Rules for the Management and the Distribution of the GSM A51 Ciphering Algorithm

Version 4.1

16 December 2014

This is a Binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

The A5 algorithms are used for signalling and data privacy in the GSM system, as specified in 3GPP TS 43.020 and 3GPP 42.009. The use of the algorithms is mandatory and variations and their use are described in SG.08. These rules apply to the A5/1 algorithm only as distribution of A5/2 ceased in November 2004 in line with GSMA Board policy and A5/3, which has been published, is available at the GSM Association's web site (www.gsmworld.com).

2 Rules for the Management of the A5/1 Algorithm by the Gsm Association Administrator

2.1. The GSM Association has been nominated to manage the distribution of the detailed specification of the A5/1 algorithm according to the following set of rules.

2.2. The detailed specification of the A5/1 algorithm is contained in a confidential document kept by the GSM Association administrator. The GSM Association administrator is the only party which is authorised to produce numbered copies of the documentation.

2.3 The distribution of the detailed specification of the A5/1 algorithm to any party requesting these specifications is done by the administrator, subject to the signature of the confidentiality and restricted usage undertaking contained in SG.02.

2.4 The administrator shall not distribute the specification to any parties other than GSM Association member network operators, GSM Association rapporteurs who have demonstrated a need to use A5 consistent with the GSM Association's aims, and manufacturers of GSM equipment containing A5.

2.5 The A5 administrator shall maintain an updated list of these undertakings and shall provide this list on request by the GSM Association chairman.

3 Rules for the Management of the A5/1 Algorithm by Network Operators

3.1 Network operators and rapporteurs, having obtained the detailed A5/1 specification from the GSM Association administrator, according to the rules defined above, are entitled to forward the specification to the parties listed subsequently in paragraph 3.4, subject to the prior signature of the confidentiality and restricted usage undertaking.

3.2 The GSM Association operator is not authorised to make any copies of the specification, and additional specifications shall be obtained from the GSM Association administrator.

3.3 Parties authorised to receive the detailed A5/1 specification from the network operators and rapporteurs, subject to the signature of the confidentiality and restricted usage undertaking, are:

- GSM network system suppliers who supply equipment containing A5 with whom the network operator or rapporteur has contracted or from whom a response to a request for tender is due;
- Manufacturers of GSM test equipment containing the A5 algorithms;

- Manufacturers of GSM system simulators containing the A5 algorithms;
- Manufacturers of MS containing the A5 algorithms;
- Manufacturers of femtocell equipment that is intended to be deployed in a manner that complies with the published 3GPP standards.

3.4. The network operator or rapporteur is obliged to forward a copy of any confidentiality and restricted usage undertakings (including those received from equipment suppliers as a result of the forwarding of the detailed A5/1 specification to sub-contractors) to the GSM Association Administrator.

3.5 For a network operator, who is not a GSM Association member, or rapporteur, but is eligible to join the GSM Association, the application of the above clauses will be decided on a case by case basis. The decision is taken by the GSM Association Fraud and Security Director with prior consultation of the GSM Association Security Group Chairman.

4 Rules for the Management of the A5/1 Algorithm by Manufacturers

4.1 A manufacturer, having obtained the detailed specification of A5 from a network operator or rapporteur, according to the rules defined above, or from the administrator, is entitled to forward the detailed A5/1 specification to his subcontractors that are involved in the development of the equipment containing the A5 algorithm, subject to the signature of the confidentiality and restricted usage undertaking.

4.2 The manufacturer is not authorised to make any copies of the detailed A5 specification and he shall request the required number of specifications from the operator, rapporteur, or from the administrator. For each party, a separate confidentiality and restricted usage undertaking shall be signed. The manufacturer is obliged to forward a copy of any such undertakings to the party from whom the algorithm was obtained.

5 Name and Address of the A5 Administrator

James Moran
Fraud and Security Group Director
GSMA Head Office
Floor 2
The Walbrook Building
25 Walbrook
London
EC4N 8AF
United Kingdom

Email: security@gsma.com

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
3.1.1	Sep 1993	Rules updated to provide clarity on rights and obligations	Plenary	SG Chair
3.1.2	May 1996	Change of Administrator from SG Chair at One2One UK	Plenary	SG Chair
3.2.0	Oct 2003	Changes made to facilitate distribution of A5 to WLL operators approved at SG#49	Plenary	James Moran, GSMA
3.3.0	Nov 2004	Changes made to remove references to A5/2 in support of GSMA Board policy to withdraw the algorithm	EMC	James Moran, GSMA
4.0	Feb 2010	Changes made to allow Femtocell suppliers to use A5/1 presented for approval at SG#73	EMC	James Moran, GSMA
4.1	12 Dec 2014	Transferred PRD from SG to FASG as SG.01 v4.1	FASG	David Chong, GSMA

Other Information

Type	Description
Document Owner	FASG
Editor / Company	James Moran, GSMA

It is our intention to provide a quality product for your use. If you find any errors or omissions, please contact us with your comments. You may notify us at prd@gsma.com

Your comments or suggestions & questions are always welcome.