TR 101 375 V1.1.1 (1998-09)

Technical Report

Security Algorithms Group of Experts (SAGE); Report on the specification, evaluation and usage of the GSM GPRS Encryption Algorithm (GEA)

Reference

DTR/SAGE-00015-1 (cqc00ics.PDF)

Keywords

security, algorithm, GSM

ETSI

Postal address

F-06921 Sophia Antipolis Cedex - FRANCE

Office address

650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16
Siret N° 348 623 562 00017 - NAF 742 C
Association à but non lucratif enregistrée à la
Sous-Préfecture de Grasse (06) N° 7803/88

Internet

secretariat@etsi.fr
http://www.etsi.fr
http://www.etsi.org

Contents

Intellectual Property Rights

IPRs essential or potentially essential to the present document may have been declared to ETSI. The information pertaining to these essential IPRs, if any, is publicly available for **ETSI members and non-members**, and can be found in SR 000 314: *"Intellectual Property Rights (IPRs); Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards"*, which is available **free of charge** from the ETSI Secretariat. Latest updates are available on the ETSI Web server (http://www.etsi.fr/ipr or http://www.etsi.org/ipr).

Pursuant to the ETSI IPR Policy, no investigation, including IPR searches, has been carried out by ETSI. No guarantee can be given as to the existence of other IPRs not referenced in SR 000 314 (or the updates on the ETSI Web server) which are, or may be, or may become, essential to the present document.

Foreword

This Technical Report (TR) has been produced by ETSI Project Security Algorithms Group of Experts (SAGE).

The work described in the present document was undertaken in response to a request made by ETSI SMG10.

1 Scope

The present document is a description of the work undertaken by SAGE STF123 to design the GSM GPRS Encryption Algorithm (GEA), and to approve its release to the ETSI Secretariat, acting as custodian for GEA on behalf of ETSI SAGE. The present document also provides some background information concerning the need for and usage of the algorithm and a summary of the procedures that are to be used by the ETSI Secretariat to distribute the algorithm specification and test data.

With regard to the design of the algorithm, the scope of the present document 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 and associated test data are documented in the Specification of GEA which consists of the following three documents.

- Document 1: Algorithm Specification;
- Document 2: Design Conformance Test Data;
- Document 3: Algorithm Input / Output Test Data.

The first two parts are confidential and their distribution will be restricted by the algorithm custodian, the ETSI secretariat, to a group of approved recipients.

With regard to the evaluation of the algorithm, the scope of the present document 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.

2 References

The following documents contain provisions which, through reference in this text, constitute provisions of the present document.

- References are either specific (identified by date of publication, edition number, version number, etc.) or non-specific.
- For a specific reference, subsequent revisions do not apply.
- For a non-specific reference, the latest version applies.
- A non-specific reference to an ETS shall also be taken to refer to later versions published as an EN with the same number.

[1] TS 101 106 (V6.0): "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); GPRS ciphering algorithm requirements (GSM 01.61 version 5.0.0)".

3 Abbreviations

For the purposes of the present document, the following abbreviations apply:

GEA	GPRS Encryption Algorithm
GPRS	General Packet Radio Service
SAGE	Security Algorithms Group of Experts

4 Structure of the present document

The material presented in the present document is organized in the subsequent clauses, as follows:

- clause 5 provides background information on GEA;
- 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 ETSI Secretariat;
- clause 7 consists of a summary of the main points in the algorithm requirements specification produced by ETSI SMG10;
- clause 8 describes the way in which ETSI SAGE STF123 designed the algorithm and produced the specification and associated test data;
- clause 9 gives an overview of the evaluation work carried out by that STF and the conclusions of their evaluation;
- clause 10 summarizes the result of the SAGE internal approval procedures;
- clause 11 outlines the possibilities to use the algorithm;
- clause 12 provides a description of the way in which the documents containing the algorithm specification and test data will be managed.

5 Background to the GEA

Within the GSM community the need for enhanced data services in GSM have been identified. To fulfil this need ETSI SMG defined a new service for GSM: the General Packet Radio Service (GPRS). Security is an important aspect for this service and it was considered that, just like the regular GSM service, the GPRS service required authentication and confidentiality.

Authentication in GPRS can be achieved using the regular GSM authentication mechanism. However due to the use of different protocols the confidentiality for GPRS could not be realized using the standard GSM encryption.

Therefore SMG10 identified the need to develop a special standard encryption algorithm for GPRS. SMG10 drafted a detailed requirements specification for such an encryption algorithm [1]. Then ETSI SAGE was asked to design the algorithm. To carry out this work ETSI SAGE set up a Special Task Force (STF123) which designed the algorithm and called it GEA.

6 SAGE STF123 work plan

The start of the work of SAGE STF123 was delayed several times because of procedural problems in making available the required funding. STF 123 carried out some preliminary activities in the last quarter of 1997 and decided to formally start work in January even though no funding for the work was guaranteed at that moment (the actual funding for the work was not made available until April 1998 when the ETSI board decided to fully fund the work).

The design was finalized early May 1998. By the second half of May the algorithm was ready for distribution via an interim custodian which was appointed pending the finalization of procedures needed to put ETSI in place as custodian.

The total resource budget for the work was 429 man-days. Of this total 387 days were funded by ETSI and 42 were funded by the individual SAGE members participating in the work.

Of the resource budget, approximately 205 days were allocated to the design of the algorithm and 150 to the evaluation. The rest was spent on algorithm usage, specification testing and management procedures.

To work was carried out by six organizations which were divided into two teams: a design team and an evaluation team. The allocation of budgets over the participating organizations was 22,5 %, 20 %, 20 %, 12,5 %, 12,5 % and 12,5 %.

The work was divided into five main tasks:

- PT management (approximately 7 % of the budget);
- design (approximately 48 % of the budget);
- evaluation (approximately 35 % of the budget);
- specification testing (approximately 5 % of the budget);
- algorithm usage and management(approximately 5 % of the budget).

7 Outline of algorithm requirements specification

The requirements for the design of the GEA were given in [1].

The functional requirements for the algorithm as formulated by ETSI SMG10 are summarized below.

7.1 Type and Parameters of Algorithm

In [1] the following requirements are stated:

The algorithm is to be a symmetric stream cipher.

The inputs are the Key (Kc), the frame dependent input (INPUT), and transfer direction (DIRECTION). The output of the ciphering algorithm is the output string (OUTPUT). Relation of the input and output parameters is illustrated in figure 1.

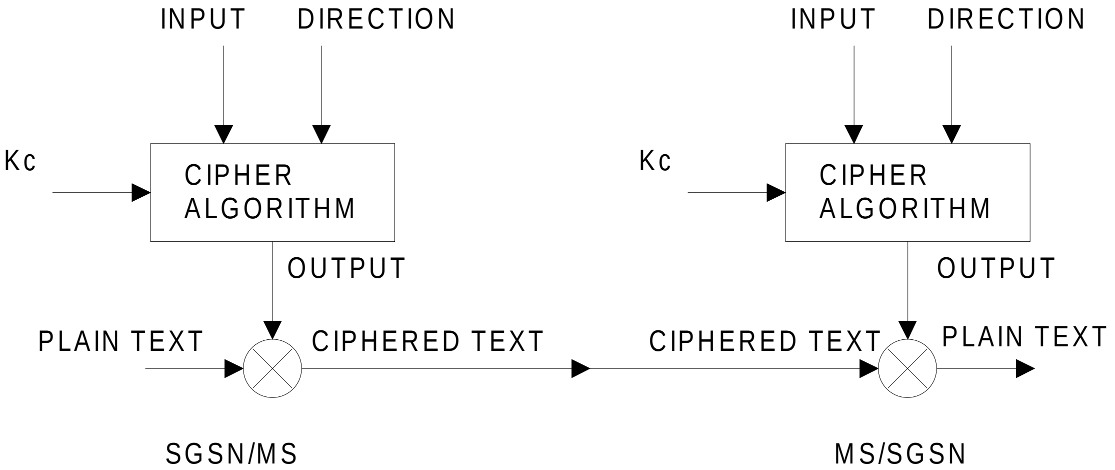

Figure 1: Basic GPRS ciphering environment

The parameters of the algorithms are to be as follows:

Kc	64 bits;
INPUT	32 bits;
DIRECTION	1 bit;
OUTPUT	1 600 octets.

7.2 Interfaces to the Algorithm

In [1] the following requirements are stated:

The following interfaces to the algorithm are defined:

- Kc:
  - K[0], K[1], ..., K[63];
    where K[i] is the Kc bit with label i;
- INPUT:
  - X[0], X[1], ..., X[31];
    where X[i] is the INPUT bit with label i;
- DIRECTION:
  - Z[0];
    where Z[0] is the DIRECTION bit with label 0;
- OUTPUT:
  - W[0], W[1], ..., W[1599];
    where W[i] is the data output octet with label i.

7.3 Modes of Operation

In [1] the following requirement is stated:

Uplink and downlink transfers are independent. Hence ciphering for uplink and downlink shall be independent from each other. This contrasts to algorithm A5 where keystreams for both directions are generated from the same input.

7.4 Implementation and Operational Considerations

In [1] the following requirements are stated:

The GPRS performance requirements are specified in GSM 02.60.

Requirements refer to an MS, which admits only 1 timeslot GPRS communication (see note 1), and to an MS, which admits GPRS communication over the maximum number of timeslots (see note 2).

NOTE 1: An MS which admits only one time slot GPRS communication, the maximum capacity in each direction is 21,4 kbit/s (total rate up to 42,8 kbit/s), 12 initializations per second are assumed (assuming packet length of 500 octets) (scenario 1).

NOTE 2: An MS would have a maximum throughput of all 8 timeslots in both directions each transmitting and receiving at their maximum rate of 21,4 kbit/s (total rate up to 342,4 kbit/s), 100 initializations per second are assumed (assuming packet length of 500 octets) (scenario 2).

The performance requirements, on the GPRS ciphering algorithm, as used in scenario 1, are expected to be similar to the performance of the existing A5 algorithm.

It is also expected that the performance increases linearly depending on the number of timeslots, the MS is able to use for GPRS.

7.5 Resilience of Algorithm

In [1] the following requirements are stated:

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

The security shall provide at least comparable protection as the baseline security provided by the GSM encryption algorithms.

ETSI SAGE are required to design the algorithm to a strength which reflects the above qualitative requirements.

7.6 Restrictions on Export

In [1] the following requirements are stated:

An algorithm with minimal restrictions on exports when licensed and managed as described in clause 5 is desired because of the global use of GSM.

(The referenced clause 5 is that of document [1] which outlines the Algorithm Usage and Management as described in clauses 11 and 12 of the present document.)

8 Algorithm design

8.1 Design criteria

The requirements for the design of the GEA outlined in clause 7 and parts of [1] were translated by STF123 to a number of design criteria and starting points for the design. These are summarized below.

ALGORITHM BASICS

- The algorithm shall be a stream cipher.
- The algorithm input parameters are a 64-bit key, and a 32-bit IV and a single bit "direction" flag.
- The algorithm should be generally exportable taking into account current export restrictions.
- The strength should be optimized taking into account the above requirement.

IMPLEMENTATION CONSTRAINTS

- The preferred method of implementation is in hardware therefore algorithm design may take a bit-orientated approach in preference to a byte-orientated approach.
- Before release of the final algorithm specification there should, if possible, be an assessment by potential implementers that the complexity and performance of the algorithm are acceptable.

PLAIN TEXT DATA

- The payload can vary between 5 and 1 600 octets (including the FCS).
- Normal use of the algorithm is either short packets (25 to 50 octets) or long packets (500 to 1 000 octets).
- Packet size is dependent on the application and no assumption can be made that successive packets are likely to be of the same length.

ALGORITHM OUTPUT

- The minimum length of the output string is 5 octets.
- The maximum length (1 600 octets) of the output string is the maximum length of the payload of the LLC frame, including the FCS (Frame Check Sequence, 3 octets).

8.2 Design methodology

The algorithm was designed using an iterative, interactive and phased approach which is summarized below:

- **Phase 1:** The design team produced a first design proposal for the algorithm. This was presented for consideration by the evaluation team.
- **Phase 2:** Based on the results from the evaluation team, the design team revised the design to produce a second design proposal for the algorithm. This design was again reviewed by the evaluation team.
- **Phase 3:** After the evaluation an algorithm design was fixed in principle. This design was subjected to a detailed analysis by the evaluation team. In parallel a modified version of the algorithm design, which was equivalent from the point of view of complexity and performance, was provided to four interested manufacturers for a preliminary evaluation.
- **Phase 4:** Having reviewed the results of the analysis by the evaluation team and the results of the complexity and performance pre-evaluation by manufacturers, the design team prepared the final specification, and generated the conformance test data. A document containing "The rules for Management of the GEA" and a final internal SAGE evaluation report were drafted. Furthermore two test implementations were carried out to check the correctness and completeness of the specification. Finally a TR on the work undertaken was drafted (the present document).

8.3 Specification and test data

The algorithm specification and associated test data are documented in the Specification of GEA which consists of the following three documents:

- Document 1: Algorithm Specification;
- Document 2: Design Conformance Test Data;
- Document 3: Algorithm Input / Output Test Data.

The first two parts are confidential and their distribution will be restricted by the algorithm custodian, the ETSI secretariat, to a group of approved recipients (see clause 12).

Document 1 is normative and contains the formal specification of the functional elements of GEA. There are two informative annexes to Document 1. The first annex consists of illustrative diagrams to aid understanding of the specification. The second annex consists of an example programme listing of the algorithm in 'C'.

Document 2 is informative and provides design conformance test data designed to help verify implementations of the algorithm. The document identifies the relevant intermediate points in the algorithm where test data is provided. Then it gives input, internal and output parameters at these points, and provides different sets of test data listings.

Document 3 is informative and provides test data designed to help verify the correct functioning of the algorithm seen as a "black box". The document identifies the input and output interfaces and provides a number of sets for the different modes of operation of the algorithm. The test sets are designed in such a way that all elements of any functions in the algorithm are used at least once.

9 Algorithm evaluation

9.1 Evaluation criteria

The evaluation team decided to take the requirements listed in clause 7 as the basis for evaluation. In particular this means that the mathematical analysis was based on the requirements quoted in subclause 7.5.

An additional requirement was that the algorithm would pass all the usual statistical tests for stream ciphers.

9.2 Method of evaluation

The evaluation and design teams interacted at the end of the phases 1 and 2. During phase 3 there was a closer co-operation between the design and evaluation teams and the final (minor) modifications were discussed together. In addition during this phase potential manufacturers of GPRS systems assessed the complexity and performance of an equivalent algorithm.

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

- during the second and third phase of the work, a detailed mathematical analysis of the algorithm and its component functions as well as statistical analysis of the output of the algorithm in relation to the input and the key;
- an evaluation by external parties of a modified, but from complexity and performance perspective equivalent, version of the algorithm;
- final round of extensive statistical analysis of the final design in which the statistical properties of the algorithm output were tested in relation to the input and the key;
- an independent assessment of the final design by the STF of the performance of the algorithm for hardware and software implementations.

Two parties not directly involved in the design and evaluation teams also evaluated the adequacy of the specification. To this end, these parties made independent simulations of the algorithm from the specification and confirmed these 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, description and mathematical evaluation of intermediate and final algorithm designs, performance and complexity evaluation, statistical evaluation, and algebraic evaluation.

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 algorithm is a bit oriented key stream generator.
- The complexity and performance of the algorithm are such that it is suitable for implementation in hardware. This conclusion was confirmed by the pre-evaluation.

  Assessments made by the STF indicate that the achievable hardware speeds assuming a 50 MHz clock range from 3,6 (block length 50 byte) to 6,1 (block length 1 500 byte) Mbytes/sec. Software implementations may not be possible in GSM GPRS hand sets, but can be realized in the GSM GPRS infrastructure. A straightforward C implementation of the algorithm on a Pentium, 75 MHz, Windows 95 achieved speeds of from 110 (block length 50 byte) to 143 (block length 1 500 byte) kbytes/sec. On a Pentium II, 300 MHz, Windows NT 4.0 the achieved speeds range from 297 (block length 50 byte) to 391 (block length 1 500 byte) kbytes/sec.
- The algorithm passed all the statistical tests applied at the appropriate significance levels; the statistical tests which were performed on the algorithm as a whole included typical statistical tests for a stream cipher such as the Frequency test, Overlapping m-tuple test, Gap test, Run test, Coupon-Collectors test, the universal Maurer test, the Poker test, the Correlation test, the Rank test, the Linear Complexity test, the Ziv-Lempel Complexity test.

  The algorithm was also tested as a block cipher using Dependence tests with satisfactory results.
- In general the algorithm will be exportable under the current national export restrictions on cryptography applied in European countries.
- Within this operational context, the algorithm provides an adequate level of security against eavesdropping of GSM GPRS services.

10 Release of algorithm, specification and test data by SAGE

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 within its operational context the algorithm provides an adequate level of security against eavesdropping of the GSM GPRS service.
- All members of SAGE stated that they had discussed exportability of the algorithm with their appropriate national authority, and that their authority had confirmed that the algorithm was in principle exportable in its intended use as described in [1]; thus confirmation was obtained from six national authorities. Major restrictions on the export of the algorithm specification or algorithm implementations are not foreseen. In specific cases export problems for the algorithm specification or algorithm implementations can occur however.
- All members of SAGE approved release of the algorithm specification and test data to the ETSI Secretariat, acting as custodian for the GEA on behalf of ETSI SAGE. However, until the ETSI Secretariat obtains an export licence for the algorithm an interim custodian will maintain custody of the algorithm.

11 Algorithm Ownership and Usage

11.1 GEA Ownership

The algorithm and all copyright to the algorithm and test data specifications shall be owned exclusively by ETSI. The design authority for the algorithm shall be ETSI SAGE.

The algorithm specification shall not be published as an ETSI standard or otherwise made publicly available, but shall be provided to organizations that need and are entitled to receive it subject to a licence and confidentiality agreement.

The licence and confidentiality agreement shall require recipient of the specification not to attempt to patent the algorithm or otherwise register an Intellectual Property Right (IPR) relating to the algorithm or its use.

11.2 Users of the GEA specification

The algorithm specification may be made available to the following types of organizations:

- organizations which are designer of or competent to manufacture GSM GPRS systems, where the GEA is included in the systems;
- organizations which are designer of or competent to manufacture components for GSM GPRS systems, where at least one of the components includes the GEA;
- organizations which are designer of or competent to manufacture a GSM GPRS system simulator for approval testing of GSM GPRS systems, where the simulator includes the GEA; and
- organizations which are an operator of a GSM GPRS system which includes the GEA.

11.3 Licensing

Recipients of the algorithm specification, shall be required to sign a licence and confidentiality agreement.

Appropriate licence and confidentiality agreements shall be drawn up by ETSI.

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

The licence and confidentiality agreement signed by an organization that needs the algorithm specification, shall require that organization to adopt measures to ensure that handling of the algorithm specification and implementations of the algorithm are commensurate with the need to maintain confidentiality of the algorithm.

12 Management and distribution procedures for the algorithm specification

The algorithm specification and associated test data are documented: Specification of the GEA consisting of the three documents listed in subclause 8.3.

All three documents are distributed by the custodian of the algorithm, the ETSI secretariat. The contact person is:

Mr Pierre De Courcel

Fax +33 4 93 654716

ETSI

F-06921 Sophia Antipolis Cedex

France

Both Documents 1 and 2 will not be published as part of any standard or be made publicly available. Their distribution will be restricted by the algorithm custodian to a group of approved recipients, and this distribution will be subject to a "Licence and confidentiality agreement".

The detailed rules for the management and distribution of the algorithm specification and associated test data can be found in annex A.

Annex A (informative): Rules for the management of the standard GSM GPRS Encryption Algorithm (GEA)

Version1.1; May 1998

A.1 Introduction

The purpose of the present document is to specify the rules for the management of the Standard GSM GPRS Encryption Algorithm (GEA).

The management structure is defined in clause A.2. This structure is defined in terms of the principals involved in the management of the GEA (ETSI, ETSI SMG, GEA Custodian and Approved Recipients) together with the relationships and interactions between them.

The procedures for delivering the GEA to Approved Recipients are defined in clause A.3. This clause is supplemented by Appendix 1 which specifies the items which are to be delivered.

Clause A.4 is concerned with the criteria for approving an organization for receipt of the GEA and with the responsibilities of an Approved Recipient. This clause is supplemented by Appendix 2 which contains a Confidentiality and Restricted Usage Undertaking to be signed by each Approved Recipient.

Clause A.5 is concerned with the appointment and responsibilities of the GEA Custodian.

A.1.1 GEA Specification Documents

The specification of the GEA consists of the following three documents.

1 Specification of the GPRS Encryption Algorithm (GEA)

Document 1: Algorithm Specification

2 Specification of the GPRS Encryption Algorithm (GEA)

Document 2: Design Conformance Test Data

3 Specification of the GPRS Encryption Algorithm (GEA)

Document 3: Algorithm Input / Output Test Data

The rules for management as described in the present document apply for Documents 1 and 2 only. Document 3 will be a publicly available document and its distribution will not be subject to any rules.

A.2 GEA Management Structure

The management structure is depicted in figure 1. The figure shows the three principals involved in the management of the GEA and the relationships and interactions between them.

ETSI is the owners of the GEA algorithm. The ETSI Secretariat together with ETSI SMG sets the approval criteria for receipt of the algorithm (see clause A.4).

The GEA Custodian is the interface between ETSI and the Approved Recipients of the GEA.

The custodian shall be the ETSI Secretariat unless it is decided by ETSI Secretariat and/or ETSI SMG to delegate this task to a third party on the basis of an agreement signed between the latter and the ETSI Secretariat.

The GEA Custodian's duties are detailed in clause A.5. They include distributing the GEA to Approved Recipients, as detailed in clause A.3, providing limited technical advice to Approved Recipients and providing algorithm status reports to ETSI SMG.

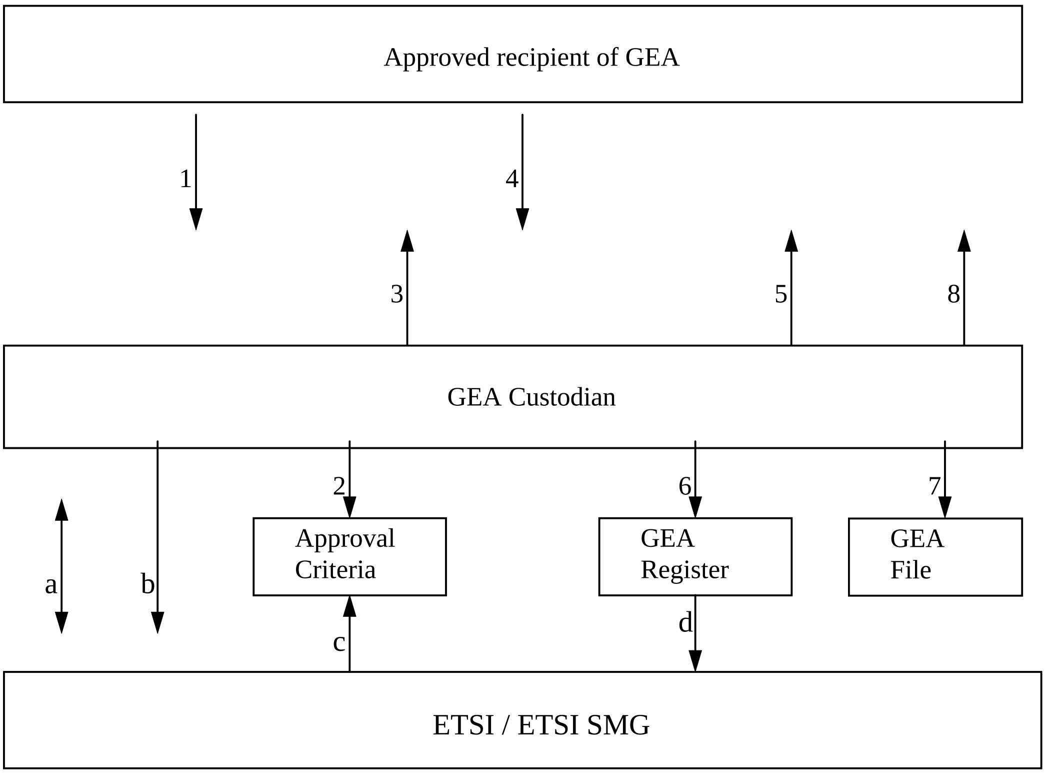

Figure A.1: GEA Management Structure

<u>Key to Figure:</u>

a = Agreement between GEA Custodian and ETSI

b = Status reports and recommendations

c = Setting of approval criteria

d = Restricted details of the GEA register

1 = Request for GEA

2 = Check of request against approval criteria

3/4 = Exchange of Confidentiality and Restricted Usage Undertaking

5 = Dispatch of GEA Specification

6 = Update the GEA register

7 = Document filing

8 = Technical advice

A.3 Distribution Procedures

A.3.1 Distribution by GEA Custodian

The following procedures for distributing the GEA to Approved Recipients are defined with reference to figure 1.

- The GEA Custodian receives a written request for N copies of the GEA Specification (see note 1), where N should not be bigger than six.
- The GEA Custodian checks whether the requesting organization meets the approval criteria (see clause A.4).
- If the request is approved, the GEA Custodian dispatches 2 copies of the Confidentiality and Restricted Usage Undertaking (as given in Appendix 2) for signature by the Approved Recipient (see notes 2 and 6) together with a copy of the present document (Rules for the Management of the Standard GSM GPRS Encryption Algorithm).
- Both copies of the Confidentiality and Restricted Usage Undertaking must be signed by the approved recipient (see notes 5 and 7) and returned to the GEA Custodian, together with the payment of charges if any.
- The GEA Custodian sends up to N (note 3) numbered copies of the GEA Specification to the Approved Recipient, together with one countersigned copy of the returned Confidentiality and Restricted Usage Undertaking and a covering letter (see notes 4 and 6).
- The GEA Custodian updates the GEA Register by recording the name and address of the recipient, the numbers of the copies of the GEA Specification delivered and the date of delivery. If the original request is not approved, the GEA Custodian records the name and address of the requesting organization and the reason for rejecting the request in the GEA Register (see also note 8).
- The GEA Custodian countersigns and files the second returned copy of the Confidentiality and Restricted Usage Undertaking in the GEA File together with a copy of the covering letter sent to the Approved Recipient.

NOTE 1: Requests for the GEA Specification may be made directly to the GEA Custodian or through ETSI, where appropriate.

NOTE 2: The confidentiality and Restricted Usage Undertaking specifies the number of copies requested.

NOTE 3: The covering letter specifies the numbers of the copies delivered.

NOTE 4: The GEA Custodian sends all items listed in Appendix 1. Requests for part of the package of items are rejected.

NOTE 5: An organization may request the specification on behalf of a second organization to which it is subcontracting work which requires the specification. In this case, the first organization is responsible for returning a Confidentiality and Restricted Usage Undertaking signed by the second organization. Refer to the Transfer details given in A.3.2.

NOTE 6: Under normal circumstances the Custodian is expected to respond within 25 working days, excluding the delay of the procedures with the National Authorities.

NOTE 7: The approved recipient has to be a legal representative of the receiving organization.

NOTE 8: If a GEA Specification is returned to the GEA Custodian (for example the recipient may decide not to make use of the information), then the GEA Custodian destroys the specification and enter a note to this effect in the GEA Register.

A.3.2 Transfers by a Beneficiary

An organization which has already been approved and has obtained GEA specification may transfer one or more of these specifications to a second organization which requires the specification.

In this case, the first organization shall ensure that the second organization meets the approval criteria. The first organization shall get the second organization to sign two copies of the Confidentiality and Restricted Usage Undertaking. The first organization then sends these to the GEA Custodian, together with the numbers of the specifications which are to be transferred.

The GEA Custodian then enters the transfer details in the GEA Register, countersigns the Confidentiality and Restricted Usage Undertakings, returns one of these together with a covering letter to the first organization , and files the other and a copy of the letter in the GEA File.

The first organization is responsible for passing (a copy of) the countersigned Confidentiality and Restricted Usage Undertaking to the second organization.

A.4 Approval Criteria

The approval criteria are set by the ETSI Secretariat together with ETSI SMG and maintained by the GEA Custodian. The GEA Custodian may recommend changes to these criteria.

In order for an organization to be considered an Approved Recipient of the GEA it has to satisfy at least one of the following criteria:

- The organization is designer of or competent to manufacture GSM GPRS systems, where the GEA is included in the systems.
- The organization is designer of or competent to manufacture components for GSM GPRS systems, where at least one of the components includes the GEA.
- The organization is designer of or competent to manufacture a GSM GPRS system simulator for approval testing of GSM GPRS systems, where the simulator includes the GEA.
- The organization is an operator of a GSM GPRS system which includes the GEA.

The GEA Custodian will decide whether an organization requesting the GEA Specification may be considered to be an Approved Recipient. Any doubtful cases will be referred back to ETSI Secretariat or ETSI SMG.

A.5 The GEA Custodian

A.5.1 Responsibilities

The GEA Custodian is expected to perform the following tasks:

- To approve requests for the GEA by reference to the Approval Criteria given in clause A.4.
- To exchange the Confidentiality and Restricted Usage Undertaking with Approved Recipients as described in clause A.3.
- To obtain the Administrative authorization and export licences required by the National Authorities of its country if any.
- To distribute the GEA Specification as detailed in clause A.3 (see note 1).
- To maintain the GEA Register as described in clause A.3.
- To hold in custody the contents of the GEA File as specified in clause A.3.
- To provide recipients of the GEA with limited technical support, i.e., answer written queries arising from the specification or test data (see note 2).
- To advise ETSI/ETSI SMG of any problems arising with the approval criteria.
- In the light of written queries from recipients of the GEA Specification, to make recommendations to ETSI/ETSI SMG for improvements / corrections to the specification and, subject to ETSI/ETSI SMG approval, make and distribute the changes (see note 3).
- To provide ETSI/ETSI SMG with information from the GEA Register when requested to do so.

NOTE 1: Registered postage will be used. If recipients require a different delivery service then they can be expected to pay the full costs.

NOTE 2: The GEA Custodian will only endeavour to answer questions relating to the GEA Specification. He is not expected to provide technical support for development programmes.

NOTE 3: Numbered copies of any changes to the GEA Specification must be automatically distributed to all recipients of the specification and a record of the distribution entered in the GEA Register.

A.5.2 Appointment

The GEA Custodian is:

ETSI Secretariat

The contact person is:

Mr Pierre De Courcel

Fax +33 4 93 65 47 16

ETSI

F-06921 Sophia Antipolis Cedex

France

Until the Custodian has arranged all administrative procedures required, an Interim Custodian will be appointed. This Interim Custodian is:

KPN Research, the Netherlands

The contact person is:

Mr Gert Roelofsen

Fax +31 70 3326477

KPN Research

PO Box 421

NL-2260 AK Leidschendam

The Netherlands

Both the GEA Custodian as well as the Interim Custodian will ask a fee from the recipient to cover the cost of distribution of the specification document 1 and specification document 2. This fee is set to ECU 1 000,-per request.

Both the GEA Custodian as the Interim Custodian may ask an optional fee from the recipient to cover the cost of distribution of the specification document 3.

All requests for either the GEA specification document 1 and specification document should be addressed to the indicated contact person or to ETSI.

Appendix 1: Items delivered to Approved Recipient of GEA

ITEM-1: Up to N numbered copies to the GEA Specification where N is the number of copies requested.

ITEM-2: A countersigned Confidentiality and Restricted Usage Undertaking.

ITEM-3: A cover letter from and signed by the GEA Custodian listing the delivered items (ITEM-1 and ITEM-2 above) and the numbers of the specifications delivered (see note).

NOTE: In case of a transfer (see A.3.2), only ITEM-2 and the cover letter are delivered. Moreover, the cover letter details the numbers of the transferred specifications.

Appendix 2: Confidentiality and Restricted Usage Undertaking

CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING

relating to

the GEA algorithm for the protection of the information exchanged over the radio channels of a GSM General Packet Radio Service (GPRS) System .

BETWEEN

(COMPANY NAME) ....

(COMPANY ADDRESS) ....

....

....

....

hereinafter called: the BENEFICIARY;

AND

(COMPANY NAME) ....

(COMPANY ADDRESS) ....

....

....

....

hereinafter called: the CUSTODIAN.

Whereas

The BENEFICIARY has alleged supported by additional information provided, that he fulfils at least one of the following criteria:

- He is designer of or competent to manufacture GSM GPRS where GSM GPRS Standard Encryption Algorithm (hereinafter referred to as GEA) is included in the systems.
- He is designer of or competent to manufacture components for GSM GPRS systems where at least one of the components include the GEA.
- He is designer of or competent to manufacture GSM GPRS system simulator for approval testing of GSM GPRS systems where the simulator includes the GEA.

The CUSTODIAN undertakes to give to the BENEFICIARY:

- registered copies of the detailed specification of the confidentiality algorithm for protection of the information exchanged over the radio channels of a GSM GPRS system.

The BENEFICIARY undertakes:

1) To keep strictly confidential all information contained in the detailed specification of the GEA and all related communications written or verbal which have been associated with that information before and after the signature of the present undertaking (the "INFORMATION").

2) Not to make copies of the GEA specifications (all copies of these specifications must be produced, numbered and registered by the GEA Custodian).

3) Not to disclose the INFORMATION to any third party without prior and explicit authorization in writing by the CUSTODIAN.

4) To the best of his ability to take measures to avoid that his personnel disclose to third parties, without prior and explicit authorization in writing by the CUSTODIAN, all or part of the INFORMATION.

5) To use the INFORMATION in the GEA specification exclusively for the provision of GSM GPRS components, systems or services, thus refraining from making any other use of the GEA or information in the GEA specification.

6) Not to register, or attempt to register, any IPR (patents or the like rights) relating to the GEA and containing all or part of the INFORMATION.

7) To design his equipment, to the best of his ability, in a manner that protects the GEA from disclosure and ensures that it cannot be used for any purpose other than to provide the GSM GPRS services for which it is intended.

   These services are specified in the documents: ETSI GSM 02.60 (GPRS Service Description: Stage 1), ETSI GSM 03.60 (GPRS Service Description: Stage 2), and ETSI GSM 3.64 (Overall description of the GPRS Radio Interface: Stage 2).

8) Not to subcontract any part of the design and build of his equipment, or the provision of his GSM GPRS services, which requires a knowledge of the GEA, to any organization which has not signed the Confidentiality and Restricted Usage Undertaking.

9) Not to publish a description or analysis of any aspects which may disclose the operation of the GEA in any document that is circulated outside the premises of the BENEFICIARY.

The above restriction shall not apply to information which:

- is or subsequently becomes (other than by breach by the BENEFICIARY of its obligations under this agreement) public knowledge; or

- is received by the BENEFICIARY without restriction on disclosure or use from a third party and without breach by a third party of any obligations of confidentiality to the CUSTODIAN.

If, after five years from the effective date hereof, the BENEFICIARY has not used the INFORMATION, or if he is no more active in the business mentioned above, he shall return the written INFORMATION which he has received. The BENEFICIARY is not authorized to keep copies or photocopies; it is forbidden for him to make any further use of the INFORMATION.

In the event that the BENEFICIARY breaches the obligations of confidentiality imposed on him pursuant to clause 1 to 9 above and ETSI demonstrates that it has suffered loss as a direct result of such breach, the BENEFICIARY agrees to indemnify ETSI for such reasonable losses which are a direct result of such breach provided that such indemnity shall not extend to any losses incurred by ETSI as a result of any third party claiming against ETSI for any consequential or incidental losses (including loss of profits) suffered by that third party.

All disputes which derive from the present undertaking or its interpretation shall be settled by the Court of Justice situated in Grasse (Alpes Maritimes), in accordance with the procedures of this Court of Arbitration and with the application of French Law regarding questions of interpretation.

The obligations of confidentiality herein shall not apply vis-à-vis other BENEFICIARIES. Evidence of being a BENEFICIARY shall be given by providing a certified copy of this undertaking duly undersigned.

This undertaking supersedes all prior confidentiality and restricted scope undertakings between the parties and constitutes the entire agreement between the parties. All amendments to this undertaking shall be agreed in writing and signed by a duly authorized representative of each of the parties.

Made in two originals, one of which is for the PROVIDER, the other for the BENEFICIARY.

For the CUSTODIAN	For the BENEFICIARY
....	....
.... (Name, Title (typed))	.... (Name, Title (typed))
.... (Date)	.... (Date)

History

Document history		
V1.1.1	September 1998	Publication

ISBN 2-7437-2503-6
Dépôt légal : Septembre 1998