

Security Group
GSM Association

ETSI SAGE

Title: **Provisional work plan for the design of the SAGE GSM A5/3 Task Force (SAGE GSM A5/3 TF)**

Source: KPN Research Version: 00.01

File: A53 algo plan.doc Date: 16/05/01

This document constitutes an initial work plan for the design of GSM A/3 algorithm by a dedicated ETSI SAGE Task Force.

The following assumptions are made.

1. The A5/3 will be based on KASUMI. The GSM Association will confirm before the start of the work that neither 3GPP/ETSI nor Mitsubishi have IPR problems with the use of KASUMI.
2. The work will not start before a definitive requirements specification for the A5/3 has been provided by the GSM Association to SAGE
3. The work will be carried out an ETSI SAGE Special Task Force. The work can only start if ETSI and the GSM Association have agreed on the terms and conditions for such a task force.
4. Any evaluation of the algorithm by external independent evaluators is not a part of this work plan. If required SAGE might co-ordinate the external evaluation, though in principle it would be preferred that the GSM Association undertakes this task.
5. The work will not start before there is clear agreement between SAGE and the GSM Association about the publication of the final design and evaluation report (deliverable D4 in this work plan)

1. Description of tasks, key deliverables and responsibilities

This section describes a first description of tasks, key deliverables and responsibilities. These descriptions might be different from those in the definitive work plan that will be drafted after the requirements outlined above are fulfilled. Additional partners might be added in the final work plan.

The following three tasks are envisaged:

- Project management and coordination
- Design and specification
- Evaluation

1.1 A - project management and coordination

This includes

SG052_01

1. management/liaison
2. general reporting
3. arranging external evaluation (if required)

This task includes the following activities.

- Draft and maintain project plan.
- Arranging and chairing coordination meetings.
- Liaise with relevant 3GPP and GSM Association groups
- Coordinate the external liaison (if required)
- Publication of results

Partners: KPN Research, Telia

Responsibilities:

To be assigned

1.2 B – Design and specification

This task includes the following activities:

4. algorithm design
5. formal specification and verification
6. Production of test values and specification testing

This task includes the following activities:

- Draft of design criteria.
- Design of A5/3 based on KASUMI mode
- Formal specification (**Deliverable D1**)
- Specification testing
- Design conformance test data (**Deliverable D2**)
- Algorithm input/output test data (**Deliverable D3**)
-

Partners: Deutsche Telecom, France Telecom, Vodafone,
Possibly Nokia, Mitsubishi

Responsibilities:

To be assigned

1.3 C - Evaluation

This includes

7. mathematical and performance evaluation
8. external evaluation report

This task includes the following activities.

- Draft of evaluation criteria
- Statistical tests if these need to be carried out.
- Mathematical evaluation of consecutive proposals of Kasumi Modes.
- Estimates of performance and complexity
- Design and Evaluation report (**Deliverable D4**)

Partners: Deutsche Telekom, Thalesgroup (Thomson)
Possibly BT, Gemplus,

Responsibilities:

To be assigned

2. Manpower allocation

The draft global funding allocation over the tasks is shown in the table below. The detailed allocation will be fixed in the final work plan.

	BT	DT	FT	Gem plus	KPN	Mitsubishi	Nokia	Telia	Thomson	Vodafone	Total
Management											1.75
Design Specif											4.50
Evaluation											2.75
Total											9.00

Depending on what the Task force is required to do for organising the external evaluation the total amount of funding might be (slightly) increased.

Milestones 2000

To be defined

5. Participants in 3GPP AF Task Force

To be decided