Source: **Chairman TSG SA**

Title: **Report to PCG#10 on work in TSG-SA**

Agenda: **4**

Document for:

Decision	
Discussion	
Information	**X**

1 Main events since last meeting

In the period October 2002 (PCG#09) to May 2003 (PCG#10) TSG-SA have held two TSG-SA plenary meeting, TSG-SA#18 (New Orleans, 9 – 12 December 2002) and TSG-SA#19 (Birmingham, 17 – 20 March 2003). Further to TSG-SA plenaries, a number of meetings of the TSG-SA working groups have taken place. At the TSG-SA#11 an election of chairman and vice-chairmen of TSG-SA took place and resulted in election of Niels Peter Skov Andersen of Motorola as TSG-SA chairman, Gary Jones T-Mobile and Hiroshi Nakamura NTT DoCoMo as Vice-chairmen.

2 Technical work in TSG-SA

The work of TSG-SA consists of three main parts: technical work within TSG-SA, technical co-ordination between the TSGs and project management. In the period TSG-SA have been working in all three areas. The technical work within TSG-SA is organised in 5 working groups dealing with the service aspects, architecture, security, codec aspects and telecom management.

In addition to the plenary meetings and the working group meetings TSG-SA has held one ad-hoc meeting in conjunction with each plenary on the subject of “3GPP Future Evolution”. The purpose of organising the ad-hoc was to collect inspiration for the future evolution of the 3GPP based systems.

2.1 Work related to Service Aspects

The service requirements and associated stage 1 documentation for release ‘99 and release 4 and release 5 are considered complete and the necessary adjustments and clarification caused by the stage 2 and stage 3 work done. TSG-SA WG1 (S1) has therefore commence work on identifying functionalities and specifying the requirements for the next releases, taking into account the results from the 3GPP Future Evolution workshop. One of the key items is the further evolution of the IP Multimedia Subsystem beyond its first phase completed in Release 5. Even though the overall process put in place by TSG-SA allow for medium to long term work and planning, the main focus has been on issues in the time frame of the release. As reported to the previous PCG meeting at TSG-SA #15 it

was agreed to plan for a “long term vision” creation kick-off meeting in conjunction with TSG-SA #17. This kick-off meeting took place during TSG_SA#17 and drafted a set of terms of references for the further work to establish a vision of the 3GPP Future Evolution. Also proposals for outline and type of deliverables were elaborated. Meetings to further progress the issue were held in conjunction with TSG SA #18 and TSG SA#19. The resulting deliverable from the work is expected to be completed by September 2003. A draft of the draft technical report is provide for information in Tdoc PCG#10(03)17.

2.2 Architecture related work

The architectural work related to the IP based network has been stable in the period and the key decisions for the IM subsystem kept unchanged, i.e., the selection of SIP as Call Control model and utilisation of IPv6. Generally, releases 99, 4 and 5 are considered stable and the focus of the architecture related work is related to release 6 on items.

2.3 Security related work

Has reported earlier to PCG the introduction of IP Multimedia Subsystem introduces significant changes to the network architecture, these changes requires a substantial work effort in order to ensure that all security aspects are considered and handled correct. This was handled in the release 5 timeframe and there is now no major outstanding items for release 5.

At TSG SA#18 the concept of second UMTS encryption and integrity protection algorithms (UEA2 and UIA2) for backup purposes was introduced. TSG SA supported the principle of creating backup algorithms. TSG SA WG3 was then asked to provide figures for the expected funding costs and to inform TSG SA whether a mandatory implementation date for the new algorithms was intended, and if so, the expected timing for this. TSG SA WG3 presented to a provisional work plan (TD SP-030074 attached to this status report) for a SAGE-led Task Force was presented. It indicates a 7-10 months working period. The shorter period is envisaged if no external evaluation of the resulting algorithms is considered to be needed (e.g. because sufficient confidence has been attained by other means). The extended period is needed in case external evaluation is deemed necessary. TSG SA have not yet taken a position on the need for an external evaluation at this meeting but chose to wait for the results from the SAGE Task Force and a recommendation from SAGE as to if external evaluation should be needed. Start of work is possible when the funding is made available.

The budget for the work is estimated to be 16 MM (man months) in case of no external evaluation. To cater for an eventual external evaluation a further budget of 4 MM should be reserved***. PCG is invited consider provision of the funding.***

2.4 Codec related work

The codec work in TSG-SA WG4 (S4) for release 99, 4 and 5 is found stable and no significant changes expected. Only remaining open issue for Release 5 is TR 26.937 “RTP Usage model” which is currently being finalized based on comments received from other WGs. This non-critical TR brings additional information to characterize the PS Streaming Service.

2.5 Work related to telecom management

TSG-SA has in the past reported to PCG that TSG-SA wished TSG-SA WG5 (S5) to complete the specifications at the same time as other parts of the release. However, parts of the telecom management specifications build on the core specifications and can therefore not be fully completed before the core specifications are completed. On this background TSG-SA have found it acceptable

that a delay of 3 month compared to close of the release could occur for some telecom management specifications. This goal was not completely fulfilled in the case of Release 99 and Release 4, however the majority the specifications were completed at the requested point in time and remaining specifications within the time of one additional meeting cycle (3 month). The telecom management specifications for release 99 and release 4 are considered stable. A similar situation occurred for Release 5 where the telecom management related specifications first were fully ready in September 2002. However, this represent a clear improvement compared to the previous releases and already now the telecom management work for Release 6 is well progressed.

Also in the area of telecom management specifications some cooperation with the corresponding 3GPP2 groups has been established. According to information available to TSG-SA, 3GPP2 plans to build some of their telecom management specifications on basis of the 3GPP specifications as delta specifications. TSG-SA welcomes this harmonisation of telecom management specifications across standards. TSG-SA does not foresee any negative impact on the 3GPP timescales and workload due to this.

3 Technical co-ordination

3.1 Issues related TSG-CN

As reported to the previous PCG meeting TSG SA has in cooperation with TSG-CN reviewed the liaison statement from IETF raising concern about the way 3GPP in certain cases have made use of SIP, which IETF believe is not in line with the intentions and thus longer term could cause problems. As response to this a 3GPP action plan to review and potentially fix the issues identified by IETF has been elaborated. In addition a reply to IETF indicating that 3GPP are reviewing the issues raises has been drafted and sent. TSG SA has taken note of the progress on resolving the identified issues.

3.2 Issues related to TSG-RAN

TSG-RAN's work creating and organising work items for future releases has been noted. TSG-SA has also taken note of the fact that TSG-RAN still needs to perform substantial work on error corrections for the Release 99 set of specifications. As this reduces the time available for work on the next releases TSG-SA notes that TSG-RAN has had need to prioritise the work for the next releases. TSG-SA has taken this into account in the review of the overall project plan. Further TSG-SA has taken note of the completion of major work items such as HSDPA as part of Release 5.

3.3 Co-ordination with TSG-T

TSG-T has informed TSG-SA about the progress in elaboration of test specifications and the associated abstract test suites. TSG-SA further has noted the elaboration of priorities for the completion of the remaining work based on input from the industry. In general no major issues has raised between TSG SA and TSG-T, only the usual coordination of the requirement and architectural work with the technical work of TGS T.

3.4 Co-ordination with TSG-GERAN

TSG-GERAN continues in a manner equal to that of the other TSGs to provide an overview of its activities and work plan. The work plan for TSG GERAN is now been integrated in the overall work plan for 3GPP. In the period the main areas of contact between TSG SA and TSG GERAN have been in the area of Architecture and security issues related to the introduction of GERAN support for the Iu interface and TSG GERAN's considerations about potential enhancements to A and Gb interfaces.

These activities have involved mainly involved TSG SA WG2 and WG3.

4 Requirements for support in 2003/2004

As earlier reported TSG-SA does not see any major changes in its requirement for support in 2004 compared to 2002and 2003, and sees no reason to change the requirement that the same number of man month as for 2003 are budgeted for 2004. Currently the only additional task requiring dedicated funding which have been identified is the second UMTS encryption and integrity protection algorithms (UEA2 and UIA2) for backup purposes.

5 Release 99, 4 and 5

As indicated earlier in this report TSG-SA have reviewed the status of the project in co-operation with the other TSGs. Based on the status report provided, TSG-SA concludes that all release 99, release 4 and release 5 items have been completed and the releases can be considered stable However, TSG-SA foresees there still for a while will be a need for corrective changes to Release 99 especially in the area of the radio access network. These corrective changes might reach a second peak when larger scale of network deployment based on the specification starts.

6 Beyond Release 5

As the content of Release 5 has only just been functionally completed, it is to early to date and provide a full and stable overview of the content of the following Releases. Tdoc PCG#10(03)14 provides an first indication of the potential content of Release 6.

Based on the input form the other TSGs TSG SA have discussed the target date for Release 6 and so far concluded that an earliest target date for Release 6 to be December 2003 or March 2004.

It is perhaps worth reiterating that the work on defining a content of a release is based on the principles for a release agreed at TSG-SA#09 and confirmed by PCG#05. These principles are:

- A release shall consist of a well-defined, stable and internally consistent set of functions;
- A release shall be documented in a maintained, consistent stream of specifications;
- Essential corrections to a stable or frozen release shall be included in the applicable release;
- New or changed functionality shall be included in new (rather than retrospectively in old) releases.

As a part of these principles it was also agreed that the overall road map should be controlled by the 3GPP Project plan (i.e. a “3GPP Road Map”) and not as in the past by the Releases. The content of the Release should be based upon the work plan with a well-defined closing time for the content of a Release (6 – 9 months before completion of a particular Release).

8 General Management issues

At TSG SA plenary meetings some discussion of the relation between TSG SA and 3GPP in general and the Open Mobile Alliance known as OMA tend to take place. However, it is still found that the original conclusion still is valid. OMA should be considered as a clear co-operation partner for 3GPP. The terms of reference for 3GPP is not and should not be affected by this new body and the work of OMA from a 3GPP point of view is to be seen as complementary to 3GPPs work. Finally, there is for the time being no need for a specific cooperation agreement or similar, as Liaisons with OMA in the

usual way seems to fulfil the current needs.

As reported earlier, when establishing the overall status for the release 1999 it was realised that it was been difficult to link together the work items of the different TSGs in order to understand whether or not all part of a service or functionality is being completed according to the target. To help overcoming this problem for future releases a working model was elaborated and agreed. This working model has now been in place for a while and allows the work items of the different TSGs to be linked into a hierarchical structure, based on three levels feature, building block and work task. This process has now enter a phase where it is a routine within the work of 3GPP and is very useful in the discussions around the content and target dates for releases. Extract of the overall work plan is provided to PCG for consideration in Tdoc PCG#10(03)13 and Tdoc PCG#10(03)14.

Technical Specification Group Services and System Aspects **TSGS#19(03)0074**
Meeting #19, Birmingham, UK, 17-20 March 2003

Title: **Provisional work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2**
Source: **SA WG3**
Agenda Item: **7.3.2**
Document for: **Endorsement**

At TSG SA meeting #18, SA WG3 were requested to provide a work plan and funding estimation for the design of a second backup confidentiality and integrity algorithms (UEA2 and UIA2).

The attached document was presented to SA WG3 #27 by ETSI SAGE and SA WG3 agreed to forwarded it to TSG SA for endorsement and to request the necessary funding to the 3GPP PCG.

Action: **TSG SA are asked to endorse the provisional work plan from ETSI SAGE and to request the necessary funding from the PCG.**

3GPP TSG SA WG3 Security — S3#27 **S3-030086**

25. – 28. November 2002

Sophia Antipolis, France

Source: **Vodafone / SAGE chairman**
Title: **Provisional work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2**
Document for: **Approval**
Agenda Item: **5.3/6.5**

This attached document constitutes an initial work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2 by a dedicated ETSI SAGE Task Force.

Title:	**Provisional work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2 (MCC Task Force *nnnnnnn*)**		
Source:	Steve Babbage, Vodafone	Version:	01.01
File:	F89-2 algo plan.doc	Date:	20/02/03

This document constitutes an initial work plan for the design of the 3GPP confidentiality and integrity algorithms UEA2 and UIA2 by a dedicated ETSI SAGE Task Force.

The following assumptions are made.

1. The existing algorithms UEA1 and UIA1 are both modes of operation of a block cipher KASUMI. The design of UEA2 and UIA2 could in principle follow one of two approaches:
   (a) just replace KASUMI by a different block cipher (or other keyed function);
   (b) do something substantially different, probably involving a different sort of fundamental cryptographic primitive.

   It is an essential requirement on the design of the new algorithms that they be substantially different from UEA1 and UIA1, so that an attack on one set of algorithms is unlikely to affect the other. However, the SAGE task force is very confident in the robustness of the modes of operation selected for UEA1 and UIA1, and hence are confident that any attack on UEA1 and UIA1 will result from an attack on KASUMI itself. Option (a) is therefore believed to be acceptable. And option (a) seems much more likely to succeed than option (b) — it is not at all clear what other approach might work.

   The conclusion of all this is that, while a small amount of time may be spent investigating option (b), the working assumption is that option (a) will be followed, i.e. the new designs will just replace KASUMI by a different block cipher (not necessarily with the same block size).
2. The Algorithm Design Authority (ADA) is 3GPP SA3.
3. The work will be carried out by an ETSI SAGE Special Task Force. The work can only start if ETSI and 3GPP have agreed on the terms and conditions for such a task force and ETSI has issued the STF contracts.
4. It is left the ADA to decide whether evaluation of the new designs by external experts is required. (The Task Force will advise on this question.)

1. Description of tasks, key deliverables and responsibilities

The key deliverables from the project are as follows:

D1 – Algorithm specification
D2 – Implementors' detailed test data
D3 – Algorithm input/output test data
D4 – Design and evaluation report
D5 – Final public report on the project

The following three tasks are envisaged:

A - Project management, coordination and liaison
B - Design and specification
C - Evaluation

1.1 A - project management, coordination and liaison

This task includes the following activities:
(i) Draft and maintain project plan
(ii) Arranging and chairing coordination meetings
(iii) General liaison with 3GPP and ETSI, and contractual issues
(iv) Editing a short public report on the design and evaluation work at the end of the project
(v) Provision of any other formal reports where necessary
(vi) Coordination of external evaluation work and results, if required
(vii) Publication of results

Partners: Vodafone, Telia

Responsibilities:
Vodafone: Project management
Telia: D5, liaison

1.2 B – Design and specification

This task includes the following activities:
(viii) Draft of design criteria
(ix) Investigation of alternative design approaches ["option (b)" in the assumptions on page 1]
(x) Selection of a block cipher — or design of a new block cipher, if no existing design is felt suitable
(xi) Producing a C implementation of the algorithms
(xii) Formal specification of the algorithm (***Deliverable D1***)
(xiii) Implementors' detailed test data (***Deliverable D2***)
(xiv) Algorithm input/output test data (***Deliverable D3***)

Partners: BT, Deutsche Telekom, Mitsubishi, Nokia, Vodafone

Responsibilities:
D1, C implementation: BT
D2 and D3: Deutsche Telekom
Design approaches: Nokia, Vodafone
Design: BT, Mitsubishi, Nokia

1.3 C - Evaluation

This task includes the following activities:
(xv) Draft of evaluation criteria
(xvi) Evaluation of candidate public or other existing block ciphers in terms of
- strength (including difference from UEA1 / UIA1)
- performance and complexity, especially in hardware
- IPR issues

(xvii) Evaluation of specific design proposals against the same criteria
(xviii) Statistical tests if these need to be carried out
(xix) Producing a second, independent implementation of the algorithms
(xx) Verification of the clarity and accuracy of deliverables D1–D3
(xxi) Design and evaluation report (***Deliverable D4***)

Partners: All

Responsibilities:
Thales: D4
All: Candidate block cipher evaluation

Gemplus, France Telecom, KPN, Thales: Cryptanalytic evaluation of design proposals
Deutsche Telekom: Specification testing
Mitsubishi, Nokia: Performance and complexity evaluation

2. Budget allocation

The proposed funding allocation over the tasks and partners is shown in the table below. All figures are in man months.

	BT	DT	FT	Gemplus	KPN/TNO	Mitsubishi	Nokia	Telia	Thales	Vodafone	Total
Manage-ment								0.75		1.00	1.75
Design, Specify	1.75	1.50				0.50	0.75			0.75	5.25
Evalu-ation	0.50	0.50	1.25	1.00	1.00	1.00	1.00	0.50	1.75	0.50	9.00
Total	2.25	2.00	1.25	1.00	1.00	1.50	1.75	1.25	1.75	2.25	16.00

All partners will provide their own additional funding (the amounts of own funding are not shown in the table)

SAGE may agree internally to redistribute this budget amongst the task force members before the contracts are drawn up, without increasing the total.

3. Planning

The planning is shown in the table below.

Month	1	2	3	4	5	6	7–9	7* or 10*
Activity								
A Management	(ii, iii, v) General liaison and ongoing management							
	(i) Fix plan				(vi) Advise on requirements for public evaluation; coordinate it if required		*Public evaluation if required*	(iv) Public report D5
B Design and specification	(viii) Design criteria		(xii, xiii, xiv) First draft / outline of D1/D2/D3		(xii, xiii, xiv) Provisionally final draft of D1/D2/D3			*(x, xii, xiii, xiv) Revise design and D1/D2/D3 if necessary*
	(ix) Investigate alternative design approaches		(x) First design proposal	(xi) C implementation	(x) Second design proposal	(xi) Revise C implementation		
C Evaluation	(xv) Evaluation criteria					(xix, xx) Second implementation; QA of D1-D3		*(xix, xx) Modify impl'n; QA of D1-D3*
	(xvi) Evaluation of existing block ciphers			(xvii) Evaluation of first proposal		(xvii, xviii) Evaluation of second proposal		*(xvii) Assess public evaluation results*
					(xxi) First draft of design and evaluation report D4			(xxi) Final design and evaluation report D4
Month	1	2	3	4	5	6	7–9	7* or 10*

* If the project runs over the summer, then an additional slippage of around one month should be allowed for the holiday period

4. Participants in Task Force

Vodafone

Steve Babbage (***Task Force Leader)*** Tel: +44 1 635 676209
Vodafone Group R&D (UK) Fax: + 44 1 635 231776
The Courtyard
2-4 London Road
Newbury Berkshire RG14 1JX
UK email steve.babbage@vodafone.com

Nick Bone Tel: +44 1 635 682129
Vodafone Group R&D (UK) Fax: + 44 1 635 676147
The Courtyard
2-4 London Road
Newbury Berkshire RG14 1JX
UK email nick.bone@vodafone.com

TNO (acting for KPN Research)

Boaz S. Gelbord Tel: +31 70 332 5170
TNO Fax: +31 70 332 6477
?????????
The Netherlands email B.S.Gelbord@telecom.tno.nl

Telia

Per Christoffersson (***Deputy Task Force Leader***) Tel: +46 8 7073547
Telia Promotor Fax: +46 8 7073599
Cylindervägen
131 87 Nacka Strand
Sweden email per.e.christoffersson@telia.se

BT

David Parkinson Tel: +44 1473 646236
Admin 2 pp 6 Fax: +44 1473 620455
BT Laboratories
Martlesham Heath
Ipswich
Suffolk IP5 3RE
UK email: dparkins@alien.bt.co.uk

Deutsche Telekom

Tobias Martin (ESZ1g) Tel: +49 6151 83 8841
T-Systems Nova Fax: +49 6151 83 4464
Am Kavalleriesand 3
D-64295 Darmstadt
Germany email Tobias.Martin@t-systems.com

Tim Schneider (ESZ1jb) Tel: +49 6151 83 5680
T-Nova Deutsche Telekom Fax: +49 6151 83 4464
Am Kavalleriesand
D-64295 Darmstadt
Germany email Tim.Schneider@t-systems.com

France Télécom
Henri Gilbert
FTR&D/DTL/SSR
38-40 Rue du Général Leclerc
F-92794 Issy-les-Moulineaux Cedex
France

Tel: +33 1 45 29 54 97
Fax: +33 1 45 29 65 19
email henri.gilbert@francetelecom.com

Gemplus
(mrs) Helena Handschuh
GemPlus
34, rue Guynemer
F-92447 Issy-les-Moulineaux Cedex
France

Tel: +33 14648 2037
Fax: + 33 1 4648 2004
email helena.handschuh@gemplus.com

Mitsubishi
Mitsuru Matsui
Mitsubishi Electric Corp.
5-1-1 Ofuna
Kamakura 247-8501
Japan

Tel: +81 467 41 2181
Fax: +81-467-41-2185
email matsui@iss.isl.melco.co.jp

Nokia
(mrs) Kaisa Nyberg
Nokia Research Center
P.O.Box 407
FIN-00045 Nokia Group
Finland
(Visiting address: Itämerenkatu 11-13, FIN-00180 Helsinki)

Tel: +358 7180 37384
Fax: +358 7180 36850
email Kaisa.Nyberg@nokia.com

Thales
Leif Nilsen
Thales
PO Box 22 ØKern
N-0508 Oslo 5
Norway
(Visiting address: Østre Aker vei 33, Økern, Oslo, Norway)

Tel: +47 22 638 447
Fax: +47 22 638 497
email: leif.nilsen@no.thalesgroup.com