3G PD 30.810 v1.0.0 (1999-10)

Permanent Document

3rd Generation Partnership Project 3GPP work program Project co-ordination aspects Project Plan for Security (3G PD 30.810 version 1.0.0)



This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification.

Specifications and reports for implementation of the 3GPP TM system should be obtained via the 3GPP Organisational Partners' Publications Offices.

Technical Specification Group Services and System Aspects Meeting #5, Kyongju, Korea, 11-13 October 1999

Reference

Work Item Location services in UMTS

Keywords

Location services (LCS),
Digital cellular telecommunications system,
Universal Mobile Telecommunication System (UMTS),
UTRA, UTRAN, IMT-2000

3GPP

Postal address

3GPP support office address

650 Route des Lucioles - Sophia Antipolis Valbonne - FRANCE Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet

http://www.3gpp.org

Contents

Forev	word	4
1	Scope	Δ
2	References	
3	Release 99	
3.1	Work identified to fullfill the requirements for R99	
3.1.1	Work to be done by TSG SA	
3.1.1.		
3.1.1.		
3.1.1.3		
3.1.1.4	·	
3.1.1.		
3.1.2	Work to be done by TSG RAN	
3.1.2.	·	
3.1.2.2		
3.1.2.3		
3.1.2.4		
3.1.3	Work to be done by TSG CN	
3.1.3.	1 Work to be done by WG N1	9
3.1.3.2	= · · · · · · · · · · · · · · · · · · ·	
3.1.3.3	Work to be done by WG N3	12
3.1.4	Work to be done by TSG T	
3.1.4.		
3.1.4.2	_ ·····	
3.1.4.3	Work to be done by WG T3	14
3.1.5	Work to be done by ETSI SAGE	
3.2	List of all the deliverables applicable to the subject	
3.3	Time plan	18
4	Release 00	19
5	Change history	20
6	Annex A: Scope of the security co-ordination ad-hoc group	21
7	Annex B: Contact person	22

Foreword

[to be added by ETSI MCC]

1 Scope

This Permanent document describes the work program for the security architecture in UMTS.

TSG-S3 has prime responsibility for all security-related specification work in 3GPP, but it will rely on the co-operation of other TSG WGs to ensure that security specifications are appropriately integrated into all relevant 3GPP specifications.

2 References

References may be made to:

- a) specific versions of publications (identified by date of publication, edition number, version number, etc.), in which case, subsequent revisions to the referenced document do not apply; or
- b) all versions up to and including the identified version (identified by "up to and including" before the version identity); or
- c) all versions subsequent to and including the identified version (identified by "onwards" following the version identity); or
- d) publications without mention of a specific version, in which case the latest version applies.

A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

3 Release 99

3.1 Work identified to fullfill the requirements for R99

3.1.1 Work to be done by TSG SA

3.1.1.1 Work to be done by WG S1

None identified

3.1.1.2 Work to be done by WG S2

Item	Specification required	Issues	Milestones
User identity	Stage 2 description	Probably, not all issues have yet	1: Feasibility study
confidentiality		been discovered. Current issues	2: First draft CR
		are:	3: CR approved by TSG
			4: MCC provide draft R'99
		a) how to route to correct HLR.	spec
			5: First corrections to errors
		b) this is an HE feature, but what	in consolidated CRs
		changes are mandatory in all	
		VPLMNs	

	1	<u> </u>	
		c) time synchronisation of	
		encrypted IMSI between VPLMN and mobile.	
Authentication			
and key			
agreement			
Access link		Architectural impact of separate	1: Outline description
integrity		CS/PS nodes	r.
protection		Key establishment during	
		intersystem handover	
Access link		Architectural impact of separate	1: Outline description
confidentiality		CS/PS nodes	
		Key establishment during	
		intersystem handover	
Secure UMTS-			
GSM			
interoperation			
Network-wide			
encryption			
User equipment			
identification			
Core network			
signalling			
security			
Fraud			
information			
gathering			
system			
USIM			
application			
security			
Visibility and configurability			
Mobile			
Execution			
Environment			
Security			
Location			
services			
Lawful			
interception			
architecture			
IP security			
11 Security	<u></u>		

3.1.1.3 Work to be done by WG S3 $\,$

Item	Specification required	Issues	Milestones
User identity	Specification of enhanced		1: Description available in
confidentiality	mechanism.		33.102
Authentication	Specification of enhanced	An enhancement to the GSM	1: Description available in
and key	mechanism.	scheme based on the use of	33.102 (fall-back scheme in
agreement		sequence numbers has been	Annex)
		specified in 33.102. A fall-back	
		mechanism is also available in an	
		annex to 33.102. This fall-back	
		could be used if there are	
		problems with the sequence	
		numbers based scheme. At this	
		stage the sequence numbers	

		based scheme should be considered to be the working assumption.	
Access link integrity protection	Specification of mechanism	Termination point at user: USIM or UE Termination point in network: RNC or MSC/SGSN	1: Description available in 33.102. 2: Decision on termination point in network 3: Decision on termination point at user
Access link confidentiality	Specification of mechanism		1: Description available in 33.102.
Secure UMTS- GSM interoperation	Specification of mechanism		1: Description available in 33.102.
Network-wide encryption	Specification of mechanism		1: Description available in 33.102 2: Identification of 'hooks'
User equipment identification	Specification of mechanism		1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Core network signalling security	Specification of mechanism and key management architecture.		1: Description available in 33.102.
Fraud information gathering system	Specification of mechanism		As per GSM
USIM application security	Specification of mechanism		As per GSM
Visibility and configurability	Specification of mechanism		1: Outline description
Mobile Execution Environment Security	Specification of mechanism		As per GSM
Location services	Specification of mechanism		As per GSM
Lawful interception architecture	Specification of mechanism		Reuse of existing GSM specification
IP security	Specification of mechanism		Outline specification / placeholder in release R99?

3.1.1.4 Work to be done by WG S4

None identified

3.1.1.5 Work to be done by WG S5

None identified

3.1.2 Work to be done by TSG RAN

3.1.2.1 Work to be done by WG R1

None identified

3.1.2.2 Work to be done by WG R2

Item	Specification required	Issues	Milestones
User identity	1	Handling of paging with IMSI	1: Outline description
confidentiality			2: First draft CR
Commodition			3: CR approved by TSG
			4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs
Authentication		Handling of cipher/integrity key	1: Outline description
		changes due to authentication	1. Outilile description
and key			
agreement	Garage Circles	during RRC connection.	1. 0. 41 1
Access link	Specification of integrity		1: Outline description
integrity	functions in RAN (if UTRAN		2: First draft CR
protection	based).		3: CR approved by TSG
			4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs
Access link	Specification of ciphering		1: Outline description in
confidentiality	functions in RAN MAC and		25.301
	RLC.		2: MCC provide draft R'99
			spec
			3: First corrections to errors
			in consolidated CRs
Secure UMTS-			
GSM			
interoperation			
Network-wide	Specification of ciphering	Must be possible to separate	1: Outline description of
encryption	functions in RAN.	ciphering on user traffic and	hooks
		signalling information.	2: First draft CR for hooks
			3: CR approved by TSG
			4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs
User equipment			
identification			
Core network			
signalling			
security			
Fraud			
information			
gathering			
system			
USIM			
application			
security			
Visibility and			
configurability			
Mobile			
Execution			
LACCULIOII			

Environment Security		
Location services	Integration of mechanism in RAN specifications	1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Lawful interception architecture		
IP security		

3.1.2.3 Work to be done by WG R3 $\,$

Item	Specification required	Issues	Milestones
User identity confidentiality		Handling of paging from second CN node when mobile is already in an RRC connection with the first node	1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Authentication and key agreement		Handling of cipher/integrity key changes due to authentication during RRC connection. Handling of issues arising from 2 core network nodes. Hard handover between RNCs and/or BSCs. Authentication while a SRNC relocation is queued. Handover between RNC and BSC in a non-anchor MSC. Etc	1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Access link integrity protection	Modification of RANAP messages (probably only if checking is UTRAN based): Cipher mode command Cipher mode complete Cipher mode reject	Messages could be renamed security mode. Handling of integrity key(s) at handover/relocation including: Handling of issues arising from 2 core network nodes. Hard handover between RNCs and/or BSCs. Authentication while a SRNC relocation is queued. Handover between RNC and BSC in a non-anchor MSC. Etc.	1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Access link confidentiality	Specification of RANAP messages: Cipher mode command Cipher mode complete Cipher mode reject	Handling of cipher keys at intersystem handover, including: Handling of issues arising from 2 core network nodes. Hard handover between RNCs and/or BSCs. Starting encryption while a SRNC relocation is queued. Handover between RNC and BSC in a non-anchor MSC.	1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs

Secure UMTS- GSM			
interoperation			
Network-wide	May involve modification to	Must be possible to separate	1: Outline description of
encryption	following RANAP messages:	ciphering on user traffic and	hooks
	Cipher mode command	signalling information.	2: First draft CR for hooks
	Cipher mode complete		3: CR approved by TSG
	Cipher mode reject		4: MCC provide draft R'99
	May require new RANAP		spec
	messages.		5: First corrections to errors
			in consolidated CRs
User equipment			
identification			
Core network			
signalling			
security			
Fraud			
information			
gathering			
system			
USIM			
application			
security			
Visibility and			
configurability			
Mobile			
Execution			
Environment			
Security			
Location			
services			
Lawful			
interception			
architecture			
IP security			

3.1.2.4 Work to be done by WG R4

None identified

3.1.3 Work to be done by TSG CN

3.1.3.1 Work to be done by WG N1

Item	Specification required	Issues	Milestones
User identity	Modification of GMM and	Modification of all GMM and	1: First draft CR
confidentiality	MM Identity Response	MM messages which carry	2: CR approved by TSG
	message to contain encrypted	IMSI?	3: MCC provide draft R'99
	user identity. Modification of		spec
	IMSI detach message.		4: First corrections to errors
			in consolidated CRs
Authentication	Modification of MM and	Support for intersystem	1: Outline description
and key	GMM messages:	operation	2: First draft CR
agreement	Authentication request		3: CR approved by TSG
	Authentication response		4: MCC provide draft R'99
	Location updating request		spec
	CM service request		5: First corrections to errors
	CM re-establishment request		in consolidated CRs
	"Paging response"		

	Similar GMM messages		
Access link integrity protection	Modification of MM and GMM messages, eg Authentication request Authentication response Location updating request CM service request CM re-establishment request IMSI detach "Paging response"	Integrity checking of the MSC's "initial L3 messages" when in GSM coverage might require the "Message Authentication Code" to be added to Classmark 3 and the UE to support "early classmark sending". Handling of out of sequence messages.	1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Access link confidentiality	Changes to 09.08 needed for inter-MSC handover. Changes to 03.60 and 09.60 needed for inter-SGSN change.		1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Secure UMTS- GSM interoperation			
Network-wide encryption	May involve modification to following MM (and similar		1: Outline description of hooks
	GMM) messages: Authentication request Authentication response Location updating request CM service request CM re-establishment request Paging response		2: First draft CR for hooks 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
User equipment identification		Specification of additional MM and GMM messages for terminal authentication.	
Core network signalling security			
Fraud information gathering system			
USIM application security			
Visibility and configurability Mobile			
Execution Environment Security			
Location services			
Lawful interception architecture IP security			

3.1.3.2 Work to be done by WG N2 $\,$

Item Specification req	uired Issues	Milestones
------------------------	--------------	------------

User identity confidentiality	Modification of MAP Send Authentication Info to contain encrypted user identity.	How to route to the correct HLR (eg when an HPLMN has many HLRs)	1: Feasibility study (start and) complete 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Authentication and key agreement	Modification of MAP messages: MAP_Authenticate MAP_Send_Authentication_I nfo MAP_Send_Identification	Support for intersystem operation	1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Access link integrity protection			
Access link confidentiality			
Secure UMTS- GSM interoperation			
Network-wide encryption	Specification of end-to-end signalling procedures for network-wide cipher establishment	Specification of synchronisation mechanism Note: the exact split of work between N2 and N3 is not clear.	1: Outline description of hooks 2: First draft CR for hooks 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
User equipment identification		Specification of additional MAP messages for terminal authentication.	
Core network signalling security	Integration of ciphering and integrity protection in certain MAP signalling messages. Specification of new MAP messages for key management.		
Fraud information gathering system	Specification of CAMEL procedures including those on the PS side.		Part of CAMEL phase 3
USIM application security			
Visibility and configurability Mobile			
Execution Environment Security			
Location services	Signalling to transfer privacy settings		1: Outline description 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors

		in consolidated CRs
Lawful		
interception		
architecture		
IP security		

3.1.3.3 Work to be done by WG N3

Item	Specification required	Issues	Milestones
User identity	1		
confidentiality			
Authentication			
and key			
agreement			
Access link			
integrity			
protection			
Access link			
confidentiality			
Secure UMTS- GSM			
interoperation			
Network-wide	Specification of end-to-end	Specification of synchronisation	1: Outline description of
encryption	signalling procedures for	mechanism.	hooks
	network-wide cipher establishment.	Note: the exact split of work between N2 and N3 is not clear.	2: First draft CR for hooks 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
User equipment			In components of the
identification			
Core network			
signalling			
security			
Fraud			
information			
gathering			
system			
USIM			
application			
security			
Visibility and			
configurability			
Mobile			
Execution			
Environment			
Security			
Location			
services			
Lawful			
interception			
architecture			
IP security			

3.1.4 Work to be done by TSG T

3.1.4.1 Work to be done by WG T1

Item	Specification required	Issues	Milestones
User identity			
confidentiality			
Authentication			
and key			
agreement			
Access link			
integrity			
protection			
Access link			
confidentiality			
Secure UMTS-			
GSM			
interoperation			
Network-wide			
encryption			
User equipment	Specification of tests for	Development of suitable test	
identification	checking the security of	r	
	terminal identification and		
	authentication information		
Core network			
signalling			
security			
Fraud			
information			
gathering			
system			
USIM			
application			
security			
Visibility and			
configurability			
Mobile			
Execution			
Environment			
Security			
Location			
services			
Lawful			
interception			
architecture			
IP security			

3.1.4.2 Work to be done by WG T2

Item	Specification required	Issues	Milestones
User identity			
confidentiality			
Authentication			
and key			
agreement			
Access link			
integrity			
protection			
Access link			

confidentiality			
Secure UMTS-			
GSM			
interoperation			
Network-wide			
encryption			
	C		
User equipment identification	Specification of capabilities		
	for terminal authentication.		
Core network			
signalling			
security			
Fraud			
information			
gathering			
system			
USIM			
application			
security			
Visibility and	Specification of terminal		1: Outline description
configurability	capabilities		2: First draft CR
			3: CR approved by TSG
			4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs
Mobile	Specification of terminal		1: Outline description
Execution	capabilities		2: First draft CR
Environment	capabilities		3: CR approved by TSG
Security			4: MCC provide draft R'99
Security			spec
			5: First corrections to errors
			in consolidated CRs
Location	MMI to influence privacy		1: Outline description
services			2: First draft CR
services	settings.		
			3: CR approved by TSG
			4: MCC provide draft R'99
			spec
			5: First corrections to errors
.			in consolidated CRs
Lawful			
interception			
	1	I	
architecture IP security			

3.1.4.3 Work to be done by WG T3

Item	Specification required	Issues	Milestones
User identity confidentiality	Specification of USIM interface to allow ME to	Means for the SIM to prevent transmission of the unencrypted	1: First draft CR
Confidentiality	request encrypted user	IMSI over the radio interface.	2: CR approved by TSG 3: MCC provide draft R'99
	identity		spec
			4: First corrections to errors
			in consolidated CRs
Authentication	Specification of USIM		1: Outline description
and key	interface to allow UE to		2: First draft CR
agreement	request authentication and		3: CR approved by TSG
	key agreement.		4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs

A 1: 1	G 'C' ' CHGDA	T IIGDA	1.0.4: 1. : .:
Access link	Specification of USIM	Integrity termination on USIM	1: Outline description
integrity	interface to allow UE to	believed to be feasible if only a	2: First draft CR
protection	request	few messages are protected.	3: CR approved by TSG
	generation/verification of		4: MCC provide draft R'99
	integrity protected messages		spec
	(if integrity is terminated on		5: First corrections to errors
	USIM)		in consolidated CRs
Access link			
confidentiality			
Secure UMTS-			
GSM			
interoperation			
Network-wide	Specification of USIM		1: Outline description of
encryption	interface for network-wide		hooks
	encryption.		2: First draft CR for hooks
			3: CR approved by TSG
			4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs
User equipment			
identification			
Core network			
signalling			
security			
Fraud			
information			
gathering			
system			
USIM	Specification of security		1: Outline description
application	message formats and security		2: First draft CR
security	functionality required on		3: CR approved by TSG
	USIM.		4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs
Visibility and	USIM control parameters		1: Outline description
configurability	_		2: First draft CR
			3: CR approved by TSG
			4: MCC provide draft R'99
			spec
			5: First corrections to errors
			in consolidated CRs
Mobile	Specification of security		1: Outline description
Execution	functionality on USIM.		2: First draft CR
Environment			3: CR approved by TSG
Security			4: MCC provide draft R'99
· · · · · · · · · · · · · · ·			spec
			5: First corrections to errors
			in consolidated CRs
Location			
services			
Lawful			
interception			
architecture			
IP security			

3.1.5 Work to be done by ETSI SAGE

Item	Specification required	Issues	Milestones
110111	b b c c i i c a i c q i i c q i i c q	133463	Willestolles

	ı	
User identity		
confidentiality		
Authentication		
and key		
agreement		
Access link	Specification of algorithm	Delivery of algorithm
integrity		
protection		
Access link	Specification of algorithm	Delivery of algorithm
confidentiality		
Secure UMTS-		
GSM		
interoperation		
Network-wide	Specification of algorithm (if	 1: decision on same/different
encryption	different to cipher algorithm	algorithm
	in RAN)	
User equipment		
identification		
Core network	Specification of algorithms.	Candidate cipher (BEANO)
signalling		is available.
security		
Fraud		
information		
gathering		
system		
USIM		
application		
security		
Visibility and		
configurability		
Mobile		
Execution		
Environment		
Security		
Location		
services		
Lawful		
interception		
architecture		
IP security		

3.2 List of all the deliverables applicable to the subject

	Status of specifications						
Del#	Title	Working Group	Editor	Completion date	Comment		
	Security threats and requirements			SA#3.	CRs may be required at SA#6 to refine or clarify some security requirements.		

TS33.102	Security architecture	S3	Bart Vinck (Siemens Atea), Stefan Pütz (T- Mobil).	Approved at SA#3. 11 CRs approved at SA#4. CRs for approval at SA#5.	More CRs expected at SA#6.
TS33.103	Integration guidelines	S3	Colin Blanchard (BT).	For approval at SA#5.	CRs may be required at SA#6 to align with architecture.
TS33.105	Cryptographic algorithm requirements	S3	Takeshi Chikazawa (Mitsubishi).	Approved at SA#4. CRs for approval at SA#5.	CRs may be required at SA#6 to align with architecture.
TS33.106	Lawful interception requirements	S3	Berthold Wilhelm (RegTP).	Approved at TSG-SA #4.	CRs expected at SA#6.
TS33.107	Lawful interception architecture and functions	S3	Berthold Wilhelm (RegTP).	Approval at SA#6 planned.	Originally planned for approval at SA#5.
TS33.120	Security principles and objectives	S3	Timothy Wright (Vodafone).	Approved at SA#3.	Stable.
TR33.900	Guide to 3G security	S3	Charles Brookson (UK DTI).	Approval at SA#6 planned.	Draft presented at S3#6.
TR33.901	Criteria for cryptographic algorithm design process	S3	Rolf Blom (Ericsson).	Approved at SA#4.	Stable.
TRxx.xxx	Formal analysis of security mechanisms	S3	Günther Horn (Siemens).	For approval at SA#5.	Additional analyses may be added.

3.3 Time plan

This time plan is a project plan, including the completion date of all the deliverables.

The plans are included in the attached Excel spreadsheet.

4 Release 00

Out of scope.

5 Change history

			Cha	ange histor	y
SA2 No.	TDoc. No.	CR. No.	Section affected	New version	Subject/Comments

6 Annex A: Scope of the security co-ordination ad-hoc group

This ad hoc group is intended to produce, maintain and monitor the work plan for the delivery of a consistent security specifications for release 99.

[Insert scope of the ad-hoc group (copy-paste from the overall project plan)]

The work items being progressed in TSG-S3 are listed in the table below. Each work item addresses a particular security issue and is assigned a particular priority which includes whether or not the feature or mechanism should be specified in Release 99. This table is an updated version of a table presented to TSG-S#4 in Tdoc SP-99284.

Table 2: Priorities of security work items assigned by TSG-S3

	Work item	Priority
1	User identity confidentiality	The specification of an enhanced mechanism to help guard against active attacks against user identity confidentiality on the radio interface is essential in R99. Note that only the transport mechanism needs to be specified. The exact mechanism to protect the user identity can be home operator dependant. The specification of algorithm requirements and interfaces is also essential for R99, although the algorithms themselves can be home operator dependant and do not need to be specified.
2	Authentication and key agreement	The specification of an enhanced mechanism to help guard against active attacks on the radio interface is essential for R99. Furthermore, the specification of algorithm requirements and interfaces is also essential for R99, although the algorithms themselves can be home operator dependant and do not need to be specified.
3	Access link integrity protection	This is a new security mechanism in UMTS introduced to help guard against active attacks on the radio interface. The specification of the message authentication mechanism is essential in R99.
4	Access link confidentiality	The GSM ciphering mechanism cannot be used in the new access network and the GSM algorithms are unsuitable. The specification of a new ciphering mechanism and algorithm is essential in R99.
6	Secure GSM-UMTS interoperation.	Owing to the requirements for both CS and PS 'handover' between UMTS and GSM and to the requirements to be able to perform roaming between GSM and UMTS networks, for all these items, dual mode UMTS/GSM operational aspects need to be specified in R99.
7	Network-wide encryption	Appropriate 'hooks' must be provided in the R99 specification so that network-wide encryption can be introduced in later releases. It may be possible to re-use the algorithm for ciphering in the UTRAN. If a new algorithm is required then its specification can be left to later releases providing that appropriate 'hooks' are incorporated into the R99 specification.
8	User equipment identification	TSG-SA have recommended that TSG-S3 specify a secure mechanism in R99. The mechanism will require manufacturers to secure terminal identities and associated authentication data.
9	Core network signalling security	Although this is a high priority item, it is recognised that implementable specifications might not be achievable in R99. A cipher algorithm designed by ETSI SAGE for this purpose called BEANO is already available. Off-the-shelf algorithms are likely to be suitable for the message authentication functions.
10	Fraud information	The GSM mechanism can be used. Enhancements will be considered in later

	gathering system	releases.
11	USIM application security	The GSM mechanisms can be used. Enhancements will be considered in later releases.
12	Visibility and configurability	An encryption indicator should be included in R99. Other items are of lower priority and will be considered in later releases.
13	Mobile Execution Environment Security	The GSM mechanisms will be enhanced in R99.
14	Location services	Specification of privacy mechanism is essential in R99. Can be largely based on GSM Location Services privacy mechanisms.
15	Lawful interception architecture	The specification of a lawful interception architecture is essential in R99. This architecture can be largely based on the GSM/GPRS architecture.
16	IP security	Some support for mobile IP has been added to R99 at a late stage. There will be security issues but it may be difficult to address these in any substantial way in R99 because of time constraints. An outline specification or placeholder will be included in the R99 security architecture. Detailed specification of appropriate security features will probably have to wait until R00.

7 Annex B: Contact person

Group	Contact person*	Email
S2	Chris Pudney	Chris.Pudney@vf.vodafone.co.uk
S3	Peter Howard	Peter.Howard@vf.vodafone.co.uk
T2	Kevin Holley	Kevin.Holley@bt.com
T3	Klaus Vedder*	Klaus.Vedder@gdm.de
	Still to nominate	-
R2	Jukku Vialen	Jukka.Vialen@RESEARCH.NOKIA.COM
R3	Atte Länsisalmi	Atte.Lansisalmi@nokia.com
N1	Hannu Heitalahati	Hannu.Hietalahti@NOKIA.COM
N2	Ian Park	Ian.Park@vf.vodafone.co.uk
N3	Norbert Klehn	Norbert.Klehn@icn.siemens.de
N-SS	Steffen Habermann*	Steffen.Habermann@t-mobil.de
	Still to nominate	
UMTS-GSM	Francois Courau	Francois.courau@alcatel.fr
interoperation		
coordination		
group		

^{*}Where no contact person is nominated the chair man of the group is contact person

Project plan for security features R99

attached to SP-99395

User Identity Confidentiality

•		•		1999									1999																		2000		
													1999								2000										2000		
	<u>gust</u>		<u>Septe</u>				Octob				Nover				<u>Dece</u>				Janua			<u>Febru</u>	•			March	_			<u>April</u>			
	-20 2327	303	610	13-17	2024	271	48		1822	2529 15	812	1519	2226	293 610		2024	2731	37	1014	1721	2428	314	711	1418	2125	283			2024	2731	37	1014	1721
TSG SA								xxx00							00xxx													00xxx					
WG2	xxxxx			XXXXX						xxxxx				xxxxx																			
Feasibility study						circulate	e by en	nail		complete feasi	bility stu	dy																					
CR to 23.121										first draft CR				complete CR						correct (
CR to 23.060										first draft CR				complete CR						correct (CR												
WG3						00xxx				0xxx0		0xxxx		0xxx0						00xxx					0xxx0							0xxx0	
33.102 out	ine spec									complete spec				correc	t spec																		
TSG RAN							00xxx								xxx00																		
WG2 xx	XXX				xxxx0					0xxxx				xxxxx																			
RRC specification, layer 3											asibility s	study		first dra						complet			_		correct	CR							
WG3	XXXXX	l,			xxxxx					XXXXX				xxxxx						-	XXXX												
Assess feasibility study for im														Assess	feasibilit	y study				f	irst dra	ft CRs	_		comple	ete CRs				correct	CRs		
TSG CN		00xxx					00xxx								xxx00																		
WG1 xx	XXX				0xxx0					xxxxx				xxxxx					0xxxx	0.00													
CR to 24.008 MM														Read feasibility					first dra				compl					correct					
CR to 24.008 GMM														Read feasibility					first dra				comple					correct					
CR to 03.22														Read feasibility					first dra				comple					correct					
CR to 29.018														Read feasibility	study				first dra				compl	ete CR				correct	CR				
WG2				xxxxx								XXXXX								xxxxx													
CR to 29.002 for VLR													asibility							first draft				comple				correct					
CR to 29.002 for SGSN													asibility	,						first draft first draft				comple				correct					
CR to 23.018												Read te	asibility											comple	ete CR			correct	CR				
WG3 (not concerned)				xxxxx					XXXXX					xxxxx						, ,	XXXX												
TSG T	xxxx0						000xx								xxx00																		
WG1 (not concerned)	xxxx0						UUUXX							000xx																			
WG1 (not concerned)							xxx00						xxxxx	UUUXX								xxxxx											
WG2 (flot concerned) WG3							xxx00			0xxx0			AAXXX	00xxx								****											
CR to 31.102							AAAUU				asibility s	study		first dra							comple	ete CR				correct	CR						
CR to 31.102			1	1	1			l		read le	asionity S	мачу	1	inst ure	un OR	1			1	1 1	omple	ore or	1	I	1	Conect	UK.	I	l				

Authentication and key agreement

and

Access Link Integrity Protection

and

Access Link Confidentiality

and

anu																																			
Secure GSM-UM1	S inte	erope	ratio	n		1999									1999									2000										2000	
	Augus	et .		Septe	mher			Octob	er				Nover	mher				Decen	nher			Janua	arv		Februa	ırv			March	,			April		
	_					20-24	271			10_22	2520				22.26	202				2721				24_20			1410	21_25			12_17			27	1014 1721
TSG SA	1020	2321	303	010	13-17	2024	271	46	xxx00	1022	25-25	13	012	1319	2220	293		00xxx	2024	2731	37	1014	1721	2426	314	711	1418	2123	20-3		00xxx	2024	2731	3,	1014 1721
WG2		xxxxx			xxxxx				AAAOO		xxxxx					xxxxx		OUAAA													OOXXX				
CR to 23.060		AAAAA			AAAAA						first dra	aft				complet	e CR				correc	t CR													
WG3							00xxx				0xxx0	-		0xxxx			0xxx0						00xxx					0xxx0							0xxx0
33.102, authentication		outline	spec				compl	lete spec						correct	spec																			$\overline{}$	
33.102, integrity		outline	spec				compl	lete spec	-					correct	spec																				
33.102, confidentiality		outline	spec				compl	lete spec						correct	spec																				
33.102, interoperation		principle	s establish	ed			outline	spec			add PS	domain		complet	te spec	c	correct	spec																	
TSG RAN								00xxx										xxx00																	
	xxxxx					xxxx0						0xxxx				х	XXXX																		
25.301						draft te:	ĸt					text cor	npleted			te	ext cor	rrected																	
25.321 (MAC)						draft te:						text cor	npleted					rrected																	
25.322 (RLC)						draft te:						text cor						rrected																	
25.331 (RRC)						draft te:	ĸt					text cor	npleted					rrected																	
WG3		xxxxx				xxxxx					xxxxx						XXXX							xxxxx											
25.413 (RANAP)						draft te:	ĸt				text co	mpleted				te		rrected																	
TSG CN			00ххх					00xxx										xxx00																	
	xxxxx					0xxx0					xxxxx					XXXXX						0xxxx													
CR to 24.008 MM											first dra					complet						correc													
CR to 24.008 GMN											first dra					complet						correc													
CR to 29.008											first dra					complet						correc													
CR to 29.060 WG2											first dra	iπ				complet	еск					correc													
CR to 29.002 for VLF					first dra									comple	to CD								correct	L CD											
CR to 29.002 for SGSN	_				first dra									comple									correc												
TSG T					ilist ura	111		000xx						comple	ie Ck			xxx00					conec	ICK											
WG1 (not concerned)								UUUAA								0	000xx	******																	
WG2 (not concerned)								xxx00							xxxxx		JOOKK																		
(i.o. co.icemed,								- IAAOO																											
WG3		xxxx0						xxx00				0xxx0				0	00xxx								xxxxx										
CR to 31.102								first dra	ft			comple	ete CR				correct	CR																	
ETSI SAGE								xxxxx										xxxxx																	
Spec of Integrity algorithm																		delivere	d																
Spec of confidentiality alg.																		delivere	:d																

Network Wide En	crypt	ion			1999										1999									2000										2000		
	Augus			Septe	mber			Octob	oer				Nove	mber				Decer	nber			Janua	irv		<u>Februa</u>	rv			March	1			April			
	_	2327			13-17	2024				1822	2529				2226	293				2731			•			-	1418				1317	2024	-	37	1014 17	-21
TSG SA									xxx00									00xxx													00xxx					
WG2		xxxxx			xxxxx						xxxxx					xxxxx																				
CR to 23.121																																				
CR to 23.060)																																			
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102, id of hooks	outline	spec									output I	.S					comple	ete spec					correct	spec												
TSG RAN								00xxx										00xxx																		
WG2	xxxxx					xxxx0						0xxxx					xxxxx																			
identify impacted specs												specs ic	dentified	I																						
do changes																	first dra	ıft			comple	ete CR														
WG3		xxxxx				xxxxx					xxxxx						xxxxx							xxxxx												
identify impacted specs	i										specs ic	dentified																								
do changes	:																first dra	ıft			comple	ete CR														
TSG CN			00ххх					00xxx			0xxx0							xxx00																		
	xxxxx					0xxx0					xxxxx					xxxxx						0xxxx														
identify impacted specs	:										specs io	dentified																								
do changes																first draf	t					comple	ete CR													
WG2					xxxxx									xxxxx									XXXXX													
identify impacted specs														specs i	dentified																					
do changes																							first dra	ft			comple	ete CR								
WG3					xxxxx					xxxxx						XXXXX								XXXXX												
identify impacted specs																specs id	entified																			
do changes																			first draf	ft				comple	ete CR											
TSG T								00xxx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2 (not concerned)								xxx00							xxxxx										xxxxx											
WG3		хххх0						ххх00				0xxx0					00xxx																			
changes to 31,102	:												identify	if char	nges are	needed																1				

User Equipment	Ident	tificati	on		1999										1999									2000										2000		
	Augi	<u>ust</u>		Sep	otember			<u>Octob</u>	<u>oer</u>				Nove	mber				Decer	nber			Janua	ry		<u>Februa</u>	ary			Marcl	<u>1</u>			<u>April</u>			
	162	0 2327	303	61	10 13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014	1721
TSG SA									xxx00									xxx00													00xxx					
WG2 (not concerne	d)	xxxxx			xxxxx						xxxxx					xxxxx																				
Wo							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.1	02										outline	spec					comple	ete spec					correct	CR												
TSG CN			00xxx					00xxx										xxx00																		
	31 xxxx	х				0xxx0					xxxxx					xxxxx						0xxxx														
CR to 24.008 N	M										first dra	ft CR				comple	ete CR					correct	CR													
CR to 24.008 GM											first dra	ft CR				comple	ete CR					correct	CR													
Wo	G2				xxxxx									xxxxx									XXXXX													
CR to 29.002 for V														first dra	aft CR								comple	te CR			correc	t CR							<u> </u>	
CR to 29.002 for SG:	SN													first dra	aft CR								comple	te CR			correc	t CR								
TSG T								000xx										xxx00																		
WG	i1																000xx																			
development of te	est																			f	irst draft	t CR												ļ ļ		
We	G2							ххх00							xxxxx										xxxxx											
terminal authentication ca	oabilities																																			
WG3 (not concerne	d)	xxxx0						ххх00				0xxx0					00xxx																			

Core Network Si	gnalli	ng Se	curity	y 1	999										1999									2000										2000		
	Augu	<u>st</u>		Septem	ber			Octob	<u>oer</u>				Nove	mber				Decer	nber			<u>Janua</u>	ıry		<u>Februa</u>	ıry			March	<u>1</u>			<u>April</u>			
	1620	2327	303	610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014	1721
TSG SA									xxx00									00xxx													00xxx					
WG	3						00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102, MAP securi	ty outline	spec					comple	ete spec						correct	spec																					
33.102, CAP/INAP securi	ty										outline	spec					comple	ete spec					correct	spec												
33.102, GTP securi	ty										outline	spec with	MAP/IF	P for R00	in mind		comple	ete spec	:				correct	spec												
TSG CN			00xxx					00xxx										xxx00																		
WG	2			х	xxxx									xxxxx									xxxxx													
CR to 29.00)2																						first dra	ft CR												
SAGE																																				
delivery of algorith	m BEANO	availabl	е																																	

Fraud Information	n Gat	herin	g Ser	vice	1999										1999									2000										2000		
	Augus	st		Septe	mber			Octo	oer				Nove	mber				Dece	mber			Janua	ıry		Febru	ary			March	1			April			
	1620	2327	303	610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014 1	1721
TSG SA									00xxx									00xxx													00xxx					
WG	3						00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
	same a	s GSM									support	for PS se	ssion																							
TSG CN			00xxx					00xxx										xxx00																		
WG	2				xxxxx									xxxxx									xxxxx													
procedures for SGSN side	in 23.078				draft C	R								comple	ete CR								correct	CR												
procedures for SGSN side	in 29.078				draft C	R								comple	ete CR								correct	CR												

USIM applicat	ion sec	urity			1999										1999									2000										2000		
	<u>Aug</u>	<u>ust</u>		Septe	mber			Octob	<u>oer</u>				Nove	mber				Dece	mber			Janua	iry		Februa	ary			Marcl	<u>1</u>			<u>April</u>			
	162	0 2327	303	610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014	1721
TSG SA									xxx00									00xxx													00xxx					
	WG3						00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
	spec	in GSM 03	.48								create 3	GPP spe	ec																							
TSG T								000xx										xxx00																		
	WG3	xxxx0						xxx00				0xxx0					00xxx																			

Visability and cor	nfigura	ability	y		1999										1999									2000										2000		
	Augus	<u>t</u>		Septe	<u>mber</u>			Octob	<u>oer</u>				Nove	mber				Decer	nber			<u>Janua</u>	ry		Februa	ary			March	1			<u>April</u>			
	1620	2327	303	610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014	1721
TSG SA									xxx00									xxx00													00xxx					
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102											outline s	spec		comple	te spec								correct	spec												
TSG T								000xx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2								xxx00							xxxxx										xxxxx											
Terminal capabilities																																				
WG3		хххх0						xxx00				0xxx0					00xxx																			
Control parameters on USIN	1, CR to 3	31.102																																		

MeXE							1999					2000												2000											
	August		Septe	mber			Octob	oer				Nove	mber				Dece	mber			Janua	у		Februa	ary			March	1			April			
	1620 232	7 303	610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014	1721
TSG SA								xxx00									00xxx													00xxx					
WG:	3					00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
review 23.05	7									review I	MExE sed	curity an	d send L	S to MExE																					
TSG T							000xx										xxx00																		
WG1 (not concerned)															000xx																			
WG:	2						xxx00							xxxxx										xxxxx											
terminal capabilitie	s																																		
WG2 MExE subgroup	D						xxx00							xxxxx										xxxxx											
23.05																																			
WG:	3 xxxx0						xxx00				0xxx0					00xxx																			
Security functions on USIM			1																																

Location Services	ocation Services (Security aspects) 1999										1999											2000												2000				
	<u>August</u> <u>Septem</u> 16-20 23-27 30-3 6-10							Octob	<u>oer</u>				Noven	<u>nber</u>				Decer	mber			<u>Janua</u>	ry		<u>Februa</u>	ry			March	1			<u>April</u>					
	1620	2327	303	610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293			2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014 1721			
TSG SA									xxx00									00xxx													00xxx							
WG2		xxxxx			XXXXX						XXXXX					xxxxx																						
MOS							00				0 0			•			0xxx0						00					00							00			
WG3							00xxx				0xxx0			0xxxx			UXXXU						00xxx					0xxx0							0xxx0			
TSG RAN								00xxx										xxx00																				
WG1 (not concerned)																																						
WG2 (not concerned)	xxxxx					0xxxx						0xxxx					xxxxx																					
WG3 (not concerned)		xxxxx				xxxxx					XXXXX						XXXXX							xxxxx														
MCA (not none of)																																						
WG4 (not concerned) ITU-AH (not concerned)																																						
TSG CN			00xxx					00xxx										xxx00																				
	xxxxx		JUANA			0xxx0		OUAAA			xxxxx					xxxxx		жжо				0xxxx																
Signalling for privacy contro	ol																																	-				
WG2					xxxxx									xxxxx									xxxxx															
CR to 29.002 for privacy co																																						
WG3 (not concerned)					XXXXX					xxxxx						xxxxx								xxxxx														
TOO T								000																														
TSG T								000xx									000	xxx00																				
WG1 (not concerned) WG2								xxx00							xxxxx		000xx								xxxxx													
MMI to control privacy								XXXUU							AAAXX										****													
WG3 (not concerned)		xxxx0						xxx00				0xxx0					00xxx																					
(not concerned)																	JUNAN																					

Lawful Interception archit	ecture	e	1999										1999									2000										2000		
August	Sept	ember			Octob				Nover	mber				Decer	mber			Janua	у		Februa	ary			March	1			April					
1620 23	7 303	3 610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014	1721
WG3					00xxx				0xxx0			0xxxx			0xxx0	00xxx					00xxx					0xxx0							0xxx0	
SMG10 WPD								0xxx0						00xxx																				
33.106, LI requirements approved spe	ec .								CR for a	pproval																								
33 107 LL architecture draft spec (based on GSM)									final dra	ft for an	nroval										correct	nec						1	1		i		1	

IP security	1999											1999										2000												2000					
	Aug	ust		Septe	mber			Octol	ber		<u>November</u> <u>December</u>											Janua	ary		<u>Februa</u>	ary			March	1			<u>April</u>						
		0 2327	303	610	13-17	2024	271	48	1115	1822	2529	15	812	1519	2226	293	610	1317	2024	2731	37	1014	1721	2428	314	711	1418	2125	283	610	1317	2024	2731	37	1014	1721			
TSG SA									xxx00									00xxx													00xxx								
W	G2	xxxxx			xxxxx						XXXXX					xxxxx																							
								upport fo	or mobile	IP in R99																													
	G3						00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0				
33.	102										present	ation fro	m S2				outline	spec or	placeh	older		_																	
TSG CN	-		00xxx					00xxx										xxx00																					
W	G1 xxxx	X				0xxx0					XXXXX					XXXXX						0xxxx																	
W	G2				xxxxx									xxxxx									xxxxx																
-																																							
TSG T								000xx										xxx00																					
WG1 (not concerne	ed)																000xx																						
WG2 (not concern	ed)							xxx00							xxxxx																								
W	IG3	xxxx0						xxx00				0xxx0					00xxx								xxxxx														