~~Tokyo, Japan, 6-9/3/2000~~

Rev of Tdoc S2-00-590

3G PD xx.sec v0.0.3 (2000-03)

Permanent Document

3rd Generation Partnership Project
3GPP work program
Project co-ordination aspects
DRAFT R2000 Project Plan for Security
(3G PD XX.sec version 0.0.3)

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 4
1 Scope 4
2 References 4
3 Release 2000 4
3.1 DRAFT R2000 Deliverables 4
3.1.1 Architectural deliverables 4
3.1.1.1 Access network security 5
3.1.1.2 Network-based end-to-end security 5
3.1.1.3 User plane protection in access network 5
3.1.1.4 Core network security 5
3.1.1.5 Termination of packet domain encryption in GSM BSC 5
3.1.1.6 GERAN access security 6
3.1.1.7 Enhanced User Identity Confidentiality 6
3.1.2.8 Ability of terminal/USIM to reject unencrypted calls 6
3.1.2 Other security deliverables 6
3.1.2.1 Use of IP security solutions 6
3.1.2.2 FIGS 6
3.1.2.3 Secure mobile platform for applications 6
3.1.2.4 OSA/VHE security 6
3.1.2.5 Visibility and configurability 7
3.1.2.6 Study on the evolution of GSM CS algorithms 7
3.1.2.7 Study on the evolution of GSM PS algorithms and the introduction of GEA2 7
3.1.2.8 “Mandatory” GPRS encryption 7
3.1.2.9 Lawful Interception in the R’2000 architecture 7
3.2 List of all the specifications under S3 control 7
3.3 Security review procedure 9
4 Change history 10
5 Annex A: Scope of the security co-ordination ad-hoc group 11
6 Annex B: Contact people 11

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.

[GSM work items are described in this document within square brackets.]

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 2000

3.1 DRAFT R2000 Deliverables

This list has been drafted by S3. It is a collection of security work items for R00 which will eventually be translated into a structured work programme in accordance with emerging R00 working methods. In particular, planning for security deliverables will be specified in terms of building blocks, features and work tasks. Detailed timeplans have not yet been specified. However, some indication is given on the expected project phases and external dependencies for some of the security deliverables.

Depending on the requirements of the R00 working methods, security deliverables will be created based on proposals from a required minimum number of named supporting companies. To help create appropriate lines of accountability, rapporteurs may need to be assigned to some security deliverables. Some of the larger security deliverables may require the creation of dedicated working groups which will be accountable to the main S3 plenary. It is expected that any new working groups will generally meet during S3 plenary meetings, although some ad hoc meetings may be necessary.

3.1.1 Architectural deliverables

A number of new architectural principles are introduced in R00 which will create new security challenges which must be addressed at a system-wide level. This will involve the evolution of the R99 security architecture and the introduction of new security features. A comprehensive programme of work will be required to ensure that the necessary security features are build into the system architecture. Security architecture work will be split into a number of deliverables each

of which will focus on work which is reasonably self-contained. However, it is expected that some dependencies will exist between deliverables. For each security deliverable, it is expected that the work will proceed in a number of distinct phases:

- Requirements capture
- Security feature specification
- Feasibility study (optional)
- Definition of security architecture
- Integration of security architecture

One characteristic of these work items is that they depend on the availability of well-defined and well understood system architecture concepts and principles.

An initial list of draft architectural deliverables is given in the sub-sections below.

3.1.1.1 Access network security

New security features will need to be introduced to secure access to the IP multimedia core network subsystem, e.g. authentication between users and new "gateway" nodes beyond the GGSN. Evolution and/or re-use of the existing R99 architecture for authentication and key agreement will need to be considered. Signalling between the mobile and nodes beyond the GGSN may well use the radio interface user plane Radio Access Bearers. This signalling is likely to need protection. Charging and accounting issues are also likely to be important here.

Work may involve: S2, S3, R2, R3, N1, N4, [SMG 2 WP A].

3.1.1.2 Network-based end-to-end security

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

Work may involve S2, S3, R2, R3, N1, N4, [SMG 2 WP A].

3.1.1.3 User plane protection in access network

The R00 system architecture may create new requirements and/or opportunities for introducing integrity protection for user plane data in R00. This may create opportunities for providing enhanced security, e.g. for e-commerce services. Issues such as the addition of integrity protection to voice over IP services may need to be investigated since it might lead to a degradation in voice quality (because a single bit error will lead to the voice packet failing its integrity check and thus being rejected).

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

3.1.1.4 Core network security

In the early releases of R00, a minimal solution will be developed to protect MAP signalling at the application layer. In future releases of the specifications it will be necessary to extend security to other interfaces and application protocols. Many of the interfaces and protocols requiring protection will be new to R00. Application to user plane traffic will be investigated. In addition interfaces towards and within the access network (Iu, A, Iur) will also be considered.

Work may involve S2, S3, N4.

3.1.1.5 Termination of packet domain encryption in GSM BSC

The recent decision to deploy an Iu-ps interface into the R00 GSM BSC means that, at least, encryption has to be moved into the BSC. There may be an opportunity to add integrity protection at the same time. Reuse or replacement of the existing GPRS algorithms has to be considered.

Work may involve S2, S3, N1, N4, SMG 2 WP A.

3.1.1.6 GERAN access security

Opportunities for enhancing GERAN access security will be investigated such as the extension of GSM cipher keys. Feasibility studies are likely to be required.

Work may involve S2, S3, N1, N4, SMG 2 WP A.

3.1.1.7 Enhanced User Identity Confidentiality

The GSM user identity confidentiality mechanism was not enhanced in R99. It may be required to develop security mechanisms to provide a greater degree of protection against loss of user identity and location confidentiality in R00 systems.

3.1.2.8 Ability of terminal/USIM to reject unencrypted calls

It has not been possible to enhance GPRS encryption in R97/98/99 such that the terminal/SIM can reject unencrypted calls primarily because it would have involved changes to N1 specifications which have been functionally frozen. This feature shall be considered for R00. Stage 2 specifications are currently being produced by S3. The R00 feature shall be generally applicable to 3GPP (not just GPRS). It shall be independent of the radio access system and whether the connection is PS or CS.

Work may involve S3, N1, T2, T3.

3.1.2 Other security deliverables

In contrast with the architectural deliverables, these items do not require so large a degree of system-wide design.

3.1.2.1 Use of IP security solutions

Security solutions in the IP domain may use Internet security solutions as their basis (e.g. IPsec). It is possible that ‘standardised profiles’ of Internet security solutions may need to be specified. Different applications might require different profiles.

This will probably not be a standalone [feature], rather it will be a [work task] within other [features].

Work may involve just S3.

3.1.2.2 FIGS

VoIP telephony, multimedia services and other data services may impose additional requirements on FIGS functionality, especially within the R00 PS side nodes.

Work may involve S2, S3, N2.

3.1.2.3 Secure mobile platform for applications

Mobile station applications based, for example on MExE and/or involving e-commerce will probably not be able to be fully contained within the (U)SIM. Mechanisms probably need to be standardised to ensure that these kinds of applications can be deployed, operated, upgraded and deleted in a secure manner. This work will essentially be an extension of the R99 MExE security work.

Work may involve S3, T2, T3.

3.1.2.4 OSA/VHE security

This work will essentially be an extension of the R99 OSA/VHE security work.

3.1.2.5 Visibility and configurability

This work will essentially be an extension of the R99 visibility and configurability of security features work.

3.1.2.6 Study on the evolution of GSM CS algorithms

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

Work may involve S3, N1, N4, SMG 2 WP A.

3.1.2.7 Study on the evolution of GSM PS algorithms and the introduction of GEA2

Since the first GSM-GPRS encryption algorithm (GEA 1) was developed, export restrictions have been relaxed and the stronger GEA 2 can now be deployed. This may be a late topic for R99: however the work will need to be carried out during the calendar year 2000.

Work may involve S3, N1, N4

3.1.2.8 "Mandatory" GPRS encryption

This is probably another pre-R2000 topic that needs to be addressed during the calendar year 2000.

Work may involve S3, N1.

3.1.2.9 Lawful Interception in the R'2000 architecture

The separation of user and control planes and the introduction of the real-time voice over IP services, multimedia services and other data services may require some additions to the existing standards.

Work may involve S2, S3, N4.

3.2 List of all the specifications under S3 control

The following list of S3 specifications will be refined as the work programme is elaborated. It is expected that the core specifications will be contained in a new R00 version on 33.102, but other specifications will also be required.

Recent deliverables such as 22.022 and the encryption and integrity algorithm documents have not yet been added.

Status of specifications					
Del #	**Title**	**Working Group**	**Editor**		**Comment**
TS21.133	Security threats and requirements	S3	Per Christoffersson (Telia Promotor).		
TS33.102	Security architecture	S3	Bart Vinck (Siemens Atea), Stefan Pütz (T-Mobil).		
TS33.103	Integration guidelines	S3	Colin Blanchard (BT).		
TS33.105	Cryptographic algorithm requirements	S3	Takeshi Chikazawa (Mitsubishi).		

TS33.106	Lawful interception requirements	S3	Berthold Wilhelm (RegTP).		
TS33.107	Lawful interception architecture and functions	S3	Berthold Wilhelm (RegTP).		
TS33.120	Security principles and objectives	S3	Timothy Wright (Vodafone).		
TR33.900	Guide to 3G security	S3	Charles Brookson (UK DTI).		
TR33.901	Criteria for cryptographic algorithm design process	S3	Rolf Blom (Ericsson).		
TR33.902	Formal analysis of security mechanisms	S3	Günther Horn (Siemens).		

3.2.1.1.1.1.1 Time plan

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

[The plans are (* not yet *) included in the attached Excel spreadsheet.]

3.3 Security review procedure

A procedure is established to ensure that security features specified by TSG-S3 are properly integrated into other 3GPP 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 R00 can be met. Milestones for the security review procedure should be explicitly identified in the time plan.

4 Change history

Change history					
SA2 No.	**TDoc. No.**	**CR. No.**	**Section affected**	**New version**	**Subject/Comments**
0.0.3					This is a revised version of S2-000590 considered at S3#12. It contains modifications and additions to the original list proposed by S2.

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 consistent security specifications for release 2000.

The work items being progressed in TSG-S3 should be 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 2000, release 2001, etc.

The work items have not yet been prioritised. This cannot be done until the then R00 system architecture is studied and understood and the R00 work programme has been more fully elaborated .

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

	Work item	**Priority**
1		
2		
3		
4		
6		
7		
8		
9		
10		
11		
12		
13		
14		
15		
16		

6 Annex B: Contact people

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

N4	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

New contact people might be needed for S5 [and SMG 2 WP A].