TS GSM 01.56 7.0.0 (1999-05)

Technical Specification

Digital cellular telecommunications system (Phase 2+); GSM Cordless Telephony System (CTS) (Phase 1); CTS Authentication and Key Generation Algorithms Requirements (GSM 01.56 version 7.0.0 Release 1998)

GLOBAL SYSTEM FOR
MOBILE COMMUNICATIONS

Reference

DTS/SMG-100156 (xxxxx.PDF)

Keywords

Digital cellular telecommunications system,
Global System for Mobile communications
(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
Individual copies of this ETSI deliverable
can be downloaded from
http://www.etsi.org
If you find errors in the present document, send your
comment to: editor@etsi.fr

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.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 Specification (TS) has been produced by ETSI Technical Committee Special Mobile Group (SMG).

This document provides a complete description of the security functions for the GSM CTS Radio Interface authentication and related key management.

This specification is intended for use by ETSI Security Algorithms Group of Experts (SAGE) who shall be responsible for the design of the algorithms.

The contents of this TS is subject to continuing work within SMG and may change following formal SMG approval. Should SMG modify the contents of this TS it will be re-leased with an identifying change of release date and an increase in version number as follows:

Version 7.x.y

where:

7 indicates Release 1998 of GSM Phase 2+

x the second digit is incremented for all changes of substance, i.e. technical enhancements, corrections, updates, etc.

y the third digit is incremented when editorial only changes have been incorporated in the specification.

1 Scope

This specification constitutes a requirement specification for a set of associated cryptographic algorithms which is used for Cordless Telephony System (CTS) Radio Interface authentication and key management in the GSM Cordless Telephony System.

This specification is intended to provide ETSI SAGE with the information it requires in order to design and deliver a technical specification for such an algorithm set.

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

1.1 Organisation of this specification

The material presented in the subsequent clauses of this specification is organised as follows:

subclause 1.2 provides some background to the production of this specification.

clauses 4 and 5 describe the context in which the algorithm set and its specification are intended to be used.
Clause 4 outlines the intended use of the algorithm set in terms of which organisations shall be entitled to use it, what they shall use it for, where it shall be used, and how it shall be implemented.
Clause 5 describes the intended use of the algorithm specification set in terms of who shall own it, who shall use it, and how and under what conditions the specification shall be provided to those users.

clause 6 specifies the functional requirements for the algorithm set. This covers the type and parameters of the algorithm, the interface to the algorithm set, the envisaged modes of operation of the algorithm set, implementation and operational considerations which may have an impact on the design of the algorithm set and requirements on the resilience of the algorithm set.

clause 7 details requirements on the algorithm set specification and associated test data deliverables.

clause 8 addresses quality assurance requirements, needed to give confidence in the design of the algorithm set and the adequacy of the algorithm set specification and test data.

clause 9 is a summary of the deliverables expected from ETSI SAGE.

1.2 Motivation

Discussions within SMG led to the conclusion that GSM-CTS can only be provided on a commercially solid and successful basis if appropriate security features are integrated into the system. In particular it was decided to standardise mechanisms both authentication and key generation algorithms.

Consequently an annex to GSM 03.20 was produced, which specifies the security features of the CTS. It was also concluded that, in order to support inter-operability between equipment, and in line with the policy for GSM, a set of standard ETSI algorithms for CTS Radio Interface authentication and key management needs to be specified.

The implementation of the algorithm set is mandatory, the implementation shall be in line with this specification.

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

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

3 Definitions and abbreviations

3.1 Definitions

All definitions used in this specification are specified in GSM 03.20 Annex E.

3.2 Abbreviations

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

CTS	Cordless Telephony System
SAGE	Security Algorithms Group of Experts
CTS-ME	CTS Mobile Equipment
MS-SIM	Mobile Station CTS Subscriber Identity Module
FP-SIM	Fixed Part CTS Subscriber Identity Module
CTS-MS	A CTS-ME combined with a CTS-SIM
CTS-FP	CTS Fixed Part
CTS-SN	CTS Service Node
FPAC	code entered by the CTS user to initialise a CTS-MS/CTS-FP
Ka	CTS authentication key for a CTS-MS/CTS-FP pair
Kc	CTS ciphering key for a CTS-MS/CTS-FP pair
Kop	CTS authentication key used for the authentication of the CTS-FP by the CTS-SN and the authentication by the CTS-FP of the signature issued by the CTS-SN
Data1	CTS data constant used for the CTS-FP authentication by the CTS-SN
Data2	CTS data sequence to be signed by the CTS-SN and sent to the CTS-FP for signature authentication
MAC1	CTS result of the computation of the CTS-FP authentication algorithm using Kop and Data1
MAC2	CTS signature of the data sequence Data2
R_{IFP}	CTS Random Initial value sent from the CTS-MS to the CTS-FP
R_{IMS}	CTS Random Initial value sent from the CTS-FP to the CTS-MS
SRES1	CTS Signed RESponse of the CTS-FP's CH1 and the Ka of the CTS-MS
SRES2	CTS Signed RESponse of the CTS-MS's CH2 and the Ka of the CTS-FP
XSRES1	CTS Signed RESponse of the CTS-FP's CH1 and the Ka of the CTS-FP (to be compared with SRES1)
XSRES2	CTS Signed RESponse of the CTS-MS's CH2 and the Ka of the CTS-MS (to be compared with SRES2)

4 Use of the CTS algorithm set

The purpose of this clause is to define those organisations for whom the algorithm set is intended, describe the type of information which the algorithm set is intended to protect, indicate possible geographical/geopolitical restrictions on the use of equipment which embodies the algorithm set, and describe the types of implementations of the algorithm set that are envisaged.

4.1 Use of the algorithm set

The algorithm set shall only be used for providing the authentication and key management as described in GSM 03.20 Annex E.

4.2 Places of Use

The algorithm set is installed in each CTS Mobile Equipment (CTS-ME) ,in each CTS Fixed Part (CTS-FP) and in each CTS Service Node (CTS-SN). The standard does not forbid future use in a CTS-SIM in later CTS phases.

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 design of the algorithm set should support software implementations for 8 bit processors. Those implementing the algorithm set shall be required through a licence and confidentiality agreement which they shall sign with ETSI, as described in subclause 5.3, to adopt suitable measures to ensure that their implementations are commensurate with the need to maintain confidentiality of the algorithm set.

5 Use of the algorithm specification

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

5.1 Ownership

The algorithm set and all copyright to the algorithm set and test data specifications shall be owned exclusively by ETSI.

The design authority for the algorithm set shall be ETSI SAGE. Amendments to the algorithm set specification may be made only by ETSI SAGE under instruction authorised by the ETSI Board.

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

The licence and confidentiality agreement shall require recipients of the specification not to attempt to patent the algorithm or otherwise register any and IPR relating to the algorithm set or its use.

5.2 Users of the specification

The algorithm set specification may be made available to those who need the algorithm set specification in order to build equipment or components (including IC cards) which embody (parts of) the algorithm set, according to the GSM-CTS standard.

5.3 Licensing

Users of the algorithm set specification shall be required to sign a restricted usage and confidentiality agreement with ETSI.

Appropriate restricted usage and confidentiality agreements shall be drawn up by ETSI.

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

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

5.4 Management of the specification

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

- ETSI shall appoint a custodian for administration of the algorithm set specification;
- an organisation which intends to build equipment or components that embody (or part of) the algorithm set may request copies of the algorithm set specification (and test data) and a licence to use the algorithm set from the custodian;
- if an organisation mentioned above is entitled to use the algorithm set, the custodian shall issue the requested algorithm specifications subject to the organisation signing a licence and confidentiality agreement;
- at least manufacturers of CTS equipment who are ETSI members are entitled to the algorithms set of specifications.

6 Functional requirements

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

6.1 Composition of the Algorithm Set and Type and Parameters of Algorithms

As specified in GSM 03.20 annex E, the algorithm set contains the following algorithms:

B1: Shall be used to compute the Kc from Ka and CH1. The algorithm shall have the following properties:

Input 1: Bit string of length |Ka|;
Input 2: Bit string of length |CH1|;

Output: Bit string of length |Kc|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known). Similarly it shall be difficult to infer any information about the Output from only the knowledge of Input 2.

B2: Shall be used to compute Ka from R_{IMS}, R_{IFP}, and FPAC. The algorithm shall have the following properties:

Input 1: Bit string of length |FPAC|;
Input 2: Bit string of length $|R_{IMS}|$;
Input 3: Bit string of length $|R_{IFP}|$;

Output: Bit string of length Ka.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2, Input 3 and Output 1 (even if the details of the algorithm are known). Similarly it shall be difficult to infer any information about the Output from only the knowledge of Input 2 and Input 3.

B3: Shall be used to compute (X)SRES1 from Ka and CH1. The algorithm shall have the following properties:

Input 1:	Bit string of length |Ka|;
Input 2:	Bit string of length |CH1|;
Output:	Bit string of length |(X)SRES1|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known). Similarly it shall be difficult to infer any information about the Output from only the knowledge of Input 2.

B4: Shall be used to compute (X)SRES2 from Ka and CH2.The algorithm shall have the following properties:

Input 1:	Bit string of length |Ka|;
Input 2:	Bit string of length |CH2|;
Output:	Bit string of length |(X)SRES2|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known). Similarly it shall be difficult to infer any information about the Output from only the knowledge of Input 2.

The mutual authentication offered by B3 and B4 shall be protected against a reflection attack (e.g. by using a key offset method).

B5: Shall be used to compute MAC1 from Kop and Data1. The algorithm shall have the following properties:

Input 1:	Bit string of length |Kop|;
Input 2:	Bit string of length |Data1|;
Output:	Bit string of length |MAC1|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known). Similarly it shall be difficult to infer any information about the Output from only the knowledge of Input 2.

B6: Shall be used to compute MAC2 from Kop and Data2. The algorithm shall have the following properties:

Input 1:	Bit string of length |Kop|;
Input 2:	Bit string of length |Data2|;
Output:	Bit string of length |MAC2|.

The algorithm should be designed such that it is difficult to infer any information about Input 1 from the knowledge of Input 2 and the Output (even if the details of the algorithm are known). Similarly it shall be difficult to infer any information about the Output from only the knowledge of Input 2.

As long as the resilience requirements on the algorithm set are not violated, all algorithms in the set do not need to be distinct and complete. Indeed large parts of algorithm specifications might be identical.

Figure 1 shows the use of B3 and B4 to obtain mutual authentication between a CTS-MS and a CTS-FP, and the use of B1 for generating the ciphering key Kcx.

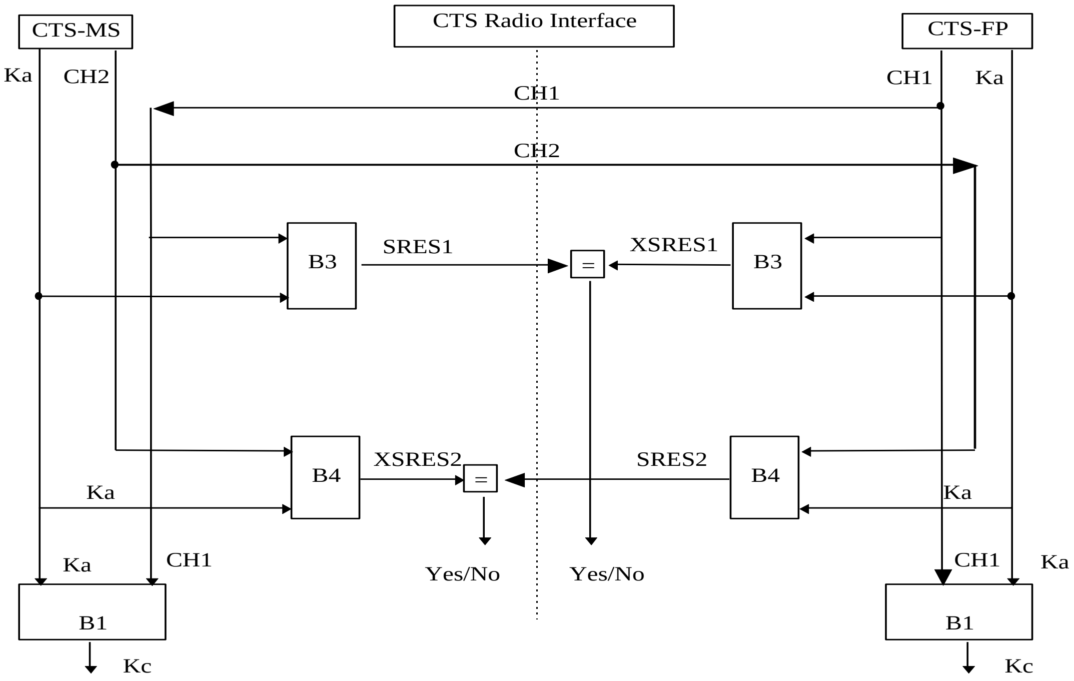

Figure 1: Mutual authentication of CTS-MS and CTS-FP using B3 and B4 and ciphering key Kcx generation by B1

Figure 2 shows the use of B2 to generate the key Ka.

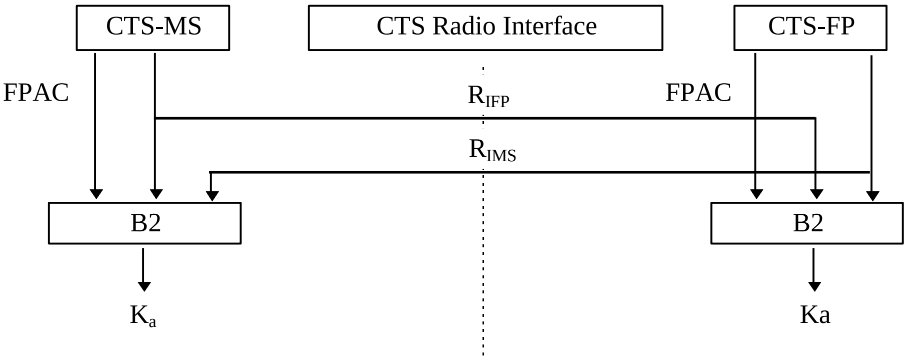

Figure 2: Generation of initial key Ka

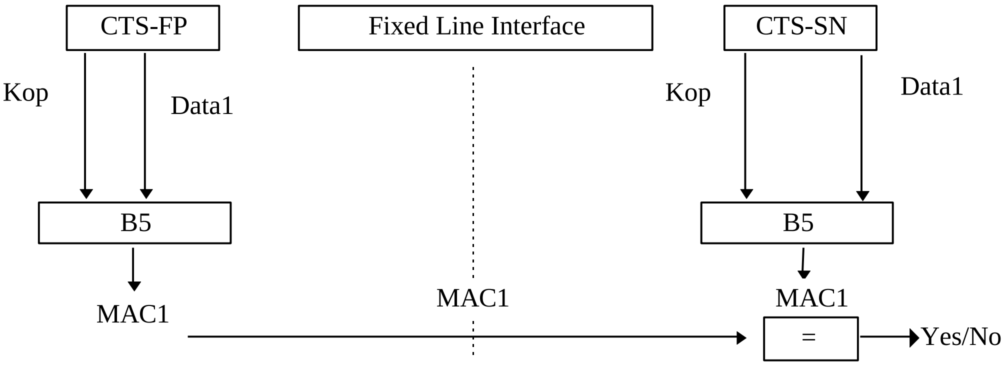

Figure 3:Computation of the result of the authentication of the CTS-FP using Kop and B5 algorithm

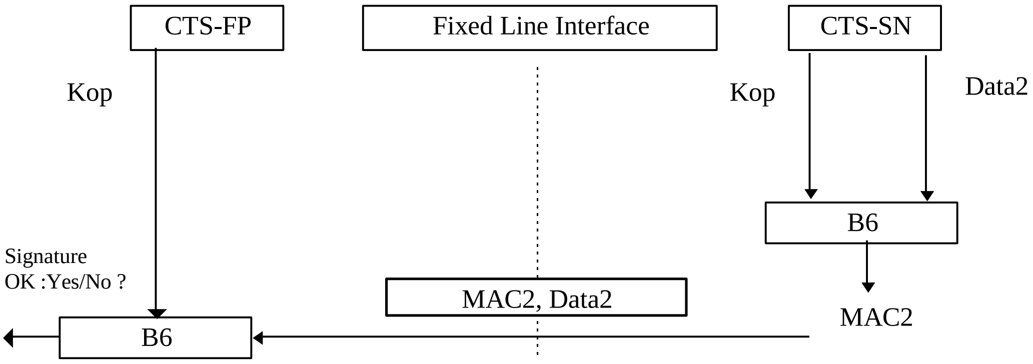

Figure 4 : Generation of the signature of the data sequence Data2 using Kop and B6

6.1.1 FPAC

The CTS-FP is equipped with a manufacturer installed FPAC code. The FPAC is unstructured data. The FPAC is used to facilitate initial mutual authentication of CTS-MS and CTS-FP and to facilitate encryption set-up.

The length of the FPAC is 128 bits.

6.1.2 CH1 and CH2

The challenge from CTS-FP to CTS-MS (CH1) and the challenge from CTS-MS to CTS-FP (CH2) are random 128 bit strings.

6.1.3 Ka

The authentication key is unstructured data. It is generated by algorithm B2 from FPAC and two random inputs R_{IMS} (generated by CTS-FP and sent to CTS-MS) and R_{IFP} (generated by CTS-MS and sent to CTS-FP). The length is 128 bits.

6.1.4 Kc

The ciphering key (Kc) is unstructured data. It is generated by algorithm B1 from the authentication key Ka and the random challenge CH1. The length is 64 bits.

6.1.5 Kop

The authentication key (Kop) is unstructured data. This key is generated from an authentication key stored on the FP-SIM and a key generation algorithm A8' as described in GSM03.20 Annex E. The length is 128 bits.

6.1.6 Data1

The data sequence (Data1) is unstructured data. It length is n bytes.

6.1.7 Data2

The data sequence (Data2) is unstructured data. It length is n bytes.

6.1.8 MAC1

The authentication result (MAC1) is unstructured data. (MAC1) is computed form Kop and Data1 using the B5 algorithm. MAC1=B5(Kop, Data1).The length is 128 bits.

6.1.9 MAC2

The signature (MAC2) is unstructured data. The signature (MAC2) is generated using Kop and a sequence Data2. MAC2=B6(Kop, Data2). The length is 128 bits.

6.1.10 SRES1 and SRES2

The response sent from CTS-MS to CTS-FP (SRES1) and the response sent from CTS-FP to CTS-MS (SRES2) are 32 bit values computed from the authentication key (Ka) and the challenges CH1 and CH2 respectively. SRES1=B3(Ka,CH1) and SRES2=B4(Ka,CH2).

6.1.11 RIMS and RIFP

The generation of Ka through algorithm B2 involves the use of two random values R_{IMS} and R_{IFP}. R_{IMS} is sent from CTS-FP to CTS-MS and R_{IFP} is sent from CTS-MS to CTS-FP. Both R_{IMS} and R_{IFP} are 64 bits long.

6.1.12 SRES1 and SRES2

The response expected by the CTS-FP (XSRES1) and the response expected by the CTS-MS (XSRES2) are 32 bit values computed from the authentication key (Ka) and the challenges CH1 and CH2 respectively. XSRES1=B3(Ka,CH1) and XSRES2=B3(Ka,CH2).

6.2 Interfaces to the Algorithm

The dimensioning and definition of the interface parameters to the algorithms described in subclause 6.1 are listed below. In this listing X[i] denoted the i-th bit of the variable X.

FPAC	128 bits:	FPAC[0], FPAC[1], …, FPAC[127]
CH1	128 bits:	CH1[0], CH1[1],…, CH1[127]
CH2	128 bits:	CH2[0], CH2[1],…, CH2[127]
Ka	128 bits:	Ka[0], Ka[1],…, Ka[127]
Kc	64 bits:	Kc [0], Kc [1],…, Kc [63]
Kop	128 bits:	Kop[0], Kop[1],…, Kop[127]

Data1	n bytes:	Data1[0], Data1[1],…, Data1[8n-1]
Data2	n bytes:	Data2[0], Data2[1],…, Data2[8n-1]
MAC1	128 bits:	MAC1[0], MAC1[1],…, MAC1[127]
MAC2	128 bits:	MAC2[0], MAC2[1],…, MAC2[127]
SRES1	32 bits	SRES1[0], SRES1[1],…, SRES1[31]
SRES2	32 bits	SRES2[0], SRES2[1],…, SRES2[31]
$\mathbf{R_{IMS}}$	64 bits:	$R_{IMS}[0]$, $R_{IMS}[1]$,…, $R_{IMS}[63]$
$\mathbf{R_{IFP}}$	64 bits:	$R_{IFP}[0]$, $R_{IFP}[1]$,…, $R_{IFP}[63]$
XSRES1	32 bits	XSRES1[0], XSRES1[1],…, XSRES1[31]
XSRES2	32 bits	XSRES2[0], XSRES2[1],…, XSRES2[31]

6.3 Implementation and Operational Considerations

The algorithm should be designed for software implementations

As a reference, the set of the algorithms should be implementable on a 6805-family of microprocessors, in particular the Motorola SC21 series and Philips 83C852 series, running at 4 MHz. However the performance of the implementation of the algorithms should favourably scale when implementation is carried out on a 16-bit or 32-bit processor which support similar logical and arithmetical operations as found on the 6805-family but with larger word size.

For the reference platform it should be possible to realise an efficient state of the art implementation such that

- for each of the algorithms B1, B3, B4, the time for one operation is less than 200 milliseconds;
- for the algorithm B2 the time for one operation is less than 250 milliseconds;
- the complete set of algorithms can be implemented using less than 3000 bytes ROM and 128 bytes RAM.

6.4 Resilience of Algorithm set

The algorithm set should be designed with a view to its continued use for a period of at least 15 years.

The algorithm set should be designed such that:

- the strength of the individual algorithms should not be significantly less than indicated by its key parameter(s);
- the requirements on the individual algorithms listed in subclause 6.1 should be fulfilled.

ETSI SAGE are required to design the algorithm set to a strength which reflects the above requirements but imposes minimal restrictions on the exportability of equipment that is fitted with the algorithm.

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.

The design of the algorithm set will have a pre-evaluation phase. Equipment manufacturers/organisations that have contributed to the funding of the SAGE design work for this algorithm set are allowed to participate in this evaluation and can get access to the algorithm specifications as they stand.

The purpose of the pre-evaluation phase is to allow manufacturers/implementators early visibility of the structure of the algorithm(s) so that they can assess what is involved in its implementation, and confirm that there are no problems in realising the design in the target environment. They will be provided with an algorithm specification that accurately reflects structure and processing requirements of the algorithm set. Any changes between pre-evaluation specification and the final specification are not expected to have any significant impact on code size or algorithm timing.

The specification shall include an annex which provides simulation code written in ANSI C. Access requires a non-disclosure agreement between the manufacturer/organisation and ETSI SAGE.

Those equipment manufacturers/organisations that do not contribute will get access to algorithm set specification only after the SAGE work has been completed.

7.1 Specification of the algorithm set

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

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

7.2 Design conformance test data

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

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

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

7.3 Algorithm set input/output test data

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

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

7.4 Format and handling of deliverables

The specification of the algorithm set 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 set 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.

The design and evaluation report should be published as an ETSI Technical Report.

8 Quality assurance requirements

This clause advises ETSI SAGE on measures needed to provide users of the algorithm set with confidence that it is fit for purpose, and users of the algorithm set 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 set

Prior to its release to the ETSI custodian, the algorithm set 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 set specification, two independent simulations of each algorithm in the set needs to be made using the specification, and confirmed against test data designed to allow verification of significant points in the execution of each algorithm in the set.

Design conformance and algorithm input/output test data needs to be generated using a simulation of each algorithm in the set 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 set, specification and test data that appropriate and adequate quality control has been applied to their production. The report shall explain the following:

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

The report shall confirm that all members of ETSI SAGE have approved the algorithm set, specification and test data.

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

9 Summary of ETSI SAGE deliverables

- Specification of the algorithm set:
    - a confidential document for delivery only to the ETSI custodian;

      The specification shall include a simulation code of the algorithm set written in ANSI C.
- Design conformance test data:
    - a confidential document for delivery only to the ETSI custodian;
- Algorithm set 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.

9.1 Pre-evaluation phase deliverables

- Specification of the algorithm set at the pre-evaluation version of the algorithm set:
  - a confidential document for delivery only to manufacturers that have contributed to funding of the algorithm design;

    The specification shall include a simulation code of the algorithm set written in ANSI C.

Annex A (informative): Status of GSM 01.56

Status of GSM 01.56	
March 1998	version 0.0.1 prepared for SMG10 CTS Ad hoc meeting #2
March 26 1998	Version 0.0.2 prepared for SMG10 #2/98
April 9 1998	Version 0.0.3 reviewed by SMG10 #2/98
July 1998	Version 0.1.1 SMG10 #3/98
November 1998	Version 0.2.0 SMG10 #4/98
January 1999	Version 0.3.0 reviewed following SMG10 #4/98
February 1999	version 1.0.0 to SMG#28 for information and approval; approved by SMG#28 to become version 7.0.0

History

Document history		
V7.0.0	May 1999	Unpublished