Report to 3GPP SA3 on 3GPP SA#8

This is a very brief report of the results of the presentation on the work of SA3 that I gave to the SA#8 meeting in Duesseldorf 26-28 June 2000.

For reference, my presentation (in power-point) is attached.

1. With the exception of CR0095 to 33.102 on emergency call handling (see 2 below), all CRs were approved. We are however asked to double check CR0088 to 33.102 to ensure correct use of USIM and ME.
2. The CR0095 to 33.102 on emergency call handling caused quite a lot of discussion with respect to how emergency calls are to be handled when the USIM is in place. It seems that some are unhappy that integrity check failure in the mobile would cause the call to be dropped. I am not unhappy about this – if you cannot trust the network, why should you progress the emergency call? I must say I also have reservations about allowing USIM absent emergency calls – but this wasn't discussed. The upshot is that I need to resolve the emergency call requirements off-line, and once that is clear we can prepare a CR.
3. All of our proposed work items for R00 were approved, subject to each having at least four sponsors. A work item without 4 sponsors, and by implication without adequate active support to do the work, will have to be abandoned. **So can each of you please let me and the author of the WI know as soon as possible, and by the latest at our meeting in August, whether you support it** – I don't really want four Vodafone companies as the sole supporters of a WI. **Can authors of the WIs please tidy them up** – there were a number of silly complaints about minor points, but we need to make sure the final work item sheets are free from error. **Can you also please review completion dates** – Dec 2001 would seem to be appropriate for most of our work.
4. The R00 WI descriptions, as presented to SA#8 are attached for reference. Would authors please note the points 5 – 8 below
5. SP-0000296 Access security for IP multimedia services – we need to take a look at possible separation of components in the multimedia terminal (see document SP-000313 which is attached).
6. SP-000308 GERAN security – the GERAN security work won't start until it is confirmed that 3GPP is responsible for GERAN; also note changes in revised version.
7. SP-000309 Lawful interception architecture – please check end date, surely this must be 2001?
8. Adrian Scrase told me that the subject of publication of the 3GPP cipher will be resolved at the partnership meeting in Beijing in two weeks time. I expressed our strong desire to see the documents. I made it clear to the whole of SA that we expected to see publication soon – on the ETSI server or elsewhere.
9. Good news on the authentication algorithm – 3GPP will fund it. I will check whether SAGE is aware of this, and whether they can deliver at the end of September – an easy task for such a fine group of cryptographers!
10. On the GEA2 front, it will be mandatory for R99 in both mobile and network.. For release 97/98, it will be optional to provide it in the mobile for use with R99 networks – this should ensure that when R99 networks become available many of the R97/98 mobiles will be able to work to them using GEA2.

11. There is a proposal to split terminal functionality so that, for example, call control could be in a PC attached to the terminal. This caused a lot of concern and debate. We are asked to look at the security implications. See document SP-000351 which is attached.

See you all in August
Regards

Michael Walker
27th June 2000

SP-000267

3GPP TSG-SA WG3 (Security)

Status report to SA#8

26-28 June, 2000

Düsseldorf, Germany

Michael Walker

Chairman 3GPP TSG-SA WG3

Content of presentation

- Document list
- Report and review of progress in S3 (AI 6.3.1)
- Questions for advice from S3 (AI 6.3.2)
- Approval of contributions from S3 (AI 6.3.3)

Document list

- S3 meeting reports - *for information*
  - SP-000268 : Report of SA WG3 meeting #11
  - SP-000269 : Report of SA WG3 meeting #12
  - SP-000270 : Report of SA WG3 meeting #13
- CRs to TS 33.102, TS 33.103, TS 33.105 and TS 22.022- *for approval*

  SP-000271, SP- 000272, SP-000273, SP-000274
- R00+ security work items - *for information/approval*

Report and review of progress in S3 (AI 6.3.1)

- Meetings
- Confidentiality/integrity algorithms
- Authentication algorithm
- Harmonisation of 3GPP/3GPP2 authentication
- Open R99 security issues
- S3 technical specifications and reports
- Integration of security features into R99 specifications
- R00+ security work programme

S3 meeting reports

- S3#11, 22-24 January 2000, Mainz (before SA#7)
  - S3-approved report available in SP-000268 - *for information*
- S3#12, 11-14 April 2000, Stockholm
  (including joint meeting with TR-45 AHAG)
  - S3-approved report available in SP-000269 - *for information*
- S3#13, 23-26 May 2000, Yokohama
  - Draft report available in SP-000270 - *for information*
- Joint S3/CN meeting, 13-14 June 2000, Sophia

Meetings scheduled after SA#8

- S3#14, 01-04 Aug 2000, Oslo
- S3#15, 12-15 Sep 2000, Arlington, Virginia (tbc)
  (including joint meeting with TR-45 AHAG)
- S3#16, 27-30 Nov 2000, Israel (tbc)

Confidentiality & authentication algorithms

- SA#7 approved report on the work performed by SAGE task force on cipher
  - Published as 3G TR 33.908
- And approved algorithms for distribution to 3GPP partners
  - Publication of algorithm specifications and report on evaluation results was delayed for procedural reasons
- SA#7 approved the development of standard authentication algorithm and SAGE work plan tabled at SA#7
  - Funding approved by 3GPP in June 00
  - Target algorithm publication by end of Sep 00

Harmonisation of 3GPP/3GPP2 authentication

- First joint meeting with AHAG during S3#12 (Apr 00)
- Further joint meeting planned during S3#15 (Sep 00)
- S3 to propose that certain clauses in 3GPP specifications are considered for joint control as they contain the stage 2 description of the 3GPP AKA
  - LS to AHAG to be agreed at S3#14 in August
- Other issues / AHAG requirements on 3GPP AKA
  - Home control of AKA - the need for R00+ work items on this is being considered by S3
  - Support for global challenge at initial registration - AHAG are considering several proposals with varying impact on 3GPP AKA and intersystem operation

Open R99 security issues (1)

- Core network security (MAP application layer security)
  - Moved to early version of R00 at SA#7
  - CRs presented for approval to CN#8 to complete work
- Core network security (GTP, MAP-over IP, new interfaces/applications in R00, key management)
  - Two R00+ work items created - key management; everything else
- Enhanced user identity confidentiality
  - Moved to R00 at SA#7
  - No R00+ work items created - no support in S3
- Authentication failure reporting to HE
  - CRs presented for approval to CN#8 to complete R99 work
- Emergency calls handling
  - CR rejected at SA#7
  - New CR tabled at SA#8 (CR95 to 33.102 considered under AI 6.3.3)

Open R99 security issues (2)

- MS behaviour on network authentication token reject
  - CRs presented for approval to CN#8 to complete R99 work (issue resolved in N1)
- R00+ work items created for
  - Network-wide encryption
  - Rejection of unenciphered connections
  - UE triggered re-authentication during connections
  - 3G location services security
  - OSA security
- Further corrective CRs expected as security features continue to be integrated into other specifications; changes possible to
  - handover, sequence number management

S3 technical specifications and reports (1)

- TS 33.120: Security principles and objectives
  - approved at SA#3 - stable
- TS 21.133: Security threats and requirements
  - approved at SA#3; 1 CR at SA#6 - stable
- TS 33.102: Security architecture
  - approved at SA#3;
    - 11 CRs approved at SA#4,
    - 10 CRs approved at SA#5;
    - 15 CRs approved at SA#6;
    - 28 CRs approved at SA#7
  - **17 CRs presented for approval at SA#8**

S3 technical specifications and reports (2)

- TS 33.103: Integration guidelines
  - approved at SA#5; 3 CRs at SA#6; 1 CR at SA#7
  - **3 CRs at SA#8** - Alignment with TS 33.102
- TS 33.105: Cryptographic algorithm requirements
  - approved at SA#4; 3 CRs approved at SA#5; 2 CRs approved at SA#6; 4 CRs at SA#7
  - **1 CR at SA#8** - Alignment with TS 33.102
- TS 33.106: Lawful interception requirements
  - approved at TSG-SA#4; 1 CR approved at SA#6 - stable
- TS 33.107: Lawful interception architecture and functions
  - approved at SA#6 - stable

S3 technical specifications and reports (3)

- TR 33.900: Guide to 3G security
  - approval at SA#7 planned; postponed until SA#8
  - **Postponed until SA#9 - content immature**
- TR 33.901: Criteria for cryptographic algorithm design
  - approved at SA#4 - stable
- TR 33.902: Formal analysis of security mechanisms
  - Approved at SA#5; 1 CR approved at SA#6 - stable
- TS 22.022: ME personalisation
  - Under S3 control since SA#6
  - **1 CR at SA#8** - Update to make specification applicable to 3GPP as well as GSM

S3 technical specifications and reports (4)

- TR 33.908: Report on confidentiality/integrity algorithm development
  - Approved at SA#7 - stable
- Publication of confidentiality/integrity algorithm specifications and evaluation has been delayed
  - TS 35.201: f6, f7 security algorithm specifications
  - TS 35.202: Kasumi algorithm specifications
  - TS 35.203: Implementation test data
  - TS 35.204: Design conformance test data
  - TR xx.xxx: Algorithm evaluation results

Integration of security into R99 specifications

- Need to ensure that S3 security features are properly integrated into the R99 specifications
- S3 is reviewing relevant specifications on
  - authentication and key agreement
  - confidentiality and integrity protection
  - secure 2G-3G inter-working - most CRs are expected to be in this area
  - others areas may follow
- S3 is identifying where corrective CRs are required with assistance of other WGs

R00+ security work programme

- Structured programme for R00+ security work items being created in conjunction with Security IGC in S2
  - 15 WI descriptions tabled at SA#8 (to be considered under AI 6.3.3)
  - further WI descriptions to be drafted at S3#14 on VHE, location
  - See latest R00+ project plan from S2
- Dependencies between WGs identified and timescales being agreed (e.g. joint meeting with CN, 13-14 June 2000)
- Security work item project phases
  - Requirements capture by S3
  - Security feature specification by S3
  - Feasibility study by S3 other WGs (optional)
  - Definition of security architecture by S3
  - Integration of security architecture by other WGs (optional)

Questions for advice from S3 (AI 6.3.2)

- No items

Approval of contributions from S3 (AI 5.3.3)

- CRs to TS 33.102 Security Architecture - 17
- CRs to TS 33.103 Integration Guidelines - 3
- CRs to TS 33.105 Cryptographic Algorithms Requirements Specification - 1
- CRs to TS 22.022 ME Personalisation - 1
- R00+ work item descriptions -15

CRs to TS 33.102 - *for approval (1)*

- SP-000271: CRs to TS 33.102 (Security Architecture)
  - CR097R1: Clarification on the meaning of the asterisk in Figure 18
  - CR103R2: Clarification of terminology in user domain
    - Replace UE with ME throughout
    - Clarification (see section 6.8.1.5) that USIM shall support 3GPP AKA and may support backwards compatibility with GSM by supporting GSM cipher key derivation function plus SIM-ME interface (GSM 11.11)

CRs to TS 33.102 - *for approval (2)*

- SP-000272: CRs to TS 33.102 (Security architecture)
  - CR080: Clarification on intersystem handover
    - hyperframe number handling
    - starting integrity protection
    - changing ciphering algorithm
    - 'handover to UTRAN complete' message not integrity protected
  - CR083: Clarification on authentication
    - changes due to incorrect implementation of CR037R1
    - MAC-S needs padding with zeros before input to f5 function
    - USIM does not store RAND for re-synchronisation
  - CR084: Changes to conversion functions for intersystem operation

CRs to TS 33.102 - *for approval (3)*

- SP-000272: CRs to TS 33.102 (Security Architecture)
  - CR088R2: The length of initial hyperframe number (START) is defined as 20 bits and the management of START values for CS /PS domains described in detail.
  - CR090: Values for the DIRECTION bit are defined for the confidentiality and integrity algorithms. The BEARER parameter is defined as the radio bearer since the logical channel identifier is not unique for one UE.
  - CR093: Removal of MAP application layer protection following decision at SA#7.
  - CR094: The requirement that the MSC/VLR or SGSN to update CK and IK at least every 24 hours removed.

CRs to TS 33.102 - *for approval (4)*

- SP-000272: CRs to TS 33.102 (Security Architecture)
  - CR095: Specifications on how emergency calls are handled are added.
  - CR096: Clarification that there is one initial hyperframe number per CN domain (CS and PS). Clarification that a new CK and IK resets the hyperframe number.
  - CR098: Replaces one instance of COUNT with COUNT-C.
  - CR100: Clarification of hyperframe number management by by using the START parameters in the description.

CRs to TS 33.102 - *for approval (5)*

- SP-000273: CRs to TS 33.102 (Security Architecture)
  - CR092: Removal of enhanced user identity confidentiality following decision at SA#7.
  - CR102: Removal of network-wide encryption specifications.
- SP-000274: CRs to TS 33.102 (Security Architecture)
  - CR089: A further sequence number generation scheme is defined which allows for a more static AuC database
  - CR091: The radio bearer identity is appended to the front of the message to be integrity protected.

CRs to TS 33.103 - *for approval*

- SP-000271: CRs to TS 33.103 v3.2.0 (Integration guidelines)
  - CR009: The sequence number length is defined as 48 bits.
- SP-000273: CRs to TS 33.103 v3.2.0 (Integration guidelines)
  - CR007: Removal of enhanced user identity confidentiality following decision at SA#7.
  - CR008: Removal of MAP application layer protection following decision at SA#7.

CRs to TS 33.105 - *for approval*

- SP-000271: CR to TS 33.105 v3.3.0 (Algorithm requirements)
  - CR011: Values for the DIRECTION bit are defined for the confidentiality and integrity algorithms. The BEARER parameter is defined as the radio bearer since the logical channel identifier is not unique for one UE.

CRs to TS 22.022 - *for approval*

- SP-000271: CR to TS 22.022 v3.1.0 (ME personalisation)
  - CR002: Update to make specification applicable to 3GPP

R00+ work item descriptions - *for information/approval (1)*

- R00+ security work item descriptions
  - SP-000296: Access security for IP multimedia services
  - SP-000297: Network based end-to-end security
  - SP-000298: User plane security
  - SP-000299: MAP application layer protection
  - SP-000300: Core network security
  - SP-000301: Key management for core network security
  - SP-000302: OSA security
  - SP-000303: MExE security
  - SP-000304: FIGs
  - SP-000305: Visibility and configurability of security

R00+ work item descriptions - *for information/approval (2)*

- R00+ security work item descriptions
  - SP-000306: Evolution of CS algorithms (A5/3 development and deployment)
  - SP-000307: Evolution of PS algorithms (GEA2 deployment)
  - SP-000308: GERAN security
  - SP-000309: Lawful interception architecture
  - SP-000310: General security enhancements

3GPP TSG-SA Meeting #8
Düsseldorf, Germany, 26 - 28 June, 2000

Tdoc SP-000313

3GPP TSG-T (Terminals) Meeting #8
Düsseldorf, Germany, 21 - 23 June, 2000

Tdoc TP-000115

LIAISON STATEMENT

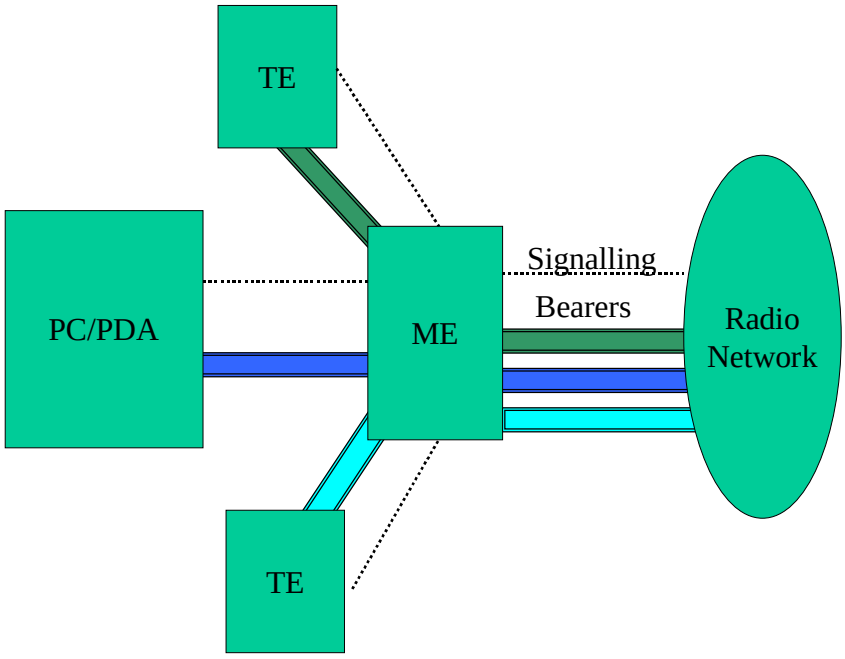
To: TSG-SA

Source: TSG-T

Title: Requirements and Scenarios for Call Handling

In the All-IP network, the UE will be required to set up multiple connections with different QoS requirements for different data streams (e.g. signalling, traffic bearers etc.). The issues described in this paper apply to scenarios outside of "All-IP", however it is the "All-IP" network which has caused some discussion in TSG-T.

TSG-T is concerned that the overall framework development has not so far included analysis of the potential for split of functions between the different components of the UE.



The above diagram illustrates an ME connected to a radio network with different TE devices requiring different bearer and signalling capabilities from the ME.

Some questions in this area, which illustrate the problem space are:

1. Is it permitted to use the ME simply as a bitpipe and have an external TE (e.g. PC software) be in control of set up, clear down and manipulation of speech and multimedia calls?

2. What are the user requirements where the UE functions are divided between ME and TE, and which scenarios are required to be supported?

3. How do we maintain security of the network and guarantee proper functionality, if we transfer all the call control functionality out of the ME and into a device whose software can easily be manipulated? How do we avoid denial of service attacks or other security attacks eg. by computing devices (possibly controlled by viruses) instructing the ME to make repeated call attempts into the radio network?

4. What happens to the certification and compliance schemes for the ME if the call control in the ME can be completely bypassed?

In order for TSG-T to understand the problem space with respect to the terminal, and understand the requirements for work items (if any) in this area it is necessary for the required service scenarios and framework to be established by TSG-SA.

It is understood that S4 is already investigating the split of multimedia calling in Release 99 to include a model where all call control is handled by an external TE (e.g. PC) so this could be also relevant to Release 99 scenarios where we have Circuit Switched Multimedia calls.

SA is invited to discuss and consider a work plan to further develop the scenarios which we want to support. In addition to the service scenarios mentioned above it is believed that amongst others this will require discussions on architecture and security aspects in the relevant working groups.

Technical Specification Group Services and System Aspects **TSGS#8(00)351**

Meeting #8, Düsseldorf, Germany, 26-28 June 2000

Source: **Ad hoc UE Split Group**

Title: **Draft Liaison Statement**

Document for: **Approval**

Agenda Item: **Postponed Items**

LIAISON STATEMENT

From: **TSG-SA**

To: **GSM Association, S1, S2, S3, S4,**
EICTA CelCom, GSM Certification Forum

Cc: **TSG-T, T2**

TSG-SA has discussed the attached paper (SP-000313) which highlights some issues and concerns associated with providing call control applications in one or more attached external devices routing calls through an ME.

The opinion of TSG-SA is that this area has not been fully studied to date and it is important to understand which scenarios should be examined in further detail. TSG-SA will revisit this subject once further information is available from the groups addressed above.

The attached document discusses several scenarios, some of which are raised by more immediate technical concerns and some of which are issues of principle.

Of immediate concern is the UE requirement to support multiple data streams. TSG-SA sees a need to establish clear requirement scenarios and would appreciate feedback on this issue, e.g. the support of multiple PDP contexts.

On the issues of principle, TSG-SA#8 recognises the Industry developments in this direction and is prepared to discuss this at future meetings. However, TSG-SA#8 is not ready to accept the proposal to provide call control applications in one or more attached external devices and routing calls through an ME; feedback on the full implications of this proposal is welcomed from the addressed groups. TSG-SA has serious concerns including the following specific issues:

- Validity of the mutual authentication between the user and the network
- Termination point for the ciphering and integrity checking
- IMEI location and security
- Validity and scope of conformance testing
- PC virus attacks
- Malicious tampering with software located in the PC
- Misuse of open connections by third parties
- Fraud (e.g. theft of service)

All of the above items imply that there is a set of functionality that should not be split.

We therefore invite the GSM Association and EICTA CelCom to consider this matter and identify what the market requirements would be for providing Mobile Multimedia and other services using devices outside of the UMTS radio handset.

Product testing and certification including IMEI security are believed to be potential problem areas, hence the GSM Certification Forum is also invited to consider the implications.

S1 is asked to study the requirements for supported scenarios.

S2 is asked to identify any architectural impacts

S3 is asked to identify security issues

S4 is asked to comment on the scenarios currently considered/included in Release 99 and provide also a view for Release 2000.

In order to help develop this work in harmony, it would be useful to copy any responses to all those on the To: and Cc: lists above.

Work Item Description

Evolution of GSM CS algorithms

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

Visibility and configurability
The user/USIM may need to be able to be request that the terminal indicates which algorithm is used. Furthermore, the user/USIM may need to be able to be request that the terminal rejects communications depending on which algorithm is used.

3 Justification

The first GSM CS algorithm has been in service for almost 10 years. It may be worthwhile examining how a new algorithm could be developed and rolled out into the network infrastructure and the mobile stations.

4 Objective

The main objectives of this work item will be to evaluate options for replacing the first GSM CS algorithm, to select an appropriate solution, to produce the necessary CRs and to ensure that a new algorithm is developed and made available for use.

5 Service Aspects

None identified.

6 MMI-Aspects

There may be an impact on the ciphering indicator (see linked work items).

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X	X	X	
No					X
Don't know	X				

10 Expected Output and Time scale (to be updated at each plenary)

A new milestone has been added and some dates have been changed (in italics) to supersede the milestones agreed at the joint CN/S3 meeting. Further revisions may be necessary so that the standards are available sooner.

Meeting	Date	Activity
	June/July	*Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles*
S3#15	September 2000	Requirements capture
S3#16	November 2000	Security feature specification: First draft
	January 2001	Feasibility study including definition of work tasks and completion of the plan for this work item
	March 2001	Definition of security architecture; first draft
	May 2001	Definition of security architecture; CRs approved
	February 2001	*Integration of security architecture: Concept presented to S2 and CN*
	March 2001	*Integration of security architecture: First draft CRs*
	April 2001	*Integration of security architecture: Complete CRs*
	May 2001	*Integration of security architecture: CRs approved at TSG level*
	June 2001	*Review of complete CRs by S3*

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Support for new GSM CS security mechanisms in R00 version of 33.102
33.103				Support for new GSM CS security mechanisms in R00 version of 33.103
33.105				Support for new GSM CS security mechanisms in R'00 version of 33.105

11 Work item raporteurs

12 Work item leadership
TSG SA WG3

13 Supporting Companies
Please mail cbrookson@iee.org if your company is willing to support this work item.

14 Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a h This is a **“Feature”.**

Work Item Description

Evolution of GSM PS algorithms

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

Visibility and configurability
The user/USIM may need to be able to be request that the terminal indicates which algorithm is used. Furthermore, the user/USIM may need to be able to be request that the terminal rejects communications depending on which algorithm is used.

GERAN security
The recent decision to deploy an Iu-ps interface into the R00 GSN BSC will involve moving PS encryption termination into the GSM BSS. New PS encryption mechanisms and algorithms will therefore need to be developed.

3 Justification

Since the first GSM PS algorithm was developed, export restrictions have been relaxed and the stronger GEA2 can now be deployed. This work item will examine how GEA2 could be rolled out into the network infrastructure and the mobile stations. It will also investigate the development and deployment of new algorithms for the PS domain (see linked work items).

4 Objective

A first objective of this work item is to produce the necessary CRs and to ensure that GEA2 can be deployed.

A second objective will be to investigate the development and deployment of new algorithms for the PS domain (see linked work items).

5 Service Aspects

None identified.

6 MMI-Aspects

There may be an impact on the ciphering indicator (see linked work items).

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X	X	X	

No					X
Don't know	X				

10 Expected Output and Time scale (to be updated at each plenary)

New milestones have been added (in italics) and some have been removed to supersede the milestones agreed at the joint CN/S3 meeting.

Meeting	**Date**	**Activity**
S3#13	23-26 May 2000	Requirements capture, and identification of all work tasks
	June/July	*Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles*
CN/S3 joint	*13-14 June 2000*	*Decision to create CRs making GEAx support optional also for R97 to preserve commonality between R97 and R98 and to allow for early roll-out of GEA2 in R97 terminals. Companies to check that no backwards compatibility issues exist.*
CN#8	*21-23 June 2000*	*Final decision on whether GEAx support is optional also for R97.*
SMG#32/SA#8	*June 2000*	*Definition of security architecture: CRs approved at TSG level*
	August 2000	Integration of security architecture: Concept presented to S2 and CN
	September 2000	Integration of security architecture: Complete CRs
	October 2001	Integration of security architecture: CRs approved at TSG level

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Support for new GSM PS security mechanisms in R00 version of 33.102
33.103				Support for new GSM PS security mechanisms in R00 version of 33.103
33.105				Support for new GSM PS security mechanisms in R'00 version of 33.105

11 Work item raporteurs

12 Work item leadership

TSG SA WG3

13 **Supporting Companies**

Please mail cbrookson@iee.org if your company is willing to support this work item.

14 **Classification of the WI (if known)**

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a This is a **"Feature".**

Work Item Description

Title: MExE security

1 3GPP Work Area

	Radio Access
	Core Network
X	Services

2 Linked work items

Authentication between mobile and "Gatekeeper" Integrity protection for Mobile to "Gatekeeper" signalling Virtual Home Environment / Open Systems Architecture Security SIM Application Toolkit Security.

3 Justification

MExE is based on the concept of identifying external standards suitable for supporting services from User Equipment (UE), and bringing them into the 3GPP scope by direct reference (i.e. WAP). Recent developments in the support of a new small-footprint Java platform, and co-operation with the SDR Forum requires extension of the existing MExE specifications to update and incorporate these latest developments. Further detailed work is also required to define the support of the user profile and other areas.
From the network operator's perspective, it is essential that such developments incorporate security features to preserve the integrity of the network and protect the confidentiality and integrity of third party and end user data and applications.

4 Objective

To conduct a threat analysis for MExE and review the security features documented in 3G TS 23.057 for effectiveness in countering those threats and to agree any necessary CR's with T2, to S3 (Services and Systems Aspects - Security) and T2 (Terminals - MExE) specifications.

MExE Release 2000 targets the following areas:-

- Provision of secure download mechanism and capabilities to support Software Defined Radio (SDR) concepts
- Improved security
- Investigation of Terminal Commands (e.g. AT command support)
- Support of terminal parts of the VHE / User Profile
- Third MExE classmark
- Investigate SIM Application Toolkit / OSA / CAMEL interaction to provided advanced services

5 Service Aspects

MExE supports services via MExE executables in the UE. However, Mobile Station applications based, e.g. on MExE and/or involving e-commerce will probably not be able to be fully contained within the (U)SIM. Mechanisms probably need to be standardised to ensure that these kinds of applications can be deployed, operated, upgraded and deleted in a secure manner.

6 MMI-Aspects

MExE supports MMI enhancements via applications and browsers in line with the principles of VHE

7 Charging Aspects

MExE enables MExE executables to potentially support charging for services. MExE will liase with TSG-S5 for charging-related issues.

8 Security Aspects

This is a Security Item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes	X	X			
No			X		
Don't know				X	

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
MExE	27th-29th June, Tokyo, Japan	Agreement of this WID
S3#14	August 1-4, 2000	Presentation to S3 of Release 2000 MExE
	Aug/Sept 2000	Email discussion group on threats and countermeasures
MExE	28th August-1st September, Galway, Ireland	
S3#15	September 2000	Presentation to S3 of threat and countermeasure analysis
MExE	26th-28th September, Finland	
S3#16	November, 2000	Agree implementation of any new security features for MExE Release 2000 Approval of any CR's to S3 and T2 specifications required.
MExE	27th Nobember-1st December, Tokyo, Japan	
	December 2000	Email Discussion on Final CR's
	2001	Final CR's approved at TSG level April 2001

-
-

-

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Possible expanded scope and place of use for existing security features
23.057				Possible CR,s depending on result of threat analysis

11 Work item raporteurs

Colin Blanchard
Network Security Design
MLB1 PP8
BT Advanced Communications Technology Centre
Adastral Park
Ipswich
IP5 5RE
Phone +44 1473 605353
Fax +44 1473 623910
colin.blanchard@bt.com

12 Work item leadership

TSG SA WG3
With T2 as secondary responsibility

13 Supporting Companies

BT
Motorola
Vodafone
Please mail me if your company is willing to support this work item.

14 Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

Work Item Description

Title: **User plane protection in access network**

To provide authentication and integrity for the user data (Voice, Messages, Signalling, etc.) of a 3G network.

1 3GPP Work Area

	Radio Access
	Core Network
X	Services

2 Linked work items

There is related work items in S3: "Access network security for IP-based services"
"Ability of terminal/USIM to reject unencrypted connections"

3 Justification

With the provision of mobile services in R00 there will be a need to provide integrity and security of the user data transacted in the service. This work item will identify a standard and consistent way to secure the transfer of information.

4 Objective

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.

5 Service Aspects

This WI implies that there will be a standard way of incorporating these mechanisms into services so that the use of the security aspects of all services is consistent. The work item will need to take into account current security procedures for existing or currently defined services.

6 MMI-Aspects

There will be no MMI aspect other than the mechinism to indicate to the user that normal intergraty protection is not available, as detailed in WI "Ability of terminal/USIM to reject unencrypted connections"

7 Charging Aspects

None/Text

8 Security Aspects

9 Impacts

Work Tasks may involve S2, S3, R2, R3, N1, [SMG 2 WP A].

Affects:	USIM	ME	AN	CN	Others
Yes		X	X	X	
No	X				
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

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

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102		Security Architecture		Include USS
33.103		Security Integration Guidelines		Include USS
21.133		Security Threats and Requirements		Include USS

11 Work item raporteurs

Stuart Ward Orange;stuart.ward@orange.co.uk

12 Work item leadership

SA3

13 Supporting Companies

Orange (???)

Anyone else please

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)

Work Item Description

Title

Lawful Interception in the 3GPP R'2000 architecture

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

3GPP release 2000 architecture and services

3 Justification

The release 99 lawful interception specifications reflect the basic release 99 architecture with separated circuit and packet data services. The 3GPP release 2000 architecture introduces several functions and services which need to be addressed by lawful interception. These include release 2000 service models, for example SIP and H.323 enabled features, which need to be addressed as part of packet interception. In addition, the latest CAMEL and Location services also need to addressed for a release 2000 lawful interception system. Interception implications of the interworking between the 3G MSC and the 3G GSN will also be addressed. Finally, any end to end encryption offered in release 2000 requires consideration in the lawful interception standards.

4 Objective

The objective of this work item is to create a lawful interception specification for the latest release 2000 architecture and services as described in the above justification.

5 Service Aspects

None

6 MMI-Aspects

None

7 Charging Aspects

None

8 Security Aspects

Enhanced Lawful Interception specifications

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes				X	None

No	x	x	x		
Don't know					

10 ~~10~~ Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
S3/CN joint meeting	June/July, 2000	Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles.
S3#14	August 2000	Requirements capture
S3#15	September 2000	Feature specification
S3#16	November 2001	Definition of architecture: Complete CRs
SA#10	December, 2000	Definition of architecture: CRs approved at TSG level

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
33.106 v 4.x.x	Lawful Interception Requirements	SA3 WG LI	None	S3 November	S3 Dec	Update to existing document.
33.107 v 4.x.x	Lawful Interception Architecture and Functions	SA3 WG LI	None	S3 November	S3 Dec	Update to existing document

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
TS 33.106	1	Lawful Interception Requirements	SA6, December 99	
TS 33.107	Initial Rel	Lawful Interception Architecture and Functions	SA6, December 99	

11 Work item raporteurs

Berthold Wilhelm

12 Work item leadership

3GPP S3

13 Supporting Companies

Mannessman Mobilfunk
Motorola
Siemens
T-Mobil

14 Classification of the WI (if known)

	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

(one Work Item identified as a feature)

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)

Work Item Description

Visibility of configurability of security

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

Greater visibility of security features (ciphering, security context) and configurability of some of these features is seen as an important way to inform and protect the user and the network operator from certain types of attacks, in particular potential breach of the confidentiality of user data.

4 Objective

Due to the fact that security is not homogenous in mobile networks, a roaming user may need to be informed of the security level applied within a network. Therefore it is necessary to be able to provide greater visibility of active security features to the user. This includes an indication of ciphering and an indication of the security context (3G security context or 2G security context).
Furthermore, it can be desirable to provide means to configure a user equipment to request certain security features in order to access a service.
This may include :

- Rejection of non ciphered connections for both incoming calls and set-up calls
- Possibility to select which ciphering algorithm(s) can be used (amongst the ones available in the terminal), and a rejection of the connection in case none of the selected ones can be used
- Requiring an authentication before getting access to a certain service
- Rejection of connections established in a 2G security context instead of a 3G one (case where a 2G authentication has been performed)

Emergency calls shall be an exception and shall not be rejected.
A more complete description of the feature can be found in section 5.5 of document TS 33.102.

The objective is to make this feature available for PS connections whatever the access network (GSM BSS/GERAN or UTRAN).

5 Service Aspects

Input from S1 will probably be required in order to define precisely which options of configuration of security shall be offered to user and/or network operators.

6 MMI-Aspects

None identified

7 Charging Aspects

None identified

8 Security Aspects

The work item is a security item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes	X	X		X	
No			X		X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
S3#14	August 1-4, 2000	First draft of a mechanism to handle rejection of non-ciphered connections
S3#15	September 2000	Approval of CR to S3 specifications for rejection of non-ciphered connections
TSG#10	December, 2000	Approval of complete CR for rejection of non ciphered connections

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				The feature already exists in section 5, mechanisms should be provided in section 6.

11 Work item raporteurs

Sébastien Nguyen Ngoc, France Telecom
Sebastien.nguyenngoc@francetelecom.fr
Tel: +33 145 29 47 31
Fax: +33 145 29 65 19

12 Work item leadership

TSG SA WG3

13 Supporting Companies

France Telecom…

Telia
T-mobil

14 Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

The WI is listed as a feature in S3-000318, but has no building block defined.
It might need a building block to reject a connection (regardless of what criteria are used to reject the call, ciphering on/off, valid algorithm or not…).

Work Item Description

Title

Core network security
(formerly called the full solution)

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

- Related work is in N2 and N4 to specify the solutions developed by S3.

3 Justification

An identified security weakness in 2G systems is the absence of security in SS7 networks. This was formerly perceived not to be a problem, since this network was the province of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions.

This work item describes ongoing work in S3, which had been originally tasked by SA to S3 under the name of “MAP Security”, an early version of which had originally been included in R’99.

4 Objective

Various protocols and interfaces are used for signaling in and between core networks. These include among the applications MAP, CAP, and GTP, among the interfaces Iu, A, and Iur, and possibly other applications or interfaces that are new to R’00 or have yet to be identified. The security characteristics that have been identified as being in need of protection are confidentiality, integrity, and authentication. These will be ensured by standard procedures, based on cryptographic techniques.

This work might also be extended to protection of the user plane.

Within this WI MAP Application Security has been separated out into its own work item as a sort-of minimal solution, for completion for R’00; MAP-over-IP is foreseen as belonging to this WI proper and not to the minimal solution. In addition, the protection of GTP has a high time priority; completion of this aspects of the feature is expected well in advance of the others.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The work item is a security item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes				X	
No	X	X	X		X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
CN/S3 joint meeting	June 13-14, 2000	Presentation by S2 of R'00 architecture
CN	July-August, 2000	Specification of the protocol stacks of the core network interfaces
S3	June-July, 2000	Requirements capture GTP signalling security Feasibility study of GTP signalling security, including definition of work tasks and completion of plan
S3#14	August 1-4, 2000	Requirements capture (CAP, MAP-over-IP, etc.) Feature specification of GTP signalling security
S3#15	September 12-15, 2000	Specification of other security features (CAP, MAP-over-IP, etc.) Approval of GTP CRs
SA#9	September 25-28, 2000	Approval of GTP CRs
N4#5	November 13-17, 2000	N4 approval of GTP CRs
S3#16	November 27-30, 2000	Feasibility study, including definition of work tasks and completion of plan
CN#10	December 6-8, 2000	Approval of GTP CRs
S3#17	January, 2001	Definition of security architecture, first draft
S3#18	February, 2001	Approval of CRs to the drafts Integration of security architecture (presentation to other WGs)
S3#19	March, 2001	S3 approval of final versions
SA#12, CN#12	June, 2001	Approval of final versions

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Re-inclusion and extension of core network signaling security in 33.102 (R'00 for MAP and GTP, R'01 for the rest)
33.103				Re-inclusion and extension of core network signaling security in 33.102 (R'00 for MAP and GTP, R'01 for the rest)
33.105				Inclusion of core network signaling security algorithm requirements in 33.102 (R'00 for MAP and GTP, R'01 for the rest)

11 Work item raporteurs

Robert Lubarsky, T-Mobil
Robert.Lubarsky@T-Mobil.de
Tel +49 228 936 3340
Fax +49 228 936 3199

12 Work item leadership

TSG SA WG3

13 Supporting Companies

T-Mobil, Vodafone, Ericsson, Telenor

14 Classification of the WI (if known)

X	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

Core network signaling security: protection of MAP Application Layer
Core network security: key exchange and distribution
Other possibilities:

GTP signaling security
CAMEL signaling security
Building blocks from N2, N4, S2, S5

14b The WI is a Building Block: parent feature „provision of IP based multimedia services“

Work Item Description

Title

Key management for core network security

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

MAP application layer security
The MAP application layer security work item involves the protection of MAP dialogues between core network elements by integrating protection mechanisms into the MAP application. This allows for MAP-over-SS7 links to be protected with no impact on the SS7 stack.

Core network security
The core network security work item involves the extension of the minimal solution to cover other applications and interfaces including GTP signalling. The full solutions will also look at mechanisms to protect new core network interfaces and applications which are introduced in the R00 system architecture.

3 Justification

Two other work items on core network security are tasked with defining mechanisms to protect traffic on transmission links within the core network. These mechanisms will require the necessary keys to be established at each involved network element. Because of the number of keys involved and the rate at which they must be changed, it is desirable for an automated key management mechanism to be used. In order to support inter-operation between operators and multi-vendor core networks, it is also desirable for such a solution to be standardised.

4 Objective

The main objective of this work item is to specify key management standards for core network security including MAP application layer security. The mechanisms specified must allow for scaleable, flexible and cost-effective architecture(s) to be built to support key management towards core network elements. This work item will also study the management of security policies between network elements.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes				X	
No	X	X	X		X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Dates for the IP/IKE-based solution to be added at S3#14.

Meeting	Date	Activity
CN/S3 joint meeting	June 13-14, 2000	Feedback from CN about the practicability of an IP/IKE-based key management solution versus the previously specified ISO-based solution for which N4 have developed CRs to implement the protocols using MAP.
	June/July, 2000	Contributions solicited to determine if MAP-based key management is to be specified.
S3#14	August 1-4, 2000	Decide whether a MAP-based key management solution will be specified. Decide on dates for and IP/IKE-based solution.
CN#9	September, 2000	Completion of MAP-based key management CRs by CN (if S3 decided to work on this solution).

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Re-inclusion of core network signalling security key management architecture in a R00 version of 33.102
33.103				Re-inclusion of core network signalling security key management architecture in a R00 version of 33.103
33.105				Inclusion of core network signalling security key management architecture algorithm requirements in a R'00 version of 33.105

11 Work item raporteurs

Peter Howard, Vodafone
Peter.Howard@vf.vodafone.co.uk
Tel +44 1635 676206
Fax +44 1635 231721

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Siemens
Motorola
Telenor
Vodafone

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14b The WI is a Building Block: parent Features/Building Blocks “core network security: full solution” and “core network solution: minimal solution”.

Work Item Description

Title

Core network signaling security: protection of MAP Application Layer
(formerly the minimal solution)

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

- Related work is in N4 to specify the solutions developed by S3.
- A separate work item was defined by S3 to develop the key management and distribution scheme (old MAP security layer I&II).
- Core network security (formerly the full solution)

3 Justification

An identified security weakness in 2G systems is the absence of security in SS7 networks. This was formerly perceived not to be a problem, since this network was the province of a small number of large institutions. This is no longer the case, and so there is now a need for security precautions.

This work item describes ongoing work in S3, which had been originally tasked by SA to S3 under the name of “MAP Security”, an early version of which had originally been included in R’99.

4 Objective

The MAP protocol is used for signaling in and between core networks. It is the objective of this work item to protect all sensitive data transmitted via MAP, e.g. authentication data and user related data. The security characteristics that have been identified as being in need of protection are confidentiality, integrity, and authentication. These will be ensured by standard procedures, based on cryptographic techniques.

The topic has been split into three work items, a solution for MAP protection at the application layer (formerly called the minimal solution), a solution for protection of other protocols (the full solution), and the key management distribution. The minimal solution is defined to specify protection of MAP signaling in R00 (as already earlier defined by MAP security layer III in the original R99 proposal).

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The work item is a security item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes				X	
No	X	X	X		X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
CN/S3 joint meeting	June 13-14, 2000	Key management and distribution has been split-up from min/full solution
CN#8	June 2000	Approval of CN4 CR on TS 29.002
S3#14	August 1-4, 2000	Completion of work (selection of algorithms and algorithm identifiers; CRs on TS 33.102, TS 33.103, TS 33.105)
SA#9	September 2000	Approval of CR

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Re-inclusion of core network signaling security in a R'00 version of 33.102
33.103				Re-inclusion of core network signaling security in a R'00 version of 33.103
33.105				Inclusion of core network signaling security algorithm requirements in a R'00 version of 33.105

11 Work item raporteurs

Robert Lubarsky, T-Mobil
Robert.Lubarsky@T-Mobil.de
Tel +49 228 936 3340
Fax +49 228 936 3199

12 Work item leadership

TSG SA WG3

13 Supporting Companies

T-Mobil, Vodafone, Ericsson, Telenor

14 Classification of the WI (if known)

X	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a This WI is a Feature. This Feature has no active Building Blocks.
14b The WI is a Building Block: parent Feature core network security.

Work Item Description

FIGS enhancements

The GSM Fraud Information Gathering System (FIGS) feature provides the means for the HPLMN to monitor the activities of its subscribers in a VPLMN. The VPLMN collects information about a defined set of activities on monitored subscribers and sends this information back to the HPLMN. This enables the HPLMN to clear certain types of calls and so stop fraudulent use of the GSM system. GSM FIGs only covers connection-orientated services.

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified.

3 Justification

In order to maintain an HPLMN's ability to limit its exposure to fraud, it is necessary to extend FIGS functionality to cover new services, domains and subsystems introduced in the R99/R00 system architecture.

4 Objective

The main objective of this work item will be to extend FIGS functionality to cover PS services offered by the PS domain, and SIP and H.323 enabled services offered by the IP multimedia (IM) domain. For example, it must be possible for an HPLMN to be able to gather information on Voice-over-IP call activity offered by an IM ~~domain~~ subsystem in a VPLMN. The work item will investigate whether CAMEL can be used to extend fraud information gathering capabilities to new domains and subsystems in R99/R00.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes				X	
No	X	X	X		X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Timescales for extending FIGS to the R99 PS domain probably need to be brought forward. A new milestone has therefore been added (in italics) to supplement the milestones agreed at the joint CN/S3 meeting.

Meeting	Date	Activity
	June/July	Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles
S3#14	*August 2000*	*Identification of milestones for extending FIGS to PS domain*
S3#15	September 2000	Requirements capture
S3#16	November 2000	First draft
	January 2001	Feasibility study including definition of work tasks and completion of the plan for this work item
	March 2001	Definition of security architecture; CRs approved
	April 2001	Integration of security architecture: Concept presented to S2 and CN
	July 2001	Integration of security architecture: First draft CRs
	October 2001	Integration of security architecture: Complete CRs
	December 2001	Integration of security architecture: CRs approved at TSG level
		Review of complete CRs by S3

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
To be allocated	Fraud Information Gathering System (FIGS); Service requirements – Stage 0	S3	None		March 2001	Update to GSM document.
To be allocated	Fraud Information Gathering System (FIGS); Service description – Stage 1	S3	None		March 2001	Update to GSM document.
To be allocated	Fraud Information Gathering System (FIGS); Service description – Stage 2	S3	None		March 2001	Update to GSM document.

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
01.31		Fraud Information Gathering System (FIGS); Service requirements – Stage 0		
02.31		Fraud Information Gathering System (FIGS); Service description – Stage 1		
03.31		Fraud Information Gathering System (FIGS); Service description – Stage 2		

11 Work item rapporteurs

Peter Howard, Vodafone
Peter.Howard@vf.vodafone.co.uk
Tel +44 1635 676206
Fax +44 1635 231721

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Vodafone

Please mail the rapporteur if your company is willing to support this work item.

14 Classification of the WI (if known)

	Feature (go to 14a)
(X)	Building Block (go to 14b)
	Work Task (go to 14c)

14b This is a **Building Block** of the Feature "**Provisioning of IP-based multimedia services".**

Work Item Description

Title

General ~~R99~~ security enhancements

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

This work item is intended to cover miscellaneous security enhancements ~~to R99~~ which are not covered by any other security work item. Examples of miscellaneous items include:

- ~~Feasbility~~Feasibility of an authentication vector revocation mechanism
- Feasibility of positive ~~A~~authentication result reporting
- Feasibility of control of lifetime of SA
- UE triggered authentication
- Retention of P-TMSI signature

4 Objective

The general objective of this work item is to produce the necessary CRs which provide the identified miscellaneous security enhancements.

5 Service Aspects

None identified.

6 MMI-Aspects

None identified.

7 Charging Aspects

None identified.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

The following examples only have an impact on CN:

- Feasibility of an authentication vector revocation mechanism
- Feasibility of positive ~~A~~authentication result reporting
- Feasibility of control of lifetime of ~~Sa~~security association (cipher/integrity keys established after an authentication)

The following examples have an impact on ME, AN and CN

- UE triggered authentication
- Retention of P-TMSI signature

Affects:	USIM	ME	AN	CN	Others
Yes					
No					
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Feasibility of an authentication vector revocation mechanism
N4 will look at this issue in July 2000 and respond to S3. Target for S3 decision/~~implemetation~~implementation: December 2000.

Feasibility of postive ~~A~~authentication result reporting
N4 will look at this issue in July 2000 and respond to S3. ~~S3 feel that it is~~May be acceptable to only support this for 3GPP2 subscribers[1]. Target for S3 decision/implementation: December 2000

Feasibility of control of lifetime of security association~~SA~~
Target for S3 decision/implementation: December 2000

UE triggered authentication
Target completion date: December 2000

Retention of P-TMSI signature
No security issues were identified with removal of P-TMSI signature from service request. BT asked to clarify that removal only addresses the service request. Decision to be made at CN#8.
Any further changes to P-TMSI signature should be approved by S3 plenary first. In the long term S3 need to describe the P-TMSI signature concept in 03.20/33.102 to ensure good visibility.

Meeting	Date	Activity

[1] ~~We haven't really discussed this in a S3 meeting, but its fine by me~~

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments

11 Work item raporteurs

Peter Howard, Vodafone
Peter.Howard@vf.vodafone.co.uk
Tel +44 1635 676206
Fax +44 1635 231721

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Telenor
Nokia
Vodafone

14 Classification of the WI (if known)

Various

	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

Work Item Description

OSA Security

1 3GPP Work Area

	Radio Access
X	Core Network
X	Services

2 Linked work items

None identified

3 Justification

The Open Service Architecture (OSA) defines an architecture that enables operator and third party applications to make use of network functionality through an open standardised interface (the OSA Interface). Network/server centric applications can reside outside the core network and make use of service capability features offered through the OSA interface. Applications may also belong to the network operator domain although running outside the core network.

From the network operator's perspective, it is essential that such an open interface incorporate security features to preserve the integrity of the network and protect the confidentiality and integrity of third party and end user data and applications.

A secure OSA interface is key enabler for the Virtual Home Environment (VHE) concept for personal service environment (PSE) portability across network boundaries and between terminals. For example, users are consistently presented with the same personalised features, User Interface customisation and services in whatever network and whatever terminal (within the capabilities of the terminal and the network), wherever the user may be located.

4 Objective

To conduct a threat analysis for the Open Service Architecture and review the security features documented in 3G TS 23.127 for effectiveness in countering those threats and to agree any necessary CR's to S3 and S2 specifications.

The Open Service Architecture consists of three parts:

1) **Applications**, e.g. VPN, conferencing, location based applications.
2) **Service Capability Servers**, providing the applications with service capability features, which are abstractions from underlying network functionality
3) **Framework**, providing applications with basic mechanisms that enable them to make use of the service capabilities in the network. This includes the framework service capability feature (SCF) known as Trust and Security Management (TSM). The TSM Service Capability Features provide:

- **Authentication**: The authentication model of OSA is a peer-to-peer model. The application must authenticate the framework and vice versa. The application must be authenticated before it is allowed to use any other OSA interface. The challenge response protocol actually used is implementation dependent, but assumed to in accordance with CHAP (RFC 1994)

- **Authorisation**: The framework provides access control functions to authorise the access to service capability features or service data for any API operation from a client, with the specified security level, context, domain, etc.

- **Discovery of framework and network service capability features**. After successful authentication, applications can obtain available framework interface classes and use the discovery interface to obtain information on authorised network service capability features. The Discovery

interface can be used at any time after successful authentication.

- **Establishment of service agreement**. Before any application can interact with a network service capability feature, a service agreement must be established. A service agreement may consist of an off-line (e.g. by physically passing messages) and an on-line part. The application has to sign (cryptographic) the on-line part of the service agreement before it is allowed to access any network service capability feature.

The review will also consider "End-user" related security aspects. The Home Environment is entitled to provide service capabilities to an application with regard to a specific end-user if the following conditions are met:

1) The end-user is subscribed to the application, an end-user is authorised to use an application only when he or she is subscribed to it.
2) The end-user has activated the application
3) The usage of this network service capability does not violate the end-users privacy as the Home Environment may permit an end-user to set privacy options. For instance, it may permit the end-user to decide whether his or her location may be provided to 3rd parties, or whether he or she accepts information to be pushed to his or her terminal.

5 Service Aspects

Input from S1 and S2 will be required in order fully understand how the interface will be used by third parties to create new services.

6 MMI-Aspects

Not yet investigated

7 Charging Aspects

none

8 Security Aspects

The work item is a security item.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X		X	
No					X
Don't know	X				

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
S3#14	August 1-4, 2000	Presentation to S3 of Trust and Security Management framework service capability feature (SCF)
S3#15	September 2000	Presentation to S3 of threat and countermeasure analysis
S3#16	November, 2000	Decision if implementation is to be standardised and how much reuse can be made of, 3G AKA as "PrescribedMethod", Network certificates and security associations etc Approval of any CR's to S3 and S2 specifications required
	December 2000	Final CR's to Security Architecture TS 33.102 approved at TSG level

	April 2001	Integration of security architecture Complete CRs
	June 2001	CRs approved at TSG level

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Possible expanded scope and place of use for existing security features
23.127				Possible CR,s depending on result of threat analysis

11 Work item raporteurs

Colin Blanchard
Network Security Design
MLB1 PP8
BT Advanced Communications Technology Centre
Adastral Park
Ipswich
IP5 5RE
Phone +44 1473 605353
Fax +44 1473 623910
colin.blanchard@bt.com

12 Work item leadership

TSG SA WG3

13 Supporting Companies

BT
Ericsson

14 Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

Work Item Description

Title: Access security for IP-based services

1 3GPP Work Area

	Radio Access
X	Core Network
	Services

2 Linked work items

1. There are related work items in S3: “User plane protection in access network”, “Core Network Solution” and “Lawful Interception in the R’2000 architecture”
2. There is a related work item in S2: “An architecture for Call control and roaming to support IP-based multimedia services in UMTS”

3 Justification

The work item “An architecture for Call control and roaming to support IP-based multimedia services in UMTS” describes the ongoing work in 3GPP for R00, which has been initially tasked by SA to S2 under the “all-IP option” by SA#4 (6/99).

TSG-S3 has prime responsibility for all security-related specification work in 3GPP including the new all-IP architecture and secure access to IM-services.

4 Objective

The objective with this WI is to solve the security aspects that are related to secure access for the new IP Multimedia services, IM services in R00. The IM services will include different applications like voice, video and data. The trustrelations and the security services between the end-user, the IM CN subsystem, the PS-domain and the CS-domain shall be defined. Also the mechanisms for registration/authentication of a roaming/non-roaming end-user making registration to the IM CN subsystem using SIP will be treated in this WI. This shall include the definition of the needed encryption and integrity mechanisms for protection of the control plane and the user plane. The evolution and/or reuse of the existing R99 architecture for authentication and key agreement shall be considered.

5 Service Aspects

yes, the end-user shall be able to access the services located at the home IM CN subsystem wherever the end-user may roam to. It shall also be possible to use different access technology to connect the “IP multimedia CN Subsystem” e.g. xDSL, wireline and Wireless LAN etc.

6 MMI-Aspects

yes, visibility and configurability. Issues like visibility of offered security level and user interaction shall be studied.

7 Charging Aspects

none identified

8 Security Aspects

yes, this WI issues security features

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes		X		X	
No			X		X
Don't know	X				

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
	June/July, 2000	Presentation by S2 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
-	-	*Definition of security architecture*
	December, 2000	CRs approved
-	-	*Integration of security architecture*
	February, 2001	Concept presented to CN, RAN, T and GERAN
	March, 2001	First draft CRs
	April, 2001	Complete CRs
	June, 2001	CRs approved at TSG level
	June, 2001	Review of complete CRs by S3

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				Include IP-base services
21.333				Include IP-base services

11 Work item raporteurs

N.N.

12 Work item leadership

S3

13 Supporting Companies

Ericsson, Nokia, ….

Please indicate if your company should also be here!

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14b The WI is a Building Block: parent feature

“Provisioning of IP-based multimedia services”

Work Item Description - draft

Network-based end-to-end security

1 3GPP Work Area

X	Radio Access
X	Core Network
X	Services

2 Linked work items

There are five related work items in S3:

- User plane protection in access network
- Access security for IP-based services
- Core network security: full solution
- Lawful interception in the R00 architecture
- Visibility and configurability

3 Justification

The R00 system architecture may create new requirements and/or opportunities for extending user plane traffic security further back into the core network. In addition it may allow for security mechanisms to be applied on an end-to-end basis, providing that the necessary lawful interception requirements are addressed when encryption is applied. This work will take advantage of concepts and hooks for network-wide encryption which have been considered in R99.

4 Objective

The overall objective of this WI is to specify a network-based security architecture which provides security features to users on an end-to-end basis. The architecture is expected to be based on an evolution / re-use of the existing R99 security architecture.

The main security feature to be provided is expected to be encryption. However, the specification of other security features (e.g. authentication and integrity protection) will also be investigated.

The work may involve defining an appropriate key management architecture to support the end-to-end security mechanisms and the integration of these into the system architecture. Where possible this would be based on an evolution / re-use of the existing R99 authentication and key agreement mechanism. Some key management concepts for end-to-end security were presented in an old version of the R99 security architecture (33.102 v3.4.0).

The work may involve the specification of the end-to-end security mechanisms and the integration of these mechanisms into the system architecture. This work would involve the specification of an end-to-end security mode control mechanism which will handle algorithm selection, mode selection and user control. It would also involve the specification of any necessary end-to-end synchronisation mechanisms.

5 Service Aspects

Service requirements for end-to-end security need to be identified and addressed in conjunction with S1.

6 MMI-Aspects

Visibility and configurability of end-to-end security will be important. For example, the existing ciphering indicator may need to be enhanced to indicate whether or not the call is encrypted on an end-to-end basis.

7 Charging Aspects

End-to-end security may be considered to be a value-added service, especially if it is not, or cannot, be provided as a default.

8 Security Aspects

The main aspect of this work item is security.

9 Impacts

Affects:	USIM	ME	AN	CN	Others
Yes	X	X	X	X	
No					X
Don't know					

10 Expected Output and Time scale (to be updated at each plenary)

Meeting	Date	Activity
S3/CN joint meeting	13-14 June, 2000	Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles. Feedback from CN on feasibility of network-based end-to-end security.
S3#15~~4~~	September 2000~~August 1-4, 2000~~	Requirements capture ~~and feature specification~~
S3#16	November 2000	Feature specification
~~S3#15~~	~~September~~ January 200~~0~~	Feasibility study, including definition of Work Tasks and completion of the plan for this Feature
~~S3#16~~	~~November~~March, 200~~0~~	~~Outline d~~Definition of security architecture~~ (e.g. first draft CRs). Concept presented to CN, RAN, T GERAN.~~: CRs approved
~~S3#17~~	~~January 2001~~	~~Integration of security architecture~~ ~~First draft CRs March 2001~~ ~~Complete CRs April 2001~~ ~~CRs approved at TSG level May 2001~~ ~~Review of complete CRs by S3 June 2001~~ ~~First corrective CRs prepared July 2001~~ ~~Corrections agreed at TSG level August 2001~~
	April 2001	Concept presented to CN, RAN, T and GERAN
	July 2001	Integration of security architecture: First draft CRs
	October 2001	Integration of security architecture: Complete CRs
	December 2001	Integration of security architecture: CRs approved at TSG level

This table will be finalised when the plan for this feature is complete (see milestones above)

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102				
33.103				
33.105				

11 Work item raporteurs

Peter Howard
Communications Security and Advanced Development
Vodafone Ltd
The Courtyard
2-4 London Road
Newbury
RG14 1JX
Phone +44 1635 676206
Fax +44 1635 231721
peter.howard@vf.vodafone.co.uk

12 Work item leadership

TSG SA WG3

13 Supporting Companies

Vodafone
Please mail me if your company is willing to support this work item.

14 Classification of the WI (if known)

(X)	Feature (go to 14a)
	Building Block (go to 14b)
	Work Task (go to 14c)

Work Item Description

GERAN security

The GERAN R00 radio access network is a GSM BSS connected via a Iu-ps interface to a packet-switched core network and includes a major redesign of the R99 GSM/GPRS control plane. The GERAN security work item consists of the provision of access link security services such as confidentiality and message integrity between the MS and the GERAN.

1 3GPP Work Area

X	Radio Access
X	Core Network
	Services

2 Linked work items

The work item is linked to other GERAN-related work items.

3 Justification

Compared to GSM/GPRS R99 radio access networks, the upgrade to GERAN R00 includes a major redesign of the radio access network architecture. In order to protect service delivery via GERAN, a security architecture has to be designed that protects against the threats that are envisaged.

4 Objective

The overall objectives are 1) to provide user and signalling data in the GERAN with a level of protection that is as good or better than the level of protection offered in UTRAN and 2) to employ a security architecture that has as much compatibility with the security architecture for UTRAN.

This includes encryption mechanisms applied to both user data and signalling data~~,~~ that extends to a node beyond the base station (if feasible) and uses a symmetric session (ciphering) key of up to 128 bits (if feasible).

This includes integrity mechanisms applied to signalling data and -if possible- also to user data~~,~~ that extends to a node beyond the base station (if feasible) and uses symmetric session (integrity) key of up to 128 bits (if feasible).

This includes security mode negotiation procedures to securely select a ciphering and integrity mode.

This includes the specification of requirements and the selection of suitable ciphering and message authentication algorithms for the above security services.

This includes the specification of handover procedures to and from the legacy GSM BSS and UTRAN.

This work item will study whether after the relocation of the termination of ciphering (and integrity) from the SGSN to the radio access network the LLC layer is still required.

GERAN security relies on the existing UMTS and GSM authentication and key agreement mechanisms to conduct mutual authentication between MS and network and to establish session keys.

5 Service Aspects

The GERAN security features will be generic, i.e., application or service-independent.

6 MMI-Aspects

The GERAN security features will be transparent to the user, with the exception of the mandatory presence of a ciphering indicator in the ME and the ability for users and home networks to configure whether non-encrypted connections are acceptable. These exceptions however will be dealt with in a separate work item that is not radio access network-specific.

7 Charging Aspects

None.

8 Security Aspects

A set of algorithms shall be provided that has withstood peer review.

The security mode negotiation procedure shall withstand active attacks.

The security mode negotiation procedure shall allow for future introduction of new algorithms.

9 Impacts

Affects	USIM	ME	AN	CN	Others
Yes		X	X		
No	X				
Don't know	~~X~~			X	

10 Expected Output and Time scale (to be updated at each plenary)

Protocol specification

Stage	Date	Action
1	Aug. 00, SA-3#14	GERAN group presents stable GERAN architecture to SA-3
	Sep. 00, SA-3#15	SA-3 specifies the security requirements
	Nov. 00, SA-3#16	SA-3 specifies the security features
2	Jan. 01	SA-3 conducts feasibility study
	Jan. 01	SA-3 specifies GERAN security architecture (Stage 2)
	Mar. 01	SA approves final GERAN security architecture (Stage 2)
3	Feb. 01	SA-3 presents GERAN security architecture to CN, T and GERAN
	Mar. 01	CN, T and GERAN write draft Stage 3 CRs
	Apr. 01	CN, T and GERAN approve final Stage 3 CRs
	Jun. 01	SA-3 reviews final Stage 3 CRs
	Jun. 01	CN, T, RAN approve final Stage 3 CRs

Algorithm specification

Stage	Date	Action
1	Jan. 01	SA-3 specifies the algorithm requirements
	Jan. 01	SA-3 selects a mechanism for algorithm development
	Jan. 01	SA arranges funding
3	Jun. 01	SA-3 approves the algorithms developed
	Oct. 01	3GPP partners publicise algorithm specifications

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
	??					

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102		Security architecture	~~January~~March, 2001	
33.103		Security integration guidelines	~~January~~March, 2001	
33.105		Cryptographic algorithm requirements	January, 2001	

11 Work item rapporteurs

~~N.N.~~Bart Vinck, Siemens AG, Tel: +49-89-722 25644, e-mail: bart.vinck@icn.siemens.de

12 Work item leadership

SA 3

13 Supporting Companies

Ericsson, Siemens, T-Mobil

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

The work item is child of the feature GERAN.

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)

Work Item Description

GERAN security

The GERAN R00 radio access network is a GSM BSS connected via a Iu-ps, Gb, A, or Iu-cs (FFS) interface to a GSM/UMTS~~packet switched~~ core network and includes a major redesign of the R99 GSM/GPRS control plane. The GERAN security work item consists of the provision of access link security services such as confidentiality and message integrity between the MS and the GERAN.

1 3GPP Work Area

X	Radio Access
X	Core Network
	Services

2 Linked work items

The work item is linked to other GERAN-related work items.

3 Justification

Compared to GSM/GPRS R99 radio access networks, the upgrade to GERAN R00 includes a major redesign of the radio access network architecture. In order to protect service delivery via GERAN, a security architecture has to be designed that protects against the threats that are envisaged.

4 Objective

The overall objectives are 1) to provide user and signalling data in the GERAN with a level of protection that is as good or better than the level of protection offered in UTRAN and 2) to employ a security architecture that has as much compatibility with the security architecture for UTRAN.

This includes encryption mechanisms applied to both user data and signalling data~~,~~ that extends to a node beyond the base station (if feasible) and uses a symmetric session (ciphering) key of up to 128 bits (if feasible).

This includes integrity mechanisms applied to signalling data and -if possible- also to user data~~,~~ that extends to a node beyond the base station (if feasible) and uses symmetric session (integrity) key of up to 128 bits (if feasible).

This includes security mode negotiation procedures to securely select a ciphering and integrity mode.

This includes the specification of requirements and the selection of suitable ciphering and message authentication algorithms for the above security services.

This includes the specification of handover procedures to and from the legacy GSM BSS and UTRAN.

This work item will study whether after the relocation of the termination of ciphering (and integrity) from the SGSN to the radio access network the LLC layer is still required.

GERAN security relies on the existing UMTS and GSM authentication and key agreement mechanisms to conduct mutual authentication between MS and network and to establish session keys.

5 Service Aspects

The GERAN security features will be generic, i.e., application or service-independent.

6 MMI-Aspects

The GERAN security features will be transparent to the user, with the exception of the mandatory presence of a ciphering indicator in the ME and the ability for users and home networks to configure whether non-encrypted connections are acceptable. These exceptions however will be dealt with in a separate work item that is not radio access network-specific.

7 Charging Aspects

None.

8 Security Aspects

A set of algorithms shall be provided that has withstood peer review.

The security mode negotiation procedure shall withstand active attacks.

The security mode negotiation procedure shall allow for future introduction of new algorithms.

9 Impacts

Affects	USIM	ME	AN	CN	Others
Yes		X	X		
No	X				
Don't know	~~X~~			X	

10 Expected Output and Time scale (to be updated at each plenary)

Protocol specification

Stage	Date	Action
1	Aug. 00, SA-3#14	GERAN group presents stable GERAN architecture to SA-3
	Sep. 00, SA-3#15	SA-3 specifies the security requirements
	Nov. 00, SA-3#16	SA-3 specifies the security features
2	Jan. 01	SA-3 conducts feasibility study
	Jan. 01	SA-3 specifies GERAN security architecture (Stage 2)
	Mar. 01	SA approves final GERAN security architecture (Stage 2)
3	Feb. 01	SA-3 presents GERAN security architecture to CN, T and GERAN
	Mar. 01	CN, T and GERAN write draft Stage 3 CRs
	Apr. 01	CN, T and GERAN approve final Stage 3 CRs
	Jun. 01	SA-3 reviews final Stage 3 CRs
	Jun. 01	CN, T, RAN approve final Stage 3 CRs

Algorithm specification

Stage	Date	Action
1	Jan. 01	SA-3 specifies the algorithm requirements
	Jan. 01	SA-3 selects a mechanism for algorithm development
	Jan. 01	SA arranges funding
3	Jun. 01	SA-3 approves the algorithms developed
	Oct. 01	3GPP partners publicise algorithm specifications

New specifications						
Spec No.	Title	Prime rsp. WG	2ndary rsp. WG(s)	Presented for information at plenary#	Approved at plenary#	Comments
	??					

Affected existing specifications				
Spec No.	CR	Subject	Approved at plenary#	Comments
33.102		Security architecture	~~January~~March, 2001	
33.103		Security integration guidelines	~~January~~March, 2001	
33.105		Cryptographic algorithm requirements	January, 2001	

11 Work item rapporteurs

~~N.N.~~Bart Vinck, Siemens AG, Tel: +49-89-722 25644, e-mail: bart.vinck@icn.siemens.de

12 Work item leadership

SA 3

13 Supporting Companies

Ericsson, Siemens, T-Mobil-, SBC Communications

14 Classification of the WI (if known)

	Feature (go to 14a)
X	Building Block (go to 14b)
	Work Task (go to 14c)

14a The WI is a Feature: List of building blocks under this feature

(list of Work Items identified as building blocks)

14b The WI is a Building Block: parent Feature

The work item is child of the feature GERAN.

14c The WI is a Work Task: parent Building Block

(one Work Item identified as a building block)