at different layers, secure separation of authentication and key management functionality (BSF) from application traffic, etc.).
4. SA3 must decide to which features the GAA shall apply.
5. Discovery of BSF and / or AP by UE is to be clarified.

It was agreed to introduce the new term Generic Bootstrapping Architecture (GBA) which refers to the bootstrapping of shared secrets using the AKA protocol. It was noted that subscriber certificates is one of many applications which may make use of the GBA. The GAA may be realised using the GBA or subscriber certificates.

5.2 Different models and potential migration paths

TD S3z030008 Proposal for Generic Authentication Architecture. This was introduced by Nokia and proposes that a model based on the bootstrapping of shared secrets using the AKA protocol and the use of subscriber certificates is adopted for GAA such that some services can be secured using shared secrets and other services can be secured using subscriber certificates. The contribution states that allowing both symmetric and asymmetric key management solutions is preferable as it gives most flexibility to operators and service providers.

TD S3z030011 Generic Authentication Architecture evaluation. This was introduced by Siemens and includes a list of potential applications of a GAA. It was noted that GUP may be an additional application of a GAA (see Brad Owen's email to SA3 email list on 23rd July resulting from AP 29/08). It was clarified that rules are needed to protect against man-in-the-middle tunnelled authentication attacks in the optimised case described in section 6.2.2 of the contribution. Siemens were requested to prepare a further contribution on this for the next meeting. It was clarified that end-to-end security requirements between AS and UE are for further study – see section 4 of the contribution. The contribution proposed that the development of a GAA is based on the following statements:

1. A GAA should be based on TS SSC.
2. TS SSC should be modified and extended (if possible) to cover the case of a co-located AP in an optimal way, if feasible.
3. A GAA should respect the requirements on a GAA defined in S3z030003.
4. A GAA should respect the HSS-related guidelines in S3-030460.
5. SA3 must decide to which Rel 6 GAA should apply in which way.
6. Concrete security solution for a particular feature shall be specified in the pertinent TS, but as much reference as possible should be made to an update TS SSC.
7. A GAA should be designed in such a way that it is compatible with the use of reverse http authentication proxies.
8. The open issues relating to authentication proxies need to be solved.
9. Security aspects of the network configuration need to be studied further. In particular, it needs to be investigated whether a physical separation of the authentication and key agreement functionality from the application traffic enhances security.

TD S3z030025 IETF status report on HTTP Digest AKAv2. This was introduced by Ericsson and reports that the HTTP Digest AKAv2 has been submitted for Expert Review in IETF. Ericsson has also submitted a request to IANA for the HTTP Digest AKA algorithm value "AKAv2" to be assigned. SA WG3 is requested to review the draft and provide comments to the authors. It is expected that changes can still be made to the document after the Expert Review is completed in IETF. It is expected that the review will be quicker than the AKAv1 review. The latest version of the AKAv2 internet draft was attached to the contribution and presented by Ericsson. Some concerns were raised about the following statement in the internet draft: "The rules for an user agent for choosing among multiple authentication schemes and algorithms are as defined in [RFC3310] except that the user agent MUST choose "AKAv2" if both "AKAv1" and "AKAv2" are present." A new formulation may be needed to ensure that this does not conflict with IMS since it is not the intention of SA WG3 to use AKAv2 for IMS.

TD S3z030024 Generic Authentication Architecture based on AAA and AKAv2. This was introduced by Ericsson and proposes an AAA-based solution where protocol A in the BSF-based architecture is not needed. The contribution address some of the open issues relating to authentication proxies that were mentioned in TD S3z030011. Some concerns were raised that the proposal would not be generic enough solution if it were only applicable to HTTP-based applications. It is for further study whether the TLS tunnel is always needed between the UE and the Application Server. If AKAv2 is used both outside and inside a tunnel then a man-in-the-middle tunnelled authentication attack is possible. It was clarified that the authentication is run from the AAA server rather than from the NAF, which limits the problem of synchronisation failures due to interleaving authentication vectors.

TD S3z030029 Analysis of different approaches for GAA. This was introduced by Nortel Networks and reviews the pros and cons of four candidates for a GAA and looks at their applicability to several 3GPP and non-3GPP features. Nortel Networks supports a subscriber certificates based approach for GAA but may accept the use of SIM/AKA for some services for which time to market is critical e.g. 3G-WLAN. There was some disagreement with the claim in the contribution that we "can't assume all MBMS services will use HTTP – probably none will not all MBMS services will use HTTP". The following recommendations in the contribution were considered:

> 1) For each of the new 3GPP R6+ features, a single one of the above approaches should be chosen
>
> 2) 3GPP should develop some design criteria for this choice, so that it is not made independently for each service.
>
> 3) 3GPP should pursue only one of the general-purpose approaches – once the decision has been made to follow a general-purpose approach, there does not seem to be a strong argument for continue specifying two approaches.

Based on recommendation 1 it was agreed to have one authentication method per service for Release 6. However migration to other methods in future releases is not precluded.

Summary of proposals for a GAA

There are essentially three proposals under consideration:

> Siemens/Nokia: Start with BSF-based architecture and include special cases for an Authentication Proxy (AP) and a PKI portal as the NAF. Allow migration to subscriber certificates based approach.
>
> Ericsson: Start with Authentication Proxy / AAA based approach and migrate to a subscriber certificates based approach.
>
> Nortel Networks: Start now with a subscriber certificates based approach but allow SIM/AKA to be used for time critical Rel-6 features like WLAN.

It was clarified that the use of subscriber certificates as a GAA does not necessarily imply that the AKA protocol is used to bootstrap the provision of the certificate to the subscriber. Other provisioning methods such as the use of a long term key pair on a WIM are conceivable.

It is for further study if there is a way to remove the interface between the UE and the BSF/AAA (protocol A) as proposed in the Ericsson contribution.

It was agreed that an update of the diagram in section 6.2 of TD S3z030011 could be used to represent the architectural solutions under consideration for GAA.

AP 0309/01: G. Horn to update the diagram in section 6.2 of TD S3z030011 so that it captures the architectural solutions under consideration for GAA.

It was agreed that the GAA will be further developed based on the diagram to be provided by G. Horn and based on the open issues identified in TD S3z030003 and TD S3z030011.

With regard to the organization of specifications, it was agreed as a working assumption that the GAA (e.g. specification of the AKA bootstrapping architecture and special NAFs for the Authentication Proxy and the PKI portal) should be included in the same TS as the Support for Subscriber Certificates (SSC) feature. This working assumption may have to be revisited at SA3#30. The use of the GAA for a particular application should be included in the TS for that application (e.g.TSs for presence, MBMS, etc.).

5.3 Applicability to current work items (Presence, MBMS, WLAN,…)

TD S3z030010 MBMS Key distribution. Section 2.2 of the contribution was introduced by Siemens. It proposes that TLS is not used for MBMS key distribution since this solution is not extensible towards the UICC if a UICC based application may be required in the future.

TD S3z030018 MBMS Key distribution. This was introducted by Nokia and proposes that the AKA bootstrapping architecture (now called GBA) can be used for MBMS, presence and WLAN scenario 3. It was also proposed that migration to certificate-based solution should be allowed in later releases.

6 MBMS technical issues

6.1 Status of the draft TS after S3#29

TD S3z030028 MBMS security TS 33.246v0.2.0. This was introduced by "3". It was agreed to delete the editor's note at the end of section 4.1.4. It was agreed that changes made by the ad hoc meeting will be marked differently to those made at SA3#29.

TD S3z030017 MBMS architecture TS 23.246v2.0.0. This was introduced by Nortel Networks. The security section (section 9) was reviewed. The first security requirement to allow use of SIM and USIM contradicts the decision at the SA WG3/SA WG2 joint meeting in Milan in February that only the USIM should be used. The third requirement states that integrity protection is mandatory but it is optional in the SA WG3 specification. It was also suggested that SA WG2 replace section 9 with a reference to the MBMS security TS. It was agreed that the chairman would raise these comments at SA plenary.

AP 0309/02: Chairman to raise SA WG3 comments on MBMS architecture TS 23.246 at the SA#21 plenary meeting.

It was also discussed what is meant by the inclusion of security functions in Figure 7. If it represents the normal PS domain authentication and key agreement then there is no problem, but if it represents MBMS layer security functions then it contradicts the current proposals in SA WG3 for MBMS security. It was agreed that the rapporteur of the MBMS security TS should obtain clarification on this from SA WG2.

AP 0309/03: A. Escott to obtain clarification on what is meant by the inclusion of security functions in Figure 7 of the MBMS architecture TS 23.246v2.0.0.

6.2 Key management requirements (results from AP 29/11)

TD S3z030002 Key management requirements (results of AP 29/11). This was introduced by BT. The requirements were discussed. Some of the requirements were felt to be acceptable to the ad hoc group whilst others were found to be unacceptable to some delegates. BT were requested to prepare a CR to TS 33.246 to add the identified security requirements that were not considered to be controversial. The remaining controversial requirements should be included in a separate CR for email discussion before the next meeting. The identified service requirements/assumptions should be tabled in a draft LS to SA WG1 for consideration at SA3#30.

AP 0309/04: C. Blanchard to distribute any proposed pseudo CRs arising from AP29/11 which add potentially controversial MBMS security requirements to the SA WG3 email list for comment prior to SA3#30.

TD S3z030012 (U)SIM clone and MBMS security. This was introduced by Samsung and proposes to change MBMS keys that never leave the USIM frequently (e.g. BAK in the 3GPP2 scheme) to mitigate against (U)SIM cloning. It was clarified that the (U)SIM cloning possibilities mentioned in the paper refer to SIMs which implement COMP128. It was noted that the GSM Association has recommended against using COMP128 for several years now. **It was therefore agreed that the general statements in the contribution that any (U)SIM can be cloned were not accurate.** Alternative reasons to update MBMS keys frequently do however exist. In particular it was agreed that frequent rekeying of the traffic encryption key (TEK) is needed to make it difficult for a malicious UE to leak information that can be used by others to get unauthorised access to multicast content.

TD S3z030013 Unauthorized access to multicast data analysis. This was introduced by Samsung and proposes to change MBMS keys frequently to mitigate against unauthorized access to multicast data. It was agreed that the arguments in the contribution were valid.

TD S3z030019 MBMS – Key management requirements comparison. This was introduced by Nokia and includes an evaluation of three MBMS key management solutions against a set of requirements. There was some concern that the evaluation has been done against requirements that had not been agreed by SA WG3 rather than the agreed requirements from the MBMS security TS. Nokia clarified that they do not see LKH as beneficial for MBMS application. It was also clarified that the decision between the simple solution and the two tiered solution depends on how frequent rekeying will be done. Some concern was raised about the reliability of ptm key distribution. It was noted that reliability issues may be overcome by repeating keying information during the multicast transmission.

6.3 Different approaches for key management

TD S3z030005 MBMS re-keying : Analyze PTP and LKH. This was introduced by Huawei and includes an analysis of several issues related to the PTP and LKH re-keying methods. It is proposed that issues should be clearly identified and analyzed before selecting a re-keying solution. Some concerns were raised about the load on the common channel that would arise if the LKH scheme were adopted.

TD S3z030006 Using CK with switching command. This was introduced by Huawei and proposes a mechanism for switching between MBMS traffic encryption keys. It has to be decided whether there is an explicit switching command or whether it is an inband key identifier.

TD S3z030007 MBMS Security Architecture. This was introduced by Qualcomm and proposes a pseudo CR to the MBMS security TS. The changes to annex A and annex B were agreed. However the changes to include the 3GPP2 mechanism in the main body of the TS cannot be agreed until a decision on the high level solution for MBMS key management has been made. The details of the 3GPP2 key management architecture were discussed. It was suggested that if someone breaks one UICC to discover RK then the whole system is compromised because the attacker can calculate all BAKs and publish them on the Internet. The operator does not know which UICC is leaking the BAKs and therefore cannot stop the leak unless he changes all USIMs. It was suggested that there are techniques to detect which USIM is leaking the BAKs, but it is for further study whether it is cost effective to introduce such techniques. It was clarified that in the 3GPP2 scheme BAK rekeying is for subscription management and SK rekeying is to protect against malicious UEs from leaking MBMS key material. It was also noted that mechanisms exist to remove members from multicast groups using a delete BAK operation which avoids having to rekey the remaining members in the group. The delete BAK operator can be disguised so that a malicious UE cannot block it in order to continue to have access to content sent to the multicast group.

TD S3z030014 Comparison between ptp re-keying and re-keying based on LKH. This was introduced by Samsung and proposes that SA WG3 should develop the MBMS key management and distribution mechanisms based on LKH principles and that it is up to the operator to decide whether ptp based re-keying or LKH based re-keying shall be adopted for one specific MBMS service. Some doubts were expressed about the claimed benefits of LKH. It was acknowledged that LKH can help reduce the cost of rekeying. However, if the primary reason for frequent rekeying is to make it difficult for malicious UEs to leaking MBMS key material rather than to efficiently, quickly and securely remove someone from a multicast group for charging or subscription management reasons, then PTP rekeying is required for all schemes including LKH. Moreover, in the LKH scheme PTP rekeying is potentially more complex than for simple schemes because the amount of key material which needs to be changed is greater.

TD S3z030015 User grouping for MBMS key distribution. This was introduced by Samsung and proposes a grouping mechanism for LKH based on IMSI. The possibility to arrange groups based on UE location to allow certain rekeying messages to be sent only to certain parts of the network was discussed. This implies that rekeying messages are sent in a separate MBMS service. It is for further study whether the advantages of grouping based on location warrants its cost. It was noted that this mechanism cannot be agreed until a decision is taken on whether LKH should be adopted.

TD S3z030016 MBMS service activation and Initial TEK distribution. This was introduced by Samsung. The contribution evaluates several methods to ensure that the initial TEK is not distributed too early and proposes a solution where a joining availability time is included in the service announcement. It was agreed that the requirement being addressed is a valid security requirement but it was not possible to agree a solution at this time. The issues in the paper should be considered during the design of the key management architecture.

TD S3z030020 MBMS – Combined Re-keying Method. This was introduced by Nokia. The contribution evaluates several key management methods and proposes a combined method which makes the use of the UICC optional. It was clarified that the main difference between the combined method with UICC and the 3GPP2 method is that SK(TEK) is generated in the BM-SC and sent encrypted to the UICC rather than generated directly on the UICC~~the BAK is generated in the BM-SC and sent encrypted to the UICC rather than generated directly on the UICC~~. It was also clarified that the combined method assumes that AKA is used to establish the KEK. Some concerns were raised because the combined solution might use more bandwidth because it sends encrypted TEKs rather than information which may be used to generate the TEKs (i.e. an SK_RAND may be shorter than an encrypted TEK). It was proposed that the simple PTP model and combined rekeying method are pursued in parallel so that the simple PTP model could be adopted if the UICC specifications are not completed on time for Rel-6. The simple PTP model might be preferable to the Combined rekeying method without UICC if the complexity in the combined method to support PTM rekeying and the ability to migrate to a UICC is too high.

It was agreed that the hybrid method and the LKH method should not be pursued for Rel-6 and that a decision should be taken at SA3#30 to select one of the following candidates:

- Simple PTP method
- Combined rekeying method
- 3GPP2 method

In order to help decide on the way forward contributions are needed on whether a mandatory requirement to update the UICC is acceptable. In particular, the feasibility of updating UICC/USIMs over-the-air should be investigated (see section 7.6 of the attachment to TD S3z030030). Also, contributions were invited on the difference in use of bandwidth between the Simple PTP method and the Combined rekeying method.

TD S3z030010 (revisited): MBMS Key distribution. This was introduced by Siemens. Several open issues were identified. It was clarified that MIKEY supports UDP (see section 5.5 of the internet draft). More study is required on whether MIKEY over . The optimisation of MIKEY suggested in the contribution should be considered as part of a 3GPP profile since changes to the internet draft should be avoided (see S3z030027 for the status of MIKEY in IETF). A decision will be made between UDP and HTTP at SA3#30. It was argued that UDP is preferable so as to keep the number and size of messages for rekeying as low as possible. The conclusions of the contribution were noted.

TD S3z030021 Progress report on MBMS 3GPP2 solution. This was introduced by Gemplus. The contribution was noted.

TD S3z030022 Updating Encryption Keys For MBMS. This was introduced by Qualcomm. The contribution provides estimates of the signalling overhead in delivering keys in a purely point-to-point manner. ~~It was stated that the cost of a point-to-point re-key is comparable to the cost of a location update which is typically scheduled every 2 hours.~~ The concern was raised that frequent point-to-point re-keying is infeasible owing to the burden on common channels. The analogy was made that the cost of a point-to-point re-key is comparable to the cost of a location update which is typically scheduled every 2 hours at best. This analysis should be taken into account when reviewing the key management options. The contribution was then noted.

TD S3z030023 Integrating Key Management with the Underlying Protocol. This was introduced by Qualcomm and shows how the 3GPP2 mechanism can be integrated into SRTP. The contribution was noted.

TD S3z030026 Introducing SRTP in TS 33.246. This was introduced by Ericsson and provides an update of an Ericsson contribution to SA3#29 (TD S3z030368). The contribution proposes to select SRTP as the security protocol for streaming MBMS media. It was noted that one advantage of the alternative IP layer solution is that it could be used for both streaming and download. (TS 22.246 includes descriptions of both streaming and download MBMS services). It was clarified that a new header would be needed if SK_RAND in the 3GPP2 scheme would need to be encapsulated into IPsec (see TD S3z030023). Some security concerns were raised about the use of predictable sequence numbers to generate the short term encryption keys in SRTP – the 3GPP2 scheme uses unpredictable SK_RAND instead. It was agreed to add an editor's note to the TS to say that if SRTP is chosen then the master key identifier can be used to indicate the current MBMS key whichever key management scheme is chosen.

TD S3z030027 Introducing MIKEY in TS 33.246. This was introduced by Ericsson. The authentication part of the contribution was skipped since the meeting already made a working assumption on this. The section on PTM was also skipped for similar reasons. The proposed CR to incorporate MIKEY was withdrawn since it is dependant on open issues. MIKEY has passed IESG Security review and the IESG last call. MIKEY is now in the queue waiting for the final IESG review. An RFC is likely to be published during 2003. It was clarified that MIKEY could be terminated in either the UICC or the terminal. It was also clarified that MIKEY currently only supports PTP but it could be enhanced to support PTM if needed. ~~It was suggested that SIM OTA could be an alternative to MIKEY.~~ It was not possible to agree a working assumption to use MIKEY because there are doubts about whether it could be used if we select the 3GPP2 solution and also doubts about the feasibility of terminating MIKEY in the UICC. It was agreed to add an editor's note to the TS to say that MIKEY is being considered as the method for carrying keys. It was suggested that SIM OTA could be an alternative to MIKEY.

6.4 Other MBMS issues

There were no contributions under this agenda item.

7 AOB

Delegates were reminded about the CRs on early UE handling which are currently under email approval.

A recent attack on GSM security published at Crypto '03 was discussed. The GSMA have issued advice to its members. The information is available from the GSM Infocentre web site.

The chairman announced that CN WG1 had requested a joint meeting with SA WG3 during the SA3#30 meeting. It was agreed that the joint meeting should start on Monday 6th October in the morning and the SA3 plenary should start on Tuesday 7th October in the morning. The joint meeting can continue on Tuesday 7th if needed.

8 Close

The Chairman, V. Niemi, thanked delegates for their hard work during the meeting and the hosts for the facilities. He then closed the meeting.

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

Name	Company	e-mail	Mobile Phone	Phone	Fax	3GPP	ORG
Mr. Jorge Abellan Sevilla	SchlumbergerSema	jorge.abellan@slb.com		+33 1 46 00 59 33	+33 1 46 00 59 31	FR	ETSI
Mr. Colin Blanchard	BT Group Plc	colin.blanchard@bt.com	+44 7711 191835	+44 1473 605353	+44 1473 623910	GB	ETSI
Mr. Marc Blommaert	SIEMENS ATEA NV	marc.blommaert@siemens.com		+32 14 25 34 11	+32 14 25 33 39	BE	ETSI
Mr. Krister Boman	ERICSSON LM	krister.boman@ericsson.com	+46 70 246 9095	+46 31 747 4055		SE	ETSI
Mr. Mauro Castagno	TELECOM ITALIA S.p.A.	mauro.castagno@telecomitalia.it		+39 0112285203	+39 0112287056	IT	ETSI
Mr. Sharat Chander	AT&T Wireless Services, Inc.	sharat.chander@attws.com	+1 435 894 7756	+1 425 580 6596	+1 425 580 6811	US	T1
Mr. Per Christoffersson	TeliaSonera AB	per.christoffersson@teliasonera.com		+46 705 925100		SE	ETSI
Mr. Hubert Ertl	GIESECKE & DEVRIENT GmbH	hubert.ertl@de.gi-de.com	+49 172 8691159	+49 89 4119 2796	+49 89 4119 2921	DE	ETSI
Dr. Adrian Escott	3	adrian.escott@three.co.uk		+44 7782 325254	+44 1628 766012	GB	ETSI
Mr. Louis Finkelstein	MOTOROLA JAPAN LTD	louis.finkelstein@motorola.com		+1 847 576 4441	+1 847 538 4593	JP	ARIB
Mr. Jean-Bernard Fischer	OBERTHUR CARD SYSTEMS S.A.	jb.fischer@oberthurcs.com		+33 141 38 18 93	+33 141 38 48 23	FR	ETSI
Mr. Philip Ginzboorg	NOKIA Corporation	philip.ginzboorg@nokia.com		+358 5 0483 6224	+358 9 4376 6852	FI	ETSI
Mr. Guenther Horn	SIEMENS AG	guenther.horn@siemens.com		+49 8963 641494	+49 8963 648000	DE	ETSI
Mr. Peter Howard	VODAFONE Group Plc	peter.howard@vodafone.com	+44 7787 154058	+44 1635 676206	+44 1635 231721	GB	ETSI
Mr. Robert Jaksa	HUAWEI TECHNOLOGIES Co. Ltd.	rjaksa@futurewei.com		+1 972 509 5599	+1 972 509 0309	CN	ETSI
Mr. Vesa Lehtovirta	ERICSSON LM	vesa.lehtovirta@ericsson.com		+358405093314		SE	ETSI
Mrs. Claire Mousset	NORTEL NETWORKS (EUROPE)	cmousset@nortelnetworks.com		+33 4255806596	+33 4255806811	GB	ETSI
Mr. Valtteri Niemi	NOKIA Corporation	valtteri.niemi@nokia.com		+358 50 4837 327	+358 9 437 66850	FI	ETSI
Miss Mireille Pauliac	GEMPLUS Card International	mireille.pauliac@GEMPLUS.COM		+33 4 42365441	+33 4 42365792	FR	ETSI
Mr. Bengt Sahlin	ERICSSON LM	Bengt.Sahlin@lmf.ericsson.se		+358 40 778 4580	+358 9 299 3401	SE	ETSI
Mr. James Semple	QUALCOMM EUROPE S.A.R.L.	c_jsemple@qualcomm.com		+447880791303		FR	ETSI
Mr. Adrianus Van Ewijk	ALCATEL S.A.	adrianus.van_ewijk@alcatel.be		+3232409358		FR	ETSI
Ms. Annelies Van Moffaert	ALCATEL S.A.	annelies.van_moffaert@alcatel.be		+32 3 240 83 58	+32 3 240 48 88	FR	ETSI
Mr. Tommi Viitanen	Nokia Telecommunications Inc.	tommi.viitanen@nokia.com		+358405131090	+358718075300	US	T1
Ms. Huang Yingxin	HUAWEI TECHNOLOGIES Co. Ltd.	huangyx@huawei.com		+861068427711	+861068421891	CN	ETSI
Mr. Yanmin Zhu	Samsung Electronics Co., Ltd	zym@samsung.co.kr		+861068427711	+861068481898	KR	TTA

26 attendees

Annex B: List of documents

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3z030001	Proposed agenda and objectives for the ad hoc meeting on GAA and MBMS	SA WG3 Chairman	2	Approval		
S3z030002	Key management requirements (results of AP 29/11)	BT Group	6.2	Discussion		
S3z030003	Generic Authentication Architecture requirements	Siemens	5.1	Discussion / Decision		
S3z030004	Liaison Statement (from SA WG2) on Generic Authentication Architecture	SA WG2	4	Action		Noted
S3z030005	MBMS re-keying : Analyze PTP and LKH	Huawei Technologies Co., Ltd.	6.3	Discussion / Decision		
S3z030006	Using CK with switching command	Huawei Technologies Co., Ltd.	6.3	Discussion / Decision		
S3z030007	Pseudo-CR to 33.246: MBMS Security Architecture	BT Group, Gemplus, Giesecke and Devrient, Lucent Technologies, Qualcomm Europe, SchlumbergerSema	6.3	Approval		Pseudo-CR in attachment
S3z030008	Proposal for Generic Authentication Architecture	Nokia	5.2	Discussion / Decision / Approval		
S3z030009	USIM enhancements for MBMS support	SchlumbergerSema, Gemplus, Giesecke and Devrient, Qualcomm	4	Information		
S3z030010	MBMS Key distribution	Siemens	5.3, 6.3	Discussion		
S3z030011	Generic Authentication Architecture evaluation	Siemens	5.2	Discussion / Decision		
S3z030012	(U)SIM clone and MBMS security	Samsung	6.2	Discussion		
S3z030013	Unauthorized access to multicast data analysis	Samsung	6.2	Discussion		
S3z030014	Comparison between ptp re-keying and re-keying based on LKH	Samsung	6.3	Discussion / Decision		
S3z030015	User grouping for MBMS key distribution	Samsung	6.3	Discussion / Decision		
S3z030016	MBMS service activation and Initial TEK distribution	Samsung	6.3	Discussion / Decision		
S3z030017	Latest version of SA2's TS 23.246 on MBMS	Nortel Networks	6.1	Information		
S3z030018	Generic Authentication Architecture and Release 6 services	Nokia	5.3	Discussion		
S3z030019	MBMS – Key management requirements comparison	Nokia	6.2	Discussion		
S3z030020	MBMS – Combined Re-keying Method	Nokia	6.3	Discussion		
S3z030021	Progress report on MBMS 3GPP2 solution	Gemplus, Oberthur, Qualcomm Europe, SchlumbergerSema	6.3	Discussion / Decision		
S3z030022	Updating Encryption Keys For MBMS	QUALCOMM Europe	6.3	Discussion / Decision		
S3z030023	Integrating Key Management with the Underlying Protocol	QUALCOMM Europe	6.3	Discussion		
S3z030024	Generic Authentication Architecture based on AAA and AKAv2	Ericsson	5.2	Discussion / Decision		

TD number	Title	Source	Agenda	Document for	Replaced by	Status / Comment
S3z030025	IETF status report on HTTP Digest AKAv2	Ericsson	5.2	Information		
S3z030026	Introducing SRTP in TS 33.246	Ericsson	6.3	Discussion / Decision		
S3z030027	Introducing MIKEY in TS 33.246	Ericsson	6.3	Discussion / Decision		
S3z030028	Draft 3GPP TS 33.246 V0.2.0: Security of Multimedia Broadcast/Multicast Service (Rel-6)	Rapporteur	6.1	Information		
S3z030029	Analysis of different approaches for GAA	Nortel Networks	5.2	Discussion / Decision		
S3z030030	LS on potential USIM impact of the MBMS security framework	T3	4	Action		Noted
S3z030031	Reply LS on clarification of MBMS charging issues	SA1	4	Action		Noted

Annex C: List of Liaisons

C.1 Liaisons to the meeting

TD number	Title	Source TD	Comment/Status
S3z030004	Liaison Statement (from SA WG2) on Generic Authentication Architecture	S2-033262	Noted
S3z030030	LS on potential USIM impact of the MBMS security framework	T3-030697	Noted
S3z030031	Reply LS on clarification of MBMS charging issues	S1-030997	Noted

Annex D: Actions from the meeting

AP 0309/01: G. Horn to update the diagram in section 6.2 of TD S3z030011 so that it captures the architectural solutions under consideration for GAA.

AP 0309/02: Chairman to raise SA WG3 comments on MBMS architecture TS 23.246 at the SA#21 plenary meeting.

AP 0309/03: A. Escott to obtain clarification on what is meant by the inclusion of security functions in Figure 7 of the MBMS architecture TS 23.246v2.0.0.

AP 0309/04: C. Blanchard to distribute any proposed pseudo CRs arising from AP29/11 which add potentially controversial MBMS security requirements to the SA WG3 email list for comment prior to SA3#30.