**3GPP TSG-CN 3GPP / TSG-SA WG3**
**Joint Meeting**
**Sophia France**
**13th - 15th June 2000**

***NP-00xxxx***

***DRAFT***

# Third Generation Partnership Project

## DRAFT REPORT v1.0.0

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

Sophia, France
13th - 15th 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 opened the meeting at 14:00 on 13th June 2000.

# 2 Approval of the Agenda

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

**CONTENT:** The document contains the meeting Agenda

**RESULT:** The Agenda was **AGREED**

# 3 Allocation of documents to agenda

Documents were allocated to agenda items on-line, and the situation projected during the meeting on the OHP / BARCO.

# 4 Presentation of S2 Architecture Status

**NP-0000208:** **3GPP Release 2000 Discussion Document.** Presented by Liz Daniel, of Lucent.

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

**DISCUSSION**: **Mikko, Nokia:** Questions on ROAMING. Response: May have roaming between operators, AND roaming between the PS and the CS domains, depending on availability of IP multimedia services.

**Stephen H, Ericsson:** To what level are IP v.4 and IP v.6 interoperable? **Response**: Clients may support dual stacks, or tunnel IP v.4 through IP v.6

**Yun-Chao Hu, Ericsson:** Has IMSI been agreed as the identifier for the application level registration? **Response**: Use of UMSI has yet to be decided by S2 – may be deferred to S3.

**Nigel, Lucent:** Do the two MGWs have the same functionalities? **Response**: Can have 2 distinct MGWs or compact them into a single MGW with the same functionality.

**Henry, BT:** What IETF specifications have been examined by S2? **Response**: S2 have only examined SIP, and expect CN to study the requirement of extensions.

**Yun-Chao Hu, Ericsson:** What about SGSN? **Response**: S2 have agreed on a feasibility for splitting SGSN.

**Yun-Chao Hu, Ericsson:** Will SIP only be used for control? **Response**: S2 have examined H.248 for the use of control.

**Peter H, Vodafone:** Timescales? **Response**: Architecture 80% complete by the September plenary.

**Bart, Siemens:** What about MAP? **Response**: MAP will not be used within the IP Multimedia network, possibly used for interworking to MAP networks.

**Yun-Chao Hu, Ericsson:** Is Transcoder free operation stable for N4 to continue work? **Response**: S2 will regard the high level operation, and have not examined the information flow. **(This will be handled in tomorrows CN/S2 meeting)**

**Hannu, Nokia:** Stability of SIP Stage 2? **Response**: Not 80% stable, but there are some areas of work that are stable enough for CN to begin work.

**Niemi, Nokia:** Securing the IMSI? **Response**: IMSI is outside of the PLMN, raises a concern of security.

**Peter H, Vodafone:** IMSI – business model is based on roaming? **Response**: Could mean 2 separate identifiers, S3 needs to consider this.

**Yun-Chao Hu, Ericsson:** IMSI security, Process based on IETF mechanisms – has IMSI been take to IETF? **Response**: Not yet taken to IETF, and other identifiers within IETF have not been examined.

**Stephen H, Ericsson:** IMSI security is end to end? **Response**: With IP v.6, the assumption is that security is end to end.

**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**: **Mikko, Nokia:** Some WIs are targeted for completed for 2001, what is the impact on R2000? **Response:** S3 has only identified the phases, S2 have done the project planning that gives these completion dates.

**Stephen H:** Suggested using the best level of accuracy for completion dates, and if this means work items are moved to R01, then this should be indicated.

**Peter K, Ericsson**: Stressed the importance of setting priorities for work items. **Response:** this has been examined and initially 3 categories have been proposed by S2.

**RESULT:** The document was **DISCUSSED**

# 6 Review of status and requirements on CN for security items (Taken from S3 proposal in F/BB/TW Matrix+ item 5.13)

**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

**RESULT:** The document was **DISCUSSED**

## 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].

| **Event** | **Expected date** |
|---|---|
| Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles | June/July 2000 |
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Building Block. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to CN, RAN, T and GERAN: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

**Comments to the Project Plan (contained in NP-000198)**

**Hannu:** Considering the dates given, Is this for R00 or R01? **Response:** The modification of the dates was made by S2. This means this cannot be complete by the end of year 2000.

**Peter** mentioned that S3 do not yet have a full understanding of the scope of work required for this function. Hence dates are difficult to confirm.

- **Modification of Stage 2 “CRs to TS 33.102 approved for the Definition of Security Architecture” December 2000.**

- **Integration of security architecture Stage 3 “CRs approved at TSG level” moved to June 2001 and Corrections agreed at TSG level  to September 2001**

**Comments to the Work Item sheet (contained in NP-000199)**

Add indication of SERVICES as 3GPP work aspects.

**Hannu:** Indicate the expected input on this work item from other working groups

Should not need to schedule for **Corrective CRs**

## 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].

| **Event** | **Expected date** |
|---|---|
| presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles | June/July 2000 |
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Feature. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to CN, RAN, T and GERAN: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

**Comments to the Project Plan (contained in NP-000199)**

- **Definition of security architecture - CRs approved moved to March 2001**

- **Integration of security architecture - CRs approved at TSG level moved to December 2001**

**Comments to the Work Item sheet (contained in NP-000198)**

None made during the meeting

## 6.3 User plane protection in access network

***Note No Work Item Description sheet yet.***

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].

| **Event** | **Expected date** |
|---|---|
| presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles | June/July 2000 |
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to CN, RAN, T and GERAN: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

**Comments to the Project Plan (contained in NP-000199)**

**Peter:** This may be a feature in its’ own right, with similar priority to the above work item. However if this is a building block for security in the IM domain , then it must be considered High priority

**Stephen:** General comment, RAN should review proposed dates and priorities.

- **Definition of security architecture - CRs approved moved to March 2001**
- **Integration of security architecture - CRs approved at TSG level moved to December 2001**

**Comments to the Work Item sheet (contained in NP-000198)**

Will be updated to reflect the changes above

## 6.4 Core network security: minimal solution

### 6.4.1 Status report on the integration of security features into MAP (LS in S3-000382)

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.

| **Event** | **Expected date** |
|---|---|
| Completion of ongoing work in S3 | S3#13   23 - 26 May 2000; Tokyo; DoCoMo |
| Completion of ongoing work in N4 | TSG #9: June 2000 |
| Completion of GTP security. | November 2000 |
| Completion of work in S5 | TSG #10: September 2000 |

**Comments to the Project Plan (contained in NP-000199)**

- **Completion GTP will be moved to “full solution”**
- **S5 dependency may be deleted from both solutions – S5 SHALL be informed**
- **Shift of dates required**

**Comments to the Work Item sheet (contained in NP-000198)**

Identical to minimal solution, and requires to be updates to reflect the changes given above.

**NP-0000200:** **[S3-000383 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**: **Ian Park:** This work has been covered by Vodafone and Ericsson. However, there are some concerns raised during e-mail discussion on MAP layer 3 security CR, requires S3 to specify which code points should be used.

**Agreed to it being INTEGER- type.** This implies S3 have to specify the mapping between the integer and the algorithm type (33.102). Ian Park will send out a mail to this effect to the N4 mail exploder.

**The same holds for the HASH algorithm identifier.**

**NOTE:** Key Management has to be an integral part of the minimal CN security solution.

**The open question is:** Do S3 want a MAP based Layer 1 and 2 for Key Exchange and Key Distribution?

**Note:** The CRs from N4 for Layer 1&2 have been kept separate from the layer 3 solution. This means that there can be

**The GLR should always know the required KEY as it is a part of the visited network**

**PROPOSED SOLUTION:**

**1. CN Security Minimal Solution**

**2. CN Security Full Solution**

**Propose to add a third work item, “MAP Security and Key management”**

**This was agreed by the meeting.**

**RESULT:** The document was **DISCUSSED**

### 6.4.2 IP-based key management versus MAP-based key management for core network security (LS in S3-000359 plus further inputs from S3 expected)

The meeting has agree to the production of a new Work Item KEY Management

MAP solution – a decision on whether to continue is required at the next S3 meeting (August 2000)

Vodafone will continue work on the IEK solution in parallel. Technical contributions are requested on both solutions.

If N4 have advance indication of S3s decision to use the MAP solution, they should be able to finalise the level 2/3 Crs at the N4 meeting (28th August), to be approved at the September 2000 Plenary.

## 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.

| **Event** | **Expected date** |
|---|---|
| Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles | June/July 2000 |
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to CN, RAN, T and GERAN: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

- ➢ **Separate out GTP Security – that can be completed earlier (Dec 2000)**
- ➢ **Remaining Work CRs approved at TSG level by June 2001**

### 6.5.1 Security options for MAP-over-IP

**NP-000200:** **(S3-000364 Part of the file) LS from S3 to N4 on Security for MAP over IP?**

**DISCUSSION:** High level only discussion within N4. MAP will most probably be considered as an application, and we will still use TCAP on the lower levels.

Resolution expected by N4 during their July meeting – Feedback to S3 for their August Meeting.

**RESULT:** The document was **NOTED**

### 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:** **(S3-000363- 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.

**Stage 2 document will also need to be updated – S3 will inform S2 of this requirement.**

**RESULT:** The document was **NOTED**

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

**DISCUSSION:** Layer 1 and 2 issue. Layer 3 already handled in the MAP protocol machine. The LS can be considered as additional information.

**RESULT:** The document was **NOTED**

### 6.5.3 Security policy mechanism for CN signalling security

No input for this agenda item.

## 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.

| **Event** | **Expected date** |
|---|---|
| Presentation by SMG 2 to S3/SMG 10 of well-defined and understandable system architecture concepts and principles | S3#14 August 2000 |
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to CN, T and GERAN: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |
| Production of new algorithm(s) by eg, SAGE ? | Requirements complete August 2000<br>Funding arranged January 2001<br>Work completed June 2001<br>Publication completed October 2001 |

**Comments to the Project Plan (contained in NP-000199)**

- **Provides commonality with the UTRAN Security Architecture**
- **GERAN propose termination in the BTS (as opposed to BSC above) hence this WI title and scope may change accordingly**
- **This requires discussion between S3 and SMG2 – CN will await outcome**
- **This is a high priority for SMG2 in Release 2000 – the above dates should change**
- **MOVE Definition of Security architecture - CRs approved in Dec 2000**
- **MOVE Integration of Security architecture - CRs Approved at TSG level in June 2001**

**Comments to the Work Item sheet (contained in NP-000198)**

Same comments as above apply.

3GPP Work Areas – CN needs to be marked.

Additional objective “study the future of the LLC layer“

Work plan and work item titles need to be aligned. (use GERAN SECURITY)

NO impacts on USIM

Additional objective Move ciphering into BSC from BTS

***Rapporteur will modify as required.***

## 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.

| **Event** | **Expected date** |
|---|---|
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to S2, CN, RAN, T and GERAN: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

**Comments to the Project Plan (contained in NP-000199)**

- **Little interest in this Work Item for R00 – no objection to REMOVING this work item**
- **this was agreed by the meeting**

## 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.

| **Event** | **Expected date** |
|---|---|
| presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles | June/July 2000 |
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to CN and S2:<br>February<br>2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

**Comments to the Project Plan (contained in NP-000199)**

- **Based on CAMEL, but is not the ONLY tool for FIGS**
- **FIGS will be applicable to IP Multimedia**
- **FIGS priority LOW – S3 CRs March 2001, CN Completion Dec 2001**
- **No work Item yet, will be produced by SA#8**

## 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.

| **Event** | **Expected date** |
|---|---|
| presentation by N5 to S3 of well-defined and understandable system architecture concepts and principles | S3#14, August 2000 |
| Requirements capture | S3#15 September 2000 |

|  |  |
|---|---|
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to CN, S2 and T: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

**Comments to the Project Plan (contained in NP-000199)**

- **Priority HIGH – S3 CRs Dec 2000, CN Completion June 2001**
-

**Comments to the Work Item sheet (contained in NP-000198)**

No impacts to charging

## 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.

| **Event** | **Expected date** |
|---|---|
| Requirements capture | S3#15 September 2000 |
| Security feature specification | First draft: S3#16 November 2000 |
| Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item. | January 2001 |
| Definition of security architecture | First draft March 2001<br>CRs approved: May 2001 |
| Integration of security architecture | Concept presented to S2, T, CN, RAN and GERAN: February 2001<br>First draft CRs March 2001<br>Complete CRs April 2001<br>CRs approved at TSG level May 2001<br>Review of complete CRs by S3 June 2001<br>First corrective CRs prepared July 2001<br>Corrections agreed at TSG level August 2001 |

**Comments to the Project Plan (contained in NP-000199)**

- **S3 Conclude work in September 2000 CN December 2000**

**Comments to the Work Item sheet (contained in NP-000198)**

Description in the requires expanding.
Indicates activity of CN (requires X)
clarification required from S3 on:

- conditions for rejecting call require further study
- network behavior following call rejection
- What happens to the PDP context
- Domains (ps cs umts)
- indication to the user
- does this also apply to SMS

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

## 6.12 Study on the evolution of GSM CS algorithms

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

### 6.13.1 GPRS issues - ability to negotiate GEA2 in N1 specifications

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

**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.

- **CRs to be generated for R97/R98 where classmark changes are optional**

- **GAE2 Negotiation agreed as option for R97 and R98 and mandatory for R99 hence no change to the R99 CRs**

**RESULT:** The document was **NOTED**

**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**

## 6.14 Lawful Interception in the R'2000 architecture

- **S3 complete Dec 2000 CN complete June 2001**

## 6.15 General Enhancements of the R'99 Security Architecture

### 6.15.1 Feasibility of an authentication vector revocation mechanism

**Note:** (input from S3 is expected)

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

**DISCUSSION:** The AHAG recommendations:

1 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.
2 that the Home System have a mechanism to control the duration of the Security Association (SA).
3 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;

N4 will examine this in the July meeting.

**RESULT:** The document was **NOTED**

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

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

The scope of such work must be defined and the WG from which the WI description originates must also be defined. CN1 proposes that such definitions are input to the R00 planning workshop in Nice on the 14.-15. June 2000 with the goal of approving the project plan at the TSG plenary #8 in June.

- **AGREED to be a R00 Item**
- **Work Items required from S3**

**RESULT:** The document was **NOTED**

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

**DISCUSSION:** Issue emerging from N1.

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 decision will be made at the CN meeting next week – Feedback require by interested companies at that meeting**

**RESULT:** The document was **NOTED**

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

No covered in the meeting

## 8 Identification of next steps/future meetings

Future joint S3/CN meetings to be planned on a supply and demand basis.

## 9 Close of Meeting

The CN/S3 Meeting closed at 13:50 on 15th June 2000.