

S3-000313

(rev S3-000305)

3G PD XX.sec v0.0.4 (2000-04)

**Permanent
Document**

**3rd Generation Partnership Project
3GPP work program
Project co-ordination aspects
DRAFT R2000 Project Plan for Security
(3G PD XX.sec version 0.0.4)**



The present document has been developed within the 3rd Generation Partnership Project (3GPP™) and may be further elaborated for the purposes of 3GPP.

The present document has not been subject to any approval process by the 3GPP Organisational Partners and shall not be implemented. This Specification is provided for future development work within 3GPP only. The Organisational Partners accept no liability for any use of this Specification. Specifications and reports for implementation of the 3GPP™ system should be obtained via the 3GPP Organisational Partners' Publications Offices.

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	6
3.1.1.3 User plane protection in access network.....	6
3.1.1.4 Core network security.....	7
3.1.1.5 Termination of packet domain encryption in GSM BSC.....	8
3.1.1.6 GERAN access security.....	9
3.1.1.7 Enhanced User Identity Confidentiality	9
3.1.2.8 Ability of terminal/USIM to reject unencrypted calls	10
3.1.2 Other security deliverables	10
3.1.2.1 Use of IP security solutions	10
3.1.2.2 FIGS	11
3.1.2.3 Secure mobile platform for applications.....	11
3.1.2.4 OSA/VHE security	12
3.1.2.5 Visibility and configurability.....	13
3.1.2.6 Study on the evolution of GSM CS algorithms	13
3.1.2.7 Study on the evolution of GSM PS algorithms and the introduction of GEA2	14
3.1.2.8 "Mandatory" GPRS encryption	14
3.1.2.9 Lawful Interception in the R'2000 architecture.....	14
3.2 List of all the specifications under S3 control.....	15
3.3 Security review procedure	17
4 Change history	18
5 Annex A: Scope of the security co-ordination ad-hoc group.....	19
6 Annex B: Contact people	19

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 and beyond

3.1 DRAFT R2000 DeliverablesWork Items

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

~~Depending on the requirements of the R00 working methods, s~~Security ~~work items deliverables~~ will be created based on proposals from a required minimum number of named supporting companies. To help create appropriate lines of accountability, rapporteurs ~~will may need to~~ be assigned to ~~eachsome~~ security ~~work item deliverables~~. Some of the larger security ~~work items 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 ~~built~~ into the system architecture. Security architecture work will be split into a number

of [building blocks/deliverables](#) each of which will focus on work which is reasonably self-contained. However, it is expected that some dependencies will exist between [building blocks/deliverables](#). For each security [work item/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 [work items/deliverables](#) is given in the sub-sections below.

3.1.1.1 Access network security [for IP-based services](#)

This is a **Building Block** for the feature “**Provisioning of IP-based multimedia services**”.

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 ([eg provision for integrity checking as well as encryption](#)). Charging and accounting issues are also likely to be important [here](#).

Work [Tasks](#) may involve: S2, S3, [S5](#), R2, R3, [T3](#), N1, N4, [SMG 2 WP A].

Event	Expected date
Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Requirements capture	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Building Block.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture	Concept presented to CN, RAN, T and GERAN: February 2001 First draft CRs March 2001 Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001

3.1.1.2 Network-based end-to-end security

This is a Feature.

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 [it](#) 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 [Tasks](#) may involve S2, S3, R2, R3, N1, N4, [SMG 2 WP A].

<u>Event</u>	<u>Expected date</u>
presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Requirements capture	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Feature.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture	Concept presented to CN, RAN, T and GERAN: February 2001 First draft CRs March 2001 Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001

3.1.1.3 User plane protection in access network

This is a Feature. It may also be a (sub)building block for other work items, eg for the building block "Access network security for IP-based services".

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 [Tasks](#) may involve S2, S3, R2, R3, N1, [SMG 2 WP A].

<u>Event</u>	<u>Expected date</u>
presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles	S3#13 23 - 26 May 2000; Tokyo; DoCoMo

Requirements capture	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture	Concept presented to CN, RAN, T and GERAN: February 2001 First draft CRs March 2001 Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001

[3.1.1.4 Core network security: minimal solution](#)

This is a **Feature**. This 'minimal solution' is a feature in its own right. It is also a **Building Block** of the feature "**Core Network security: full solution**".

[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.](#)

[Work Tasks may involve S2, S3, N4.](#)

Event	Expected date
Completion of ongoing work in S3	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Completion of ongoing work in N4	TSG #9: June 2000
Completion of profile of IPsec by S3. This is the S3 Work Task "Use of IP security solutions".	TSG #9: June 2000
Completion of work in S5	TSG #10: September 2000

[3.1.1.43.1.1.5 Core network security: full solution](#)

This **feature** is the 'full solution'. It is also a **Building Block** for the feature "**Provisioning of IP-based multimedia services**".

[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 [Tasks](#) may involve S2, S3, N4.

Event	Expected date
Presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Requirements capture	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture One (of many) of the Work Tasks is "Use of IP security solutions".	Concept presented to CN, RAN, T and GERAN: February 2001 First draft CRs March 2001 Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001

[3.1.1.53.1.1.6 GERAN access security/termination of packet domain encryption in GSM BSC](#)

This is a **Building Block** of the Feature "GERAN" which may be included in the plan of the ICG group '[Bearer and Access Stratum](#)'.

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. [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 [Tasks](#) may involve S2, S3, N1, N4, SMG 2 WP A, [SAGE](#).

Event	Expected date
Presentation by SMG 2 to S3/SMG 10 of well-defined and understandable system architecture concepts and principles	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Requirements capture	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000

	<u>CRs approved: S3#17 January 2001</u>
<u>Integration of security architecture</u>	<u>Concept presented to CN, T and GERAN:</u> <u>February 2001</u> <u>First draft CRs March 2001</u> <u>Complete CRs April 2001</u> <u>CRs approved at TSG level May 2001</u> <u>Review of complete CRs by S3 June 2001</u> <u>First corrective CRs prepared July 2001</u> <u>Corrections agreed at TSG level August 2001</u>
<u>Production of new algorithm(s) by eg. SAGE ?</u>	<u>Requirements complete August 2000</u> <u>Funding arranged January 2001</u> <u>Work completed June 2001</u> <u>Publication completed October 2001</u>

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

This is a Feature.

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.

Work Tasks may involve S2, S3, N1, N4, RAN 2, RAN 3, T2, T3, SMG 2 WP A.

<u>Event</u>	<u>Expected date</u>
<u>Requirements capture</u>	<u>S3#13 23 - 26 May 2000; Tokyo; DoCoMo</u>
<u>Security feature specification</u>	<u>S3#14 1-4 August 2000</u>
<u>Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.</u>	<u>S3#15 September 2000</u>
<u>Definition of security architecture</u>	<u>First draft: S3#16 November 2000</u> <u>CRs approved: S3#17 January 2001</u>
<u>Integration of security architecture</u>	<u>Concept presented to S2, CN, RAN, T and GERAN:</u> <u>February 2001</u> <u>First draft CRs March 2001</u>

	Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001
--	---

3.1.2.8 Ability of terminal/USIM to reject unencrypted [connectionsealls](#)

[This is a Feature.](#)

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 [Tasks](#) may involve S3, N1, T2, T3, [RAN 2, SMG 2 WP A](#).

Event	Expected date
Requirements capture	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Security feature specification	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#14 1-4 August 2000
Definition of security architecture	First draft: S3#15 September 2000 CRs approved: S3#16 November 2000
Integration of security architecture	Concept presented to CN, RAN, T and GERAN: January 2001 First draft CRs February 2001 Complete CRs March 2001 CRs approved at TSG level April 2001 Review of complete CRs by S3 May 2001 First corrective CRs prepared June 2001 Corrections agreed at TSG level July 2001

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

[This is an S3 Work Task. It is needed, at least, for the Features/Building Block “Core network security: full solution”; and “Core network security: minimal solution”.](#)

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 Tasks may involve just S3.

<u>Event</u>	<u>Expected date</u>
<u>Profile of IPsec</u>	<u>S3#13 23 - 26 May 2000; Tokyo; DoCoMo</u>

3.1.2.2 FIGS

This is a **Building Block** of the Feature **“Provisioning of IP-based multimedia services”**.

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

Work Tasks may involve S2, S3, N2.

<u>Event</u>	<u>Expected date</u>
<u>presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles</u>	<u>S3#13 23 - 26 May 2000; Tokyo; DoCoMo</u>
<u>Requirements capture</u>	<u>S3 / CN WGs Joint ad-hoc 14-15 June 2000</u>
<u>Security feature specification</u>	<u>S3#14 1-4 August 2000</u>
<u>Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.</u>	<u>S3#15 September 2000</u>
<u>Definition of security architecture</u>	<u>First draft: S3#16 November 2000</u> <u>CRs approved: S3#17 January 2001</u>
<u>Integration of security architecture</u>	<u>Concept presented to CN and S2: February 2001</u> <u>First draft CRs March 2001</u> <u>Complete CRs April 2001</u> <u>CRs approved at TSG level May 2001</u> <u>Review of complete CRs by S3 June 2001</u> <u>First corrective CRs prepared July 2001</u> <u>Corrections agreed at TSG level August 2001</u>

3.1.2.3 Secure mobile platform for applications

This is a **Building Block** of the Feature **“MExE”**. Note: this **Building Block** is not yet identified by ICG **‘Service platforms’**.

Mobile station applications based, for example on MExE and/or involving e-commerce will need to be deployed, operated, upgraded and deleted in a secure manner. Security mechanisms will involve the use of the (U)SIM, 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 [Tasks](#) may involve S3, T2, T3.

Event	Expected date
Requirements capture	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture	Concept presented to CN, RAN, T and GERAN: February 2001 First draft CRs March 2001 Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001

3.1.2.4 OSA/VHE security

This is the **Building Block** called “**Improvements to VHE/OSA security**” by the **Feature “VHE/OSA”** which is part of ICG **‘Service platforms’**.

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

[Work Tasks](#) may involve S3, N5 and N4.

Event	Expected date
presentation by N5 to S3 of well-defined and understandable system architecture concepts and principles	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Requirements capture	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture	Concept presented to CN, S2 and T: February 2001 First draft CRs March 2001 Complete CRs April 2001

	CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001
--	--

3.1.2.5 Visibility and configurability

[This is a Feature.](#)

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

[Work Tasks might involve S3, T2, T3, RAN 2, SMG 2 WPA and N1.](#)

Event	Expected date
Requirements capture	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#15 September 2000
Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture	Concept presented to S2, T, CN, RAN and GERAN: February 2001 First draft CRs March 2001 Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001

3.1.2.6 Study on the evolution of GSM CS algorithms

[This is a Feature.](#)

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 [Tasks](#) may involve S3, N1, N4, SMG 2 WP A.

Event	Expected date
Requirements capture	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Security feature specification	S3#14 1-4 August 2000
Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.	S3#15 September 2000

Definition of security architecture	First draft: S3#16 November 2000 CRs approved: S3#17 January 2001
Integration of security architecture	Concept presented to CN, RAN, T and GERAN: February 2001 First draft CRs March 2001 Complete CRs April 2001 CRs approved at TSG level May 2001 Review of complete CRs by S3 June 2001 First corrective CRs prepared July 2001 Corrections agreed at TSG level August 2001

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

[This is a Feature.](#)

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 [Tasks](#) may involve S3, N1, N4

Event	Expected date
Requirements capture, and identification of all Work Tasks.	S3#13 23 - 26 May 2000; Tokyo; DoCoMo
Definition of security architecture	S3 / CN WGs Joint ad-hoc 14-15 June 2000
Integration of security architecture	Concept presented to CN, RAN, T and GERAN: August 2000 Complete CRs September 2000 CRs approved at TSG level October 2000 Review of complete CRs by S3 November 2000 First corrective CRs prepared December 2000 Corrections agreed at TSG level January 2001

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.~~

3.1.2.8 Lawful Interception in the R'2000 architecture

This is a (SUB)Building Block for the Features "Provisioning of IP-based multimedia services" and "Enable bearer independent Circuit-switched network architecture". Note that the latter dependency is not yet identified by ICG 'Call Control and Roaming'.

Note also that this is likely to be more of a **sub-building block** rather than directly under a **feature**.

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 Tasks may involve S2, S3, N4.

<u>Event</u>	<u>Expected date</u>
<u>presentation by S2 to S3 of well-defined and understandable system architecture concepts and principles</u>	<u>S3#13 23 - 26 May 2000; Tokyo; DoCoMo</u>
<u>Requirements capture</u>	<u>S3 / CN WGs Joint ad-hoc 14-15 June 2000</u>
<u>Security feature specification</u>	<u>S3#14 1-4 August 2000</u>
<u>Feasibility study, including definition of Work Tasks and completion of the plan for this Work Item.</u>	<u>S3#15 September 2000</u>
<u>Definition of security architecture</u>	<u>First draft: S3#16 November 2000</u> <u>CRs approved: S3#17 January 2001</u>
<u>Integration of security architecture</u>	<u>Concept presented to CN, RAN, T and GERAN: February 2001</u> <u>First draft CRs March 2001</u> <u>Complete CRs April 2001</u> <u>CRs approved at TSG level May 2001</u> <u>Review of complete CRs by S3 June 2001</u> <u>First corrective CRs prepared July 2001</u> <u>Corrections agreed at TSG level August 2001</u>

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	Jukka 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].