Confidentiality Agreement for the COMP128 Family of Example A3 and A8 Algorithms

Version 3.4

16 December 2014

This is a Binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Access to and distribution of this document is restricted to the persons permitted by the security classification. This document is confidential to the Association and is subject to copyright protection. This document is to be used only for the purposes for which it has been supplied and information contained in it must not be disclosed or in any other way made available, in whole or in part, to persons other than those permitted under the security classification without the prior written approval of the Association.

Copyright Notice

Disclaimer

The GSM Association ("Association") makes no representation, warranty or undertaking (express or implied) with respect to and does not accept any responsibility for, and hereby disclaims liability for the accuracy or completeness or timeliness of the information contained in this document. The information contained in this document may be subject to change without prior notice.

Antitrust Notice

The information contain herein is in full compliance with the GSM Association's antitrust compliance policy.

Table of Contents

1. Confidentiality and Restricted Usage Undertaking

relating to

THE GSM EXAMPLE ALGORITHMS COMP128, COMP128-2 AND COMP128-3 USED FOR AUTHENTICATION AND CIPHER KEY GENERATION.

BETWEEN THE BENEFICIARY:

_____

_____

_____

_____
[Company name and address]

AND THE PROVIDER:

_____

_____

_____

_____
[Company name and address]

2 Role of the Beneficiary

The BENEFICIARY is one of the following parties:

- A GSM Association member or rapporteur or a company acting on behalf of a GSM Association member or rapporteur;
- A GSM network operator's system supplier, manufacturer or subcontractor who supplies at least one of the following equipment-.
- GSM Authentication Centres (AUC) containing the A3/A8 algorithm;
- GSM Subscriber Identity Modules (SIM) containing the A3/A8 algorithm;
- GSM test equipment containing the A3/A8 algorithm;
- GSM system simulators containing the A3/A8 algorithm.

3. Role of the Provider

The PROVIDER who is authorised to transfer the confidential information mentioned below to the BENEFICIARY in his role as:

- The GSM Association A3/A8 administrator;
- A GSM Association member or rapporteur or a company acting on behalf of a GSM Association member or rapporteur, who received the confidential information from the A3/A8 administrator;
- A supplier or manufacturer of GSM equipment as described above who received the confidential information from a GSM Association member or rapporteur or directly from the GSM Association administrator.

4. Obligations

The PROVIDER undertakes:

4.1. to give to the BENEFICIARY, the BENEFICIARY having signed the undertaking, [.....] registered copies of the detailed specification of the COMP128, COMP128-2 AND COMP128-3 algorithms for authentication and cipher key generation in the GSM system and provided by GSM numbered [.....to.....]

4.2. to forward a copy of all signed CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKINGs known to the PROVIDER to other former PROVIDER and to the GSM Association A3/A8 administrator(s);

The Beneficiary undertakes:

4.3. to keep strictly confidential all information in the detailed specification, or electronic implementations thereof, here above mentioned and all related communication, written or verbal, which has been associated with that information, and after the signature of this undertaking (the "INFORMATION");

4.4. not to make any copies or photocopies of the documentation provided, even for internal usage;

4.5. not to disclose the INFORMATION to any party without prior and explicit authorisation in writing by the PROVIDER;

4.6. to take all measures which are necessary to avoid that his personnel disclose all or part of the INFORMATION to third parties, without prior explicit authorisation in writing by the PROVIDER;

4.7. to use the COMP128, COMP128-2 AND COMP128-3 algorithms for the sole purpose to procure, design, manufacture or supply equipment for authentication and cipher key generation in the GSM system that require the algorithm A3/A8; all other usage of the INFORMATION is prohibited;

4.8. to grant licenses on fair, reasonable and non-discriminatory terms and conditions, under all ESSENTIAL patents resulting from the implementation of the COMP128,

COMP128-2 AND COMP128-3 algorithms, proposed by GSM for use, sale and or manufacture of equipment in countries represented in GSM Association.
[ESSENTIAL patent shall mean a patent which is implemented by the equipment or operation thereof, where it is not technically possible to make, sell or operate equipment which complies with the specification of COMP128, COMP128-2 AND COMP128-3 algorithms provided by GSM without infringing that patent.]

4.9. not to register any Intellectual Property Rights containing all or part of the INFORMATION;

4.10. to make best efforts in the design and manufacture of equipment authorised by the present undertaking, in order that the algorithm here above identified cannot be used for other applications than those explicitly defined in the ETSI/GSM standard (GSM technical specification 3GPP TS 43.020 and 3GPP TS 42.009);

4.11. not to sub-contract any part of the design and manufacturing of equipment authorised by the present undertaking to any entity who has not forwarded a signed CONFIDENTIALITY AND RESTRICTED USAGE UNDERTAKING.

If, after eight years from the date of undertaking, and the BENEFICIARY has not used the INFORMATION, or if he is no longer active in the business mentioned above, he shall return the written INFORMATION which he has received. The BENEFICIARY is not authorised to keep copies; it is forbidden for him to make any further use of the INFORMATION. The BENEFICIARY is bound by the clauses of this undertaking, until the totality of the INFORMATION is in the public domain.

The obligations of confidentiality herein shall not apply to any INFORMATION which the BENEFICIARY can show:

- was known to the BENEFICIARY before such INFORMATION was received; or
- is in or subsequently comes into (other than by breach of this obligations hereunder) the public domain; or
- is received by the BENEFICIARY without restriction on disclosure or use from a third party, which the BENEFICIARY reasonable believes is free to make such disclosure on such terms; or
- is developed or discovered independently without reference to the INFORMATION disclosed under this undertaking.

Evidence of being a BENEFICIARY shall be given by providing a copy of this undertaking duly signed and certified by the BENEFICIARY and the PROVIDER. This undertaking shall be construed and interpreted in accordance with the law of the country of the PROVIDER.

Made in two originals, one of which is for the PROVIDER, the other for the BENEFICIARY.

5. Names and Signatures

for the PROVIDER

_____
[signature]

_____
[name and title (typed)]

_____
[date]

for the BENEFICIARY

_____
[signature]

_____
[name and title (typed)]

_____
[date]

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
3.4	12 Dec 2014	Transferred PRD from SG to FASG as SG.04 v3.4	FASG	David Chong, GSMA

A.2 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.