Rules for the Management and Distribution of the COMP128 Family of Example A3 and A8 Algorithms

Version 3.6

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 algorithm A3/A8 is used for authentication and cipher key generation in the GSM system. The cryptographic strength of the algorithm chosen for A3/A8 is essential for all security features defined in 3GP TS 43.020 and 3GPP TS 42.009. The design of GSM allows each PLMN operator to freely choose their own A3/A8 algorithm.

The algorithms, commonly referred to as COMP128, COMP128-2 and COMP128-3, provided by the GSM Association Administrator(s) are examples to serve as a basis for A3/A8. This document defines the rules for management and distribution of the COMP128, COMP128-2 and COMP128-3 specifications to all parties. Milenage for GSM, or G-Milenage, has been published and is available to download at the GSM Association's web site (www.gsmworld.com).

2 Rules for the Management of the COMP128, COMP128-2 and COMP128-3 algorithms by a GSM Association Administrator

2.1. The GSM Association manages the distribution of the detailed specification of the example algorithms COMP128, COMP128-2 and COMP128-3 according to the following set of rules. (Name and address of the administrator is attached in the annex.)

2.2. The detailed specification of example algorithms COMP128, COMP128-2 and COMP128-3 is contained in a confidential document kept by the GSM Association A3/A8 administrator. The GSM Association administrator is the only party authorised to produce numbered copies of the documentation.

2.3. Distribution of the detailed specification of the example algorithms COMP128, COMP128-2 and COMP128-3 is done by the administrator, subject to the signature of the confidentiality and restricted usage undertaking. Distribution of the algorithm is limited to the following parties:

- Network operators who are members of the GSM Association
- GSM Association rapporteurs who have demonstrated a need to use A3/A8 consistent with the GSM Association's aims
- Manufacturers / suppliers of GSM Authentication Centres
- Manufacturers / suppliers of GSM Subscriber Identity Module cards
- Manufacturers / suppliers of GSM test equipment
- Manufacturers / suppliers of GSM system simulators
- Network Operators who are not members of the GSM Association where the purpose of the A3/A8 algorithm is to facilitate the authentication process in an inter-standard roaming environment
- Non members of the Association who have demonstrated that the A3/A8 algorithm is required by them for purposes consistent with the Association's aims. Such parties should have their application supported by at least one GSM Association member network operator. Each application is assessed on a case by case basis and the decision is taken by the Administrator in consultation with the Chairman of the Association's Security Group.

2.4. The A3/A8 administrator shall maintain an updated list of the confidentiality and restricted usage undertakings and shall provide this list on request by the GSM Association chairman.

3 Rules for the Management of the COMP128, COMP128-2 and COMP128-3 algorithms by a GSM Association Member Network Operator or Rapporteur

3.1. A network operator, having obtained the detailed specification of the COMP128, COMP128-2 and COMP128-3 algorithms from the GSM Association administrator according to the rules defined above, is entitled to forward the specification(s) to the parties listed in paragraph 3.3, subject to the prior signature of the confidentiality and restricted usage undertaking.

3.2. The GSM Association member operator is not authorised to make any copies of the specification. Any additional specifications shall be obtained from the GSM Association administrator on request.

3.3 Parties authorised to receive the A3/A8 algorithm from a GSM Association member operator are:

- Manufacturers / suppliers of GSM Authentication Centres
- Manufacturers / suppliers of GSM Subscriber Identity Modules (SIM)
- Manufacturers / suppliers of GSM test equipment
- Manufacturers / suppliers of GSM system simulators

3.4 Each party who receives a detailed specification for A3/A8 must sign a confidentiality and restricted usage undertaking. The GSM Association member network operator is obliged to forward a copy of the undertaking(s) (including undertakings received from manufacturers) to the GSM Association administrator.

3.5 It is the responsibility of the GSM Association member operator to ensure a manufacturer meets the criteria outlined in 3.3. In cases of doubt the member operator should refer to the administrator for guidance.

4 Rules for the Management of the COMP128, COMP128-2 and COMP128-3 algorithms by Manufacturers

4.1 A manufacturer having obtained the detailed specification of the COMP128, COMP128-2 and COMP128-3 algorithms from the GSM Association Administrator or a GSM Association member operator or rapporteur is entitled to forward the specification to the parties listed in paragraph 4.3 subject to the prior signature of the confidentiality and restricted usage undertaking.

4.2 The manufacturer is not authorised to make any copies of the specification. Any additional specifications can be obtained from the member network or the GSM Association Administrator on request.

4.3 Parties authorised to receive the A3/A8 algorithm from a manufacturer are;

- Subcontractors of the manufacturer / supplier which are involved in the development of equipment containing the algorithm A3/A8

4.4 Each party who receives a detailed specification of the COMP128, COMP128-2 and COMP128-3 algorithms must sign a confidentiality and restricted usage undertaking. The manufacturer is obliged to forward a copy of the undertaking(s) to the network operator, or the rapporteur, or the administrator, if applicable.

4.5 Distribution of the algorithm to manufacturers may involve the imposition of an administration charge. Application of this charge is at the discretion of the GSM Association.

5 Rules for the Management of the COMP128, COMP128-2 and COMP128-3 algorithms by Non-members of the GSM Association

5.1 A party who is not a GSM Association member, having obtained the detailed specification of the COMP128, COMP128-2 and COMP128-3 algorithms from the GSM Association Administrator is entitled to forward the specification(s) to the parties listed in paragraph 5.3, subject to the prior signature of the confidentiality and restricted usage undertaking.

5.2 The non-member is not authorised to make any copies of the specification. Any additional specifications can be obtained from the GSM Association Administrator on request.

5.3 Parties authorised to receive the COMP128, COMP128-2 and COMP128-3 algorithms from a non-member of the GSM Association are;

- Manufacturers of GSM Authentication Centres
- Manufacturers of GSM Subscriber Identity Modules
- Manufacturers of GSM test equipment
- Manufacturers of GSM system simulators

5.4 Each party who receives a detailed specification of the COMP128, COMP128-2 and COMP128-3 algorithms must sign a confidentiality and restricted usage undertaking. The non-member of the GSM Association is obliged to forward a copy of the undertaking(s) to the administrator.

5.5 Distribution of the algorithm to non-members may involve the imposition of an administration charge. Application of this charge is at the discretion of the GSM Association.

6 Annex Name and Address of the A3/A8 Administrator(s)

In respect of COMP 128, 128-2 and COMP128-3

James Moran
Fraud and Security Group Director
Floor 2
The Walbrook Building
25 Walbrook
London EC4N 8AF

Email: security@gsma.com

Tel: 020 7356 0600

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
3.6	12 Dec 2014	Transferred PRD from SG to FASG as SG.03 v3.6	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.