3GPP TSG SA WG3 Security — S3#12 **S3-000236**

11-14 April, 2000, Stockholm, Sweden

Technical Specification Group Services and System Aspects **_TSGS#7(00)0118_**
Meeting #7, Madrid, Spain, 15-17 March 2000

Source:	**ETSI SAGE**
Title:	**Work plan for the design of the 3GPP Authentication Algorithm (MCC Task Force)**
Document for:	**Information**
Agenda Item:	

ETSI SAGE

Title:	**Work plan for the design of the 3GPP Authentication Algorithm (MCC Task Force)**		
Source:	KPN Research	Version:	01.01
File:	3GPP auth algo plan.doc	Date:	09/03/00

This document constitutes a work plan for the design of the standard the 3GPP Authentication Algorithm.

1. Description of tasks, key deliverables and responsibilities

There will be five tasks:

A - Project Management;
B - Design;
C - Evaluation;
D - Specification;
E - Liaison and Publication.

The activities and key deliverables of the tasks and the allocation of responsibilities to partners are described below.

1.1 A - project management

This task includes the following activities.

- Draft and maintain project plan.
- Arranging and chairing coordination meetings.
- Editing a short public report on the design and evaluation work at completion of work with the purpose to inform 3GPP TSG-SA WG3 (***Deliverable D1)***.

Partner: KPN Research, Telia

Responsibilities:

KPN Research: Formal task force leader, end responsibility for deliverables; project plan; coordination meetings.
Telia: Deputy taskforce leader, editor for Deliverable D1.

1.2 B – Design

This task includes the following activities.

- Draft of design criteria.
- Design of modes for the algorithm including Operator Variant Parameter
- Selection/Design of example block cipher.

Partners: BT, Deutsche Telecom, KPN, Thomson, Vodafone,

Responsibilities:
BT: Design modes
Deutsche Telekom: Design criteria for example block cipher
KPN: design modes and example block cipher
Thomson: Selection/Design of example block cipher
Vodafone: Design modes

1.3 C - Evaluation

This task includes the following activities.

- Draft of evaluation criteria and statistical tests to be carried out.
- Mathematical evaluation of consecutive proposals for modes and algorithm design.
- Statistical evaluation of consecutive proposals for modes and algorithm design.
- Detailed estimates of performance and complexity of the modes and algorithm design.
- xPA and Side Channel analysis of the modes and algorithm design
- Coordinate input from "external" evaluators (if any)
- Providing a summary of the evaluation results in a public report (***Deliverable D5***)

Evaluation of algorithm will consist of extensive mathematical analysis and statistical testing, xPA and side channel evaluation as well as checking the implementation and performance complexity

Partners: BT, Deutsche Telekom, France Telecom, Gemplus, KPN, Telia

Responsibilities:
BT: Complexity evaluation example block cipher
Deutsche Telekom: Statistical evaluation; evaluation criteria; mathematical evaluation modes
France Telecom: Mathematical evaluation; evaluation criteria; xPA/side channel attacks example block cipher.
Gemplus: Complexity evaluation; xPA/side channel attacks
KPN: Statistical evaluation; mathematical evaluation.
Telia: Mathematical evaluation modes

1.4 D - Specification

- Production of the formal specification of both the modes and the example algorithm (***Deliverable D2)***.
- Detailed estimates of performance and complexity of the proposed design.
- Production of two pairs of test data reports, one for modes and one for the example algorithm ***(detailed test results in Deliverable D3; Black box test data in Deliverable D4)***.
- Production of C-code for inclusion in D2.
- Specification testing

Partners : BT, Deutsche Telekom, Telia, Vodafone

Responsibilities
BT: Formal specification documents for example block cipher; C-implementation and Test Data for example block cipher
Deutsche Telekom: Test Data for modes; check C-implementation and Test Data for example block cipher
Telia: specification testing
Vodafone: C-implementation and Formal specification documents for modes; check Test Data for modes

1.5 Liaison and publication

The objectives of this task are to liaise with the involved 3GPP and ETSI bodies an provide formal reports whenever necessary and to ensure that the specifications can be published and distributed without delays.

Partners: KPN

Responsibilities
KPN Research: ETSI and 3GPP liaison and reporting; define publication and distribution policy

The essential tasks are summarised in the table below.

Task	**Modes**	**Example Kernel (selection)**
DESIGN	BT / KPN / VOD	KPN / THOM (all)
EVALUATION		
- Side channel attacks	GEM PLUS	DT / FT / GEM PLUS
- Complexity	GEM PLUS	BT / GEM PLUS
- Statistical	DT / KPN	DT / KPN
- Mathematical	DT / FT / KPN / TEL	FT / VOD
SPECIFICATION		
- Testing	TEL + ?	TEL + ?
- C-implementation	VOD	BT / DT (check)
- Test Data (**D3, D4**)	DT / VOD (check)	BT / DT (check)
- Formal spec docs (**D2**)	VOD	BT
REPORTS		
- Public Evaluation (**D5**)	THOM	
- General (**D1**)	TEL	
MANAGEMENT , LIAISON and PUBLICATION	KPN, TEL	

Note: Gemplus participates on a voluntary basis. Other companies might also join the STF work on a voluntary basis.

2. Manpower allocation

The manpower and funding allocation over the tasks is shown in the table below.

	BT	DT	FT	Gem plus	KPN	Telia	Thom son	Voda-fone	Total
Task Force management					0.25	0.25			0.5
Design	1				0.75		0.75	0.5	3
Evaluation	0.5	1.5	2		0.75	0.75	1.25	0.5	7.25
Specification	1	1				0.5		1	3.5
Liaison & publication					0.25				0.25
Total	2.5	2.5	2	0	2	1.5	2	2	14.5

3. External independent evaluation

The planning includes an independent external evaluation. It is not clear if such an evaluation will be required by 3GPP.

The costs of an independent external evaluation are not included in the work plan. They should be estimated at about 20.000 Euro per evaluator.

the table below.

week	10			13	14			17	18				22	23			26	27			30	31	
	March 00				April 00				May 00					June 00				July 00				August	
A **Management**	Fix plan and arrange STF																						
B **Design**	Design Criteria 1st draft of modes				1st Alg design 2nd draft of modes									Final algorithm and modes design							Independent e Evaluation (N Task Force W		
	Start point design																						
C **Evaluation**					Evaluation criteria				Mathematical evaluation						Draft evaluation report (D5)					Mathematical evaluation			
							XPA/side channel evaluation													XPA/side channel			
									Statistical evaluation											Statistical evaluati			
									Complexity evaluation											Complexity evaluation			
D **Specification**									Draft Specification (D2) and Test Value Documents (D3 and D4)														
E **Liaison and publications issues**					▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨	▨
week	March 00				April 00				May 00					June 00				July 00				August	
	10			13	14			17	18				22	23			26	27			30	31	

Milestones 2000

A	week 17	first draft modes and example algorithm available
B	week 22	stable draft modes and example algorithm available
C	week 30	draft specification documents available and start external evaluation (if required)
D	week 35	Results external evaluation available (optional)
E	week 39	delivery of documents final D1, D2, D3, D4, D5

5. Participants in Task Force

To Be Completed

KPN Research
Gert Roelofsen (***Task Force Leader***) Tel: +31 70 332 6410
KPN Research Fax: +31 70 332 6477
PO BOX 421
NL-2260 AK Leidschendam
the Netherlands email G.Roelofsen@research.kpn.com
(Mailing address: St. Paulusstraat 4, 2264 XZ Leidschendam, the Netherlands)

Boaz S. Gelbord Tel: +31 70 332 -----
KPN Research Fax: +31 70 332 6477
PO BOX 421
NL-2260 AK Leidschendam
the Netherlands email B.S.Gelbord@research.kpn.com
(Mailing address: St. Paulusstraat 4, 2264 XZ Leidschendam, the Netherlands)

Telia
Per Christoffersson (***Deputy Task Force Leader***) Tel: +46 8 7073547
Telia Promotor Fax: +46 8 7073599
BOX 168
13623 Haninge
Sweden email per.e.christoffersson@telia.se
(Mailing address Marinens väg 30, 13623 Haninge)

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

Ulrich Heister (FE31b)   Tel: +49 6151 83 4220 (2906)
T-Nova Deutsche Telekom   Fax: +49 6151 83 4464
Innovationsgesellschaft mbH
Technologiezentrum
PO box D-64307 Darmstadt
Germany   email Ulrich.Heister@ telekom.de
(Mailing address: Am Kavalleriesand 3, D-64295 Darmstadt, Germany)

Tobias Martin (FE31b)   Tel: +49 6151 83 8841
T-Nova Deutsche Telekom   Fax: +49 6151 83 4464
Innovationsgesellschaft mbH
Technologiezentrum
PO box D-64307 Darmstadt
Germany   email Tobias.Martin@ telekom.de
(Mailing address: Am Kavalleriesand 3, D-64295 Darmstadt, Germany)

France Télécom

Henri Gilbert   Tel: +33 1 45 29 54 97
CNET   Fax: +33 1 45 29 65 19
PAA/TSA/SRC
38-40 Rue du Général Leclerc
F-92131 Issy-les-Moulineaux
France   email: henri.gilbert@cnet.francetelecom.fr

GempLus

Helena Handschuh

email: helena.handschuh@gemplus.com

Thomson-CSF

Leif Nilsen   Tel: +47 22 638 447
Thomson-CSF Norcom   Fax: +47 22 638 497
PO Box 22 ØKern
N-0511 Oslo 5
Norway   email: leif.nilsen@thomson-csf.no
(Mailing address: Østre Aker vei 33, Økern, Oslo, Norway)

Vodafone

Steve Babbage   Tel: +44 1 635 676209
Vodafone Ltd   Fax: + 44 1 635 231776
The Courtyard
2-4 London Road
Newbury Berkshire RG14 1JX
England   `   email: steve.babbage@vf.vodafone.co.uk

Version Control

version	date	comments
Version 01.00	09/03/00	Initial version for review
Version 01.01	14/03/00	Changed title & minor editorial changes