3GPP TSG SA WG3 Security — S3#12 S3-000227

Technical Specification

THIS DOCUMENT SHOULD BE EDITED BY THE GSM ASSOCIATION SECRETARIAT ACCORDING TO THEIR LAY OUT RULES

Requirements Specification for the GSM A5/3 Encryption Algorithm (GSM Association YYYY, version 0.~~1~~2)

Contents

Intellectual Property Rights

To be added by the GSM Association Secretariat (if needed)

Foreword

This GSM Association Technical Specification has been produced by GSM Association Security Group.

This specification for the so-called A5/3 algorithm is intended to be a mandatory standard for GSM, in addition to the already used A5/1 and A5/2 algorithms.

This document provides a Requirements Specification for the GSM A5/3 algorithm.

The specification is intended for use by the ALGORITHM DESIGN AUTHORITY, which will be responsible for the design of the algorithm.

1 Scope

This specification constitutes a requirements specification for a cryptographic GSM A5/3 algorithm that may be used as the so-called GSM A5 algorithm.

This specification is intended to provide the ALGORITHM DESIGN AUTHORITY, which will be responsible for the design of the algorithm, with the information it requires for designing and delivering a technical specification for this algorithm.

The specification covers the intended use of the algorithm and use of the algorithm specification, technical requirements on the algorithm, requirements on the algorithm specification and test data, and quality assurance requirements on both the algorithm and its documentation. The specification also outlines the background to the production of this specification.

2 References

[1] GSM 03.20: "Digital cellular telecommunications system (Phase 2+); Security related network functions"

3 Definitions and abbreviations

3.1 Definitions

ALGORITHM DESIGN AUTHORITY	A group appointed by the GSM Association to supply the specifications of the GSM A5/3 algorithm
GSM A5/3 algorithm	Encryption Algorithm which fulfils the A5 functionality in GSM and which will be made available by the GSM Association to operators of GSM systems

3.2 Abbreviations

BLOCK1	1st output BLOCK of algorithm
BLOCK2	2nd output BLOCK of algorithm
COUNT	COUNTer (sometimes called TDMA)
DSP	Digital Signal Processor
GSM	Global System for Mobile communications
K_c	GSM Cipher Key

4 Use of the GSM A5/3 Algorithm

This clause defines those organisations for whom the algorithm is intended, describes the application of the algorithm, indicates possible geographical/geopolitical restrictions on the use of equipment which embodies the algorithm, and describes the types of implementations of the algorithm that are envisaged.

4.1 Use of the algorithm

The algorithm shall only be used for GSM ~~authentication and ciphering key generation~~encryption using the A5 function as described in [1, GSM 03.20].

More specifically the use of the algorithm is as follows:

- the algorithm is used to encrypt user and signalling data over the air interface.

4.2 Places of use

The algorithm is implemented in the GSM Hand Sets and in GSM Network. It can be expected that the use of the A5/3 algorithm in GSM will lead to legal restrictions on the use or export of GSM equipment

4.3 Types of implementation

The normal method for implementing the algorithm is in hardware or DSP.

5 Use of the algorithm specification

This clause addresses ownership of the algorithm specification, defines which types of organisation are entitled to obtain a copy of the algorithm specification, and outlines how and under what conditions such organisations may obtain the specification.

5.1 Ownership

The algorithm and all copyright and IPR to the algorithm and test data specifications shall be owned exclusively by the GSM Association.

The GSM Association shall appoint the ALGORITHM DESIGN AUTHORITY for the algorithm. The GSM Association Security Group will draft a Terms of Reference for the work of the ALGORITHM DESIGN AUTHORITY.

Provided the algorithm is adequately protected by IPR or copyright owned by the GSM Association, the algorithm specification shall be openly published by the GSM Association. Use of the algorithm shall be restricted to members of the GSM Association subject to a licence agreement. Those members will, upon request, be entitled to receive test data.

NOTE: the fact that the algorithm is published will lead to legal difficulties in restricting its use. First of all it is not clear to which ~~extend~~ extent it can be protected by IPR. Furthermore it is not clear to which extend the restricted use of the published ~~A3/A8 2000+ algorithm to GSM authentication~~A5/3 only can be legally protected using a licence.

This should be reviewed by the GSM Association legal advisors before the design work is started. They will have to investigate what the possibilities are to patent/copyright a published algorithm

5.2 Users of the specification

The algorithm specification is intended for use by members of the GSM Association, which are or will be operating a GSM Network, and their hand set and infrastructure suppliers.

5.3 Licensing

NOTE: this section will have to be reviewed once the legal issues have been resolved by the GSM Association legal advisors

Users of the algorithm, and users and recipients of the algorithm specification, shall be required to sign a licence agreement.

The GSM Association is responsible for drafting appropriate licence agreements.

Licences shall be royalty free. However, the algorithm custodian may impose a small charge to cover administrative costs involved in issuing the licences.

It is envisaged that there shall be two types of licence agreements: one for GSM Network Operators entitled to use the algorithm, and one for organisations who need the algorithm specification in order to build equipment or components which embody the algorithm, as defined in subclause 5.2.

The licence agreement signed by a GSM Network shall require that organisation to comply with the restrictions on the use of the algorithm.

Comment Per: I suggest different licensing rules for handsets (all manufacturers of mobiles get the spec directly from custodian, not practical to distribute this spec through operators).

5.4 Management of the specification

NOTE: this section will have to be reviewed once the legal issues have been resolved by the GSM Association legal advisors

The GSM Association shall specify the distribution procedure for the algorithm specification. The ALGORITHM DESIGN AUTHORITY for the algorithm is expected to design the appropriate procedure for the distribution of the algorithm after consulting the GSM Association and the GSM Association Security Group.

The outline procedure has the following steps.

1. The GSM Association shall appoint a custodian for administration of the algorithm specification.
2. A GSM Operator which is a member of the GSM Association may request copies of the algorithm specification (and test data) and a licence to use the algorithm from the custodian.
3. If the GSM Operator is entitled to use the algorithm, the custodian shall issue the requested algorithm specifications and test data subject to the GSM Operator signing a licence agreement.
4. A GSM Operator who is licensed to use the algorithm may (sub)licence the use of the algorithm to an organisation which intends to build equipment or components that embody the algorithm. Such an organisation shall then be required by the GSM Operator to sign a licence issued by the custodian before using the algorithm. The GSM Operator will be responsible for this process and provide copies of the signed licence agreement to the custodian.

6 Functional requirements

The ALGORITHM DESIGN AUTHORITY for the algorithm is required to design an algorithm that satisfies the functional requirements specified in this clause.

6.1 Type and parameters of algorithm

The type and parameters of the algorithm are identical to those of the A5 algorithm, which are specified in [1, GSM 03.20] and are summarised here.

The algorithm is a binary key stream generator.

The inputs are the Key K_c and a time variant parameter COUNT.

The outputs of the ciphering algorithm are two binary blocks BLOCK1 and BLOCK2.

Relation of the input and output parameters is illustrated in figure 1.

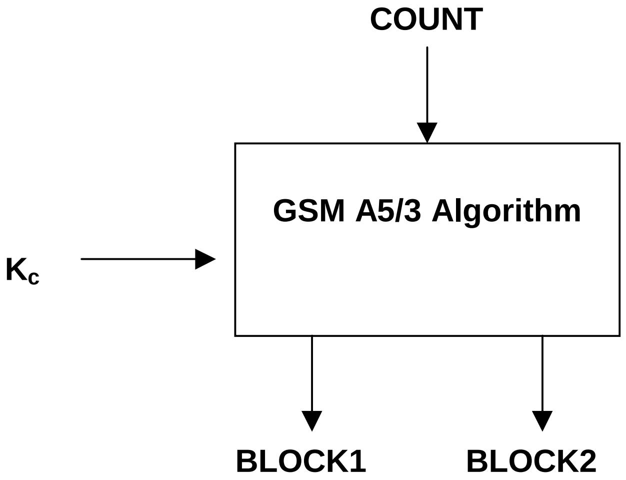

Figure 1 – Algorithm Parameters

The parameters of the algorithms are to be as follows:

K_c	54-128 bits
COUNT	22 bits
BLOCK1	114 or 348 bits
BLOCK2	114 or 348 bits

????? DO WE NEED TO SUPPORT OTHER VALUES FOR THE LENGTH OF BLOCK1 AND BLOCK2 ????

6.1.1 K_c

The encryption key (K_c) can assumed to be randomly generated unstructured data. The length of K_c is 54-128 bits. The algorithm should thus be able to deal with variable key lengths.

6.1.2 COUNT

This input COUNT is an increasing binary counter. The length of COUNT is 22 bits.

6.1.3 BLOCK1

The parameter BLOCK1 should be a random binary value with a length of 114 or 348 bits. The 114 bits are in the case of regular GSM use; the ~~248~~ 348 are in the case of use in EDGE.

6.1.4 BLOCK2

The parameter BLOCK2 should be a random binary value with a length of 114 or 348 bits. The 114 bits are in the case of regular GSM use; the ~~248~~ 348 are in the case of use in EDGE.

6.2 Interfaces to the algorithm

The following interfaces to the algorithm are defined.

- K_c: ______$K_c[0]$, $K_c[1]$, ..., $K_c[k1]$ where $K_c[j]$ is the $K_c$bit with label j and $53 \leq k1 \leq 127$.
- COUNT: COUNT[0], COUNT[1], ..., COUNT[21] where COUNT[j] is the COUNT bit with label j.
- BLOCK1: BLOCK1[0], BLOCK1[1], ..., BLOCK1[b1] where BLOCK1[j] is the BLOCK1 bit with label j and b1=114 or b1 =348.
- BLOCK2: BLOCK2[0], BLOCK2[1], ..., BLOCK2[b2] where BLOCK2[j] is the BLOCK2 bit with label j and b2=114 or b2=348.

6.3 Modes of operation

The mode of operation will be a key stream generation mode where, as described in the previous sections, input parameters are used to produce outputs blocks each with a length of 114 or 348 bits.

6.5 Implementation and operational considerations

This section should be checked with Hand Set manufacturers. The current figures are based on the A5/2 with an extra margin.

Performance requirements.
The time to produce two 114 bit blocks should be max 6 msec using a 2MHz clock.
The time to produce two 348 bit blocks should be max 10 msec using a 2MHz clock.
Remark Benno: it might need to be faster

Implementation complexity.
It should be possible to implement the algorithm in hardware using available technology with less than 4500 transistors and a layout area of less than 0.6 mm^2.

Remark Benno: we might want to allow a more complex algorithm (like e.g. the 3GPP one)

6.6 Design and evaluation principles for the algorithm

- The algorithm will be designed by the ALGORITHM DESIGN AUTHORITY appointed by the GSM Association.
- The algorithm should have IPR or copyright owned by the GSM Association.
- If possible the algorithm should be based on an existing algorithm (but this algorithm should not contain IPR).
- The algorithm will be openly published for public scrutiny. The GSM Association will decide on the moment when to start offering and distributing the Algorithm to its members.
- A number of independent and qualified parties shall, prior to the publication, evaluate the strength of the algorithm.

The algorithm needs to be designed with a view to its continuous use for a period of at least 10 (or 20) years.

Remark Benno: we need to make a specific choice

The security shall be such that

- there are no known plain text attacks on the algorithm needing significantly less operations than an exhaustive key search.

6.7 Exportability of the algorithm

????? WHAT DO WE WANT TO SAY HERE ??????

Suggestion Per: For export I suggest we use same standpoint as in 3G: mobiles shall be (and are supposed to be according to present Wassenaar, independent of key size) freely exportable. Network equipment: here we assume and accept that export control licensing may be needed, but we require "close to worldwide" use to be possible.

7 Algorithm specification and test data requirements

The ALGORITHM DESIGN AUTHORITY are required to provide four separate deliverables: a specification of the algorithm, a set of design conformance test data, a set of algorithm input/output test data and a design and evaluation report. Requirements on the specification and test data deliverables are given in this clause, those on the design and evaluation report in subclause 8.3.

7.1 Specification of the algorithm

An unambiguous specification of the algorithm needs to be provided which is suitable for use by implementers of the algorithm.

The specification shall include an annex that provides simulation code for the algorithm written in ANSI C. The specification may also include an annex containing illustrations of functional elements of the algorithm.

7.2 Design conformance test data

Design conformance test data is required to allow implementers of the algorithm to test their implementations.

The design conformance test data needs to be designed to give a high degree of confidence in the correctness of implementations of the algorithm.

The design conformance test data shall be designed so that significant points in the execution of the algorithm may be verified.

7.3 Algorithm input/output test data

Algorithm input/output test data is required to allow users of the algorithm to test the algorithm as a "black box" function.

The input/output test data shall allow users of the algorithm to perform tests for the modes of operation defined in subclause 6.3.

The input/output test data shall consist solely of data passed across the interfaces to the algorithm.

7.4 Format and handling of deliverables

The specification of the algorithm shall be produced on paper, and provided only to the GSM Association custodian (see subclause 5.4). The document shall be marked *"GSM Association restricted"* and carry the warning *"This information is subject to a licence agreement"*.

The design conformance test data shall be produced on paper, and provided only to the GSM Association custodian. The document shall be marked *" GSM Association restricted"* and carry the warning *"This information is subject to a licence agreement"*.

The algorithm input/output test data shall be produced on paper and on magnetic disc. The document and disc shall be provided to the GSM Association custodian. Special markings or warnings are not required.

8 Quality assurance requirements

This clause advises the ALGORITHM DESIGN AUTHORITY on measures needed to provide users of the algorithm with confidence that it is fit for purpose, and users of the algorithm specification and test data assurance that appropriate quality control has been exercised in their production.

The measures shall be recorded by the ALGORITHM DESIGN AUTHORITY in a design and evaluation report which shall be published by the GSM Association as a Technical Report.

8.1 Quality assurance for the algorithm

Prior to its release to the GSM Association custodian, the algorithm needs to be approved as meeting the technical requirements specified in clause 6 by all members of the ALGORITHM DESIGN AUTHORITY.

8.2 Quality assurance for the specification and test data

Prior to delivery of the algorithm specification, two independent simulations of the algorithm needs to be made using the specification, and confirmed against test data designed to allow verification of significant points in the execution of the algorithm.

Design conformance and algorithm input/output test data needs to be generated using a simulation of the algorithm produced from the specification and confirmed as above. The simulation used to produce this test data needs to be identified in the test data deliverables and retained by the ALGORITHM DESIGN AUTHORITY.

8.3 Design and evaluation report

The design and evaluation report is intended to provide evidence to potential users of the algorithm, specification and test data that appropriate and adequate quality control has been applied to their production. The report shall explain the following:

- the algorithm and test data design criteria;
- the algorithm evaluation criteria;
- the methodology used to design and evaluate the algorithm;
- the extent of the mathematical analysis and statistical testing applied to the algorithm;
- the principal conclusions of the algorithm evaluation;
- the quality control applied to the production of the algorithm specification and test data.

The report shall confirm that all members of the ALGORITHM DESIGN AUTHORITY have approved the algorithm, specification and test data.

9 Summary of the ALGORITHM DESIGN AUTHORITY deliverables

- Specification of the algorithm:
- a document for delivery only to the GSM Association custodian;

- Design conformance test data:
- a document for delivery only to the GSM Association custodian;

- Algorithm input/output test data:
- in a document and on disc for delivery to the GSM Association custodian;

- Design and evaluation report;
  - to be published as an GSM Association Technical Report.

Annex A (informative): History

Document history		
Version 0.1	January 2000	First draft for review by GSM Security 2000 group