ETSI
TECHNICAL
REPORT

ETR 278

March 1996

Source: ETSI TC-SAGE

Reference: DTR/SAGE-00014

ICS: 33.020

Key words: GSM, cipher algorithm

Security Algorithms Group of Experts (SAGE); Report on the specification and evaluation of the GSM cipher algorithm A5/2

ETSI

European Telecommunications Standards Institute

ETSI Secretariat

Postal address: F-06921 Sophia Antipolis CEDEX - FRANCE
Office address: 650 Route des Lucioles - Sophia Antipolis - Valbonne - FRANCE
X.400: c=fr, a=atlas, p=etsi, s=secretariat - **Internet:** secretariat@etsi.fr

Tel.: +33 92 94 42 00 - Fax: +33 93 65 47 16

*

Contents

Blank page

Foreword

This ETSI Technical Report (ETR) has been produced by the Security Algorithms Group of Experts (SAGE) of the European Telecommunications Standards Institute (ETSI).

This ETR is a description of the work undertaken by SAGE to design and evaluate the GSM cipher algorithm A5/2, and to approve the release of the specification to the GSM MoU.

The work described in this ETR was undertaken in response to the CEC mandate reference BC-T-045-SI.

Blank page

1 Scope

This ETSI Technical Report (ETR) provides a description of the work undertaken by ETSI SAGE to design and evaluate the GSM cipher algorithm A5/2, and to approve its release to the GSM MoU. The report also provides some background information concerning the need for the algorithm and a summary of the procedures that are to be used by the GSM MoU to distribute the algorithm specification and test data.

With regard to the design of the algorithm, the scope of this ETR is confined to a description of the design criteria, the design methodology and an outline of the content and structure of the specification and test data reports. The algorithm specification is documented in the GSM MoU Permanent Reference document: SG.52, and the associated test data is contained in the GSM MoU Permanent Reference document: SG.53. Both of these documents are subject to a GSM MoU confidentiality and restricted usage undertaking.

With regard to the evaluation of the algorithm, the scope of this ETR is restricted to a description of the evaluation criteria, the method of evaluation, the scope of the internal SAGE evaluation report and the conclusions from the evaluation that led to the technical committee approving the specification. Details of the results of the evaluation are recorded in a report which is confidential to ETSI SAGE.

This ETR includes annex A for information which is a reproduction of the MoU policy with regard to the use of A5/2.

2 References

For the purposes of this ETR, the following reference applies:

[1] Technical Specification GSM 03.20, Version 3.3.2: "European digital cellular telecommunication system (phase 1); Security-related network functions". (ETS 300 534)

3 Abbreviations

For the purposes of this ETR, the following abbreviations apply:

GSM	Global System for Mobile communications
MoU	Memorandum of Understanding

4 Structure of this ETR

This material presented in this ETR is organised in the subsequent clauses, as follows:

- clause 5 provides background information on the GSM ciphers and, in particular, on the need for a second cipher algorithm A5/2;

- clause 6 provides an outline of the work plan adopted by ETSI SAGE to design and evaluate the algorithm and to approve the algorithm specification and associated test data for release to the GSM MoU;

- clause 7 consists of a summary of the main points in the algorithm requirements specification produced by the MoU Security Group;

- clause 8 describes the way in which ETSI SAGE designed the algorithm and produced the specification and associated test data;

- clause 9 gives an overview of the evaluation work carried out by that TC and the conclusions of their evaluation;

- clause 10 summarises the result of the SAGE internal approval procedures; and

- clause 11 provides a brief description of the way in which the GSM MoU will distribute the algorithm specification and test data subject to a confidentiality and restricted usage undertaking.

5 Background to the GSM cipher algorithms

User traffic and certain signalling data is protected against eavesdropping on the GSM radio path by means of a cipher algorithm A5. The way in which the cipher is applied and controlled and the external interfaces to the algorithm are specified in the Technical Specification GSM 03.20 [1]. A specification of the algorithm is however not included in any of the Technical Specifications, but is distributed by and at the discretion of the GSM MoU to its signatories under a confidentiality and restricted usage undertaking.

Although the original GSM phase 1 Technical Specifications only allowed for one cipher algorithm, they have been adapted to allow more than one algorithm and an un-enciphered mode of operation to be used, and the phase 2 Technical Specifications will provide support for up to seven cipher algorithms to provide the functionality of A5. These enhancements are compatible with roaming, and they will enable the use of different algorithms in different regions, and allow old algorithms to be phased out and new ones phased in, should such measures be deemed necessary.

To distinguish the different cipher algorithms, the original GSM MoU algorithm has been designated A5/1, the algorithm which is the subject of this report is designated A5/2, and any subsequent algorithms will be designated A5/3, A5/4, etc. The Technical Specifications for GSM phase 1 have been enhanced to support both A5/1 and A5/2.

The algorithm A5/1 was designed and approved in 1988/9 specifically for the then contemporary group of GSM MoU signatories. In the intervening years, international interest in GSM has grown, and the MoU now attracts signatories who are deploying or proposing to deploy GSM based cellular systems in many different parts of the world. This considerable increase in the number of countries in which GSM service will be provided is leading to potential conflict with various countries' restrictions on the export of products with cryptographic security features. To pre-empt this problem, the MoU decided to develop the second algorithm, A5/2, and to establish a policy governing its use and the use of A5/1.

The MoU policy on the use of A5/1 and A5/2 is recorded in the GSM MoU Permanent Reference document: SG.08, which is appended to this report for information as annex A. The task of designing A5/2 was given to ETSI SAGE based on a requirements specification provided by the GSM MoU Security Group.

6 SAGE work plan

SAGE started work on A5/2 in November 1992 and delivered the final specification and test data to the MoU Security Rapporteur on the 31 March 1993. Delivery was originally planned for May 1993, but this was brought forward because the need for the algorithm became more urgent.

The resource budget for the work was 15,75 man-months, of which 13 man-months were funded from the ETSI Voluntary Work Programme. Of the resource budget, 6,5 man-months were allocated to the design of the algorithm and 9,25 to the evaluation.

To conduct the work, the seven organisations represented in SAGE were divided into two teams: a design team and an evaluation team. The design team consisted of two organisations budgeted to provide approximately 55 % and 45 % of the design effort. The evaluation team consisted of five organisations. The distribution of budgeted evaluation effort across these organisations was approximately 33 %, 22 %, 17 %, 14 % and 14 %.

The work was divided into five phases, phase 0, 1, 2, 3A and 3B, with resource budgets of 3,00, 3,00, 3,75, 3,00 and 3,00 man-months respectively. The work undertaken in each of these phases is outlined in clauses 8 and 9.

7 Algorithm requirements specification

The principal requirements were as follows:

- the algorithm must be designed to realise the functionality of the cipher algorithm A5 defined in the Technical Specification GSM 03.20 [1]. As such it must generate two binary sequences, BLOCK1 and BLOCK2, from a cipher key Kc and a time variable COUNT. BLOCK1 and BLOCK2 each have length 114 bits, and are used to encipher/decipher data transmitted in a GSM time slot. The cipher key has length 64 bits. The time variable COUNT has length 22 bits, and is derived from the TDMA frame number associated with the time slot carrying the data that is to be enciphered/deciphered;

- the algorithm must be implementable in hardware using no more than 4 000 transistors, and be capable of producing BLOCK1 and BLOCK2 from Kc and COUNT in at most 4,615 ms;

- the algorithm must satisfy the general privacy requirement for GSM, that is it must protect traffic on the GSM radio path so that such traffic is no more vulnerable to eavesdropping than on a Public Switched Telephone Network (PSTN) telephone line;

- the algorithm must be such that export controls in force in a number of CEPT member countries permit its use in accordance with the GSM MoU policy reproduced in annex A;

- the algorithm must be approved by all members of ETSI SAGE.

8 Algorithm design

8.1 Design criteria

The design team reflected the requirements on A5/2 in the following design criteria:

- the algorithm would be designed specifically for GSM - no attempt would be made to modify an algorithm used in other applications or to produce an algorithm which was suitable for use in other applications;

- the architecture of the algorithm would be distinct from that of A5/1, although wherever possible functional components of A5/1 would be used - thereby producing an algorithm which differed in its underlying design from A5/1, but which retained a similar level of complexity, and offered the potential for combined A5/1 and A5/2 implementations in mobile terminals with minimal increase in transistors over single implementations;

- approval of the design, in the context of the GSM MoU policy, would be sought from the appropriate authorities in the countries represented by the organisations in the design team, (a design with a structure distinct from that of A5/1 was considered essential for this approval).

8.2 Design methodology

The algorithm was designed using an iterative, interactive and phased approach which may be summarised as follows:

- **Phase 0:** the design team considered a number of different architectures for the algorithm. Of these, two were elaborated and presented for consideration by the evaluation team;

- **Phase 1:** the design team progressed the designs of both of the algorithms, detailing functions and producing complexity estimates in terms of the number of transistors and speed of operation. At the same time, the evaluation team analyzed both of the algorithm architectures. At the end of the phase, the design and evaluation work was brought together and SAGE recommended one of the algorithms to be progressed further;

- **Phase 2:** the design team drafted the specification of the selected algorithm and designed the conformance tests. The evaluation team conducted a detailed analysis. At the end of the phase modifications to the design were made in light of the evaluation results;

- **Phase 3A:** the design team prepared the final specification, and generated the conformance test data. The evaluation team re-visited their analysis in the light of changes made to the design at the end of the previous phase and re-ran a number of statistical tests.

The final phase of the work, phase 3B, was undertaken by the evaluation team and is outlined in subclause 9.2.

8.3 Specification and test data

The specification of the cipher algorithm A5/2 is divided into two main parts. The first part specifies the functional components of the algorithm, whilst the second part specifies how these components are to be used to generate the output blocks, BLOCK1 and BLOCK2, from the input, Kc and COUNT. Two informative annexes are appended to the specification. The first annex consists of illustrative figures to aid understanding of the specification. The second annex consists of a simulation programme listing of the algorithm in ANSI C.

A separate document was produced which provides test data designed to help verify implementations of the algorithm. The document identifies the points in the algorithm where test data is provided, the input, the output and at four intermediate points, and provides a total of twenty four sets of test data listings.

9 Algorithm evaluation

9.1 Evaluation criteria

The following criteria were used as a basis for the evaluation of the algorithm:

- the security of the algorithm would be assessed in the context of the structure of the GSM data (i.e. no attempt would be made to assess the suitability of the algorithm to protect data formatted in a different way);

- the design of the algorithm must be significantly different from that of A5/1;

- confirmation of the suitability of the algorithm, for use in the context of the MoU policy reproduced in annex A, would be sought from the appropriate authorities in the countries represented by the organisations in the evaluation team.

9.2 Method of evaluation

The evaluation and design teams interacted in phases 1, 2 and 3A of the work as indicated in subclause 8.2. In addition there was a final evaluation phase:

- **Phase 3B:** the results of the evaluation were collated in an evaluation report intended for SAGE information and use only.

The methods employed by the evaluation team may be summarised as follows:

- analysis of the structure of the bit sequences in the GSM protocols from the perspective of using the structure as the basis for a cryptographic attack;

- statistical analysis of the output blocks, BLOCK1 and BLOCK2, of the algorithm, their relation to each other and to the input data Kc and COUNT - complementary tests were performed by two organisations and a total of 18 different tests were conducted;

- mathematical analysis of the algorithm and its component functions.

Members of the design and evaluation teams also evaluated the adequacy of the specification. To this end, two independent simulations of the algorithm were made from the specification and confirmed against the test data.

9.3 Evaluation report

The evaluation report provides details of the work undertaken by the evaluation team and the results of their efforts. The report includes chapters on the following topics: acceptance criteria, the GSM threat environment, the structure of data transmitted on the GSM radio path, statistical and mathematical analyses of the algorithm.

The evaluation report is for internal use by SAGE, and will not be published or otherwise made available outside of SAGE.

9.4 Conclusion of evaluation

The main conclusions of the evaluation were as follows:

- the structure of the algorithm is significantly different from that of A5/1;

- the algorithm can be implemented using approximately 3 370 transistors in a layout area of 0,572 mm^2 and the two output blocks can be readily generated within 4,615 ms;

- the algorithm passed all the statistical tests applied at the appropriate significance levels; during phase 2 of the design the algorithm did fail one test, performed by an independent organisation on behalf of one of the SAGE members, but the cause was identified, a parameter of the algorithm was changed, and the test was passed during the re-run;

- the results of the mathematical analysis did not identify any features of the algorithm which could be exploited as the basis for a practical eavesdropping attack on the GSM radio path.

10 Release of algorithm, specification and test data

Prior to release of the algorithm specification and test data, the following approvals were gained:

- all members of SAGE stated that they were satisfied that the algorithm was suitable to protect against eavesdropping on the GSM radio path;

- all members of SAGE stated that they had discussed the algorithm with their appropriate national authority, and that their authority had confirmed that the algorithm was suitable for use in GSM in the context of the GSM MoU policy appended as annex A; thus confirmation was obtained from six national authorities;

- all members of SAGE approved release of the algorithm specification and test data to the MoU Security Rapporteur.

11 Distribution procedures

The specification of the cipher algorithm A5/2 and the accompanying test data will not be published as part of any standard or be made publicly available. Instead it will be distributed, like A5/1, subject to a GSM MoU confidentiality and restricted usage undertaking and the GSM MoU policy reproduced in annex A.

Network operators who are GSM MoU signatories may apply for the specification and test data from the MoU Security Rapporteur. They in turn may provide equipment manufacturers with copies, subject to the confidentiality and restricted usage undertaking.

The detailed rules for the management and disclosure of the algorithms are laid out in the GSM MoU Permanent Reference document: SG.01, and the confidentiality and restricted usage undertaking is detailed in GSM MoU Permanent Reference document: SG.02.

Annex A: GSM Memorandum of Understanding (MoU)

GSM MoU Permanent Reference document**: SG.08**

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Title : **Distribution Policy for Algorithms**

Version: 3.01.00

Date : 18 March 1993

GSM MoU classifications: - Binding
- UnRestricted

List of contents:

Language of original: English

Number of pages : 2

POLICY FOR DATA AND SIGNALLING PRIVACY ALGORITHMS

1. Background

For technical embargo reasons, COCOM and individual national export laws, the distribution of data privacy algorithms is controlled. The MOU Security Group members believe that certain rules will be enforced:

2. Rules for Distribution

2.1 The present A5/1 algorithm can be used by all CEPT members and full members of COCOM.

2.2 All COCOM proscribed countries will be covered by the existing COCOM rules. COCOM embargoes GSM for most proscribed countries, but specified proscribed countries may be eligible for GSM, where encryption is irreversibly disabled.

2.3 Another algorithm, (A5/2) will exist for any operators that do not fall into the above categories. This algorithm is at present being defined by MOU SG and will be ready by May 1993.

Exceptions to these rules will be at the discretion of MOU and national authorities, with advice, where appropriate, from other authorities and operators-

3. Comments to above for Clarification

3.1 The above policy will mean that operators may use only the appropriate algorithm in base stations.

3.2 Once the policy is fully adopted, the intention would be to minimise controls on mobiles. Future generations of mobiles shall support A5/1, A5/2 and no encryption. The protocols to support these will be available in GSM.

History

Document history	
March 1996	First Edition

ISBN 2-7437-0556-6
Dépôt légal : Mars 1996