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

Rev of Tdoc S2-00-590

3G PD xx.sec v0.0.2 (2000-03)

S3-000244

Permanent Document

3rd Generation Partnership Project
3GPP work program
Project co-ordination aspects
DRAFT R2000 Project Plan for Security
(3G PD XX.sec version 0.0.2)

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.

[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 is to be discussed/confirmed/modified/completed by S3]

3.1.1 Authentication between mobile and “Gatekeeper”

The R2000 architecture will probably introduce new nodes. The mobile may need to be authenticated by, and, authenticate these new nodes.

Work may involve S2, S3, N1, N2.

3.1.2 Integrity protection for Mobile to “Gatekeeper” signalling

Signalling between the mobile and nodes within the R2000 core network that are beyond the GGSN may well use the radio interface user plane Radio Access Bearers. This signalling is likely to need integrity protection.

Work may involve: S2, S3, R2, R3, N1, N2, [SMG 2 WP A].

3.1.3 Integrity protection for user plane data

It needs to be determined whether there IS, or, IS NOT, a requirement for this in R2000.

For e-commerce, it may be useful to protect the user plane data. However, the addition of integrity protection to voice over IP services 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].

3.1.4 Core network signalling security

In R'99, a minimal solution is being developed to protect the most sensitive information. In R'2000 security mechanisms need to be considered for all EXISTING and all NEW core network interfaces.

Work may involve S2, S3, N2.

3.1.5 FIGS

VoIP telephony may require additional FIGS functionality within the R'2000 PS side nodes.

Work may involve S2, S3, N2.

3.1.6 Lawful Interception in the R'2000 architecture

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

Work may involve S2, S3, N2.

3.1.7 Network wide encryption

Use the 'hooks' in the R'99 standard to develop this feature.

Work may involve S2, S3, R2, R3, N1, N2, [SMG 2 WP A].

3.1.8 IPsec

IPsec is likely to be used in some places within the R2000 system. IP sec has many options and a 'standardised profile' is likely to 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.

3.1.9 Secure mobile platform for applications

Mobile station applications based, eg, 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.

Work may involve S3, T2, T3.

3.1.10 [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 replacement algorithm could be developed and rolled out into the network infrastructure and the mobile stations.]

[Work may involve S3, N1, N2, SMG 2 WP A.]

3.1.11 [GEA 2]

[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 R'99: however the work will need to be carried out during the calendar year 2000.]

[Work may involve S3, N1, N2]

3.1.12 ["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.]

3.1.13 [GERAN, packet side]

[The recent decision to deploy an Iu-ps interface into the R2000 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, N2, SMG 2 WP A.]

3.1.14 Enhanced User Identity Confidentiality

Was/is this part of R'99?

3.2 List of all the deliverables applicable to the subject

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).		

3.3 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.]

3.4 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**

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.

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
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 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].