Technical Specification Group Services and System Aspects *TSGS#5(99)395*
Meeting #5, Kyongju, Korea, 11-13 October 1999

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)

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

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

		c) time synchronisation of encrypted IMSI between VPLMN and mobile.	
Authentication and key agreement			
Access link integrity protection		Architectural impact of separate CS/PS nodes Key establishment during intersystem handover	1: Outline description
Access link confidentiality		Architectural impact of separate CS/PS nodes Key establishment during intersystem handover	1: Outline description
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			

3.1.1.3 Work to be done by WG S3

Item	Specification required	Issues	Milestones
User identity confidentiality	Specification of enhanced mechanism.		1: Description available in 33.102
Authentication and key agreement	Specification of enhanced mechanism.	An enhancement to the GSM scheme based on the use of sequence numbers has been 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	1: Description available in 33.102 (fall-back scheme in Annex)

		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 confidentiality		Handling of paging with IMSI	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.	1: Outline description
Access link integrity protection	Specification of integrity functions in RAN (if UTRAN based).		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 ciphering functions in RAN MAC and RLC.		1: Outline description in 25.301 2: MCC provide draft R'99 spec 3: First corrections to errors in consolidated CRs
Secure UMTS-GSM interoperation			
Network-wide encryption	Specification of ciphering functions in RAN.	Must be possible to separate ciphering on user traffic and signalling information.	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			
Core network signalling security			
Fraud information gathering system			
USIM application security			
Visibility and configurability			
Mobile Execution			

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. 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

Secure UMTS-GSM interoperation			
Network-wide encryption	May involve modification to following RANAP messages: Cipher mode command Cipher mode complete Cipher mode reject May require new RANAP messages.	Must be possible to separate ciphering on user traffic and signalling information.	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			
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 confidentiality	Modification of GMM and MM Identity Response message to contain encrypted user identity. Modification of IMSI detach message.	Modification of all GMM and MM messages which carry IMSI?	1: First draft CR 2: CR approved by TSG 3: MCC provide draft R'99 spec 4: First corrections to errors in consolidated CRs
Authentication and key agreement	Modification of MM and GMM messages: Authentication request Authentication response Location updating request CM service request CM re-establishment request "Paging response"	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

	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 GMM) messages: Authentication request Authentication response Location updating request CM service request CM re-establishment request Paging response		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 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 required	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_Info 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 confidentiality			
Authentication and key agreement			
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			
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 identification	Specification of tests for checking the security of terminal identification and authentication information	Development of suitable test	
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			
User equipment identification	Specification of capabilities for terminal authentication.		
Core network signalling security			
Fraud information gathering system			
USIM application security			
Visibility and configurability	Specification of terminal capabilities		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
Mobile Execution Environment Security	Specification of terminal capabilities		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
Location services	MMI to influence 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			

3.1.4.3 Work to be done by WG T3

Item	Specification required	Issues	Milestones
User identity confidentiality	Specification of USIM interface to allow ME to request encrypted user identity	Means for the SIM to prevent transmission of the unencrypted IMSI over the radio interface.	1: First draft CR 2: CR approved by TSG 3: MCC provide draft R'99 spec 4: First corrections to errors in consolidated CRs
Authentication and key agreement	Specification of USIM interface to allow UE to request authentication and key agreement.		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	Specification of USIM interface to allow UE to request generation/verification of integrity protected messages (if integrity is terminated on USIM)	Integrity termination on USIM believed to be feasible if only a few messages are protected.	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			
Secure UMTS-GSM interoperation			
Network-wide encryption	Specification of USIM interface for network-wide encryption.		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			
Core network signalling security			
Fraud information gathering system			
USIM application security	Specification of security message formats and security functionality required on USIM.		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
Visibility and configurability	USIM control parameters		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
Mobile Execution Environment Security	Specification of security functionality on USIM.		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
Location services			
Lawful interception architecture			
IP security			

3.1.5 Work to be done by ETSI SAGE

Item	Specification required	Issues	Milestones

User identity confidentiality			
Authentication and key agreement			
Access link integrity protection	Specification of algorithm		Delivery of algorithm
Access link confidentiality	Specification of algorithm		Delivery of algorithm
Secure UMTS-GSM interoperation			
Network-wide encryption	Specification of algorithm (if different to cipher algorithm in RAN)		1: decision on same/different algorithm
User equipment identification			
Core network signalling security	Specification of algorithms.		Candidate cipher (BEANO) is available.
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**
TS21.133	Security threats and requirements	S3	Per Christoffersson (Telia Promotor).	Approved at 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

Change history					
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* Still to nominate	Klaus.Vedder@gdm.de
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* Still to nominate	Steffen.Habermann@t-mobil.de
UMTS-GSM interoperation coordination group	Francois Courau	Francois.courau@alcatel.fr

*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										2000			
	August			September				October					November					December			January			February				March				April				
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG2		xxxxx			xxxxx						xxxxx					xxxxx																				
Feasibility study							circulate by email				complete feasibility study																									
CR to 23.121											first draft CR					complete CR						correct CR														
CR to 23.060											first draft CR					complete CR						correct CR														
WG3							00xxx				0xxx0			0xxxx			0xxx0					00xxx					0xxx0							0xxx0		
33.102	outline spec										complete spec						correct spec																			
TSG RAN								00xxx										xxx00																		
WG2	xxxxx					xxxx0						0xxxx					xxxxx																			
RRC specification, layer 3												Read feasibility study					first draft CR					complete CR					correct CR									
WG3		xxxxx				xxxxx					xxxxx						xxxxx						xxxxx													
Assess feasibility study for impact (if any)																	Assess feasibility study						first draft CRs				complete CRs					correct CRs				
TSG CN			00xxx					00xxx										xxx00																		
WG1	xxxxx					0xxx0					xxxxx					xxxxx					0xxxx															
CR to 24.008 MM																Read feasibility study					first draft CR				complete CR					correct CR						
CR to 24.008 GMM																Read feasibility study					first draft CR				complete CR					correct CR						
CR to 03.22																Read feasibility study					first draft CR				complete CR					correct CR						
CR to 29.018																Read feasibility study					first draft CR				complete CR					correct CR						
WG2					xxxxx									xxxxx								xxxxx														
CR to 29.002 for VLR														Read feasibility study								first draft CR				complete CR				correct CR						
CR to 29.002 for SGSN														Read feasibility study								first draft CR				complete CR				correct CR						
CR to 23.018														Read feasibility study								first draft CR				complete CR				correct CR						
WG3 (not concerned)					xxxxx					xxxxx						xxxxx							xxxxx													
TSG T		xxxx0						000xx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2 (not concerned)								xxx00							xxxxx									xxxxx												
WG3								xxx00				0xxx0					00xxx																			
CR to 31.102												Read feasibility study					first draft CR					complete CR							correct CR								

X = MEETING DAY

Authentication and key agreement

and

Access Link Integrity Protection

and

Access Link Confidentiality

and

Secure GSM-UMTS interoperation

						1999									1999									2000										2000		
	August			September				October				November						December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG2		xxxxx			xxxxx						xxxxx					xxxxx																				
CR to 23.060											first draft					complete CR					correct CR															
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102, authentication		outline spec					complete spec							correct spec																						
33.102, integrity		outline spec					complete spec							correct spec																						
33.102, confidentiality		outline spec					complete spec							correct spec																						
33.102, interoperation		principles established					outline spec				add PS domain			complete spec			correct spec																			
TSG RAN								00xxx										xxx00																		
WG2	xxxxx					xxxx0						0xxxx					xxxxx																			
25.301						draft text						text completed					text corrected																			
25.321 (MAC)						draft text						text completed					text corrected																			
25.322 (RLC)						draft text						text completed					text corrected																			
25.331 (RRC)						draft text						text completed					text corrected																			
WG3		xxxxx				xxxxx					xxxxx						xxxxx							xxxxx												
25.413 (RANAP)						draft text					text completed						text corrected																			
TSG CN			00xxx					00xxx										xxx00																		
WG1	xxxxx					0xxx0					xxxxx					xxxxx						0xxxx														
CR to 24.008 MM											first draft					complete CR						correct CR														
CR to 24.008 GMM											first draft					complete CR						correct CR														
CR to 29.008											first draft					complete CR						correct CR														
CR to 29.060											first draft					complete CR						correct CR														
WG2					xxxxx									xxxxx									xxxxx													
CR to 29.002 for VLR					first draft									complete CR									correct CR													
CR to 29.002 for SGSN					first draft									complete CR									correct CR													
TSG T								000xx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2 (not concerned)								xxx00							xxxxx																					
WG3		xxxx0						xxx00				0xxx0					00xxx								xxxxx											
CR to 31.102								first draft				complete CR					correct CR																			
ETSI SAGE								xxxxx										xxxxx																		
Spec of Integrity algorithm																		delivered																		
Spec of confidentiality alg.																		delivered																		

X = MEETING DAY

Network Wide Encryption					1999										1999									2000										2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	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 LS						complete spec						correct spec													
TSG RAN								00xxx										xxx00																		
WG2	xxxxx					xxxx0						0xxxx					xxxxx																			
identify impacted specs												specs identified																								
do changes																	first draft				complete CR															
WG3		xxxxx				xxxxx					xxxxx						xxxxx							xxxxx												
identify impacted specs											specs identified																									
do changes																	first draft				complete CR															
TSG CN			00xxx					00xxx			0xxx0							xxx00																		
WG1	xxxxx					0xxx0					xxxxx					xxxxx						0xxxx														
identify impacted specs											specs identified																									
do changes																first draft						complete CR														
WG2					xxxxx									xxxxx									xxxxx													
identify impacted specs														specs identified																						
do changes																							first draft				complete CR									
WG3					xxxxx					xxxxx						xxxxx								xxxxx												
identify impacted specs																specs identified																				
do changes																			first draft					complete CR												
TSG T								00xxx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2 (not concerned)								xxx00							xxxxx										xxxxx											
WG3		xxxx0						xxx00				0xxx0					00xxx																			
changes to 31.102													identify if changes are needed																							

User Equipment Identification

					1999										1999									2000										2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG2 (not concerned)		xxxxx			xxxxx						xxxxx					xxxxx																				
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102											outline spec						complete spec						correct CR													
TSG CN			00xxx					00xxx										xxx00																		
WG1	xxxxx					0xxx0					xxxxx					xxxxx						0xxxx														
CR to 24.008 MM											first draft CR					complete CR						correct CR														
CR to 24.008 GMM											first draft CR					complete CR						correct CR														
WG2					xxxxx									xxxxx									xxxxx													
CR to 29.002 for VLR														first draft CR									complete CR				correct CR									
CR to 29.002 for SGSN														first draft CR									complete CR				correct CR									
TSG T								000xx										xxx00																		
WG1																	000xx																			
development of test																					first draft CR															
WG2								xxx00							xxxxx										xxxxx											
terminal authentication capabilities																																				
WG3 (not concerned)		xxxx0						xxx00				0xxx0					00xxx																			

Core Network Signalling Security

					1999										1999									2000										2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102, MAP security	outline spec						complete spec							correct spec																						
33.102, CAP/INAP security											outline spec						complete spec						correct spec													
33.102, GTP security											outline spec with MAP/IP for R00 in mind						complete spec						correct spec													
TSG CN			00xxx					00xxx										xxx00																		
WG2					xxxxx									xxxxx									xxxxx													
CR to 29.002																							first draft CR													
SAGE																																				
delivery of algorithm	BEANO available																																			

Fraud Information Gathering Service

					1999										1999									2000										2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
	same as GSM										support for PS session																									
TSG CN			00xxx					00xxx										xxx00																		
WG2					xxxxx									xxxxx									xxxxx													
procedures for SGSN side in 23.078					draft CR									complete CR									correct CR													
procedures for SGSN side in 29.078					draft CR									complete CR									correct CR													

USIM application security

					1999										1999								2000											2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
	spec in GSM 03.48									create 3GPP spec																									
TSG T								000xx										xxx00																		
WG3		xxxx0						xxx00				0xxx0					00xxx																			

Visability and configurability

					1999										1999								2000											2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102										outline spec			complete spec									correct spec													
TSG T								000xx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2								xxx00							xxxxx										xxxxx											
Terminal capabilities																																				
WG3		xxxx0						xxx00				0xxx0					00xxx																			
Control parameters on USIM, CR to 31.102																																				

MeXE

					1999										1999								2000											2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
review 23.057										review MExE security and send LS to MExE																									
TSG T								000xx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2								xxx00							xxxxx										xxxxx											
terminal capabilities																																				
WG2 MExE subgroup								xxx00							xxxxx										xxxxx											
23.057																																				
WG3		xxxx0						xxx00				0xxx0					00xxx																			
Security functions on USIM																																				

X = MEETING DAY

Location Services (Security aspects) 1999 1999 2000 2000

	August			September				October					November					December				January			February				March				April		
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG2		xxxxx			xxxxx						xxxxx					xxxxx																				
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
TSG RAN								00xxx										xxx00																		
WG1 (not concerned)																																				
WG2 (not concerned)	xxxxx					xxxx0						0xxxx					xxxxx																			
WG3 (not concerned)		xxxxx				xxxxx					xxxxx						xxxxx							xxxxx												
WG4 (not concerned)																																				
ITU-AH (not concerned)																																				
TSG CN			00xxx					00xxx										xxx00																		
WG1	xxxxx					0xxx0					xxxxx					xxxxx						0xxxx														
Signalling for privacy control																																				
WG2					xxxxx									xxxxx									xxxxx													
CR to 29.002 for privacy control																																				
WG3 (not concerned)					xxxxx					xxxxx						xxxxx								xxxxx												
TSG T								000xx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2								xxx00							xxxxx										xxxxx											
MMI to control privacy																																				
WG3 (not concerned)		xxxx0						xxx00				0xxx0					00xxx																			

Lawful Interception architecture 1999 1999 2000 2000

	August			September				October					November					December				January			February				March				April		
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
WG3							00xxx				0xxx0			0xxxx			0xxx0	00xxx					00xxx					0xxx0							0xxx0	
SMG10 WPD										0xxx0						00xxx																				
33.106, LI requirements	approved spec										CR for approval																									
33.107, LI architecture	draft spec (based on GSM)										final draft for approval												correct spec													

IP security

						1999									1999									2000										2000		
	August			September				October					November					December				January			February				March				April			
	16--20	23--27	30--3	6--10	13-17	20--24	27--1	4--8	11--15	18--22	25--29	1--5	8--12	15--19	22--26	29--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21	24--28	31--4	7--11	14--18	21--25	28--3	6--10	13--17	20--24	27--31	3--7	10--14	17--21
TSG SA									xxx00									00xxx													00xxx					
WG2		xxxxx			xxxxx						xxxxx					xxxxx																				
							some support for mobile IP in R99																													
WG3							00xxx				0xxx0			0xxxx			0xxx0						00xxx					0xxx0							0xxx0	
33.102											presentation from S2						outline spec or placeholder																			
TSG CN			00xxx					00xxx										xxx00																		
WG1	xxxxx					0xxx0					xxxxx					xxxxx						0xxxx														
WG2					xxxxx									xxxxx									xxxxx													
TSG T								000xx										xxx00																		
WG1 (not concerned)																	000xx																			
WG2 (not concerned)								xxx00							xxxxx																					
WG3		xxxx0						xxx00				0xxx0					00xxx								xxxxx											