3GPP TSG-CN 3GPP / TSG-SA WG3
Joint Meeting
Sophia France
13th - 14th June 2000

NP-000323

DRAFT

Third Generation Partnership Project

DRAFT REPORT v2.0.0

3GPP TSG-CN 3GPP TSG-SA WG3 Joint Meeting

Sophia, France
13th - 14th June 2000

Hosted by ETSI

Chairman: **Steven Hayes, Ericsson Inc.** Stephen.hayes@ericsson.com

MCC Support: **David Boswarthick, ETSI MCC.** david.boswarthick@etsi.fr

Table of contents

1 Opening of the Meeting

Stephen Hayes (TSG-CN Chair) opened the meeting at 14:00 on 13th June 2000. Stephen set the objectives for the meeting as:-

- Ensure that R'00 security work is coordinated between CN, CNx, and S3
- Common understanding of:
- Work item descriptions
- Work item requirements/architectural assumptions
- Work item responsibilities (F/BB/WT)
- Work item timeframes
- Work item priorities

2 Approval of the Agenda

NP-000194: **Rev. Draft Meeting Agenda.**

CONTENT: The document contains the revised Agenda

RESULT: The Agenda was **AGREED**

3 Allocation of documents to agenda

Documents were allocated to agenda items on-line. CN TDoc numbers were allocated in the meeting.

4 Presentation of S2 Architecture Status

NP-0000208: **Document.** Presented by Liz Daniels (Lucent).

CONTENT: Contains a presentation from S2 on the latest R2000 architecture, including a description of the main functional entities.

DISCUSSION: The presentation highlighted two of the major architectural initiatives. The first is the introduction of the IM subsystem. The second is the bearer independent circuit switched architecture. The recent S2 decisions to use SIP as the multimedia call control protocol and use of IP v. 6 within the IM subsystem were described.

An open issue is whether IMSI will be used as the UE identifier within the IM subsystem. S3's input on the security implications of the use of IMSI or a new additional identifier is solicited. S2 has not thoroughly considered the business models possible in the IM domain. However, there currently seems possible that the IM domain may include independent service providers that are not part of the PLMN and may or may not be trusted, thus posing an additional security risk. The usability of IMSI with IETF security protocols and systems is also an open issue.

For the bearer independent circuit switched architecture it was pointed out that this separation currently only applies to the CS domain, but a feasibility study is planned in S2 to investigate if the concept can also be applied to the PS domain.

RESULT: The document was **DISCUSSED**

5 Presentation of work items proposed by S3

NP-0000207: **Presentation of S3 Work Items.** Presented by Peter Howard, Vodafone

CONTENT: Contains a presentation of R2000 Work Items for S3

DISCUSSION: This gave an overview of the status of the work item definitions in S3 and also what the S3 expectations from the meeting were. It was noted that S3 also feels it is important to prioritize the work. The proposed work items are broken into architectural (support of the IM subsystem) and other work items that are evolutions of existing security functionality.

The relevant work item description is also discussed under a the work item topic. Work items without corresponding Work Item descriptions are indicated by italics. It was noted that S3 intends to to generate any missing work items before SA#8.

RESULT: The document was **DISCUSSED**

6 Review of status and requirements on CN for security items

NP-0000199: **R00 Project Plan for Security.** Presented by Peter Howard, Vodafone.

CONTENT: Contains two versions of the draft R00 project plan for security

- Version based on decisions taken at S3#13
- Version based on decisions taken at S3#13 incorporating changes to milestones proposed based upon S2 feedback

Only the version including the S2 feedback was discussed.

DISCUSSION: The individual sections of the project plan were discussed under each work item and any proposed changes are indicated in those sections.

It was noted that the proposed completion dates were well past the official December, 2000 release date. The chair recommended that the schedule be assessed realistically. For completion dates that slipped past December 2000, an assessment could be made as to whether this was R'00 or R'01.

It was further explained that in the schedule matrix associated with each work item that the "Definition of security architecture" row referred to the completion of stage 2 level work by S3. Approval was by TSG-SA.

The row "Integration of security architecture" referred to the completion of stage 3 level work by TSG-CN or other TSGs.

RESULT: The document was **DISCUSSED**. A new version of the project plan will be produced by Peter Howard (Vodafone) based upon the decisions of this meeting.

NP-0000198: **R00 Work Item Descriptions.** Presented by Peter Howard, Vodafone.

CONTENT: A Zip file containing the draft work items currently under discussion in S3.

DISCUSSION: Each work item is discussed in the relevant section below. The schedule within the work items should be based upon the schedules generated from the work plan.

RESULT: The document was **DISCUSSED**. Revised work items will be produced by the rapporteur based upon the decisions of this meeting.

6.1 Access security for IP-based services

This is a Building Block for the feature "Provisioning of IP-based multimedia services". New security features will need to be introduced to secure access to the IP multimedia core network subsystem, e.g. authentication between users and new "gateway" nodes beyond the GGSN. Evolution and/or re-use of the existing R99 architecture for authentication and key agreement will need to be considered. Signalling between the mobile and nodes beyond the GGSN may well use the radio interface user plane Radio Access Bearers. This signalling is likely to need protection (eg provision for integrity checking as well as encryption). Charging and accounting issues are also likely to be important. Work Tasks may involve: S2, S3, S5, R2, R3, T3, N1, N4, [SMG 2 WP A].

Section 3.1.1.1 of **NP-000199** was reviewed as part of the review of this work item. After considerable discussion it was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved – December 2000
- Integration of security architecture: CRs approved at TSG Level – June 2001

All other dates in the schedule should be adjusted to align with these anchor dates. It was noted that there is still a large amount of uncertainty about the scope of this work, so the dates in the schedule have a low confidence factor. It is expected that the schedule will be refined as the work progresses.

It was further noted that including corrective CRs in the schedule was inappropriate and should be removed (this is a generic comment applying to all the work items). S3 should also check that the terminology being used is consistent with the S2 terminology.

Within the work item description the services box should be checked.

It is expected that N1 will be the partner with S3 for this work item.

RESULT: The workplan and work item description should be updated as described above.

6.2 Network-based end-to-end security

This is a Feature. The R00 system architecture may create new requirements and/or opportunities for extending user plane traffic security further back into the core network, and additionally it may allow for security mechanisms to be applied on an end-to-end basis, providing that the necessary lawful interception requirements are addressed. This work will take advantage of concepts and hooks for network-wide encryption which have been considered in R99.
Work Tasks may involve S2, S3, R2, R3, N1, N4, [SMG 2 WP A].

Section 3.1.1.2 of **NP-000199** was reviewed as part of the review of this work item. After considerable discussion it was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved – March 2001
- Integration of security architecture: CRs approved at TSG Level – December 2001

All other dates in the schedule should be adjusted to align with these anchor dates.

This work item also includes the handling of end-to-end security in the control plan. This is required for key management support.

This item is proposed to be moved to R'01 based upon the expected completion timeframe.

The objectives in the work item description should cover the complete specification of this feature and not just the architectural work.

RESULT: The workplan and work item description should be updated as described above.

6.3 User plane protection in access network

This is a **Feature.** It may also be a **(sub)building block** for other work items, eg for the **building block** "**Access network security for IP-based services**".
The R00 system architecture may create new requirements and/or opportunities for introducing integrity protection for user plane data in R00. This may create opportunities for providing enhanced security, e.g. for e-commerce services. Issues such as the addition of integrity protection to voice over IP services may need to be investigated since it might lead to a degradation in voice quality (because a single bit error will lead to the voice packet failing its integrity check and thus being rejected).
Work Tasks may involve S2, S3, R2, R3, N1, [SMG 2 WP A].

Section 3.1.1.3 of **NP-000199** was reviewed as part of the review of this work item. After considerable discussion it was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved – March 2001
- Integration of security architecture: CRs approved at TSG Level – December 2001

All other dates in the schedule should be adjusted to align with these anchor dates. It shall be indicated in the project plan that if it is decided (by S3) that this work item is required to support "Access security for IP-based services" then the timescales for this work item must be accelerated to support that work item. It was also noted that TSG-RAN is the TSG most affected by this work item and should review the work item and dates.

No work item description currently exists for this description, but one should be provided before SA#8.

RESULT: The workplan and work item description should be updated as described above.

6.4 Core network security: minimal solution

6.4.1 Status report on the integration of security features into MAP

This is a **Feature**. This ‘minimal solution’ is a feature in its own right. It is also a **Building Block** of the feature “**Core Network security: full solution**”.
In the early versions of R00, a minimal solution will be developed to protect MAP signalling at the application layer. In future versions of the specifications it will be necessary to extend security to other interfaces and application protocols.
Work Tasks may involve S2, S3, N4.

Section 3.1.1.4 of **NP-000199** was reviewed as part of the review of this work item. It was agreed that the key management aspects should be moved to a different solution (see later section) and that this solution should refer only to the MAP layer III changes. The completion date for the “Integration of security architecture: CRs approved at TSG Level” is June 2000. This work item shall not include GTP (to be covered under the full solution). SA5 shall not be involved in this work item, but shall be informed of the transition of the key management issues to a new work item.

RESULT: The workplan and work item description should be updated as described above.

NP-0000200: **[S3-000382 part of this file].** Presented by Peter H, Vodafone.

CONTENT: Contains an LS from S3 to N4 on MAP security Layer III. It includes new text to TS 33.102 for R00.

DISCUSSION:The CRs to introduce MAP security Layer III are essentially complete and are out for review. The only known outstanding issue involves the encoding of the encryption and hash algorithm type. Options include encoding the algorithm by an enumerated type or by use of an integer. An enumerated type is very specific, but requires that the algorithms be known. An integer allows for a more flexible encoding, but allows the possibility of ambiguity. The problem is that the encryption and hash algorithms are not currently known.

RESULT: The document was **DISCUSSED.** It was agreed that the encoding type shall be integer as the algorithms. A reference will be added to 29.002 indicating that the correspondence between the integer and the algorithm is specified in 33.102. S3 will update 33.102 to contain this information. The same handling applies to the hash algorithm type encoding.

6.4.2 IP-based key management versus MAP-based key management for core network security

NP-000200 **[S3-000359 part of this file]**

CONTENT: This liaison informs N4 that S3 is studying key management.

DISCUSSION:It was agreed that a new work item should be created to address this topic. This work item will cover possible solutions including both MAP and IKE. A go/no-go solution for the MAP based key management solution is expected at the August S3 meeting. Companies are asked to provide contributions to aid in the choice of solutions at the next S3 meeting. There was an indication of support for this effort from Ericsson, Motorola, and Vodafone. It was noted that manual solutions for the key management of MAP security was an option. The issue of key distribution after VLR restart was also raised.

Vodafone agreed to act as rapporteur for this work item. A new work item will be drafted in time for the SA#8 plenary.

The issue of whether the MAP layer III security would work with a GLR was addressed but no assessment could be made at the meeting.

S5 will be kept informed of the progress of this work item since their involvement is not precluded.

Although the MAP key distribution solution timeframes are known, it is more difficult to assign a date for completion of the IKE solution (if selected). S3 will endeavor to establish target dates in the August S3 meeting.

It was also agreed that the distribution of security policy information **SP-000200[S3-000363]** is also an issue that should be covered under this work item.

RESULT: The document was **DISCUSSED.** A new work item for key management will be created. If the MAP solution is selected then the MAP key management CRs should be targeted for approval in September, 2000. The dates for a IKE solution (if selected) are tbd. Note that the solutions are not mutually exclusive.

NP-000206 **[N4-000366 part of this file]**

CONTENT: This liaison requests S3's advice on whether to standardize MAP based key management.

DISCUSSION:See above discussion

RESULT: The document was **NOTED.**

6.5 Core network security: Full solution

This **feature** is the 'full solution'. It is also a **Building Block** for the feature "**Provisioning of IP-based multimedia services".**

In the early releases of R00, a minimal solution will be developed to protect MAP signalling at the application layer. In future releases of the specifications it will be necessary to extend security to other interfaces and application protocols. Many of the interfaces and protocols requiring protection will be new to R00. Application to user plane traffic will be investigated. In addition interfaces towards and within the access network (Iu, A, Iur) will also be considered.

Work Tasks may involve S2, S3, N4.

Section 3.1.1.5 of **NP-000199** was reviewed as part of the review of this work item. It was agreed that GTP security should be part of this workitem and not the minimal solution. It was agreed that the security for GTP should be given an accelerated schedule compared to other protocols. The it was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved for GTP – September 2000
- Definition of security architecture: CRs approved for other protocols – March 2001
- Integration of security architecture: CRs approved at TSG Level for GTP – December 2000
- Integration of security architecture: CRs approved at TSG Level for other protocols – June 2001

All other dates in the schedule should be adjusted to align with these anchor dates.

The work item description should be enhanced to distinguish the full solution from the minimal solution.

RESULT: The workplan and work item description should be updated as described above.

6.5.1 Security options for MAP-over-IP

NP-000200 **[S3-000364 part of this file]**

CONTENT: This liaison requests information on how address translation is done for input on security for GTP.

DISCUSSION:N4 has not yet investigated this issue but will do so.

RESULT: N4 will investigate the issue during the July meeting and respond to S3 in time for their August meeting.

6.5.2 GTP security status (LS in S3-000386)

NP-000195: **IPSec - Is it the solution to secure GTP?** Presented by Rong Shi, of Motorola.

CONTENT: Presentation on the GTP Security and the Pros and Cons of IPSec.

DISCUSSION: Decisions on this will be made at the next S3 meeting.

RESULT: The document was **NOTED.**

NP-000206: **(N4-000363- Part of the file) LS from N4 to S3on GTP Signalling Security?**

DISCUSSION: N4 ask S3 to inform them if IPSec is the definite solution for GTP signalling2 or one solution.

RESULT: The document was **NOTED.**

NP-000200: **(S3-000386- Part of the file) RESPONSE to the ABOVE LS from N4 to S3on GTP Signalling Security?**

DISCUSSION: S3 inform N4 that they desire a single solution, but have been unable to finalize the work on this.

RESULT: The document was **DISCUSSED.** The Stage 2 document for GTP (23.060 will also need to be updated – S3 will inform S2 of this requirement.

NP-000206: **(N4-000363- Part of the file) Exclusivity of IPSec?**

DISCUSSION: Asks S3 whether IPSec is the only solution for GTP security.

RESULT: The document was **NOTED.**

6.5.3 Security policy mechanism for CN signalling security (LS in S3-000363)

NP-000200: **(S3-000363- Part of the file) LS from S3 to N4 on Security Policy information?**

DISCUSSION: Security Policy information must also be considered.

RESULT: The document was **NOTED.**

6.6 GERAN access security/termination of packet domain encryption in GSM BSC

This is a **Building Block** of the Feature “**GERAN**” which may be included in the plan of the ICG group ‘**Bearer and Access Stratum’.**
The recent decision to deploy an Iu-ps interface into the R00 GSM BSC means that, at least, encryption has to be moved into the BSC. There may be an opportunity to add integrity protection at the same time. Reuse or replacement of the existing GPRS algorithms has to be considered. Opportunities for enhancing GERAN access security will be investigated such as the extension of GSM cipher keys. Feasibility studies are likely to be required.
Work Tasks may involve S2, S3, N1, N4, SMG 2 WP A, SAGE.

Section 3.1.1.6 of **NP-000199** was reviewed as part of the review of this work item. It was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved – December 2000
- Integration of security architecture: CRs approved at TSG Level – June 2001

All other dates in the schedule should be adjusted to align with these anchor dates. SMG2 is the primary specification body affected by this work, and should review the dates.

The issue of where the encryption can terminate at the BSC has not been settled, however it should still be an objective to terminate the encryption at the BSC.

N1 may be affected due to handovers. The impact of this change on the LLC should be studied.

Termination of encryption in the BSC should be mentioned as an objective in the work item. CN should also be mentioned as impacted in the WI. USIM impacts should be marked as "N". The name of the WI (and section in the project plan) should be "GERAN Security".

RESULT: The workplan and work item description should be updated as described above.

6.7 Enhanced User Identity Confidentiality

This is a **Feature**.
The GSM user identity confidentiality mechanism was not enhanced in R99. It may be required to develop security mechanisms to provide a greater degree of protection against loss of user identity and location confidentiality in R00 systems.
Work Tasks may involve S2, S3, N1, N4, RAN 2, RAN 3, T2, T3, SMG 2 WP A.

Section 3.1.1.7 of **NP-000199** was reviewed as part of the review of this work item. It was agreed that the complexity of this enhancement now seemed to outweigh the benefits. It was agreed that this work item should be removed.

RESULT: Work item deleted.

6.8 FIGS

This is a **Building Block** of the Feature "**Provisioning of IP-based multimedia services".**
VoIP telephony, multimedia services and other data services may impose additional requirements on FIGS functionality, especially within the R00 PS side nodes.
Work Tasks may involve S2, S3, N2.

Section 3.1.2.1 of **NP-000199** was reviewed as part of the review of this work item. It was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved – March 2001
- Integration of security architecture: CRs approved at TSG Level – December 2001

All other dates in the schedule should be adjusted to align with these anchor dates.

It was noted that CAMEL is not necessarily the only mechanism for providing FIGS for the IM subsystem.

No work item yet exists, but one will be defined for SA#8.

RESULT: The workplan should be updated as described above and a work item created.

6.9 Secure mobile platform for applications

No CN Impact, hence not addressed in this meeting.

6.10 OSA/VHE security

This is the **Building Block** called "**Improvements to VHE/OSA security**" by the **Feature** "**VHE/OSA**" which is part of ICG '**Service platforms'.**
This work will essentially be an extension of the R99 OSA/VHE security work.
Work Tasks may involve S3, N5 and N4.

Section 3.1.2.3 of **NP-000199** was reviewed as part of the review of this work item. It was felt that the security issue was a major deficiency in OSA and needed to be addressed. It was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved – December 2000
- Integration of security architecture: CRs approved at TSG Level – June 2001

All other dates in the schedule should be adjusted to align with these anchor dates.

The work item description should show charging as "No impact".

6.11 Visibility and configurability including ability of terminal/USIM to reject unencrypted connections

This is a **Feature.**
This work will essentially be an extension of the R99 visibility and configurability of security features work. Work Tasks might involve S3, T2, T3, RAN 2, SMG 2 WPA and N1.

Sections 3.1.2.4 and 3.1.2.8 (misplaced) of **NP-000199** were reviewed as part of the review of this work item. The dates given only address the ability of the UE to reject unencrypted connections. The dates agreed for this item are:

- Definition of security architecture: CRs approved – September 2000
- Integration of security architecture: CRs approved at TSG Level – December 2000

All other dates in the schedule should be adjusted to align with these anchor dates.

For the rejection of unencrypted connections S3 needs to clearly specify the behaviour:

- What happens to a PDP context in event of rejection;
- Network behavior in event of rejection;
- Emergency call behavior;
- Domains covered (CS, PS, UMTS);
- What is indicated to the user;
- Explicitly how the decision to reject the call is made (what is the decision based upon?)

The question was also raised of whether this applied to SMS.

The work item should be enhanced to include the rejection of unencrypted connections.

RESULT: The workplan and work items should be updated as described above.

6.11.1 GPRS issues - feasibility of rejecting unciphered calls (see draft work item descriptions from S3) - (Positive) Authentication Reporting feature

See above.

6.12 Study on the evolution of GSM CS algorithms

Not addressed due to lack of time.

6.13 Study on the evolution of GSM PS algorithms and the introduction of GEA2

Only GEA2 issues discussed due to lack of time.

6.13.1 GPRS issues - ability to negotiate GEA2 in N1 specifications (resolved at recent N1?)

NP-000202: **LS from N1 on Support for multiple GPRS ciphering algorithms in GSM 04.08/TS 24.008.** Presented by Hannu H. (Nokia)

DISCUSSION: TSG S3 is requested to consider whether it would be acceptable to have these new functional enhancement to GPRS from R99 onwards and not GPRS R98, considering that the support is mandatory from December 2002.

It is desirable to maintain consistency between R97 and R98 since the classmarks are optional. It was also felt that companies wanting to introduce GEA2 into older releases should have that option.

It seems likely that introduction of GEA2 and it's negotiation mechanism as an option in R97 and R98 should not cause backwards compatibility problems. Further checking of this is required.

RESULT: The document was **DISCUSSED.** It was agreed that CRs would be generated for R97/R98 in which the GEA2 was optional. Companies were requested to investigate whether any incompatibilities exist due to this change.

NP-000204: **Same as Above.** Presented by Colin of BT

DISCUSSION: Support the same argument as presented in NP-000202

RESULT: The document was **NOTED**

6.13 Lawful Interception in the R'2000 architecture

This is a **(SUB)Building Block** for the **Features** "**Provisioning of IP-based multimedia services**" and "**Enable bearer independent Circuit-switched network architecture".** Note that the latter dependency is not yet identified by ICG **'Call Control and Roaming'.**
Note also that this is likely to be more of a **sub-building block** rather than directly under a **feature.**
The separation of user and control planes and the introduction of the real-time voice over IP services, multimedia services and other data services may require some additions to the existing standards.
Work Tasks may involve S2, S3, N4.

The timeplan of section 3.1.2.7 of **NP-000199** was reviewed as part of the review of this work item. It was felt this needed to complete in the IM timeframe. It was agreed that the dates should be adjusted as follows:

- Definition of security architecture: CRs approved – December 2000
- Integration of security architecture: CRs approved at TSG Level – June 2001

All other dates in the schedule should be adjusted to align with these anchor dates.

RESULT: The workplan and work item should be updated as described above.

6.14 General Enhancements of the R'99 Security Architecture

It was agreed that a new work item should be created to handle the various miscellaneous enhancements to R'99 security.

RESULT: Vodafone agreed to generate a new general work item.

6.15.1 Feasibility of an authentication vector revocation mechanism (input from S3 is expected)

NP-000196: **Feasibility of an authentication vector revocation mechanism.**

DISCUSSION: The AHAG recommendations include that 3GPP add signalling to allow the HLR to revoke the current Authentication Vector (AV) and thereby causing an AV update and that that this ability be independent of the ability to revoke a registration.

S3 have not agreed to this proposal, but have forwarded this to N4 for comments. S3 have a meeting with AHAG in September;

RESULT: The document was **DISCUSSED.** N4 will examine this in the July meeting and respond to S3.

NP-000201: **Authentication Result Reporting**

DISCUSSION: The AHAG recommendations include that 3GPP that the Serving Network (SN) report the failure of any authentication and, at the HLR's option, the success of the 3GPP AKA procedure.
S3 have not agreed to this proposal, but have forwarded this to N4 for comments. S3 have a meeting with AHAG in September.

NP-000206(N4-000364) was also discussed which asks if it is acceptable to restrict this procedure to 3GPP subscribers only. The S3 delegates felt that this restriction was acceptable.

RESULT: The document was **DISCUSSED.** N4 will examine this in the July meeting and respond to S3.

NP-000201: LS from N1 on UE triggered authentication.

DISCUSSION: CN1 recognizes the need for such a function for R00 and will begin to study the issue.

RESULT: The document was **DISCUSSED.** This will be proposed as a R'00 work item. It was not felt to be required for R'99. S3 will draft a work item description for this.

NP-000205: Retention of the P-TMSI Signature concept for GPRS Release 99.

DISCUSSION: A change request has been proposed concerning the removal of the P-TMSI Signature concept for GPRS Release 99. It is noted that it was S3's intention to have an Enhanced User Identity confidentiality feature in release 99 overcome a number of security issues associated with the TMSI concept. Since this feature is no longer in place for R99, there may be a number of benefits for retaining the P-TMSI signature concept in GPRS Release 99. These are documented in the papers from Fujitsu and Lucent. See attached N1-683 & N1-790.

S3 is asked to consider these security issues, before taking any decision to remove the P-TMSI Signature. Specifically, does the basic 3GPP AKA sequence number mechanism but without the enhanced user identity confidentiality feature, address the issues for GPRS release 99?

The S3 delegates did not feel that removal of the P-TMSI Signature in the Service accept message compromised security. Furthermore, BT is asked to revise their document to indicate that the change is only proposed for the Service Accept message.

RESULT: The document was **DISCUSSED.** The decision will be made at CN#8.

7 Review of proposed security work items and comparison to F/BB/TW matrix

Not reviewed due to lack of time

8 Identification of next steps/future meetings

No future meetings are scheduled. Future joint meetings will be setup as waranted by issues.

9 Close of Meeting

The CN/S3 Meeting closed at 13:50 on June 14, 2000.

ANNEX A: OUTPUT MATERIAL

A.1 Liaison Statements

No liaison statements were generated from this meeting.

ANNEX B: Participants List for CN / S3 Meeting

Name	e-mail	Represented Organisation	Status
		ERICSSON L.M	3GPPMEMBER-ETSI

Note – this will be added when the electronic list is available.

ANNEX C: List of Documents

NP_Tdoc	Title	Source
NP-000194	Draft CN/S2 Agenda	CN Chairman
NP-000195	IPSec solution to secure GTP	Motorola
NP-000196	Home Environment Control of AKA	Telenor
NP-000197	LS on S2 presentation to joint CN / S3 meeting on security requirements for R2000	S2
NP-000198	Draft Work Item Descriptions	Peter Howard
NP-000199	Draft R00 security work plan	Peter Howard
NP-000200	S3 outgoing LSs which are relevant to S3/CN meeting	Peter Howard
NP-000201	LS from N1 on UE triggered re-authentication (S3-000402)	Peter Howard
NP-000202	LS from N1 on GEA2 negotiation (N1-000806)	Peter Howard
NP-000203	is “Peer entry authentication and key distribution in supporting UMTS inter-network security	Motorola
NP-000204	Support for multiple GPRS ciphering algorithms in GSM 04.08/TS 24.008	BT
NP-000205	Retention of the P-TMSI Signature concept for GPRS Release 99	BT
NP-000206	LS from N4 to S3	N4
NP-000207	Presentation of work items proposed by S3, SP-00020x	S3
NP-000208	R00 Architecture	Lucent/ S2

History

Document History	
Up to 20th June 2000	DRAFT v.0.0.1 provided to a select group of delegates up to the end of the meeting.
21st June 2000	*Final v2.0.0 presented for approval at TSG#8 Meeting in Düsseldorf*