Digital cellular telecommunications system (Phase 2+); 3G Security;
Specification of the A5/3 encryption algorithms for GSM and ECSD, and the GEA3 encryption algorithm for GPRS;
Document 4: Design and evaluation report (3GPP TR 55.919 version 13.0.0 Release 13)
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 ETSI SR 000 314: "Intellectual Property Rights (IPRs): Essential, or potentially Essential, IPRs notified to ETSI in respect of ETSI standards", which is available from the ETSI Secretariat. Latest updates are available on the ETSI Web server (https://ipr.etsi.org/).

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 ETSI 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 3rd Generation Partnership Project (3GPP).

The present document may refer to technical specifications or reports using their 3GPP identities, UMTS identities or GSM identities. These should be interpreted as being references to the corresponding ETSI deliverables.

The cross reference between GSM, UMTS, 3GPP and ETSI identities can be found under http://webapp.etsi.org/key/queryform.asp.

Modal verbs terminology

In the present document "shall", "shall not", "should", "should not", "may", "need not", "will", "will not", "can" and "cannot" are to be interpreted as described in clause 3.2 of the ETSI Drafting Rules (Verbal forms for the expression of provisions).

"must" and "must not" are NOT allowed in ETSI deliverables except when used in direct citation.
Contents

Intellectual Property Rights ...................................................................................................................... 2
Foreword ........................................................................................................................................................ 2
Modal verbs terminology .............................................................................................................................. 2
Foreword ...................................................................................................................................................... 4
Introduction .................................................................................................................................................. 4
1 Scope .......................................................................................................................................................... 5
2 References .................................................................................................................................................. 5
3 Definitions, symbols and abbreviations ................................................................................................. 5
  3.1 Definitions .............................................................................................................................................. 5
  3.2 Symbols .................................................................................................................................................. 6
  3.3 Abbreviations ....................................................................................................................................... 6
4 Technical provisions .................................................................................................................................. 6
Annex B: Change history .............................................................................................................................. 7
History ......................................................................................................................................................... 8
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.

Introduction

This Report has been produced by ETSI SAGE Task Force for the design of the GSM A5/3 and GEA3 encryption algorithms.

The work described in this report was undertaken in response to a request made by Security Group GSM Association. The work was done under supervision of the ETSI Mobile Competence Centre (MCC) and the GSM Association.
1 Scope

This Technical Report has been prepared by the ETSI SAGE GSM A5/3 Task Force, and gives a detailed report on the design and evaluation of the A5/3 encryption algorithms for GSM and ECSD, and of the GEA3 encryption algorithm for GPRS (including EGPRS).

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] Void
[2] Void
[3] Void
[4] Void
[5] Void
[6] Void
[7] Void
[8] Void
[9] Void
[10] Void

Note: Reference [2] is available via http://portal.etsi.org/dvbandca/home.asp and is subject to licensing conditions described at this site.

3 Definitions, symbols and abbreviations

3.1 Definitions

3.2 Symbols
For the purposes of the present document, the symbols defined in the 3GPP Task Force Report [12] apply.

3.3 Abbreviations

4 Technical provisions
The technical provisions of the current document are contained in the 3GPP Task Force Report [2].
### Change history

<table>
<thead>
<tr>
<th>Date</th>
<th>TSG #</th>
<th>TSG Doc.</th>
<th>CR</th>
<th>Rev</th>
<th>Subject/Comment</th>
<th>Old</th>
<th>New</th>
</tr>
</thead>
<tbody>
<tr>
<td>2002-05</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>ETSI SAGE first publication</td>
<td>SAGE V1.0</td>
<td></td>
</tr>
<tr>
<td>2002-07</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Agreed at SA WG3 #24 for presentation to TSG SA #17 for approval. Converted into 3GPP TR format (TR 55.919) (Technically equivalent to SAGE V1.0)</td>
<td>SAGE V1.0</td>
<td>1.0.0</td>
</tr>
<tr>
<td>2002-09</td>
<td>SP-17</td>
<td>SP-020506</td>
<td>-</td>
<td>-</td>
<td>Approved for Release 6 - version 6.0.0</td>
<td>1.0.0</td>
<td>6.0.0</td>
</tr>
<tr>
<td>2002-12</td>
<td>SP-18</td>
<td>SP-020721</td>
<td>001</td>
<td>-</td>
<td>EGPRS algorithm</td>
<td>6.0.0</td>
<td>6.1.0</td>
</tr>
<tr>
<td>2007-12</td>
<td>SP-38</td>
<td>SP-070776</td>
<td>002</td>
<td>-</td>
<td>Conversion to pointer to export controlled document</td>
<td>6.1.0</td>
<td>7.1.0</td>
</tr>
<tr>
<td>2008-12</td>
<td>SP-42</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Upgrade to Release 8</td>
<td>7.1.0</td>
<td>8.0.0</td>
</tr>
<tr>
<td>2009-12</td>
<td>SP-46</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Upgrade to Release 9</td>
<td>8.0.0</td>
<td>9.0.0</td>
</tr>
<tr>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
<td>Note: Version 7.0.0 is a “readme” file placeholder with no technical content.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>2011-03</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Update to Rel-10 version (MCC)</td>
<td>9.0.0</td>
<td>10.0.0</td>
</tr>
<tr>
<td>2012-09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Update to Rel-11 version (MCC)</td>
<td>10.0.0</td>
<td>11.0.0</td>
</tr>
<tr>
<td>2014-09</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Update to Rel-12 version (MCC)</td>
<td>11.0.0</td>
<td>12.0.0</td>
</tr>
<tr>
<td>2016-01</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>-</td>
<td>Update to Rel-13 version (MCC)</td>
<td>12.0.0</td>
<td>13.0.0</td>
</tr>
</tbody>
</table>
## History

<table>
<thead>
<tr>
<th>Document history</th>
</tr>
</thead>
<tbody>
<tr>
<td>V13.0.0</td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
<tr>
<td></td>
</tr>
</tbody>
</table>