3GPP TSG SA WG3 NDS ad hoc **version 0.0.4**
Madrid, Spain
23-24 April 2001

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

Title: **Draft report version 0.0.4**

Document for: **INFORMATION (an updated version will be provided for comment)**

---

1 Opening of the meeting

The Chairman, Mr. Geir Koien 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

The agenda, provided in TD S3z010001 was agreed. The objectives, proposed by the SA WG3 Chairman, were discussed - the proposed primary objectives of the meeting were agreed with the addition of agreements of Local Key Distribution, based on contributions that had been provided for the ad-hoc meeting. It was noted that the recommendations made at the meeting were for e-mail approval by SA WG3 before the CN WG4 meeting on 14 May 2001, e-mail approval deadline was suggested as 4 May 2001, and was later agreed as 8 May 2001).

3 Allocation of documents to agenda items

The available documents, relevant to the NDS ad-hoc meeting, were assigned to appropriate agenda items.

4 Liaisons from other groups

It was noted that TD S3z010011 did not contain a CR from CN WG4, and this was provided in TD S3z010030.

5 Summary of events since S3#17

Peter Howard, Vodafone, provided a short summary of the events that had occurred in the SA WG3 reporting to SA Plenary meeting #11: The SA WG3 Chairman asked TSG SA to grant SA WG3 an extended deadline for submission for approval of the MAP Security requirements, as the NDS ad-hoc had been set up in order to finalise this document (TS 33.200): It was agreed that SA WG3 should submit a draft for information after their May 2001 meeting #18 by e-mail, and a version for approval at SA#12 in June 2001. This process would mean that TSG CN would not need to remove the already completed material from their Release 4 specifications (an e-mail had been sent to the SA WG3 list informing them of this).

6 Status of draft network domain security specification, TS 33.200 (Rel-4)

TD S3z010004 New version of TS 33.200. This TD was introduced by the editor, and contained an introduction to the NDS document, information of the updates made to the specification and a new version with and without revision marks.

Introduction part: This proposed a split of the document into MAP security part and an IP Security part, as the MAP Security part was expected to be completed and no further modification was expected, whereas the

IP Security parts were expected to be updated as the IP requirements develop. This received general support as it would help the MAP Security work to be completed and frozen without the need to further modify the document for IP Security requirements. It was noted that some contributions for update of the draft TS were to be discussed during the meeting before final a version could be agreed. **It was agreed to recommend this to SA WG3**.

It was noted that Ericsson had provided a contribution for inclusion of automated Key Management along with the MAP Security. Whether this can be included in Rel-4 was for further discussion.

Update information: The editor asked whether the KAC <--> MAP-NE interface should be IP-based. Delegates were asked to consider this.

Version 0.3.2 to 0.3.5 Changes: It was reported that the Iu/Iur interface section had been removed due to lack of contribution, as it is not a MAP interface. The other changes were mainly the removal of IP parts and the addition of placeholders for Rel-5 material.

Version 0.3.5 to 0.4.0: It was noted that TD S3z010024 provides editorial comments to version 0.4.0.

Review of version 0.4.0 (with revision marks): Ericsson stated that they had expected automatic key management to be included in the approved Release for MAP Security. There was some discussion and it was suggested that the WIs should be consulted on this point. It was not considered feasible for the first phase of MAP Security which could be included in time for Rel-4 (extended to June 2001). The update information document provided some discussion on this and it was agreed that the intention for the additional MAP Security material in Rel-5 should be made apparent in the Rel-4 document, it was proposed that this should be done by including the expected Rel-5 MAP Security items in an informative annex, rather than in notes as done in version 0.4.0. This proposal was generally agreed.

It was also noted that the MAP Security SA needs to be defined in the document.

The editor was asked about the progress on completion on the associated TR 33.800. It was reported that the document was in an immature condition and that it was unlikely to be worth publishing the material by June 2001. He suggested that the TR should be removed from the SA WG3 work programme, as it would not provide any useful, accurate information over the specification itself. **It was agreed to recommend the deletion of this document to SA WG3.**

Guidance on Security Parameters to CN WG4 would be needed when representatives arrived for a joint session. It was decided that these should be provided as part of LSs considered in the meeting. It was agreed that the ad-hoc should provide guidance on the content, but that the coding aspects should be left to CN WG4 for inclusion in their specifications.

7 MAP security technical issues

7.1 Security Level (i.e. component, operation or Application Context (AC))

The "discussion" parts of TD S3z010011 and TD S3z010013 were taken together:

TD S3z010011 Protection Profiles for MAP Security. This was introduced by Ericsson and proposed an agreement on the choice between 3 Protection Profiles (PPs):

- MAP Application Context level;
- MAP Operation level;
- MAP Operation Component level.

The contribution discussed the pros and cons of each level of PP and proposed that the Operation level for MAP PP structure as the best compromise between granularity of protection and complexity, while fulfilling the security requirements. Operators were asked to express their wishes on this proposal.

TD S3z010013 Protection Profiles for MAP Security. This was introduced by Siemens as an alternative proposal to the Ericsson document (TD S3z010011). Siemens proposed to have 4 Component level PPs,

where the operator would negotiate the PPs supported from the defined profiles, and suggested that it provides the best granularity and can reduce loading on the network.

Discussion of Ericsson and Siemens contributions:

Vodafone commented that handover was not included in the Siemens PP1, but that it was protected in the Ericsson contribution. It was reported that this had not been an issue in the risk analysis, but it was agreed that this should be considered for protection, and could be added to the Siemens proposal as an additional PP to be included in negotiations. It was clarified that in the Siemens scheme, the operators would negotiate a ***list*** of PPs to be used, rather than negotiating a single PP, which had been the assumption for the development of the Ericsson contribution. Ericsson requested some time to consider the implications of this mechanism.

It was generally agreed that the most sensitive messages need to be protected in Rel-4. It was also suggested that a PP to protect all protectable parameters should be included in a Rel-4 scheme, to be used in case of problems (however, it was also recognised that this would probably cause severe loading/efficiency problems).

It was agreed that in order to make progress on this matter, the DoI discussions should also be taken into account (see agenda item 7.3) and the matter discussed in an evening session.

During the evening discussions, it was concluded that the reolution of the matter depended on whether the PPs are defined on the Operation or Component level, and CN WG4 should be asked to decide on this matter, as the arguments were not security related ones. A LS to CN WG4 was drafted by P. Howard, in TD S3z010033. **<RETURN>**

Fallback indicators: The “fallback to unprotected mode indicator” is mainly to allow stepwise deployment of MAPSec (some nodes are upgraded while others aren't), so either a node will be able to apply a MAP-PP or not at all. There were some minor differences in the detail of the management and scenarios for the fallback indicator between the Ericsson and Siemens contributions, and it was agreed to discuss this in an off-line evening session in order to reach some consensus on the basic set of operations that need to be protected (including the need to protect handover authentication). **<RETURN>**

TD S3z010011 (CN WG4 LS part): Structure of the Security Header. CN WG4 asked whether a single Initialisation Vector (IV) would be sufficient to be used, e.g. in protection mode 2, if both the Encryption Algorithm and the Integrity/Authenticity Algorithm require an IV. Potential problems were raised with this when encrypting the MAC and using the same IV for integrity protection, as these should be independently generated for best security protection. This was discussed in the evening off-line group and TD S3z010031 produced, which shows the agreements for the MAPSec mode. This showed a scenario where the same IV is used for both the MAC and the integrity protection, as a practical solution, although it was noted that there was a theoretical risk in doing this. Using stream cipher for the encryption would reduce the need for padding, as may occur if block ciphering were used (the AES has a 16-byte lock size, which means that up to 16 bytes of padding may be necessary in some cases). The diagram showed the IV as being made up from a 24 or 16 bit Node ID, a 32 bit TVP and an 8 bit Clock extension. For replay protection, the Global clock synchronisation would need to be specified as small (e.g. 1 second), in order to prevent two identical IVs being generated (there is a requirement for unique IVs). It was noted that the CN specification currently reserve 18 bytes for an IV, which could be reduced, allowing compensation for padding bits.

It was agreed that a response would be created by Ericsson and included in the LS to CN WG4 (TD S3z010033, produced by P. Howard).

SA WG3 were also asked to determine the refine their algorithm selection by determining:

- the block length which is to be mandatorily supported,
- the key length which is to be mandatorily supported,
- the mode of operation for AES which is to be mandatorily supported,
- the mode of operation for AES-MAC which is to be mandatorily supported,
- the length of the Integrity Check Value which is to be mandatorily supported

in a way which minimises the overhead as far as possible while ensuring an acceptable level of security.

It was decided to discuss this in an evening session in order to provide some answers to CN WG4 in the joint session. **<RETURN>**

TD S3z010008 Comments on MAP DoI. This was presented by Siemens and suggested a number of changes:

A) Deletion of some MAPsec DoI text from the MAP DoI draft which reproduce information in the IETF IPSec DoI document and using references instead, but leaving the items which need to be maintained by 3GPP in the document (e.g Key derivation procedures).
B) KACs between two NEs is not an SA WG3 working assumption, and this should be clarified in the document. It was discussed whether KAC needs to be in the MAPsec DoI document, and it was agreed that the text should be removed, replacing it with a small introduction about the purpose of the mechanism.
C) The IETF draft MAPsec DoI RFC parts should be included in 3GPP specifications for maintenance and easier referencing reasons. The editor was asked to list the items to be added to the 3GPP MAP DoI document and those which should reference the IETF RFC document.
D) KINK should not be used, due to its immaturity compared to IKE. The editor agreed to remove this option.
E) PPs were discussed. The proposal for a 16 bit fixed-length field, to provide for adequate number of PPs to be selected was noted.
F) This suggested that there is no need for asynchronous negotiation of the SA-pairs. IKE cannot handle asynchronous negotiation and would need modification. It was agreed that this should be removed.
G) The SA duration had been agreed in SA WG3 as an absolute time value. The editor reported that this was an error in the document and that absolute time would be inserted.
H) This proposed allowing additional provision for AES-CBC (192 or 256 bit key lengths) for future use. It was noted that only 128 bit is mandatory for Rel-5. This was agreed.
I) The MAP SA payload requires specification. This was not considered appropriate for DoI, but the inclusion of SA specification and transport of the SA to the NE in SA WG3 specifications should be considered. Contributions were requested on this for SA WG3 meeting #18.

The editor agreed to provide an update of the MAPSec DoI document to SA WG3 meeting #18, taking the agreements at this ad-hoc into account. Contributions are requested on SA specification and transport. The editor thanked Siemens for their comprehensive review of the document and requested other companies to review the document and provide contributions.

7.2 ASN.1 descriptions within TS 33.200 or in TS 29.002

There were no contributions on this agenda item. It was agreed that the ASN.1 descriptions should be included in 29.002, and SA WG3 would specify the semantics for this in 33.200. This information was included in the LS to CN WG4.

7.3 MAPsec DOI

TD S3z010010: MAP DOI Status (Powerpoint presentation part). This was presented by Ericsson. There were some questions for clarification. It was recognised that the group would need to decide what will be left in the IETF Information document on MAP-DoI RFC and what should be put into 3GPP specifications for maintenance considerations.

TD S3z010012 IPsec and IKE profile for network domain security. The presentation was given by Ericsson. IKE profiling was suggested to limit cost, complexity and to improve interoperability. It was suggested that this did not limit vendors in providing additional functionality, nor 3GPP in requiring further functionality in the future.

The mandatory use of IPv6 was questioned, as this had not been a decision of SA WG3. It was decided that an LS should be written to relevant groups on this.

MAP DoI IKE profiling:

- Only phase 1 of IKE is used: The rest is MAP DoI. This was agreed.

- Only IPv6 is mandatory: This needs to be checked via an LS to SA WG2 and other relevant groups. There was no preference from the Security point of view, but there were interoperability concerns (IPv6 versus IPv4).
- Perfect Forward Secrecy (PFS) optional: This was acceptable for speed in Phase 2.
- Aggressive and Main Mode use: It was agreed that only Main Mode would be mandated (it was noted that Main Mode provides better protection against DoS attacks than Aggressive Mode, although Agressive Mode would provide better performance).
- FQDN, Only Fully Qualified Domain Names to be mandated for identities: This was agreed.
- Use of AES and SHA-1: It was agreed that AES should be used for encryption and SHA-1 for the MAC.
  It was reported that AES is useable and has an RFC number allocated already, so it could become an RFC if requested to the IETF. AES / SHA-1 for the MAC was agreed, with a note to say that AES-CBC-MAC is expected to be the preferred MAC solution for the future. **The Working Assumption that AES can be used both for encryption and MAC in IKE was agreed**. The problem with AES-CBC-MAC is the assignment of IETF number and the NIST publication of the AES modes (including AES-CBC-MAC), and the DoI editor was asked to try to expediate this and to send the draft to SA WG3, before meeting #18, for information.
- SA lifetime notification not allowed: **This was taken as a working assumption**. Input is expected at SA WG3 #18 meeting if any problems are discovered with this.
- SA deletion between KACs not allowed: This would allow the Pull mode to be easily implemented, but will make it difficult to inform other nodes of any compromise of keys. This proposal should be studied further, as the deletion function may be required in emergency/exceptional cases, limiting to use of Pull mode may cause problems in the future. It was suggested that removing deletion would necessitate a reduction on SA lifetimes to days or hours. It was also suggested that revoking SAs should be possible, perhaps using manual management action. **After some off-line discussion it was agreed that a working assumption was that SA deletion between KACs should be possible.** Delegates were asked to check the implications and report any problems by contribution to SA WG3 meeting #18.

7.4 Other general issues regarding the protection mechanism

TD S3z010006 "CR" to 33.200: Cleanup of MAPsec structure of protected operations. These proposed changes were presented in CR style on the request of the editor. The changes were reviewed and the editor asked to take them into account for the revised version of 33.200, MAPSec document and the IPSec document to be extracted from it.

7.5 Security association establishment

TD S3z010005 MAP-SA Negotiation and Distribution Procedures. This was introduced by Ericsson which set a solid and consistent basis for the specification of MAP-SA negotiation and distribution mechanisms.

From contribution summary:

S3 members are asked to consider this proposal in order to be able to reach the following agreements:

1. *Agreement on the general overview of the MAP-SA negotiation and distribution mechanisms (chapters 3.1 and 3.2).*
2. *Agreement on the principles of the "RequestSA" procedure (chapter 3.3).*
3. *Agreement on requesting CN4 to select and further develop/refine the actual protocol to be used at Ze interface (chapter 3.4) according to the requirements provided in this proposal. If this is agreed, a LS informing CN4 of such request shall be submitted as soon as possible.*
4. *Agreement on the basic functionality at the KAC and MAP-NEs in relation to MAP Security and Key Management (chapter 4.1. and 4.2).*

If these agreements can be reached, the information in this proposal could be included in TS 33.200.

Discussion:

The use of "towards" and "from" were clarified as relating to SA information, which is asymmetric. Security Policy databases are synchronised via roaming aggreements, rather than dynamically. If a NE tries to send a secure message and an indication "not allowed" is returned, the Policy database is checked to verify if fallback is allowed, before changing the SA.

A failure scenario was not included and some text on this was considered to be advantageous. Error scenarios need development and fallback scenarios were also considered as needed. There was a request for a test procedure, to be applied before implementing an upgrade to roaming agreement security policies, in order to prevent failure on live traffic when the new SA is applied.

This contribution was generally considered as a very useful start, and it was recognised that more detail was required.

Ericsson requested that this procedure should be included in the same Release as MAPSec (which was targetted for Rel-4 at this ad-hoc meeting), but this could only be done if both Stage 2 and Stage 3 specifications are completed in time for the extended finalisation date of June 2001 and it was thought unlikely that the Stage 3 would be completed by CN in time. Ericsson questioned whether the Rel-4 MAPSec would be used in practice without the inclusion of automatic Key management procedures.

The principles of the contribution were agreed, and it was noted that local Key distribution needs also to be managed in a secure way.

TD S3z010027 Proposed changes to 33.200 about KAC. This was presented by Nokia and proposed text to 33.200 to clarify that there may be several KACs in order to provide redundancy in case of failure, with one logical KAC visible at the interface. It was noted that this would require database synchronisation.

It was generally agreed that redundancy was expected to be provided in systems, but that this was an implementation issue, rather than a standardisation issue. After some off-line discussion, some complications were identified on the receiving network node side (addressing may be an issue for calling nodes) and the proposal should be further considered at the SA WG3 meeting #18 and contributions were invited.

8 Other network domain security technical issues

8.1 GTP security

This was deferred to SA WG3 meeting #18 due to lack of time at the ad-hoc meeting.

9 N4 issues

9.1 Questions from S3

The LS in TD S3z0100xx covered the questions that SA Wg3 ad-hoc addressed to CN WG4.

Local SA distribution is a much needed part of the architecture, but SA WG3 cannot provide full details at present and lack recovery procedures, so it was considered premature to ask CN WG4 to develop the protocol yet. It was thought that even if SA WG3 can agree on the outstanding issues, there may not be enough time for CN WG4 to complete their work and the Rel-5 details missing from the Rel-4 would be outlined in an informative annex. It was agreed that it would not be possible to have automatic local Key management procedures in time for Rel-4, manual local Key management would need to be implemented.

Question to CN WG4: Should MAPSec Transport be included in Rel-4 (the primary objective of this ad-hoc) without automatic Local Key management ?

BT stated that guidance on manual Key management would be required in any case if MAPSec Transport is included.

Vodafone stated that the specification of SA is needed in order to have manual Key management in Rel-4.

It was noted that the primary objective of the ad-hoc was only to attempt to complete the MAPsec transport security (Zf-interface). A Rel-4 version of TS 33.200 could therefore be completed even without the Local SA distribution (Ze-interface). It was noted that it was essential that CN4 receive answers to their LS (see TD S3z010011) in time for their meeting 14-17 May in order to achieve this. In the end it was therefore decided that S3 should for now only respond to the questions that CN4 asked in their LS (see TD S3z010011). Questions related to Local SA distribution would have to wait for Rel-5. It was further acknowledged that there was still a number of open issues for S3 to decide in order to complete the MAPsec

transport security specification and that these issues would have to be addressed by S3#18 is a Rel-4 version of TS 33.200 was to be achieved.

9.2 Clarification on output documents required for N4 plenary, 14-17 May

An evening session was held to provide the results of the discussions to CN WG4 and produced a draft which was discussed and edited on-line in the meeting. The draft was modified and agreed in TD S3z010033 (see agenda item 10.1).

It was recognised that contribution for SA WG3 meeting #18 was needed in order to update 33.200 on these issues.

10 Review of output documents

10.1 For N4 plenary, 14-17 May

TD S3z010033 LS to CN WG4 on MAP security. This was produced after discussion of the results of the evening session group to provide information to CN WG4. The contribution provided the agreements and open issues on the following topics:

- MAP protection profiles
- Structure of security header
- Algorithm mode selection for MAP security

Additionally it informs CN WG4 that the coding of MAP security elements should be contained as ASN.1 in TS 29.002 based on stage 2 specifications to be included in TS 33.200.

This LS was agreed for forwarding to CN WG4.

10.2 For S3 plenary, 21-24 May

The following list was developed on-line for reporting to SA WG3 on progress and outstanding issues:

- **Format and length of IV needs to be determined**

  An input paper from Rolf Blom and Valterri Niemi suggested that one IV of 8 octets could be sufficient if it was cleverly composed. They suggested to let the IV be composed of TVP (4 octets), a unique node identifier (3 octets) and a local clock (1 octet). The definition of the local clock needs to specified.

- **Format and construction of TVP (4 octets assumed) must be resolved**

  The exact format of the TVP, including bit ordering etc, would need to be defined. This would include defining the clock resolution (1 second suggested) and to defined a clock reference point. (it had previously been been decided to use absolute time in the TVP)
  It would also be necessary to define a clock window size.
  The meeting also decided to recommend to move the TVP from the payload to the MAPsec header. Updates to the TS to reflect this would have to be produced.

- **The Node-Id identifier must be precisely defined**

  It was suggested to let the Node-Identifier be 3 octets long and that it would be constructed by means of a hash over the E.164 Global Title for the MAP-NE. All details of the Node-Id, including the definition of the hash function, would need to be specified.

- **Specification of cryptographic algorithms to be used**

  All details regarding the choice of cryptographic algorithms (both confidentiality and integrity) needs to be defined. In addition to the specifying the algorithm identifiers (4 bits for each algorithms was suggested to be sufficient), the standard algorithms would have to be precisely specified. This would include specification of the mode to be used as well as a specification for the algorithm interface. Decisions about whether to use stream- or blockciphering would have to be made and it was noted that a streamcipher would not require

padding. This may be an issue since it was questioned whether CN4 could afford padding. Valterri Niemi mentioned that according CN4 calculations it was not clear that the MAP SendAuthenticationInfo containing a single AV could be sent without segmentation with the current security overhead requirements. This would provide a strong incentive to reduce the need for padding.

- **The integrity check value (ICV) would need to be defined.**

  In particular the length of the ICV need to be defined. It was assumed to 64 bits would be sufficient, but that 32 bits might be accepted should it be the case that this would avoid segmentation.

- **MAPsec SA defintion**

  All aspects of the SA would need to be defined This would include defining the SA liftetime, the integrity key, the confidentiality key, the algorithm identifiers, the security domain identity (=PLMN identity), SPI.

- **Protection Profiles**

  The protection profiles encoding must be specified. It was agreed that 16 bits should be used for this information element.

- **MAPsec local SA distribution procedures needs to be refined/completed**

  Although Ericsson had produced a good starting point, the need for recovery procedures as well as the need for revocation mechanisms needs to be studied further.

11 Evaluation of progress

Independent of whether SA WG3 would be able to produce a Rel-4 of 33.200 it was agreed to recommend to S3#18 that TS 33.200 should be split into two TSs (one containing MAP/SS7 material and one containing GTP/IP material). The rapporteur agreed to produce a new version of TS 33.200 with only MAPsec/SS7 material and to provide an initial draft for a new TS to cover GTP/IP security based on the GTP/IP material as found in TS 33.200 v035.

The ad-hoc had reached agreement to attempt to include MAPSec transport protocol in Rel-4.

- Peter Howard will complete the reply LS to CN WG4 based on the agreements at the ad-hoc and lead an e-mail agreement procedure for the reply LS. The e-mail agreement process will be concluded 8 May 2001 1600 CET.
- TS 33.200: Those items which cannot go into Rel-4 will go into an informative Annex of the Rel-4 document (if there is one).
- Guidelines for manual SA handling need to be included in the Rel-4 specification at SA WG3 meeting #18.
- It was concluded that a number of open items have been identified and a clearer view obtained of what is left to be done for completion of MAPSec. (see list in 10.2). Contributions on these issues are required for S3#18.

It was agreed that the SA WG3 Chairman should be consulted about these conclusions, as the situation would need to be explained by the SA WG3 Chairman at SA Plenary.

12 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, and closed the meeting.

Meeting objectives:

- The primary objective is to make technical progress on MAP security with the aim of ensuring that the necessary specifications for Rel-4 can be agreed at the N4 plenary meeting, 14-17 May, and at the S3 plenary, 21-24 May. Particular issues to resolve include the granularity of protection required (component, operation or application context) and where to specify the coding of the security parameters (directly in TS 29.002 in ASN.1 or in TS 33.200).

- A secondary objective is to make technical progress on other aspects of network domain security, especially GTP security.

- A further objective is to make technical progress on automatic security association (SA) establishment for MAP security.

A session *at the end* of the meeting (agenda item 11) shall evaluate progress and agree a recommendation to S3 plenary (cc N4) which will state which network domain security features should be presented to the June TSG plenary meetings for inclusion in Rel-4. The recommendation of the S3 ad hoc meeting shall be considered for email approval by S3 plenary prior to the N4 meeting on 14th May. The deadline for email approval shall be Friday 4th May.

Annex A: List of attendees at the SA WG3 NDS 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	jarkko@piuha.net	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
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.	Peter	Howard	VODAFONE Group Plc	peter.howard@vf.vodafone.co.uk	ETSI	x
Mr.	Jari	Jansson	Nokia	jari.jansson@nokia.com	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.	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.	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