3GPP TS 41.061 V4.0.0 (2001-03)

Technical Specification

3rd Generation Partnership Project;
Technical Specification Group Services and System Aspects;
Digital cellular telecommunications system (Phase 2+);
General Packet Radio Service (GPRS);
GPRS ciphering algorithm requirements
(Release 4)

Keywords
GSM, security, GPRS

3GPP

Postal address

3GPP support office address
650 Route des Lucioles - Sophia Antipolis
Valbonne - FRANCE
Tel.: +33 4 92 94 42 00 Fax: +33 4 93 65 47 16

Internet
http://www.3gpp.org

Contents

Foreword

This Technical Specification has been produced by the 3rd Generation Partnership Project (3GPP).

The contents of the present document are subject to continuing work within the TSG and may change following formal TSG approval. Should the TSG modify the contents of the present document, it will be re-released by the TSG with an identifying change of release date and an increase in version number as follows:

Version x.y.z

where:

- x the first digit:
  - 1 presented to TSG for information;
  - 2 presented to TSG for approval;
  - 3 or greater indicates TSG approved document under change control.
- y the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.
- z the third digit is incremented when editorial only changes have been incorporated in the document.

1 Scope

This TS constitutes a requirements specification for a cryptographic algorithm which is used to protect General Packet Radio Services (GPRS) as specified by GSM 02.60.

This TS is intended to provide the ETSI Security Algorithms Group of Experts (SAGE) with the information it requires in order to design and deliver a technical specification for such an 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

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. In the case of a reference to a 3GPP document (including a GSM document), a non-specific reference implicitly refers to the latest version of that document *in the same Release as the present document*.

[1] GSM 01.04: "Digital cellular telecommunications system (Phase 2+); Abbreviations and acronyms"

[2] GSM 02.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 1".

[3] GSM 03.60: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Service Description; Stage 2".

[4] GSM 04.64: "Digital cellular telecommunications system (Phase 2+); General Packet Radio Service (GPRS); Mobile Station-Serving GPRS Support Node (MS_SGSN) Logical Link Control (LLC) Layer Specification".

[5] TCR-TR 030: "Security Techniques Advisory Group (STAG); A guide to specifying requirements for cryptographic algorithms".

3 Definitions and abbreviations

3.1 Definitions

For the purposes of this specification, the definitions given in GSM 02.60 apply.

3.2 Abbreviations

In addition to those mentioned below, abbreviations used in this specification are listed in GSM 01.04.

ANSI	American National Standards Institute
FCS	Frame Check Sequence
GPRS	General Packet Radio Service

LLC	Logical Link Control
SAGE	Security Algorithms Group of Experts
SGSN	Serving GPRS Support Node

4 Use of the GPRS ciphering algorithm

This clause defines those organizations for whom the algorithm is intended, describe the type of information which the algorithm is intended to protect, indicate possible geographical/geopolitical restrictions on the use of equipment which embodies the algorithm, and describe the types of implementations of the algorithm that are envisaged.

4.1 Use of the algorithm

The algorithm shall only be used for providing GPRS security features, as described in GSM 02.60 and GSM 03.60.

The use of the algorithm is as follows:

- the algorithm is used to provide confidentiality and integrity protection of GPRS user data used for Point-to-Point (PTP) mobile originated and mobile terminated data transmission;
- the algorithm is used to provide data confidentiality and integrity protection of GPRS user data used for Point-to-Multipoint Group (PTM-G) mobile terminated data transmission.

- the algorithm is restricted to the MS - SGSN encryption.

4.2 Places of use

The algorithm is installed in the Serving GPRS Support Node (SGSN) and Mobile Station (MS). The MS may consist of Terminal Equipment (TE), Terminal adaptation (TA) and Mobile Equipment (ME). The MS may also be a stand alone device. The GPRS ciphering algorithm may reside in the ME, TA, TE.

Legal restrictions on the use or export of equipment containing cryptographic features that are enforced by various European Governments may prevent the use of equipment in certain countries.

4.3 Types of implementation

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

The preferred method for implementing the algorithm is in hardware as a single chip device .

In the case of a software implementation of the algorithm, legal restrictions on its export and, in certain countries, on its use is expected to be more stringent than for a hardware implementation.

5 Use of the algorithm specification

This clause addresses ownership of the algorithm specification, to define which types of organization are entitled to obtain a copy of the algorithm specification, and to outline how and under what conditions such organizations may obtain the specification.

5.1 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.

5.2 Users of the specification

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

- the service providers, including network operators, entitled to use the algorithm in the network side;
- those who need the algorithm specification in order to build equipment or components which embody the algorithm.

5.3 Licensing

Users of the algorithm, and users and 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 small charge to cover administrative costs involved in issuing the licences.

It is envisaged that there shall be two types of licence and confidentiality agreement: one for service provider of GPRS services entitled to use the algorithm, and one for organizations who need the algorithm specification in order to build equipment or components which embody the algorithm, as defined in subclause 5.2.

The licence and confidentiality agreement signed by a service provider of GPRS services shall require that organization to comply with the restrictions on the use of the algorithm.

The licence and confidentiality agreement signed by an organization that needs the algorithm specification in order to build equipment or components which embody the algorithm, shall require that organization to adopt measures to ensure that its implementations of the algorithm are commensurate with the need to maintain confidentiality of the algorithm.

5.4 Management of the specification

The distribution procedure for the algorithm specification shall be specified by ETSI. SAGE is expected to design the appropriate procedure for the distribution of the algorithm after consulting ETSI SMG 10 and the GSM MoU Security group. The outline procedure is as follows:

- ETSI shall appoint a custodian for administration of the algorithm specification;
- a service provider of GPRS services may request copies of the algorithm specification (and test data) and a licence to use the algorithm from the custodian;
- if the service provider of GPRS services is entitled to use the algorithm, the custodian shall issue the requested algorithm specifications subject to the GPRS service provider signing a licence and confidentiality agreement;
- a service provider of GPRS services who is licensed to use the algorithm may request ETSI to provide copies of the algorithm specification to an organization which intends to build equipment or components that embody the algorithm. Such an organization shall then be required by ETSI to sign a licence and confidentiality agreement before receiving the algorithm specifications from the custodian.

6 Functional requirements

ETSI SAGE are required to design an algorithm which satisfies the functional requirements specified in this clause.

6.1 Type and parameters of algorithm

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.

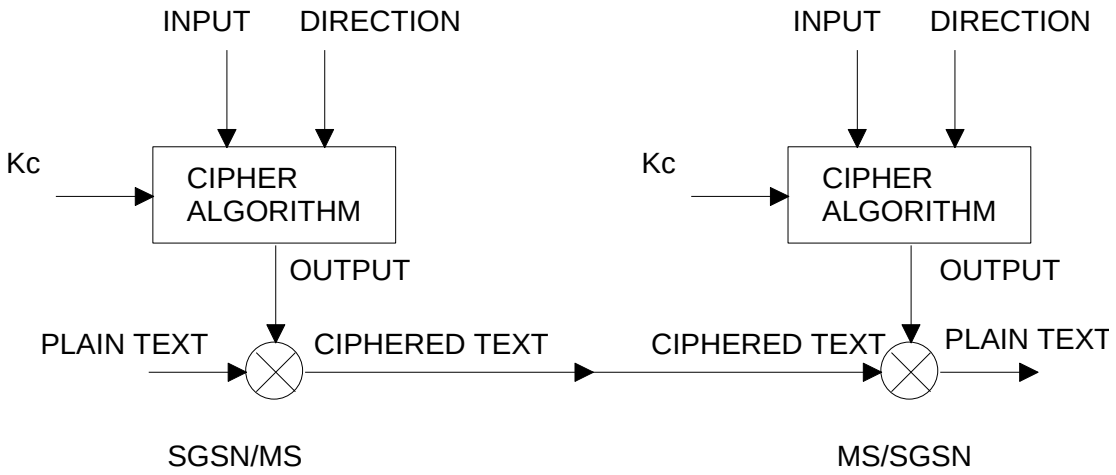

Figure1: Basic GPRS ciphering environment

The parameters of the algorithms are to be as follows:

Kc	64 bits
INPUT	32 bits
DIRECTION	1 bit
OUTPUT	1600 octets

6.1.1 Kc

The ciphering key (Kc) is unstructured data. The ciphering key is generated in the GPRS authentication and key management procedure. The length of the key is 64 bits. The key is unique for the MS when point-to-point traffic is used or it may be common for several MSs when SGSN sends same data to several MSs in point-to-multipoint transmission in PTM-G service. The Kc is never transmitted over the radio interface.

6.1.2 INPUT

This is the LLC frame dependent input parameter (32 bits) for the ciphering algorithm. Depending on the frame type, this field is derived as follows:

- For I-frames carrying user data:
  - The input value is set to a random initial value at LLC connection set-up and incremented by 1 for each new frame.
- For UI-frames carrying user data and signalling messages:
  - the input parameter is a non-repeating 32-bit value derived from the LLC header.

6.1.3 DIRECTION

This defines the direction (1bit) of the data transmission (uplink/downlink).

6.1.4 OUTPUT

This is the output of the ciphering algorithm. The maximum length (1600 octets) of the output string is the maximum length of the payload of the LLC frame, including the FCS (Frame Check Sequence, 3 octets).

The minimum length of the output string is 5 octets.

In the sender entity, the OUTPUT string is bit-wise XORed with the PLAIN TEXT and the result is sent over the radio interface. In the receiving entity, the OUTPUT string is bit-wise XORed with CIPHERED TEXT and the original PLAIN TEXT is obtained.

As an implementation optimisation it needs to be possible to generate just as many output octets as needed .

Normal use of the algorithm is either short packets (25 to 50 octets) or long packets (500 to 1000 octets).

6.1.5 PLAIN TEXT

This is the plain text consisting of the payload of the LLC frame (i.e., the information field) and the FCS. The FCS is a CRC, as described in GSM 04.64. [Ed. Note The requirements described in GSM 04.64 are the current working assumption, as the standard is not yet approved.] This means that the header part of the LLC frame is not ciphered. The maximum length of the payload is 1600 octets.

6.1.6 CIPHERED TEXT

This is the ciphered text of the plain text that is generated in the sending side by bit-wise XORing the PLAIN TEXT and OUTPUT strings.

6.2 Interfaces to the algorithm

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.

6.3 Modes of operation

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.

6.4 Implementation and operational considerations

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 initialisations 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 initialisations 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.

6.5 Resilience of the algorithm

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 Algorithm specification and test data requirements

ETSI SAGE 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 implementors of the algorithm.

The specification shall include an annex which 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 implementors 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 ETSI appointed custodian (see subclause 5.4). The document shall be marked *"Strictly ETSI confidential"* and carry the warning *"This information is subject to a licence and confidentiality agreement"*.

The design conformance test data shall be produced on paper, and provided only to the ETSI appointed custodian. The document shall be marked *"Strictly ETSI confidential"* and carry the warning *"This information is subject to a licence and confidentiality 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 ETSI appointed custodian. Special markings or warnings are not required.

8 Quality assurance requirements

This clause advises ETSI SAGE 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 ETSI SAGE in a design and evaluation report which shall be published by ETSI as a Technical Report.

8.1 Quality assurance for the algorithm

Prior to its release to the ETSI custodian, the algorithm needs to be approved as meeting the technical requirements specified in clause 6 by all members of ETSI SAGE.

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 ETSI SAGE.

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 ETSI SAGE have approved the algorithm, specification and test data.

The report shall not contain any information about the algorithm, such as design techniques used, mathematical analysis or statistical testing of components of the algorithm, which might reveal part or all of the structure or detail of the algorithm.

9 Summary of ETSI SAGE deliverables

- Specification of the algorithm:
  - a confidential document for delivery only to the ETSI custodian;
- Design conformance test data:
  - a confidential document for delivery only to the ETSI custodian;
- Algorithm input/output test data:
  - in a document and on disc for delivery to the ETSI custodian;
- Design and evaluation report;
  - to be published as an ETSI Technical Report (ETR).

Annex A (informative): Change History

Status of Technical Specification GSM 01.61		
Date	**Version**	**Remarks**
		No GSM Phase 1 version
June 1997	1.0.0	To SMG#22 for information
October 1997	2.0.0	To SMG#23 for approval
October 1997	5.0.0	TS approved by SMG#23
March 1998	6.0.0	The specification was converted to version 6.0.0 because the work item is related to Release 97. Not Published Version 5.0.0 was withdrawn
July 1998	6.0.1	Specification published as TS 101 106
April 2000	8.0.0	Release 1999 version

Change history						
TSG SA#	**Spec**	**Version**	**CR**	**<Phase>**	**New Version**	**Subject/Comment**
SP-11	01.61	8.0.0	-	Rel-4	41.061 v 4.0.0	Upgrade to Release 4 (3GPP numbering)