Security Algorithm Implementation Roadmap

Version 1.0

06 March 2020

This is a Non-binding Permanent Reference Document of the GSMA

Security Classification: Non-confidential

Copyright Notice

Disclaimer

Antitrust Notice

Table of Contents

1 Introduction

1.1 Background

The protection of digital mobile communications using cryptographic algorithms contributed enormously to reducing the level of fraud and security vulnerability that plagued first generation analogue mobile networks. A range of algorithms have been designed and introduced to protect the radio communications between mobile devices and the network. GSM, as a second generation technology, and its different successors allow mobile network operators to deploy new algorithms and retire older ones that become compromised. This feature ensures mobile users can be protected by algorithms that are fit for purpose and the security longevity of each technology can be extended.

New algorithms for the mobile industry are typically designed by the Security Algorithm Group of Experts (SAGE) at ETSI after which they are subject to public and private expert review, where appropriate. The design and choice of new algorithms is commonly based on existing cryptographic algorithms that have been through public scrutiny over many years and once developed they are published and available on the Internet for public scrutiny. Algorithms must be implemented in the mobile device and in the network and licences are usually required to permit export and use of the algorithms.

It is essential that compromised algorithms are removed from mobile devices and networks to fully protect networks and users against exploitation of known vulnerabilities. Mobile devices and networks should always implement a backup algorithm for each mobile technology in case one of the algorithms it has implemented is compromised and no longer considered to provide adequate levels of security protection. Networks without backup algorithms for specific technologies may need to temporarily fall back to a null algorithm thereby reducing their overall security posture if their only currently implemented algorithm is compromised.

1.2 Scope

This document describes the GSM, UMTS, LTE and 5G authentication, privacy and integrity protection algorithms that are used in cellular devices and networks. It provides guidance and recommendations on the best deployment options as well as the algorithms not to be used.

The document addresses a wide audience across the operator and vendor communities:

- SIM vendors, SIM and subscription managers can find the algorithms that can be implemented in the (e)UICC in the table entitled “Authentication and Key Agreement Algorithms” and in the table entitled “5G Algorithms for SUPI Encryption”.
- Mobile device manufacturers, device managers and engineers can find the algorithms implemented in mobile devices in the “Security Algorithms” tables and in the table entitled “5G Algorithms for SUPI Encryption”.
- Radio equipment vendors and radio design and operation engineers can find the algorithms implemented in the radio networks in the “Security Algorithms” tables.
- Core network vendors and core design and operation engineers can find the algorithms implemented in the core networks in the tables “Authentication and Key

Agreement Algorithms" and "5G Algorithms for SUPI Encryption" and the algorithms controlled from the core network in the other tables.

The recommendations set out in this document can be used to test and maintain an up-to-date configuration of device and network equipment.

In practice, the vast majority of operators may remain unaware of these recommendations and are likely to use the default algorithms provided by their device and network equipment suppliers. These suppliers have a crucial role to play to ensure that no compromised algorithms are supported by default on the equipment they sell and to advise their network operator customers on using the best algorithms recommended in this document.

1.3 Abbreviations

Term	Description
3GPP	Third Generation Partnership Project
AES	Advanced Encryption Standard
COCOM	Coordinating Committee for Multilateral Export Controls
EAP	Extensible Authentication Protocol
EC-GSM	Extended Coverage GSM
ECIES	Elliptic Curve Integrated Encryption Scheme
EEA	EPS Encryption Algorithm
EIA	EPS Integrity Algorithm
EPS	Evolved Packet System
eUICC	Embedded Universal Integrated Circuit Card
eNB	E Node B
GEA	GPRS Encryption Algorithm
GPRS	General Packet Radio Service
GSM	Global System for Mobile
Kc	Cipher key
LTE	Long Term Evolution
MME	Mobility Management Entity
NEA	NR Encryption Algorithm
NIA	NR Integrity Algorithm
SHA	Secure Hash Algorithm
SIDF	Subscription Identifier De-concealing Function
SIM	Subscriber Identity Module
SUPI	Subscription Permanent Identifier
UEA	UMTS Encryption Algorithm
UIA	UMTS Integrity Algorithm
UICC	Universal Integrated Circuit Card
UMTS	Universal Mobile Telecommunication System
USIM	Universal Subscriber Identity Module

2 Authentication and Key Agreement Algorithms

Algorithm	Type	Description	Comments	Recommendations
COMP128 (sometimes referred to as COMP128-1)	GSM Authentication	Original example algorithm for authentication.	This was broken in 1998.	This must not be used in networks or SIM cards. Operators still using this algorithm must phase it out as soon as possible.
COMP128-2	GSM Authentication	Variation of COMP128-1 to minimise original attack.	This was developed as a quick fix to COMP128-1.	Only produces a 54-bit Kc. Should not be used for new deployments. Where already in use, should ideally be phased out and superseded by G-Milenage or COMP128-3.
COMP128-3	GSM Authentication	64-bit Kc generation variant of COMP128-2.	This is essentially the same algorithm as COMP128-2.	Acceptable as a 2G-only algorithm, although G-Milenage should be preferred. Operators should have adopted 3G authentication even if still using 2G.
GSM-MILENAGE (sometimes referred to as G-MILENAGE)	GSM Authentication	GSM variant of Milenage, which is based on AES.	This allows operators to have customised parameters.	The best current choice for a 2G algorithm, if the operator cannot or does not want to develop their own algorithm. However, operators should have adopted 3G authentication even if still using 2G.
MILENAGE	3G, 4G and 5G Authentication	Original 3G example authentication and key agreement (AKA) algorithm, based on Rijndael/AES.	This allows operators to have customised parameters.	It is recommended that non-removable UICCs (eUICC and iUICC) support both MILENAGE and TUAK to provide resilience. In addition, the operator can develop its own algorithm. LTE and 5G require a 3G AKA algorithm such as MILENAGE or TUAK.
TUAK	3G, 4G and 5G Authentication	Alternative 3G example authentication and	This allows operators to have	An alternative to MILENAGE. It is recommended that non-

Algorithm	Type	Description	Comments	Recommendations
		key agreement algorithm, based on Keccak (which is also the basis of SHA-3).	customised parameters.	removable UICCs (eUICC and iUICC) support both MILENAGE and TUAK to provide resilience.
Additional EAP methods	Authentication in private networks	In addition to AKA based EAP methods, such as EAP-AKA' (RFC 5448) and EAP-AKA (RFC 4187), alternative EAP authentication methods can be used for private networks.	This allows private networks to interwork with authentication methods used in other industries.	EAP-TLS (RFC 5216) with TLS 1.3 (RFC 8446) default algorithms is recommended.

3 GSM Security Algorithms

Algorithm	Type	Description	Comments	Recommendations
A5/0		No encryption designation for GSM.		
A5/1	GSM Privacy	Original GSM encryption algorithm.	Low security offering.	It is still recommended to support A5/1in devices and networks, for reasons of legacy compatibility, but A5/3 should always be preferred when available.
A5/2	GSM Privacy	Variant encryption algorithm produced for COCOM export control compliance.	This was broken in 2003 and provides no protection at all. The industry agreed to remove the algorithm in 2006.	This should not be used in networks or enabled in devices.
A5/3	GSM Privacy	Encryption algorithm constructed from Kasumi.	Best widely currently supported GSM algorithm. Security is limited by the 64-bit key length.	Presently, the best widely supported algorithm.
A5/4	GSM Privacy	Variant of A5/3 with 128 bit key.	This algorithm is increasingly supported, and has begun to be deployed. Infrastructure suppliers and device	Requires USIM authentication for key support.

Algorithm	Type	Description	Comments	Recommendations
			manufacturers are encouraged to plan implementation to support operators that wish to use this algorithm.	

4 GPRS Security Algorithms

Algorithm	Type	Description	Comments	Recommendations
GEA0		No encryption designation for GPRS.		
GEA1	GPRS Privacy	Original GPRS encryption algorithm.	Least secure GPRS algorithm.	This should not be used in networks. Operators still using this algorithm should phase it out as soon as possible.
GEA2	GPRS Privacy	Additional GPRS encryption algorithm	Low security offering.	It is still recommended to support GEA2 in devices and networks, for reasons of legacy compatibility, but GEA3 should always be preferred when available.
GEA3	GPRS Privacy	Additional GPRS encryption algorithm, based on UEA1 (and hence on Kasumi).	Best currently supported GPRS algorithm. Low security due to 64-bit key length.	Devices and networks should support GEA3.
GEA4	GPRS Privacy	Variant of GEA3 with 128 bit key.	This algorithm is not currently supported and infrastructure suppliers and handset manufacturers are encouraged to plan implementation.	Requires USIM authentication for key support.
GEA5	GPRS Privacy	Additional GPRS encryption algorithm with 128-bit key, based on UEA2 (and	This algorithm was introduced to make two 128-bit	

Algorithm	Type	Description	Comments	Recommendations
		hence on SNOW 3G).	encryption algorithms (this and GEA4) available for EC-GSM.	
GIA4	GPRS Integrity	GPRS integrity algorithm with 128-bit key, based on UIA1 (and hence on Kasumi).	This and GIA5 were introduced for EC-GSM.	
GIA5	GPRS Integrity	GPRS integrity algorithm with 128-bit key, based on UIA2 (and hence on SNOW 3G).	This and GIA4 were introduced for EC-GSM.	

5 UMTS Security Algorithms

Algorithm	Type	Description	Comments	Recommendations
UEA0		No encryption designation for 3G.		
UEA1 / UIA1 (Kasumi)	3G Privacy (UEA1) and Integrity (UIA1)	Original 3G encryption and integrity algorithms, derived from MISTY.	Still strong. (Related key attack on Kasumi is not significant for UEA1 / UIA1.)	
UEA2 / UIA2 (SNOW 3G)	3G Privacy (UEA2) and Integrity (UIA2)	Additional 3G encryption and integrity algorithms, derived from SNOW 2.0.	This algorithm is not currently supported and infrastructure suppliers and device manufacturers are encouraged to plan implementation.	Devices should support both UEA1/UIA1 and UEA2/UIA2. This provides resilience against possible future cryptanalysis.

6 LTE Security Algorithms

Algorithm	Type	Description	Comments	Recommendations
EEA0		No encryption designation for LTE.		
128-EEA1 / 128-EIA1 (Snow 3G)	LTE Privacy (EEA1) and Integrity (EIA1)	One of the original LTE algorithms, with 128-bit keys.	Still strong	Mandatory to support in devices, eNBs and MMEs
128-EEA2 /	LTE Privacy	One of the original	Still strong	Mandatory to support

Algorithm	Type	Description	Comments	Recommendations
128-EIA2 (AES)	(EEA2) and Integrity (EIA2)	LTE algorithms, with 128-bit keys.		in devices, eNBs and MMEs
128-EEA3 / 128-EIA3 (ZUC)	LTE Privacy (EEA3) and Integrity (EIA3)	LTE algorithms with 128-bit keys, added at the request of Chinese operators.	Still strong	Optional to support in devices, eNBs and MMEs

7 5G Security Algorithms

Algorithm	Type	Description	Comments	Recommendations
NEA0		No encryption designation for 5G.		
128-NEA1 / 128-NIA1 (Snow 3G)	Privacy (NEA1) and Integrity (NIA1)	Identical to the corresponding LTE algorithms.	Still strong	Mandatory to support in devices and network nodes
128-NEA2 / 128-NIA2 (AES)	Privacy (NEA2) and Integrity (NIA2)	Identical to the corresponding LTE algorithms.	Still strong	Mandatory to support in devices and network nodes
128-NEA3 / 128-NIA3 (ZUC)	Privacy (NEA3) and Integrity (NIA3)	Identical to the corresponding LTE algorithms.	Still strong	Optional to support in devices and network nodes

8 5G Algorithms for SUPI (Subscriber Identity) Encryption

These are profiles of the Elliptic Curve Integrated Encryption Scheme (ECIES)			
Profile	**Description**	**Comments**	**Recommendations**
NULL-scheme	No SUPI encryption	Specified in 3GPP TS33.501, section C.2 SUPI will be in clear on the network.	Not recommended
Profile A	ECIES profile using the 256-bit elliptic curve Curve25519, with SHA-256 and 128-bit AES	Specified in 3GPP TS33.501, section C.3.4.1. Provides a 128-bit security level.	Mandatory to support in devices and SIDFs. Recommended to support in UICCs, if SUCI calculation on the USIM is desired and the operator does not want to specify its own algorithm.
Profile B	ECIES profile using the 256-bit elliptic curve secp256r1, with SHA-256 and 128-bit AES	Specified in 3GPP TS33.501, section C.3.4.2. Provides a 128-bit security level.	Mandatory to support in devices and SIDFs. Recommended to support in UICCs, if SUCI calculation on the USIM is desired and the operator does not want to specify their

			own algorithm.
Operators may also implement their own profiles in the UICC and SIDF.			

Note 1: A Key Derivation Function, based on SHA-256 and specified in 3GPP TS 33.220, is used for many standardised key derivation purposes in 3G, LTE and 5G.

Note 2: A 3GPP study TR 33.841 has concluded there is no immediate need to transition to 256-bit key lengths but that new 256-bit algorithms may be needed anyway. For example, for government use cases and better performance and cost-effectiveness in virtualized environments. 3GPP has asked ETSI SAGE to analyse new 256-bit algorithms for 5G.

ECIES would be much more seriously affected by quantum computation: the Elliptic Curve Diffie-Hellman component of ECIES could be broken very efficiently by a large scale quantum computer running Shor's algorithm. Identifying the best quantum safe alternatives for algorithms such as Elliptic Curve Diffie-Hellman is arguably the hottest research topic in cryptography today.

Note 3: Further study is required to determine whether the algorithms in section 8 should be mandated within the eUICC or not.

Annex A Document Management

A.1 Document History

Version	Date	Brief Description of Change	Approval Authority	Editor / Company
1.0	6 Mar 2020	Release 1 developed and agreed within FSAG	GSMA TG	James Moran / GSMA

A.2 Other Information

Type	Description
Document Owner	GSMA 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.