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