3GPP TSG-S2
Tokyo, Japan, 6-9/3/2000

Tdoc S2-000620
***Rev of** Tdoc S2-000461*

3G PD 30.810 v1.2.1 (2000-03)

S3-000245

Permanent Document

3rd Generation Partnership Project
3GPP work program
Project co-ordination aspects
Project Plan for Security
(3G PD 30.810 version 1.2.1)

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	Open issues	Milestones
User identity confidentiality	Stage 2 description	Probably, not all issues have yet been discovered. Current issues are : a) this is an HE feature, but what changes are mandatory in all VPLMNs***?All VPLMNs seem to need to support the handling of new ID types in MM, GMM and RANAP and the handling of the***	1: Feasibility study: Still needed. 2: First draft CR 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs

		MAP signalling to obtain the real IMSI b) Handling of paging with IMSI/VLR restart conditions c) what happens when VPLMN does not allocate a TMSI? d) handling GSM radio access network	
Authentication and key agreement		23.060 CR for notification of authentication failure to HE.	
Access link integrity protection			
Access link confidentiality			
Secure UMTS-GSM interoperation		Cipher and integrity key handling in non-anchor MSC?	
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	Open issues	Milestones
User identity confidentiality	Specification of enhanced mechanism.		1: Description available in 33.102
Authentication and key agreement		Notification of authentication failure to HE. The behaviour of the mobile when it detects a “bad network” needs to be defined carefully.	
Access link integrity protection			

Access link confidentiality			
Secure UMTS-GSM interoperation			
Network-wide encryption			1: Identification of 'hooks'
User equipment identification	Postponed from R'99		
Core network signalling security	Specification of mechanism and key management architecture.	'Profile' of IPsec needs to be produced for GTP security.	1: Specification of IPsec 'profile' in 33.102 (by SA#8).
Fraud information gathering system	Specification of mechanism		As per GSM
USIM application security	Specification of mechanism		1: GSM 03.48 to be transferred into a 3GPP specification
Visibility and configurability	Specification of mechanism		1: Outline description
Mobile Execution Environment Security	Specification of mechanism		As per GSM
Location services	Specification of mechanism	Need to identify responsibilities in other groups	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

Core Network Signalling Security: S3 have requested S5 to work on a standardised means for distributing the keys needed for this feature.

Note that, for S5, R'99 probably first finishes at SA#8.

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	Open issues	Milestones
User identity confidentiality		UMTS RACH messages only have a payload of 20 octets. The "encrypted IMSI and UDIN" is longer than this. Handling of paging with "variable length 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

		Assumes DRX period is defined by the "real IMSI" and not the "encrypted IMSI" (however this may give information on the [3] Least Significant Digits of the IMSI).	
Authentication and key agreement			
Access link integrity protection	Specification of integrity functions in RAN (if UTRAN based).	Finalisation of the definition of what RRC signalling is integrity protected. Provision of an integrity protected Handover Complete Ack?	Ongoing work. Complete by June '00
Access link confidentiality	Specification of ciphering functions in RAN MAC and RLC.	Assumed to be complete.	
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	Integration of mechanism (for handling encrypted assistance data) in RAN specifications Postpone this issue, along with much of LCS, to R'00?		
Lawful interception architecture			
IP security			

3.1.2.3 Work to be done by WG R3

Item	Specification required	Open issues	Milestones
User identity confidentiality		Assuming that RANAP connections are identified by the 'real IMSI', paging messages	2: First draft CR (still to be provided) 3: CR approved by TSG

		need to be modified to be able to also carry the 'encyrpted IMSI'. (This is, at least, for paging coordination in the RNC for "class A" UMTS mobiles)	4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
Authentication and key agreement		Handling of issues arising from 2 core network nodes: Handover between RNC and BSC in a non-anchor MSC?	
Access link integrity protection		Handling of integrity key(s) at handover/relocation between RNC and BSC in a non-anchor MSC?	
Access link confidentiality		Handling of cipher keys at intersystem handover, between RNC and BSC in a non-anchor MSC?	
Secure UMTS-GSM interoperation			
Network-wide encryption	May involve modification or new RANAP messages: any RANAP changes will be part of R'00.		2: S3 to review hooks after RAN plenary, 12/99.
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	Open 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 required. Specification of new identity type required. Handling of different RATs if EUIC is not applied to GSM.	1: CR- still to be agreed by N1: guidance from S1 and S3 requested. 2: CR approved by TSG 3: MCC provide draft R'99 spec 4: First corrections to errors in consolidated CRs
Authentication and key agreement		Open issue: what does the mobile do when it detects a 'bad' network: current proposal to treat the 'bad cell' as barred is being studied. Must be solved in R'99.	Final CRs at CN#8.
Access link integrity protection		Identification of messages which shall be integrity protected and those messages which need not be integrity protected: this is believed to be basically complete. FFS is the handling of emergency calls from (a) mobiles without SIM and (b) unregistered mobiles with a SIM. This must be solved in R'99.	Final CRs at CN#8.
Access link confidentiality		Any changes needed to 29.008?	1: Outline description 2: First draft CR: waiting for finalisation of changes in RAN3/SMG2. 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	Detailed work on full solution is part of R'00.		2: S3 to review hooks after CN plenary, 12/99.
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			

3.1.3.2 Work to be done by WG N2

Item	Specification required	Open issues	Milestones
User identity confidentiality	Modification of MAP Send Authentication Info to contain encrypted user identity.	Handling of UMTS-VLR restart. Handling of VLR restart when VLR serves both GSM and UMTS cells.	2: First CR: not yet agreed. 3: CR approved by TSG 4: MCC provide draft R'99 spec 5: First corrections to errors in consolidated CRs
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 are part of R'00		2: S3 to review hooks after CN plenary, 12/99.
User equipment identification			
Core network signalling security	Integration of ciphering and integrity protection in certain MAP signalling messages. Protection of GTP messages carrying Authentication vectors.	MAP: CRs under preparation. An evolvable solution is being developed by N2 for CN#8. This is deemed preferable by many companies in N2 to a "hard to evolve, quick fix" for CN#7. GTP: CR to 29.060 drafted referencing IPsec. LS sent to S3 requesting S3 to 'profile' IPsec.	CN#7 and SA#7 to decide whether to accept the delay of this work to CN#8.
Fraud information gathering system	Specification of CAMEL procedures including those on the PS side.		Part of CAMEL phase 3: on schedule for R'99.
USIM application security			
Visibility and configurability			
Mobile Execution			

Environment Security			
Location services	Signalling to transfer privacy settings	Work being handled by T1P1.5	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	Open 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 are part of R'00.		2: S3 to review hooks after CN plenary, 12/99.
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	Open 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	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	Open 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			
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	Open 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. ***Resolved*** ***[how? - dual mode GSM handset will send it. UMTS MS may need some of the IMSI to calculate when it will be paged?]***	1: First draft CR (progress unknown) 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.	Current RAT indicated to SIM by MS?	1: Outline description 2: First draft CR 3: CR approved by TSG (on schedule for T plenary 12/99) 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 USIM interface for network-wide encryption.	R'99 mobile should support this?	2: S3 to URGENTLY review hooks after T plenary, 12/99.
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: Transfer 03.48 to 3GPP.
Visibility and configurability	USIM control parameters		1: Outline description 2: First draft CR 3: CR approved by TSG [probably on track for T plenary, 12/99]. 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.	Handled within SMG by SMG 9 ?	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	Open 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 expected at SA#6 to clarify security requirements relating to integrity protection of user traffic.
TS33.102	Security architecture	S3	Bart Vinck (Siemens Atea), Stefan Pütz (T-Mobil).	Approved at SA#3. 11 CRs approved at SA#4. 10 CRs approved at SA#5.	CRs expected at SA#6.
TS33.103	Integration guidelines	S3	Colin Blanchard (BT).	Approved at SA#5.	CRs expected at SA#6 some of which will be to align with CRs to architecture specification.
TS33.105	Cryptographic algorithm requirements	S3	Takeshi Chikazawa (Mitsubishi).	Approved at SA#4. 3 CRs approved at SA#5.	CRs expected at SA#6.

TS33.106	Lawful interception requirements	S3	Berthold Wilhelm (RegTP).	Approved at TSG-SA #4.	CR expected at SA#6.
TS33.107	Lawful interception architecture and functions	S3	Berthold Wilhelm (RegTP).	Approval at SA#6 planned.	On course 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.	On course for approval at SA#5.
TR33.901	Criteria for cryptographic algorithm design process	S3	Rolf Blom (Ericsson).	Approved at SA#4.	Stable.
TR33.902	Formal analysis of security mechanisms	S3	Günther Horn (Siemens).	Approved at SA#5.	CR expected at SA#6 to add extra analysis of security mechanisms.

3.3 Time plan

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

For earlier versions of this plan an Excel spreadsheet was attached.However, its relevance has diminished. Unresolved issues can be assumed to be behind schedule and can be treated on a case by case basis at the TSG plenary level.

3.4 Security review procedure

A procedure is established to ensure that security features specified by TSG-S3 are properly integrated into other R99 specifications. Under this procedure all specifications identified in the security workplan should be forwarded to TSG-S3 who will conduct a security review. The review will supplement the normal liaison and co-ordination activities which will exist during preparation of the specifications.

In general, when a particular work item identified in the project plan has reached the milestone when the final specifications are available, then the specifications should be forwarded to TSG-S3 for review. Once the review has been completed by TSG-S3, appropriate action will be taken to ensure that any security problems which may have been identified are resolved.

It will be necessary to flag up areas where the work to integrate security features into other specifications is behind schedule. In some cases, it might be necessary to start the review process prior to the final specifications becoming available so that overall timescales for R99 can be met. Milestones for the security review procedure are not explicitly identified in the time plan.

Release 00

Out of scope.

•

4 Change history

Change history					
SA2 No.	**Tdoc. No.**	**CR. No.**	**Section affected**	**New version**	**Subject/Comments**
11	00-0284			V1.1.0	Prepared for Mexico meeting
12	00-0461			V1.2.0	Prepared for Tokyo (Mitaka) meeting

5 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 set of consistent security specifications for release 99.

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. The working assumption is that the radio interface encryption algorithm will be re-used for network-wide encryption.
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 gathering system	The GSM mechanism can be used. Enhancements will be considered in later 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 new security features or profiling of existing IETF security features will probably have to wait until R00.

6 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	Duncan Mills	duncan.mills@vf.vodafone.co.uk
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