

TSG SA WG3

S3-99257

Meeting #5, Sophia Antipolis, 3-6 August, 1999

Source: Secretary TSG SA WG3 (Ansgar Bergmann)

Title: Report of TSG SA WG3 Meeting #5

Status: Approved

Table of contents

1	General.....	3
2	Approval of the Agenda.....	3
3	Registration and assignment of input documents.....	3
4	Approval of the meeting report of TSG-SA3 Meeting no. 4	4
5	Review status of SA WG3 deliverables	4
6	Reports / Liaisons from other groups	4
6.1	TSG-SA and its WGs.....	4
6.1.1	SA plenary	4
6.1.2	SA WG2	5
6.2	TSG-T, TSG-CN, TSG-RAN and their sub-groups.....	6
6.2.1	TSG-T.....	6
6.2.2	TSG-CN.....	6
6.2.3	TSG-RAN.....	7
6.3	Partners and their bodies.....	7
6.3.1	TIP1.5	7
6.3.2	Report from ETSI/SAGE.....	7

7	Cryptographic algorithms	8
8	Security architecture	8
8.1	Integrity protection mechanism	8
8.2	Ciphering mechanism	9
8.3	Authentication and key agreement	9
8.4	Terminal security.....	10
8.5	Network-wide encryption	10
8.6	Core NW security.....	11
8.7	Inter-System Handover	11
8.8	Review of architecture specification	11
8.9	Enhanced user identity confidentiality.....	11
9	Integration guidelines.....	12
10	Guide to 3G security (3G TR 33.900).....	12
11	Lawful interception.....	12
12	Prioritisation and planning of work items	13
13	Future meetings	14
14	Any other business.....	14
16	Close of meeting	14
	Annex A: List of participants.....	15
	Annex B: List of documents.....	17
	Annex C Summary of actions, decisions and outgoing liaisons.....	20
	C1 Action points	20
	C2 Decisions.....	20
	C3 Outgoing liaison statements.....	21
	Annex D: Meeting report of SMG10 #2/99	22

1 General

The 3GPP TSG SA WG3 Chairman and SMG10 WG3 Chairman, Mike Walker, welcomed the delegates and thanked ETSI for hosting the meeting. The meeting was a joint meeting between SMG10 (SMG10 meeting no. #2/99) and 3GPP TSG SA WG3 S3 (meeting no. S3#5) with SMG10 sessions, S3 sessions, joint SMG10/S3 sessions and SMG10 working parties sessions.

During the meeting, the 3GPP TSG SA WG3 Vice Chairman Adam Berenzweig (Lucent) announced that he had to resign of this position. The meeting thanked Adam for his excellent work as a Vice Chairman in a time where it implied extreme overload and high responsibility.

As a new Vice Chairman of TSG SA WG3, Michael Markovici (Lucent) was elected by consensus.

2 Approval of the Agenda

S3-99215 is the draft agenda for S3#5. It was approved with some modifications:

➤ **The following agenda was approved:**

- 1 Opening of the meeting
- 2 Approval of the Agenda
- 3 Registration and assignment of input documents
- 4 Approval of the meeting report of TSG-SA3 Meeting no. 4
- 5 Review status of SA WG3 deliverables
- 6 Reports / Liaisons from other groups
 - 6.1 TSG-SA
 - 6.2 TSG-T, TSG-CN, TSG-RAN
 - 6.3 Partners and their bodies
 - 6.4 Others
- 7 Cryptographic algorithms
- 8 Security architecture
 - 8.1 Integrity protection mechanism
 - 8.2 Cipherring mechanism
 - 8.3 Authentication and key agreement
 - 8.4 Terminal security
 - 8.5 Network-wide encryption
 - 8.6 Core NW security
 - 8.7 Handover
 - 8.8 Review of architecture specification
 - 8.9 Enhanced user identity confidentiality
- 9 Integration guidelines
- 10 Guide to 3G security
- 11 Lawful interception
- 12 Prioritisation and planning of work items
- 13 Future meetings
- 14 Any other business
- 15 Close of meeting

3 Registration and assignment of input documents

See Annex B.

4 Approval of the meeting report of TSG-SA3 Meeting no. 4

➤ [The S3#4 meeting report in S3-99209 was approved.](#)

Action Points from earlier meetings:

- AP Mike Walker: to add a statement in the status report to SA#4 asking on requirements on secure IMEI: This was done.
- AP all: To investigate the question of delay caused by en/decoding: The action point was closed. Still, information on the issue is welcome.
- On list of messages to be integrity protected: This is going on.
- Response for Annex C of 33.105 from other groups has not been received, except for S2.
- Check of X20 (whether it should be specified as 24 bits, see 33.103)¹: to be done.
- CR to correct figure in 33.103: tbd
- Comments to s3-99152: superseded.
- AP on location of f9: Working assumption made during S3#5 (see section 8.1)
- AP to specify what should happen if the MS discovers that integrity is not provided: tbd
- AP to specify when to apply integrity protection (e.g., during ciphering? etc.): Answer: always, whether ciphering is applied or not
- AP all: To examine consequences of the CR in S3-99180 (modified synchronisation procedure) on the option of a global counter in 33.102: tbd

Open action points from last meeting:

- ✎ **On list of messages to be integrity protected: This is going on.**
- ✎ **Response for Annex C of 33.105 from other groups has not been received, except for S2.**
- ✎ **Check of X24: to be done.**
- ✎ **CR to correct figure in 33.103: tbd**
- ✎ **AP to specify what should happen if the MS discovers that integrity is not provided: tbd**
- ✎ **AP all: To examine consequences of the CR in S3-99180 (modified synchronisation procedure) on the option of a global counter in 33.102: tbd**

5 Review status of SA WG3 deliverables

✎ **Concerning S3-99238, the work plan of specifications with intermediate steps, it was agreed that Ansgar Bergmann should maintain an updated version on the server. Also he should create a directory in the S3 domain where the latest versions of specifications can be found that are not yet under change control.**

Note: There is a directory in the SA plenary domain where the specifications in the version at SA plenaries are stored, which is not the same.

6 Reports / Liaisons from other groups

6.1 TSG-SA and its WGs

6.1.1 SA plenary

Adam Berenzweig, SA WG3 Vice Chairman (cf. however section 1), reported from SA#4. At the time of

¹ This action point was phrased incorrectly in the S3#4 report, where "X20" was misprinted as X24, and 33.103 as 33.102.

S3#5, only a draft meeting report (version 004) of SA#4 existed; it was made available during the meeting as an unnumbered document. (The most recent version is available on TSG_SA/TSG_SA/TSGS_04/Report). The S3 report to SA#4 is S3-99242 (=SP-99293). The status of 3GPP security deliverables and priorities of work items had been presented to SA#4 in S3-99238 (=SP-99284). SA#4 had approved all specifications and change requests presented by S3, see section 5.

Among the points discussed at SA#4 are the following:

- The need to keep time scales to delivery of the cipher algorithm was expressed. It was requested that members would be able to obtain the algorithm during the evaluation period.
- Concerning the work item priorities in S3-99238, the SA WG2 Chairman reported that the 3GPP Project Plan for 3G Security is being created with the help of the SA WG3 Chairman.
- A LS from the GSM Association to TSG SA on Priorities in order to meet the time-scales (Document SP-99317) was noted at SA#4; it gives a list of security priorities as follows: Mutual Authentication, Longer Key length, SS7 Security and Network wide encryption.
- It was recognised that the Security Requirements will impact TSG CN in the main part, and some close liaison between SA WG3 and TSG CN is needed. TSG CN Chairman asked for clear guidance on the Priorities from SA WG3 with input from SA WG2. It was agreed that CN delegates should participate at the August SA WG3 meeting for discussion on this. This was agreed by TSG SA as a practical approach. There was a request also for involvement from T WG3 in the prioritisation of security requirements.
- It was clarified that the current GSM User Identity Confidentiality mechanism is not considered by S3 good enough for protection against determined attacks. The draft SA#4 report also mentions a clarification that the implementation would be optional, as in the GSM case (sic).
- SA#4 decided that the securing of Terminal Identities (IMEI Security) is an important goal.
- It was reported that the comments received from SA WG2 were not dealt with during the last S3#4 due to lack of time and that they would be taken into account at the next SA WG3 meeting.
- S3 was asked to check the use of terminology in their documents with reference to the (TSG RAN) Vocabulary document.

6.1.2 SA WG2

S3-99226 contains liaison statements received from S2. They had been approved, mostly without presentation, at the last S2 meeting:

TDoc #	Title	Answer to	Conclusion at S2	S3-99226 annex #	Conclusions of S3#5
S2-99587	Answer to S3 to the LS on Authentication for Mobile IP Operations in UMTS	S2-99548	approved.	A	xxx postponed? xxx
S2-99590	Forward to S3 and R2 (Cc T3) to T3's LS on Parameters to be stored in the USIM	S2-99560	Approved	B	xxx postponed? xxx
S2-99633	Answer to S3, T3 (Cc N2) to the LS on Interoperation between UMTS and GSM	S2-99534	Approved without presentation.	C	LS in S3-99251 (see 8.7)
S2-99634	Answer to S3, T3 (Cc N2) to the LS on Enhanced User Identity Confidentiality (check)	S2-99536	Approved without presentation.	D	LS in S3-99254 (see 8.9)
S2-99635	Answer to S3, T3 (Cc N2) to the LS on Evolution to UMTS and R99 Security Features	S2-99545	Approved without presentation.	E	S3-99254, S3-99258 (see 12)
S2-99636	LS to S3 (Cc T3, R2, R3, N1, and N2) on answer to the LS on the time constraints on the execution of cryptographic algorithms	S2-99539	Approved without presentation.	F	xxx postponed? xxx

➤ [As a liaison representative to S2, S3#5 nominated Peter Howard.](#)

6.2 TSG-T, TSG-CN, TSG-RAN and their sub-groups

6.2.1 TSG-T

S3-99221, *Liaison Statement to S3 on Baseline Capabilities - Request and Confirmation of Terminal Baseline Implementation Capabilities in the security domain* (T2-99585) and S3-99222, *Liaison Statement to S3 on Service Capabilities - Request of Terminal Service Implementation Capabilities in the security domain* (T2-99586), both source: T2, were presented by Yasushi Iwane.

In these and other T2 documents, a distinction is made between

- baseline capabilities of a terminal (capabilities the terminal has to have, even if it doesn't support any service)²;
- service capabilities of a terminal (which are in relation to services the terminal supports);
- implementation capabilities (capabilities that relate to a particular technical domain) with two sub-kinds:
 - baseline implementation capabilities (set of implementation capabilities, in each technical domain, required to enable a terminal to support the required baseline capabilities);
 - service implementation capabilities (set of implementation capabilities, in each technical domain, required to enable a terminal to support a set of Service capabilities).

The aim of S3-99221 and S3-99222 is to ask S3 for identification of the implementation capabilities within its technical domain.

Comments at S3#5:

- The line of "local authentication" might have to be deleted.
- There might be requirements for GSM-3G handover.
- Enhanced user identity confidentiality should not be an option in the table.
- For Mobile Equipment Identification, security will become mandatory but is still under investigation.

➤ [As an answer to S3-99221, S3#5 approved S3-99252, LS to T2 on Baseline Implementation Capabilities in the security domain \(this LS contains TS33.103 as an attachment\).](#)

6.2.2 TSG-CN

S3-99231, *Liaison Statement on the Super-Charger Concept*, source: N2, inviting S3 to check 3G TS 33.102 for necessary changes to introduce the super-charger concept. (This concept foresees, in order to reduce signalling traffic, to leave the subscription data at the old VLR when the subscriber moves to a new VLR area, thus skipping the cancel location procedure and enabling usage of that data (e.g., authentication vectors) later when the subscriber returns to the old VLR area.³

Günther Horn presented a proposed answer in S3-99235 and a corresponding CR to 33.102 on *Enhanced window mechanism for sequence number management* in S3-99234, both source: Siemens AG / Siemens Atea NV.

Questions and clarifications to S3-99231 at S3#5:

- ageing of security parameters in a VLR would be a problem;
- triplet re-use is not intended;
- in case of change of algorithm, a cancel location would be necessary;
- super-charger could have unwanted consequences for IST.

➤ [A revision of S3-99235 in S3-99255, Response to LS statement N2-99918 \(=S3-99231\) from N2 to S3](#)

² More precisely, the documents defines (recursively?)
baseline capabilities as capabilities that are required for a service-less terminal to operate within a network and
a service-less terminal as a terminal that has only the baseline capabilities.

³ A - yet unnumbered - technical report (Tdoc N2-99 972) on super-charger , announced as an attachment of S3-231, was in fact missing in the LS. It is available as S3-99260.

on Super-Charger concept was approved by S3#5.

S3-99232, a LS from N2 on IST for non-CAMEL subscribers, was discussed in the SMG10 part of the meeting, see annex D.

6.2.3 TSG-RAN

S3-99228 is a liaison statement from R2 to S3 on ciphering algorithm requirements indicating the length of Protocol Data Units (PDU) and Service Data Units (SDU).

Discussion in S3: S3-99228 contains essential information for SAGE. Also, the information should be included into the algorithm requirements document.

➤ S3#5 decided to include the information from S3-99228 into the algorithm requirements document (3G 33.105).

✍ **It was agreed that Peter Howard should distribute after the meeting S3-99248, CR to 33.105 on Cipher keystream block length, adding the relevant information, for discussion and if possible agreement by e-mail.**

6.3 Partners and their bodies

6.3.1 T1P1.5

S3-99225, status of LCS, was presented by Peter Howard. In particular

- The GSM specifications for LCS phase 1 (TOA) are completed. E-OTD and GSM supported GPS are intended for SMG#30, still in release 98.
- TOA is not applicable to UTRA.
LCS phase 3 is currently discussed in T1P1. Possible aspects include CAMEL interworking and lawful interception.

➤ Decision of S3 and SMG10 on work split between SMG10 and S3 on LCS: GSM LCS phase 2 will be dealt with in SMG10. For LCS phase 3, the split will be decided in due time.

See annex D for further discussion. S3-99245 sketches the message flows for LCS.

6.3.2 Report from ETSI/SAGE

Gert Roelofsen presented S3-99223, *Design of standard 3GPP Encryption and Integrity Algorithms*, source: SAGE Chairman:

ETSI SAGE is setting up a Special Task Force to carry out the design work. Funding for this Special Task Force has been confirmed. ETSI SAGE already decided that the MISTY algorithm will be the starting point for the design work. A variant of this algorithm will be the basis for the actual standard 3GPP Encryption and Integrity Algorithms. The designer of MISTY has been asked to participate in the Special Task Force designing the Algorithms. Furthermore a "Call for Experts" was sent to TSG-SA WG3. These experts, who will work on a non-funded basis, have the task to independently evaluate the (intermediate) Algorithms design proposals from the Special Task Force. ETSI SAGE has already received a number of responses on this Call for Experts. ETSI SAGE hopes to start the design work during a meeting on the 5th and 6th of August. The current planning is to have the final Algorithms specifications available by the end of October / first half of November, which would leave 4-6 weeks for the envisaged evaluation of the Algorithms by independent parties.

SAGE believes that questions related to ownership, publication policy and management of the algorithms, the decision when and how to publish the Algorithms and the formulation of the rules for management of the Algorithms specifications should be co-ordinated by TSG-SA WG3.

An evaluation of the Algorithms by independent parties between November and mid December is

envisaged. The responsibility for organising and finding the funding for this evaluation by independent parties is with TSG-SA WG3.

ETSI SAGE would welcome extension the time scale for the design of the standard 3GPP Encryption and Integrity Algorithms.

Clarifications at S3:

- SAGE understood that the integrity and cipher algorithms should allow an integrated realisation. If ciphering and integrity protection are implemented in different layers and/or network equipment, the benefits of integration would then of course be lost.
- The working assumption has been taken to use an existing algorithm (MISTY) as a starting point for the algorithm. One reason is to meet time schedules.
- S3 did not take position to the suitability of MISTY.
- PCG, UMTS Forum, European Commission and GSMA had been uncomfortable on some openness concepts of the elaboration procedure. It was clarified that S3 intends to publish the design of the algorithm.
- Mitsubishi has IPRs on MISTY, however might indicate that they will make MISTY and derivatives available free of charge. It is not intended in SAGE to re-use parts which fall under existing IPRs.
- Mike Walker commented that 3GPP should be the owner of the algorithms.
- S3 expects a report from SAGE that the evaluation by independent experts has been taken into account.
- Funding needs for the evaluation by independent experts have to be specified, September would be the time to contract them.
- Work split between paid and unpaid experts of the STF: The paid experts will elaborate the modifications to MISTY, the unpaid experts will review the work.
- GSMA is currently studying IPR aspects for security algorithms, in particular for publishing them.

7 Cryptographic algorithms

See sections 6.2.3 on enhancements of 3G TS 33.105. See section 6.3.2 on progress of development of the algorithms.

8 Security architecture

8.1 Integrity protection mechanism

General comments at S3:

- COUNT should be the same parameter as used for ciphering.
- Integrity protection for signalling would counter false base stations. However, integrity protection of user data is a requirement as well.

 **AP To take up the protection to user data against modification on the radio interface in the next meeting.**

S3-99205, *CR to TS 25.301 - Integrity control mechanism*, source: Nokia: The document proposes to perform integrity protection at the RRC layer and argues why RLC and MAC are seen as inappropriate.

S3-99217, *Location of integrity termination in the network*, source: Vodafone, proposes to terminate integrity protection in the MSC/SGSN or in both MSC/SGSN and RNC instead of the RNC alone. An advantage would be that integrity protection could be offered to a 3G user when roaming into a GSM (part of a) network without changes of the GSM BSS. The integrity protection information could be added to L3 messages which belong to MM and CM and those RRC messages which do not terminate in the RNC.

Discussion in S3:

- The importance of concepts for operation of integrated GSM/UMTS networks was stressed.
- Amongst the RRC messages terminating in the RNC, the cell update would be especially important.

- Under the assumption that not all MM and CM messages are to be integrity protected, termination in the RNC would be problematic from a protocol architecture point of view. However the working assumption is to integrity protect all MM and CM messages.

➤ **S3#5 decided to adopt the working assumption that integrity protection terminates in the RNC.**

Location of f9 algorithm in the mobile station (UE or USIM): The following aspects were discussed at S3#5:

- power consumption: It was reported that power consumption is not significantly increased when the SIM holds f9;
- performance aspects: e.g., how frequently the function is invoked, which delay is acceptable;
- re-use of parts of the cipher algorithm;
- necessity to transport the key at the SIM/UE interface.

➤ **S3#5 decided to adopt the working assumption to locate f9 in the UE.**

8.2 Ciphering mechanism


S3-99233, *Further clarifications of the MAC based ciphering solution*, source: Nokia, analyses some aspects of MAC based ciphering. It concludes that Nokia withdraws the proposal to adopt MAC based ciphering for non-transparent data and proposes RLC layer level instead.

S3-99210, *LS from R3 on Ciphering mechanisms in case of multiple RABs (R3-99790)*, source: R3, questions whether the possibility should be provided to only cipher a subset of the Radio Access Bearers (RAB) assigned to a user.

Later in the meeting, Adam Berenzweig and Peter Howard presented S3-99247, LS to R3 on *Ciphering in the case of multiple RABs*. The LS confirms that it is not necessary to provide a mechanism where only a subset of simultaneous Radio Access Bearers assigned to a single user are ciphered. Moreover, even when security is provided at the application layer for a subset of the Radio Access Bearers (e.g. data bearers supporting secure IP services), access link encryption should still be applied to these bearers.

➤ **S3-99247, LS to R3 on Ciphering in the case of multiple RABs, was approved by S3#5.**

S3-99224, *CR to 33.102 on Cipher keys on control and user planes*, source: Vodafone: This CR was further discussed.

 **Later in the meeting it was decided that Peter Howard should distribute S3-99246, CR to 33.102 on Cipher key setting, with the aim to reduce the options for the handling of cipher keys generated in different domains, for e-mail discussion and, if possible, agreement in S3.**

8.3 Authentication and key agreement

Multiple authentication vectors and keys: S3-99212, *Liaison statement (LS) from 3GPP TSG-T3 to 3GPP TSG-S3 on Multiple authentication algorithms and keys*, source: T3, asks whether the USIM should be able to manage multiple authentication algorithms and keys.

➤ **As a response. S3#5 approved a LS to T3, C1, C2, R3 in S3-99259 (revision of S3-99249), Response to LS from TSG T3 (S3-99212) on Multiple Authentication Algorithms and Keys.**

Main points: The authentication mechanisms currently do not explicitly require support for multiple authentication algorithms or keys. However it could be useful for disaster recovering such as (e.g.) all the authentication keys in the network being disclosed. Therefore S3 will produce a mechanism to support such a feature. Any mechanism that provides authentication algorithm or key identification to the mobile would obviously impact the air interface and core network signalling messages.

Order of authentication vectors: Stefan Pütz presented S3-99230, *A Possible Problem of the UMTS AKA Mechanism*, Source: T-Mobil, Deutsche Telekom, indicating the potential problem that during transmission, the order of authentication vectors from AuC to SN/VLR might be changed, and

proposing as a possible solution to add the sequence numbers in the clear on MAP. As a response, S3-99236, *Response to doc 99230 "A Possible Problem of the UMTS AKA Mechanism" from T-Mobil/Deutsche Telekom*, source: Siemens AG / Siemens Atea NV, was presented by Günther Horn, explaining that the preservation of order is guaranteed by SS7 protocol mechanisms, and that therefore the argument stated in contribution S3-99230 is not a valid reason to include the sequence number in the clear in authentication vectors. However, see section 6.2.2 on S3-99234 and S3-99256 for a companion contribution by Siemens proposing to include the sequence number in the clear in authentication vectors for a different reason.

Enhanced window mechanism for sequence number management: Contribution S3-99234, source: Siemens AG, was presented by Günther Horn, which proposes an enhanced window mechanism for sequence number management in the authentication scheme. It allows the SN to determine whether authentication vectors it has in storage will still be accepted by the MS.

➤ [A corresponding CR to 33.102 in S3-99256 \(rev. of S3-99234\) was approved by S3#5.](#)

8.4 Terminal security

The intention of S3 to work on terminal security had been presented at SA#4, and endorsed, see section 6.1.1.

It was clarified at S3#5 that WAP has performed work on security mainly in the application area, not on secure device identification.

Wael Adi presented S3-99168, *Provable Terminal Identity with a Public-Key Mechanism*, source: W. Adi, Bosch Telecom. This document had already been available at S3#4. An earlier contribution to the topic had been S3-99127. The slides of his presentation xxx are in S3-99250.

 **Wael Adi to provide the slides (S3-99250)**

Clarifications of the proposal:

- Implementation in existing hardware units: This refers to hardware in the network.
- The intention is to use one centralised trusted centre throughout of the world. Instead of a centralised trusted centre, a distributed data base might be used, keeping a black list.
- The manufacturers could provide a box verifying the signature of mobiles.

Mike Walker commented that

- a concept where manufacturers have to register every terminal produced in a central register would not be realistic (for example, because they don't want quantity of their production to become public);
- similarly, a centralised trusted centre is not realistic.

Next steps for terminal security:

- to establish a document listing potential applications and the requirements from these applications to a mechanism;
- then to study possible mechanisms
- then to select a mechanism.

8.5 Network-wide encryption

Peter Howard presented S3-99218, *Synchronisation mechanisms for network-wide encryption*, source: Vodafone. The document reports on the ongoing work of Vodafone on end-to-end synchronisation and requests involvement from other 3GPP members. Vodafone confirms that voice is the main application in mind, although the feature should also be applicable to data bearers. The document concludes that, because the structure of the network-wide traffic channel for TFO speech and for some data services is not fully defined, it is difficult to determine whether an appropriate framing structure could be used for network-wide encryption; otherwise synchronisation information might have to be added in the traffic channel. Methods could be to use an explicitly defined end-to-end signalling channel as in TETRA, or to insert synchronisation data into the end-to-end cipher stream (as is the alternative mechanism in

TETRA).

Comments at S3: Requirements on the end-to-end channel should be defined before the structure has been fixed.

S3-99218 was noted by S3#5.

Peter Howard presented S3-99216, *Hooks for network-wide encryption*, source: Vodafone.

Conclusions at S3#5:

- [- The radio interface ciphering algorithm should be re-used. \(TETRA re-uses the access algorithm for end-to-end and has a second algorithm for use by the police.\)](#)
- [- Hooks should be defined in the September S3 meeting.](#)
- [- Information relevant for the co-ordination with other 3GPP groups should be contained in S3-99258 \(S2 then will do the co-ordination\).](#)
- [- The technical information should go into the integration guidelines \(3G TS 33.103\).](#)

8.6 Core NW security

No input had been received.

8.7 Inter-System Handover

S3#5 studied S3-99226 annex C (=S2-99633), a LS from S2 on interoperation between UMTS and GSM answering to an earlier LS from S3 to S2 in S3-99190. The LS expresses S2 agreement that re-authentication at inter-system hand-over is feasible.

This was noted with satisfaction by S3#5. To further the liaison,

- [S3 approved S3-99251, LS to S2, copy to N2 and T3, on Security interoperation between UMTS and GSM.](#)

Main points:

- S3 intend to present a paper on security interoperation at the joint T3/S2/S3 USIM meeting on 24th August and would welcome S2 participation at that meeting⁴.
- S3 also believe that the security interoperation mechanisms being proposed are of interest to N2 and would encourage representation from N2 at the joint meeting.

Stefan Pütz presented S3-99227, *A Modified Handover Mechanism between GSM and UMTS*, source: T-Mobil. It should be further evaluated together with the earlier contributions on the topic.

- ✍ **S3 will try to produce (via e-mail correspondence) a document for the joint USIM meeting on 24th August with a single preferred mechanism.**

8.8 Review of architecture specification

- [An extra-ordinary meeting S3#5bis on 25 August 1999 in Bonn \(hosts: T-Mobil/Detecon\) was agreed with scope restricted to CRs to 33.102.](#)

8.9 Enhanced user identity confidentiality

Peter Howard presented S3-99213, *Enhanced User Identity Confidentiality*, a LS to S2, C2, R2, T3 that had

⁴ It was noted that S2 is meeting that week at ETSI.

been drafted by Stefan Pütz as an action point from S3#4, then agreed in S3 by e-mail and distributed to the addressed groups in July.

Response from N2 to S3-99213: Peter Howard reported that CN2 did not have time to handle this LS at their recent meeting; however, he was able to relay some informal comments from the CN2 chair Ian Park (Vodafone) concerning the potential inability of the HE to route MAP messages to the appropriate HLR if the IMSI/IMUI is encrypted at the SCCP layer.

Response from S2 to S3-99213: S3-99226 annex D (=S2-99634), *Answer to the liaison on Enhanced User Identity Confidentiality*, a Liaison Statement from S2 to S3 and T3 (cc N2): This document

- informs that S2 would like to clarify the format of IMUI;
- asks whether S3 if feels a need to define the format if IMUI differently from⁵ the GSM IMSI
- recommends that if not, S2 recommend using the term IMSI [meant is: instead of IMUI, suggesting the conclusion that in this case, EMUI should better be called EMSI] in all the specifications;
- mentions problems in roaming conditions (if the visited network didn't implement this new enhanced user identity confidentiality; also expressing the impression of S2 that in any case, this would imply some modifications in visited networks, and may not be acceptable for R99.

➤ **As a response to S3-99226 annex D (=S2-99634), S3#5 approved S3-99254, LS to S2 on Response to the LS on Enhanced User Identity Confidentiality (S2-99634/S3-99226d):**

- insisting (with reference to the SA approved 33.102 version 3.1.0, *3G Security: Security Architecture*) that an enhanced transport mechanism between SN and HE has to be standardised, to be mandatory in R99, even if that this functionality is required in each visited SN;
- asking S2 to make sure that the appropriate extension will be added to the relevant documents;
- clarifying that S3 sees no need for the format of the IMUI being different from the GSM IMSI, but nevertheless sees no need of changing the term IMUI to IMSI in all their specifications, reasoning that the same format of two identifiers (e.g. IMUI and IMSI) does not imply necessarily that these are equal.

Further discussion of user identity confidentiality in S3#5: Bart Vinck pointed to the lack of an alternative for cleartext IMSI-paging which compromises user identity confidentiality after all.

S3-99226 annex E (=S2-99635), Answer to S3, T3 (Cc N2) to the LS on Evolution to UMTS and R99 Security Features: See section 12.

9 Integration guidelines

33.103 draft version 1.1.0 in S3-99240 was discussed in S3#5⁶. Comments were taken by the rapporteur.

➤ **Another editing session on 33.103 should be convened.**

10 Guide to 3G security (3G TR 33.900)

 **A draft of the Guide to 3G security (3G TR 33.900) will be distributed by Charles Brookson via e-mail.**

11 Lawful interception

Berthold Wilhelm presented a CR to 33.106 in S3-99219 and a version 0.0.1 of 33.107, *Lawful interception architecture and functions*, in S3-99220. They were noted by S3#5.

⁵ "The constructions *different from*, *different to*, and *different than* are all found in the works of writers of English during the past. Nowadays, however, the most widely acceptable preposition to use after *different* is *from*." (Collins concise dictionary, 3rd edition)

⁶ The document indicates Version 1.0.1, however for non-editorial changes, the middle digit should be increased.

Comments at S3#5:

- The requirement specification (33.106) states that the handover interfaces HI1, 2, 3 are not standardized. It should be considered whether they should then be shown in Figure 1 of 33.107.
- Location services are not mentioned in 33.107.
- It was clarified that "visiting and roaming networks" means visited networks.

Conclusions of S3#5:

- [A new version of 33.107 is expected for the September meeting \(S3#6\), so that the specification can be presented to SA#5 \(starting 11 October in Korea\) for information and approval.](#)
- [An elaborated CR to 33.106 is expected for the September meeting \(S3#6\).](#)

12 Prioritisation and planning of work items

Outstanding technical issues for R99: S3#5 summarised the outstanding technical issues for R99: Contributions are needed in the following areas:

- Key freshness
- Management of sequence number
- Inter system hand-over
- Number of permanent keys in the USIM
- Integrity of user traffic
- What happens if MS discovers that integrity protection is not provided
- Algorithms for authentication (guidelines etc.)
- Update of ciphering section in 33.102 including CR to align with RAN description
- Cipher key selection in RNC
- Start of ciphering
- Hooks for NW wide encryption
- Terminal security (IMEI)
- IMUI paging
- Mobile IP
- VHE security
- <xxx further points from Bart xxx>

 **Bart Vinck announced that he would provide some additional points areas were technical work is necessary.**

Security project co-ordination: S3-99226 annex E (=S2-99635), *Answer to S3, T3 (Cc N2) to the LS on Evolution to UMTS and R99 Security Features*, questions whether enhanced user identity confidentiality should be a R99 feature, whether Core Network Signalling Security can be introduced for R99, and proposes that the phasing issues shall be reviewed in the S2 Security Project Co-ordination ad Hoc Group.

For a response of S3#5 to the question of enhanced user identity confidentiality, see section 8.9 on S3-99254.

For the security project co-ordination:

- [S3-99258, revising S3-99239 was approved to be sent to S2.](#)

 **Peter Howard should provide an electronic copy of S3-99258.**

13 Future meetings

Group	from	to	location, host	Comments
Joint meeting with T3 and S2	990824	990824	Bonn, T-Mobil	
S3#5bis	990825	990825	Bonn, T-Mobil/Detecon	Scope restricted to CRs to 33.102
S3#6	990929	991001	Sophia Antipolis, ETSI	
S3#7	991026	991027	Den Haag	

Preparation of joint meeting with T3/S3/S2: S3 would like to discuss the following agenda items:

- addressing of algorithms and keys
- handover/roaming/interoperation between GSM and UMTS
- Resources for cryptographic algorithms in the USIM
- Enhanced user identity confidentiality
- IMUI / IMSI relationship

14 Any other business

None.

16 Close of meeting

The meeting was closed.

Annex A: List of participants**Chairman**

WALKER Michael VODAFONE Group Plc GB

Vice Chairmen

PÜTZ Stefan Deutsche Telekom MobilNet DE

MARKOVICI Michael (Lucent) US
(succeeding Adam BERENZWEIG)

SECRETARY

BERGMANN Ansgar ETSI MCC (Detecon) DE

BARNES Nigel MOTOROLA Ltd GB

BERENZWEIG Adam Lucent Technologies EMEA B.V. NL

BLANCHARD Colin BT GB

BLOM Rolf ERICSSON L.M. SE

BROOKSON Charles DTI GB

CHIKAZAWA Takeshi Mitsubishi Electric Corp JP

CHRISTOFFERSSON Per TELIA PROMOTOR AB SE

COLLINS Simon PRAESIDIUM SERVICE LTD GB

FENN John B SAMSUNG Electronics GB

FINKELSTEIN Louis Motorola US

HIROIKE Akira NTT DoCoMo JP

HOLMSTRÖM Kasper NOKIA Corporation FI

HORN Guenther SIEMENS AG DE

HOWARD Peter VODAFONE Group Plc GB

IWANE Yasushi Mitsubishi Electric Co. JP

JACZYNSKI Rafal POLKOMTEL S.A. PL

KØIEN Geir TELENOR AS NO

MARKOVICI Michael Lucent Technologies US

MILES David F BT Cellnet GB

NGUYEN NGOC Sebastien France Telecom FR

NIEMI Valtteri Nokia Research Center FI

NYBERG Petri	SONERA Limited	FI
RANTALAINEN Timo	NOKIA Corporation	FI
ROELOFSEN Gert	KPN	NL
SCHUERMANN Rosita	MANNESMANN Mobilfunk GmbH	DE
SCHULZE Hans-Joachim	MANNESMANN Mobilfunk GmbH	DE
SEMPLE James	ICO Services Ltd	GB
TIETZ Benno	MANNESMANN Mobilfunk GmbH	DE
TRAUTMANN Peter	Reg TP	DE
VINCK Bart	SIEMENS ATEA NV	BE

Annex B: List of documents

S3-99205	CR to TS 25.301 - Integrity control mechanism	Nokia	8.1
S3-99206	Response to "CR to TS 25.301 - Integrity control mechanism"	Vodafone	8.1
S3-99207	Liaison statement answer on IST for non-CAMEL subscribers	S3, SMG10	for info
S3-99208	LS to S2 on Time constraints on the execution of cryptographic algorithms	S3	for info
S3-99209	Approved meeting report of TSG SA WG3 #4 meeting		
S3-99210	LS from R3 on Ciphering mechanisms in case of multiple RABs (R3-99790)	R3	8.2
S3-99211	LIAISON STATEMENT from T2 / SMG4 to WAP WTA DC, CC: WAP WSG, Specification Committee, S3, SMG10 on Support of WAP public library functions in MEXE Release 98	T2, SMG4	for info
S3-99212	Liaison statement (LS) from 3GPP TSG-T3 to 3GPP TSG-S3 on Multiple authentication algorithms and keys	T3	8.3
S3-99213	LS from S3 to TSG S2, TSG C2, TSG R2, TSG T3 on Enhanced User Identity Confidentiality	S3	8.9
S3-99214	Change Request to GSM 02.09, GSM 02.16, GSM 03.03 and GSM 11.10 to ensure IMEI security (AP99-079, P99-438)	GSMA TWG, GSMA SG	8.4
S3-99215	Draft agenda for S3#05 and SMG10#2-99, 990803-990806	Chairman	
S3-99216	Hooks for network-wide encryption	Vodafone	8.5
S3-99217	Location of integrity termination in the network	Vodafone	8.1
S3-99218	Synchronisation mechanisms for network-wide encryption	Vodafone	8.5
S3-99219	CR to 33.106	RegTP	11
S3-99220	3G TS 33.107 Lawful Interception Architecture and Functions, V0.0.1	RegTP	11
S3-99221	Liaison Statement to S3 on Baseline Capabilities - Request and Confirmation of Terminal Baseline Implementation Capabilities in the security domain (T2-99585)	T2	6.2
S3-99222	Liaison Statement to S3 on Service Capabilities - Request of Terminal Service Implementation Capabilities in the security domain (T2-99586)	T2	6.2
S3-99223	Design of standard 3GPP Encryption and Integrity Algorithms (SAGE (99) 37)	Chairman ETSI SAGE	7
S3-99224	CR to 33.102 on Cipher keys on control and user planes	Vodafone	8.2
S3-99225	Status of LCS specifications	Tim Wright, Vodafone	6.4
S3-99226	LSs from S2	S2	6.1
S3-99227	A Modified Handover Mechanism between GSM and UMTS	T-Mobil	8.7
S3-	LS to SA3 on Ciphering Algorithm Requirements	R2	6.2

99228			
S3-99229	Liaison statement on chosen Logical and Transport Channel on the Radio Interface for Cell Broadcast Service in UMTS	R2	- ⁷
S3-99230	A Possible Problem of the UMTS AKA Mechanism	T-Mobil	8.3
S3-99231	Liaison Statement on the Super-Charger Concept	N2	6.2
S3-99232	Liaison statement response on IST for non-CAMEL subscribers (=AP99-087)	N2	6.2
S3-99233	Further clarifications of the MAC based ciphering solution	Nokia	8.1
S3-99234	Enhanced window mechanism	Siemens	8.3
S3-99235	Proposed response to 231	Siemens	6.2
S3-99236	Response to doc 99230 "A Possible Problem of the UMTS AKA Mechanism" from T-Mobil/Deutsche Telekom, source:	Siemens AG / Siemens Atea NV	8.3
S3-99237	Proposed cipher algorithm	Lucent	7
S3-99238	SA 284 – status of deliverables, priorities of work items	S3	12
S3-99239	S3 Workplan as presented to S2 (S2-99514)	Vodafone	12
S3-99240	Integration guidelines (33.103)	Rapporteur	9
S3-99241	not used		
S3-99242	S3 Report to SA#4	Chairman	6.1.1
S3-99243	SP-99238, LS from S1 to SA and SMG on Work transfer from SMG1 to 3GPP	S1	for info
S3-99244	SP-99334, Workplan for R00	R00 drafting group	for info
S3-99245	Description of LCS message flow		Annex D
S3-99246	CR to 33.102 on Cipher key setting	PH	8.2
S3-99247	LS to R3 on Ciphering in the case of multiple RABs	S3	8.2
S3-99248	CR to 33.105 on <i>Cipher keystream block length</i>	PH	6.2.3
S3-249	proposed LS to T3, C1, C2, R3 - Response to LS from TSG T3 (S3-99212) on Multiple Authentication Algorithms and Keys (rev. in S3-99259)		8.3
S3-99250	Slides from Wael Adi on terminal security	WA	8.4
S3-99251	LS to S2, copy to T3, N2 on Security interoperation between UMTS and GSM	S3	8.7
S3-99252	LS to T2 on Baseline Implementation Capabilities in the security domain	S3	6.2.1

⁷ This LS doesn't address S3.

S3-99253	-- reserved for PH --	PH	
S3-99254	Response to the LS on Enhanced User Identity Confidentiality (S2-99634/S3-99226d)	S3	8.9
S3-99255	Response to LS statement N2-99918 (=S3-99231) from N2 to S3 on Super-Charger concept	S3	6.2.2
S3-99256	CR to 33.102 on Enhanced window mechanism for sequence number management in authentication scheme (rev. of S3-99234)	S3	6.2.2
S3-99257	[reserved for approved S3#5 report]		
S3-99258	S3 Workplan (rev of S3-99239)	S3	8.5
S3-99259	LS to T3, N1, N2, R3 on Response to LS from TSG T3 (S3-99212) on Multiple Authentication Algorithms and Keys (rev. of 249)		8.3
S3-99260	Technical report on Super-Charger (attachment to S3-99231)		6.2.2

Annex C Summary of actions, decisions and outgoing liaisons

C1 Action points

- ✎ On list of messages to be integrity protected: This is going on.
- ✎ Response for Annex C of 33.105 from other groups has not been received, except for S2.
- ✎ Check of X24: to be done.
- ✎ CR to correct figure in 33.103: tbd
- ✎ AP to specify what should happen if the MS discovers that integrity is not provided: tbd
- ✎ AP all: To examine consequences of the CR in S3-99180 (modified synchronisation procedure) on the option of a global counter in 33.102: tbd
- ✎ Concerning S3-99238, the work plan of specifications with intermediate steps, it was agreed that Ansgar Bergmann should maintain an updated version on the server. Also e should create a directory in the S3 domain where the latest versions of specifications can be found that are not yet under change control.
- ✎ It was agreed that Peter Howard should distribute after the meeting S3-99248, CR to 33.105 on *Cipher keystream block length*, adding the relevant information, for discussion and if possible agreement by e-mail.
- ✎ AP To take up the protection to user data against modification on the radio interface in the next meeting.
- ✎ Later in the meeting it was decided that Peter Howard should distribute S3-99246, CR to 33.102 on *Cipher key setting*, with the aim to reduce the options for the handling of cipher keys generated in different domains, for e-mail discussion and, if possible, agreement in S3.
- ✎ Wael Adi to provide the slides (S3-99250)
- ✎ S3 will try to produce (via e-mail correspondence) a document for the joint USIM meeting on 24th August with a single preferred mechanism.
- ✎ A draft of the Guide to 3G security (3G TR 33.900) will be distributed by Charles Brookson via e-mail.
- ✎ Bart Vinck announced that he would provide some additional points areas where technical work is necessary.
- ✎ Peter Howard should provide an electronic copy of S3-99258.

C2 Decisions

- The agenda was approved
- The S3#4 meeting report in S3-99209 was approved.
- As a liaison representative to S2, S3#5 nominated Peter Howard.
- As an answer to S3-99221, S3#5 approved S3-99252, LS to T2 on Baseline Implementation Capabilities in the security domain (this LS contains TS33.103 as an attachment).
- A revision of S3-99235 in S3-99255, Response to LS statement N2-99918 (=S3-99231) from N2 to S3

on Super-Charger concept was approved by S3#5.

- A CR to 33.102 on Enhanced window mechanism for sequence number management in authentication scheme (rev. of S3-99234) in S3-99256 was approved by S3#5.
- S3#5 decided to include the information from S3-99228 into the algorithm requirements document (3G 33.105).
- Decision of S3 and SMG10 on work split between SMG10 and S3 on LCS: GSM LCS phase 2 will be dealt with in SMG10. For LCS phase 3, the split will be decided in due time.
- S3#5 decided to adopt the working assumption that integrity protection terminates in the RNC.
- S3#5 decided to adopt the working assumption to locate f9 in the UE.
- S3-99247, LS to R3 on Cipherring in the case of multiple RABs, was approved by S3#5.
- As a response, S3#5 approved a LS to T3, C1, C2, R3 in S3-99259 (revision of S3-99249), Response to LS from TSG T3 (S3-99212) on Multiple Authentication Algorithms and Keys.
- - The radio interface cipherring algorithm should be re-used. (TETRA re-uses the access algorithm for end-to-end and has a second algorithm for use by the police.)
- - Hooks should be defined in the September S3 meeting.
- - Information relevant for the co-ordination with other 3GPP groups should be contained in S3-99258 (S2 then will do the co-ordination).
- - The technical information should go into the integration guidelines (3G TS 33.103).
- S3 approved S3-99251, LS to S2, copy to N2 and T3, on Security interoperation between UMTS and GSM.
- An extra-ordinary meeting S3#5bis on 25 August 1999 in Bonn (hosts: T-Mobil/Detecon) was agreed with scope restricted to CRs to 33.102.
- As a response, S3#5 approved S3-99254, LS to S2 on Response to the LS on Enhanced User Identity Confidentiality (S2-99634/S3-99226d):
- Another editing session on 33.103 should be convened.
- A new version of 33.107 is expected for the September meeting (S3#6), so that the specification can be presented to SA#5 (starting 11 October in Korea) for information and approval.
- An elaborated CR to 33.106 is expected for the September meeting (S3#6).
- S3-99258, revising S3-99239 was approved to be sent to S2.

C3 Outgoing liaison statements

Doc. Ref.	Title	Sent to:	Copy to	Status: Sent / Dates
S3-99247		R3		990822
S3-99251		S2	N2, T3	990818
S3-99252		T2		990822
S3-99254		S2		990822
S3-99255		N2		990822

S3-99258		S2		
S3-99259		T3, C1, C2, R3		

Annex D: Meeting report of SMG10 #2/99

[separate file]