Security requirement

Operational Security Policies for Mobile Networks

Deutsche Telekom Group

Version	1.3
Date	Dec 1, 2023
Status	Released

Publication Details

Published by
Deutsche Telekom AG
Vorstandsbereich Technology & Innovation
Chief Security Officer

Reuterstrasse 65, 53315 Bonn
Germany

File name	Document number	Document type
	3.38	Security requirement

Version	State	Status
1.3	Dec 1, 2023	Released

Contact	Validity	Released by
Telekom Security psa.telekom.de	Dec 1, 2023 - Nov 30, 2028	Stefan Pütz, Leiter SEC-T-TST

Summary
Operational Security Policies for Mobile Networks
This document was created based on the general security policies of the Group and gives guidance on selection of 3GPP-network-related security options for mobile network equipment and Deutsche Telekom Group SIM cards (UICC). The requirements shall be met in order to protect Deutsche Telekom Group customers and networks against attacks and fraud, and to protect customers' privacy.

Table of Contents

1. Introduction

This document has been prepared based on the general security policies of the Group.

The security requirement is used as a basis for an approval in the PSA process, among other things. It also serves as an implementation standard in units which do not participate in the PSA process. These requirements shall be taken into account from the very beginning, including during the planning and decision-making processes. When implementing these security requirements, the precedence of national, international and supranational law shall be observed.

1. Objective

This document gives guidance to Deutsche Telekom Group companies which operate mobile networks according to 3GPP standards (i.e., GSM/GPRS, UMTS, LTE and 5G) on how to select security options defined in the standards. Common IMS and interfaces to other networks are out of scope. The requirements are applicable to UICCs, network elements and network configuration.

Several security functions are defined as “optional to implement” by the standards, so it is important to know which of those options must be requested from vendors. The standards do not define if and how an operator should use security functions. Such decisions are left to an operator’s policy, and the present document fills this gap.
It is not intended to give an introduction or overview of mobile network security in this document, but references to relevant specifications are included for further reading. Therefore, mandatory security functions that are required for the system to work are not listed as requirements. Reference is a basic glossary of mobile network terms and definitions, and gives an overview of security-related network functions in GSM, GPRS, UMTS, LTE and 5G (see annex C, [1] to [13]).

2. Responsibilities

This requirement document can be used for different purposes: it may serve as Deutsche Telekom Group -internal guideline for system owners, and it provides requirements for an integration service, delivery, or development contract.

The person responsible for the system (system owner) must ensure, that the requirements within this document will be fulfilled. In case the document is used as part of a contract, the Deutsche Telekom Group system owner transfers responsibility to comply with the requirements to the vendor/contractor. The vendor/contractor must clearly indicate if requirements will not be fulfilled, so that system owner can find a workaround.

3. Entry into effect

In the domestic and international Group companies, subsidiaries and legal business units the security requirements shall become binding upon approval by the respective management / Board of Management or by the unit authorized by such for this purpose.

Upon entry into effect the requirements shall be binding for all mobile networks and devices (if sold by Deutsche Telekom Group), according to 3GPP standards, which are put into productive operation for the first time. It is recommended that existing systems achieve a comparable level of security, making sure that the economic efforts are adequate.

2. Entity Authentication

2.1. Network requirements

Req 1	The network must authenticate subscribers by their Universal Subscriber Identity Module (USIM) when they access the network.

Authentication using the USIM application on the Universal Integrated Circuit Card (UICC) is also called primary authentication. For this document, the term UICC also includes the predecessor “SIM card”.
Reference: [2] 3GPP TS 33.102 – 3G Security Architecture, clause 6.3.

Motivation: Proper authentication is the basis for network access control and correct billing.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-1/1.3

Req 2	The network must regularly re-authenticate subscribers by their USIM.

Networks must find an adequate balance between increased security vs. increased data load and increased call setup time due to frequent re-authentication. Increasing security by frequent re-authentication is more important for Radio Access Technologies (RAT) using weaker security mechanisms, in particular for 2G.
According to 3GPP standards, networks can re-authenticate subscribers at any time and as often as the network operator wishes (see [3] clause 7.2.1 or [11] clause 6.2.3.1), even during ongoing calls without interrupting them. However, re-authentication criteria are not standardised. Mobile Switching Center (MSC), Serving GPRS supported node (SGSN), Mobility Management Entity (MME) and Access and Moblity Management Function (AMF) implementations typically allow to define re-authentication criteria based on time, events, and data volume.

Recommended settings for re-authentication of a subscriber with adequate balance between security benefit and performance drawback are to authenticate:
Event-based:

- every attach
- every mobile originated or mobile terminated Short Message System (SMS) transferred over GSM EDGE Radio Access Network (GERAN)
- every N-th regular location update
- every N-th periodic location update (this results in a maximum time between authentications)
- every N-th billing-relevant event caused by the subscriber (N=1 for 2G when radio attacks are being performed)

Time-based:

- after 1 hour for users attached to GERAN
- after 5 hours for users attached to Universal Mobile Telecommunications System (UMTS)
- after 12 to 24 hours for users attached to Long Term Evolution (LTE) or New Radio (5G)

Volume-based:

- after M signalling messages in general, or of a particular type
- after P bytes of messages transferred

M, N, and P shall be configurable to allow the Public Land Mobile Network (PLMN) operator to set and change these values.
In general, N should be in the range of 1-15. Careful planning is needed and should involve national engineering and security departments. An example parameter set for recommended settings can be found in annex D.
M and P should be set to a value that in regular situations, the event-based or time-based triggers apply. Only in cases where a large number of signalling messages is being sent within a short timeframe, the volume-based triggers should apply.
Stationary mobile devices are to be considered, too. For those, the event-based triggers often have no effect. The time-based triggers, also listed above, raise a re-authentication in these cases.
Depending on roaming contracts, inbound roamers may be authenticated more frequently than domestic subscribers.
Users in the context of this requirement are all sorts of mobile devices, including, but not limited to, mobile subscribers, Internet of Things (IoT) and mobile home routers.

Additional information to be considered:

- Authentication processes creating signalling traffic might cause overload situations.
- 2G is used in old elevator systems, which cannot be easily upgraded to a different RAT.
- 3G technology is used for remote maintenance services in wind energy plants.
- There is no need to immediately authenticate a subscriber when one of the above triggers occurs. Authentication should be performed with the next signalling message exchanges. This reduces battery consumption of the mobile device.

Motivation: Full re-authentication is necessary for several reasons. It generates new session key material, which helps in case an old session key has been compromised. It limits fraud potential by ensuring that the USIM is still inserted in the mobile device. It establishes a defined security state, independent of mobility or user equipment history. Authenticating in particular billing-relevant events (such as mobile originated calls and mobile originated SMS) strengthen billing integrity and help to handle disputes.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-2/1.3

Req 3	The network must re-authenticate the subscriber as soon as possible after hand-in from a legacy or foreign RAT in order to establish the strongest possible security context.

Backward compatibility features such as key conversion functions allow coexistence of Global System for Mobile Communications (GSM) / General Packet Radio Service (GPRS), UMTS, LTE and 5G networks. However, strength of keys and security features may be limited by the originating RAT. To give an example: at handover from GSM to UMTS, the network may expand the existing 64-bit GSM key to 128-bit, but the cryptographic key strength still remains 64 bits. The subscriber must be re-authenticated in order to benefit from all security features of the more advanced RAT.
Note: According to 3GPP standards, networks can re-authenticate subscribers at any time and as often as the network operator wishes (see [3] clause 7.2.1 or [11] clause 6.2.3.1).

Motivation: Backward compatibility will severely limit security of new technologies unless re-authentication is performed quickly after handover. This requirement can not efficiently be mapped to static re-authentication criteria listed in Req 2.

For this requirement the following threats are relevant:

- Unauthorized access to the system
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-3/1.3

Req 4	Network elements must evaluate re-authentication criteria per subscriber.

In order to prevent massive network load due to signalling traffic, all subscribers must not be re-authenticated at the same time. Instead, for every mobile device a timer must be used to track the up-to-dateness of its state of authentication and to trigger re-authentication processes. This is to be implemented per International Mobile Subscriber Identity (IMSI) / Subscription Permanent Identifier (SUPI).

A User Equipment (UE) can be in the RRC_CONNECTED or in the RRC_INACTIVE state, if a Radio Resource Control (RRC) connection has been already established, or in the RRC_IDLE state if an RRC connection does not yet exist.
If a subscriber is in RRC_INACTIVE or RRC_IDLE state, the re-authentication process must be started just after reconnection.

Note: According to 3GPP standards, networks can re-authenticate subscribers at any time and as often as the network operator wishes (see [3] clause 7.2.1 or [11] clause 6.2.3.1)

Motivation: Only per-subscriber evaluation causes deterministic results. Evaluation based on average values (e.g., every N-th call per MSC instead per subscriber) can result in specific subscribers not being authenticated for a very long time.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-4/1.3

Req 5	The network must enforce local authentication / fast re-authentication in addition to full authentication.

Several RATs implement mechanisms where both peers of a communication (usually mobile device and base station) authenticate each other by verifying that both are still in possession of a valid session key. These are:

- local authentication by counter-check in UMTS (clause 6.4.7 in [2])
- local authentication by counter-check in Evolved Packet System (EPS) (clause 7.5 in [3])
- local authentication by counter-check in 5G (clause 6.13 in [11])
- fast re-authentication in WLAN interworking (clause 6.1.4 in [4])
- fast re-authentication in non-3GPP access (clauses 6.3. and 8.2.3 in [5])

In fast re-authentication only a certain part of the session keys is updated. Keys in Hardware Security Modules remain unaffected.

Motivation: These lighter authentication mechanisms are an efficient means to maintain security between full re-authentications without impacting the Home Subscriber Server (HSS) or Authentication, Authorization and Accounting (AAA) server.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-5/1.3

Req 6	Full authentication in GSM, GPRS, UMTS and Evolved Packet System (EPS) must use UMTS Authentication and Key Agreement (AKA) or newer AKA, unless the subscriber has only a legacy SIM card without a USIM application.

According to [2] and [3] clause 6.1.1, multiple interworking scenarios between GSM and UMTS as well as between GSM and EPS or UMTS and EPS are possible, but some of them sacrifice security for compatibility. Since all networks support at least Release 99 (Rel-99), there is no more need for the lower security scenarios unless a subscriber has no USIM. Therefore, it is not permitted to switch network elements to pre-Rel-99 behaviour to enforce a fall back to GSM AKA when UMTS AKA, EPS AKA or Extensible Authentication Protocol AKA Prime (EAP-AKA') could be used.

Note: Roaming scenarios need to consider the release status of the roaming partner network. In consideration of the time between Rel-99 (introduction of 3G in 1999) and today, networks support not only Rel-99, but already Rel-8 (introduction of 4G) and newer releases.

Motivation: Running UMTS AKA instead of GSM AKA, or EPS AKA instead of UMTS AKA respectively, greatly enhances security, because it provides mutual authentication and establishes a UMTS or newer security context.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-6/1.3

Req 7	Access to 5G Core (5GC) or EPS with a 2G SIM or a SIM application on a UICC must not be granted.

A UE with a 2G SIM is considered to be in limited service mode in 5G. Thus, there may be unauthenticated emergency sessions for unauthenticated UEs in limited service mode.

Reference: [3] 3GPP TS 33.401 – EPS Security Architecture, clause 6.1.1.

Motivation: Running EPS AKA or newer instead of GSM AKA greatly enhances security, because it provides mutual authentication and establishes an EPS or newer security context.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-7/1.3

Req 8	If the UICC is utilised for non-3GPP access network authentication and contains a USIM, then authentication must not be based on GSM AKA.

At present, 3GPP has specified GSM/GPRS, UMTS, LTE and 5G access technologies. This requirement applies to any non-3GPP access technology, but most common are IEEE WLAN (WIFI) networks and WiMAX. For transport of AKA over EAP, this requirement is in line with 3GPP specifications [4], [5] clause 6.1 and [11] clause 6.1.1.1. Nevertheless, some vendors suggest using EAP-SIM only by ignoring the USIM and forcing the UICC into SIM mode. This is not allowed. EAP-AKA or EAP-AKA' (for Evolved Packet Core (EPC) and 5GC) must be used instead of EAP-SIM. Neither the SIM application nor service No. 38 (virtual SIM mode) of the USIM application must be used.

Motivation: GSM AKA provides weaker security than UMTS or EPS AKA: It does not prevent replay attacks and does not provide sufficient network authentication. In order to prevent bidding-down attacks, both the network and the mobile device must be able to independently request optimal security if a USIM is present.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-8/1.3

Req 9	Network Elements must only fetch one UMTS, EPS or 5GC Authentication Vector (AV) per subscriber for immediate use.

Reference: [3] 3GPP TS 33.401 – EPS Security Architecture, clause 6.1.1.

Motivation: Unlike in 2G, storing multiple AVs for later use in different network elements will lead to synchronisation errors. The errors are caused by failed freshness checks in the USIM, when interleaved authentications of different elements use older sequence numbers. Therefore, the desired efficiency gain by fetching AVs in batches will have the opposite effect and actually reduces efficiency. Index schemes for sequence number management could help but are not standardised and typically not implemented in HSS / Home Location Register (HLR) / Authentication Centre (AuC).

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Disruption of availability
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-9/1.3

Req 10	Packet-switched emergency sessions must only be enabled, if an associated emergency service is properly set up.

Packet-switched emergency sessions only make sense when a suitable emergency service (e.g., VoIP) is configured

on top. Detailed information can be found in clause 2.1.2.2 EPC of [13].

Motivation: Allowing emergency sessions in the packet-switched core network without proper configuration may open unexpected security holes. For example, misuse of emergency calls or extended usage (denial of service attack) by callers with unknown IMSI or International Mobile Equipment Identity (IMEI). Packet-switched data transmission could potentially be used without the possibility to trace such a transmission down to a specific subscriber.

For this requirement the following threats are relevant:
- Disruption of availability
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-10/1.3

2.2. UICC requirements

Req 11	New UICCs must contain a USIM application with an authentication algorithm approved by Deutsche Telekom Security.

Approved algorithms are country-specific variants of:

- COMPNAT for legacy SIM application (only in 2G scenarios; Deutsche Telekom Group proprietary)
- SAM for USIM or Integrated SIM (ISIM) applications (Deutsche Telekom Group proprietary)
- MILENAGE for USIM or ISIM applications
- TUAK for USIM or ISIM applications

Motivation: Weak authentication algorithms can be attacked, so that the secret long-term key can be revealed. Moreover, some not approved authentication algorithms for GSM provide weak cipher keys with less than 64-bit entropy. Country-specific variants add protection in case of a limited security breach.

For this requirement the following threats are relevant:
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-11/1.3

Req 12	5GC networks must not use subscriber permanent identities (SUPI) for network access. Instead, the subscriber concealed identifier (SUCI) must always be used. Schemes for SUPI concealment must be used according to the list below.

- NULL scheme must not be used in live networks (only allowed in test networks)
- Scheme A (curve25519) must be preferred
- Scheme B (secp256r1) must be used alternatively

3GPP specified that in 5G the SUPI must never be sent in plain text over the air interface (see [11] clause 5.2.5) and is instead concealed inside the privacy preserving SUCI. For SUCIs containing IMSI based SUPI, the UE in essence conceals the Mobile Subscriber Identification Number (MSIN) part of the IMSI. On the 5G operator-side, the Subscription Identifier De-concealing Function (SIDF) of the Unified Data Management (UDM) is responsible for de-concealment of the SUCI and resolves the SUPI from the SUCI based on the protection scheme used to generate the SUCI (see [11] annex C.3.1). Also, for initial attach the SUCI must be used. Furthermore, primary authentication using the SUCI must

be supported by AMF and Security Anchor Function (SEAF) (see [11] clause 5.5.3 and 5.6).

Motivation: Use of temporary identities protects subscriber privacy because they can not be identified by sniffing on the radio link.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-12/1.3

Req 13	The network must use temporary subscriber identities over radio links.

3GPP specified access-technology specific mechanisms that map the permanent subscriber identity (IMSI) to temporary pseudonyms. Networks must allocate and make use of these pseudonyms (Temporary MSI (TMSI) / Packet-TMSI (P-TMSI) [2], Global Unique Temporary Identifier (GUTI) [3], Subscription Concealed Identifier (SUCI) [11], re-authentication identity [4]). There is one exception: IMSI should be used when the serving network cannot retrieve the IMSI based on the GUTI by which the user identifies itself on the radio path (see [3] clause 6.1.3), e. g. when a subscriber connects to a network for the first time, there is no previously allocated pseudonym (except for 5G, where SUCI is used for initial authentication, too). In this case, the permanent identity must be used once.

Some femtocell implementations request the permanent identity after every hand-in, instead of fetching the previously allocated temporary identity from the network. This behaviour is not allowed because tracking subscribers over the radio would become easy if the permanent identity is used after each handover.

Motivation: Use of temporary identities protects subscriber privacy because subscribers cannot be identified by sniffing on the radio link.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-13/1.3

Req 14	The network must (re-)allocate temporary subscriber identities only after successful activation of non-access stratum (NAS) security.

This requirement is described in detail by 3GPP in [11] clause 6.12.3.

Motivation: An attacker can match temporary identities to the permanent identity if allocation is done in the clear.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Disruption of availability
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-14/1.3

Req 15	The network must allocate a new temporary subscriber identity after each periodic and normal location/tracking/routing area update.

The respective periodic update timer should be set between one and five hours for GSM Circuit-Switched, and to the default of 54 minutes for GPRS Mobility Management (see [6] clause 11.2.2). Timer values for UMTS, EPS and 5G may be freely selected but should not be longer than 24h.

Motivation: An attacker can track subscribers over the radio if the temporary identity is not changed regularly.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-15/1.3

Req 16	A new temporary subscriber identity must always be an unpredictable value that does not allow correlation with previously used temporary subscriber identities.

The purpose of the temporary subscriber identity is to not reveal the permanent identifier of a mobile subscriber [3], [11], [12] section 2.8.1. This also implies that any sort of temporary subscriber identities shall not be created in a way that correlations with previously assigned temporary subscriber identities can be made.
Every temporary subscriber identity that is created shall be random, unpredictable and independent of any other temporary subscriber identity. It shall not be possible to correlate it with any other temporary subscriber identity.

Motivation: An attacker can track subscribers over the radio if the temporary identity can be correlated with previously used temporary subscriber identity.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized use of services or resources
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-16/1.3

Req 17	The network must only request the device identity IMEI after initiation of NAS security.

Requesting the IMEI unencrypted is only permitted in special cases:
- for unauthenticated emergency calls, if required for misuse handling or mandated by national law
- for troubleshooting cases with issues related to specific devices
- for network-based workarounds of severe problems related to specific devices

Reference: [3] 3GPP TS 33.401 – EPS Security Architecture, clause 5.1.1.

Motivation: The IMEI is a permanent identity that can be linked to a subscriber.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-17/1.3

3. Integrity Protection over the UNI

Protection of the User-to-Network Interface (UNI) mainly intends to protect the radio interface. Some protection layers may extend further into the network than just the radio link, however. It was a design choice, due to legal reasons, to separate ciphering and integrity protection. Therefore, the use of algorithms for Authenticated Encryption with Associated Data (AEAD), as methods which encrypt and integrity protect in one single operation, are out of scope within existing specifications.

3.1. Integrity Protection for UMTS

Req 18	UMTS networks must support and enforce integrity protection of traffic using UMTS Integrity Algorithm (UIA) 0 (only emergency sessions), UIA1 (Kasumi) and UIA2 (SNOW 3G).

The 3GPP standard [2] (clauses 6.4.2 “1)” and 6.5.6) requires that both networks (Radio Network Controler (RNC)) and mobile devices must use integrity protection and terminate the connection attempt if the other side does not support integrity. This requirement emphasizes that integrity protection must always be used, even if most implementations allow to disable integrity, e.g., for test purposes.

Integrity protection of emergency calls depends on successful authentication (see [2] clause 6.4.9). NULL algorithm (UIA0) is only allowed to unauthenticated emergency calls.

Note: From Rel-7 onwards, the 3GPP standard [2] also requires support of UIA2 (SNOW 3G) in networks and mobile devices.

Motivation: Integrity protection is an essential security measure. It helps to ensure correct billing, prevent man-in-the-middle attacks and message modification etc.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-18/1.3

3.2. Integrity Protection for EPS

Req 19	LTE/EPC networks must enforce integrity protection of NAS and Radio Resource Control (RRC) Signalling Plane.

RRC signalling belongs to the access stratum (AS).
The 3GPP standard [3], clause 5.1.4 requires that both networks and mobile devices must use integrity protection and terminate the connection attempt if the other side does not support integrity. This requirement emphasizes that integrity protection must always be used, even if most implementations allow to disable integrity, e.g., for test purposes.

Integrity protection of emergency calls depends on successful authentication (see [3] clause 15). NULL algorithm (EPS Integrity Algorithm EIA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, AS security terminates in the eNodeB and NAS signalling security terminates in the MME. Therefore, both elements must be checked independently for compliance.

Motivation: Integrity protection is an essential security measure. It helps to ensure correct billing, prevent man-in-the-middle attacks and message modification etc.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-19/1.3

Req 20	LTE/EPC networks must support integrity protection algorithms EIA0 (only emergency sessions), EIA1 (SNOW 3G) and EIA2 (AES) for NAS and RRC (AS) Signalling Plane.

The 3GPP standard [3], clause 5.1.4.2 requires and this requirement emphasizes that both algorithms must always be supported, even if some vendors try to implement only one of them. One of the algorithms must be used. EIA2 must be set as preferred algorithm in the network because it has been tested more extensively. The number of test cases with EIA1 has been reduced in official conformance tests.

Integrity protection of emergency calls depends on successful authentication (see [3] clause 15). NULL algorithm (EIA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, AS security terminates in the eNodeB and NAS signalling security terminates in the MME/AMF. Therefore, both elements must be checked independently for compliance.

Motivation: LTE/EPC was designed with two security algorithms from the start to allow quick migration in case one algorithm is broken. Unlike UMTS, but similar to GSM, the LTE security algorithms are implemented in the base stations and the MME. Having two algorithms supported in each base station avoids massive cost for HW swap in case of an algorithm change.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-20/1.3

3.3. Integrity Protection for 5GC

Req 21	5GC networks must enforce integrity protection of User Plane, NAS and RRC (AS) Signalling Plane.

On the one hand, this is realized by user plane integrity protection (UPIP). The UE shall activate integrity protection of user data based on the indication sent by the gNodeB (see [11] clause 5.3.3).
On the other hand, the 3GPP standard [11] requires that both networks (ng-eNodeB, gNodeB and AMF) and mobile devices must use integrity protection and terminate the connection attempt if the other side does not support integrity. If the LTE air interface (E-UTRA) is connected to 5GC, the UE must indicate that it supports UPIP with an ng-eNB. This requirement emphasizes that integrity protection must always be used, even if most implementations allow to disable integrity, e.g., for test purposes.

Integrity protection of emergency calls depends on successful authentication (see [11] clause 10). NULL algorithm (NIA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, AS security terminates in the ng-eNodeB/gNodeB and NAS signalling security terminates

in the MME/AMF. Therefore, both elements must be checked independently for compliance.

Motivation: Integrity protection is an essential security measure. It helps to ensure correct billing, prevent man-in-the-middle attacks and message modification etc.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-21/1.3

Req 22	5GC networks must support integrity protection algorithms New Radio Integrity Algorithm (NIA) 0 (only emergency sessions), 128-NIA1 (SNOW 3G) and 128-NIA2 (AES) for NAS and RRC (AS) Signalling Plane. NIA2 must be activated as preferred algorithm in the network.

The 3GPP standard [11], clause 5.2.3 requires and this requirement emphasizes that both algorithms (NIA1 and NIA2) must always be supported, even if some vendors try to implement only one of them. One of the algorithms must be used. NIA2 must be set as preferred algorithm in the network, because it has been tested more extensively. The number of test cases with NIA1 has been reduced in official conformance tests.

Integrity protection of emergency calls depends on successful authentication (see [11] clause 10). NULL algorithm (NIA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, AS security terminates in the ng-eNodeB/gNodeB and NAS signalling security terminates in the MME/AMF. Therefore, both elements must be checked independently for compliance.

Motivation: LTE/EPC and 5GC was designed with two security algorithms from the start to allow quick migration in case one algorithm is broken. Having two algorithms supported in each base station avoids massive costs for Hardware (HW) swap in case of an algorithm change.

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Disruption of availability
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-22/1.3

4. Confidentiality Protection over the UNI

Protection of the User-to-Network Interface (UNI) mainly intends to protect the radio interface. Some protection layers may extend further into the network than just the radio link, however. It was a design choice, due to legal reasons, to separate ciphering and integrity protection. Therefore, the use of algorithms for Authenticated Encryption with Associated Data (AEAD), as methods which encrypt and integrity protect in one single operation, are out of scope within existing specifications.

4.1. Confidentiality Protection for GSM and GPRS

Req 23	GSM and GPRS networks must enforce ciphering of all traffic.

This requirement has several consequences:

- the network must exclude the NULL algorithms A5/0 and GPRS Encryption Algorithm (GEA) 0 from the list of allowed ciphering algorithms
- the network must enable ciphering using the Cipher Mode Command immediately after connection establishment
- mobile devices that do not support ciphering must be rejected

Ciphering of emergency calls depends on successful authentication (see [2] clause 6.4.9). NULL algorithms are only allowed to unauthenticated emergency calls.

Note: Some signalling messages may not be ciphered, as listed in [2].

Motivation: GSM and GPRS have no integrity protection. Therefore, ciphering is the only means to ensure correct billing and prevent attacks like targeted message modification etc. Moreover, certain services like SMS TAN rely on protected message transfer. Establishment of secure connections should not depend on mobile device capability alone.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-23/1.3

Req 24	For GSM networks encryption algorithms according to the list below must be used.

- A5/0 must be forbidden by the network (see Req 23)
- A5/1 must be supported optionally (see note below)
- A5/2 must not be supported
- A5/3 must be supported
- A5/4 must be supported and preferred to A5/3, but must be disabled until sufficiently tested and released

At minimum, it must be possible to upgrade new network elements and should be possible to upgrade new mobile devices remotely without HW change to A5/3 and A5/4. A5/4 uses the same base algorithm as A5/3 (Kasumi), but uses 128-bit cipher key length (instead of 64-bit). A5/4 must be sufficiently tested before release. Reason to keep A5/4 disabled currently is that enabling of A5/4 in mobile devices without any test capabilities in mobile networks may

lead to faulty implementations.

Note: A5/2 must be completely removed or permanently disabled in mobile devices because otherwise false base stations could force the device to use A5/2 and retrieve a GSM cipher key Kc by breaking the algorithm. Due to a key recovery attack against a GEA1 capable mobile device, traffic encrypted by GEA3, A5/1 or A5/3 on such a device (using 64-bit cipher keys) can be decrypted and becomes a weak point that undermines the security of strong algorithms. Mobile devices using A5/4 (128-bit key length) are not vulnerable to these attacks.

Motivation: A common set of algorithms is necessary to allow interoperability in a secure manner.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-24/1.3

Req 25	For GPRS networks encryption algorithms according to the list below must be used.

- GEA0 MUST be forbidden by the network (see Req 23)
- GEA1 MUST be supported by the network (mobile device exception, see note below)
- GEA2 MUST be supported
- GEA3 MUST be supported and preferred to GEA2
- GEA4 MUST be supported and preferred to GEA3

At minimum, it must be possible to upgrade new network elements and mobile devices remotely without HW change to GEA3 and GEA4. GEA4 uses the same base algorithm as GEA3 (Kasumi), but uses 128-bit cipher key length (instead of 64-bit). GEA4 must be sufficiently tested before release. Reason to keep GEA4 disabled currently is that enabling of GEA4 in mobile devices without any test capabilities in mobile networks may lead to faulty implementations. When GEA4 will be ready to launch in mobile networks this would not be possible due to these interworking issues.

Note: GEA1 MUST NOT be supported by new mobile devices.
Due to a key recovery attack, released in April 2021, against a GEA1 capable mobile device, the mere presence of GEA1 on the device becomes a weak point that undermines the security of strong algorithms. This impacts the security of GSM calls and texts as well as GPRS sessions (only affects device-side implementations of GEA1). Mobile devices using GEA4 (128-bit key length) are not vulnerable to these attacks.

Motivation: A common set of algorithms is necessary to allow interoperability in a secure manner.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-25/1.3

4.2. Confidentiality Protection for UMTS

Req 26	UMTS networks must support and enforce confidentiality protection of traffic using UMTS Encryption Algorithm (UEA) 1 (Kasumi).

This requirement has several consequences:

- the network must exclude the NULL algorithm UEA0 from the list of allowed ciphering algorithms
- the network must enable ciphering using the Security Mode Command immediately after connection establishment
- mobile devices that do not support ciphering must be rejected

Ciphering of emergency calls depends on successful authentication (see [2] clause 6.4.9). NULL algorithm (UEA0) is only allowed to unauthenticated emergency calls.

Note: From Rel-7 onwards, the 3GPP standard [2], clause 6.6.6 also requires support of UEA2 (SNOW 3G) in networks and mobile devices.

Motivation: Certain services like SMS TAN rely on protected message transfer. Establishment of secure connections should not depend on mobile device capability alone.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-26/1.3

4.3. Confidentiality Protection for EPS

Req 27	LTE/EPC networks must enforce confidentiality protection of the User Plane, and NAS and RRC (AS) Signalling Plane.

This requirement has several consequences:

- the network must exclude the NULL algorithm EPS Encryption Algorithm (EEA) 0 from the list of allowed ciphering algorithms
- the network must enable ciphering using the Security Mode Command immediately after connection establishment for the respective traffic type
- mobile devices that do not support ciphering must be rejected

Ciphering of emergency calls depends on successful authentication (see [3] clause 15). NULL algorithm (EEA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, User Plane and AS security terminate in the eNodeB, NAS signalling security terminates in the MME. Therefore, both elements must be checked independently for compliance.

Motivation: Certain services rely on protected message transfer. Establishment of secure connections should not depend on mobile device capability alone.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-27/1.3

Req 28	LTE/EPC networks must support confidentiality protection algorithms EEA1 (SNOW 3G) and EEA2 (AES) for User Plane, and for NAS and RRC (AS) Signalling Plane.

The 3GPP standard [3] requires that both algorithms must be supported. This requirement emphasizes that both algorithms must always be supported, even if some vendors try to implement only one of them. Either of the algorithms can be used. EEA2 should be set as preferred algorithm in the network because it has been tested more extensively. The number of tests cases with EEA1 has been reduced in official conformance tests.

Ciphering of emergency calls depends on successful authentication (see [3] clause 15). NULL algorithm (EEA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, User Plane and AS security terminate in the eNodeB, NAS signalling security terminates in the MME. Therefore, both elements must be checked independently for compliance.

Reference: [3] 3GPP TS 33.401 – EPS Security Architecture, clause 5.1.3.2

Motivation: LTE/EPC was designed with two security algorithms from the start to allow quick migration in case one algorithm is broken. Unlike UMTS, but similar to GSM, the LTE security algorithms are implemented in the base stations and the MME. Having two algorithms supported in each base station avoids massive cost for HW swap in case of an algorithm change.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-28/1.3

4.4. Confidentiality Protection for 5GC

Req 29	5GC networks must enforce confidentiality protection of the User Plane, NAS and RRC (AS) Signalling Plane.

This requirement has several consequences:

- the network must exclude the NULL algorithm New Radio Encryption Algorithm (NEA) 0 from the list of allowed ciphering algorithms
- the network must enable ciphering using the Security Mode Command immediately after connection establishment for the respective traffic type
- mobile devices that do not support ciphering must be rejected

Ciphering of emergency calls depends on successful authentication (see [11] clause 10). NULL algorithm (NEA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, User Plane and AS security terminate in the ng-eNodeB/gNodeB, NAS signalling security terminates in the AMF. Therefore, both elements must be checked independently for compliance.

Reference: [11] 3GPP TS 33.501 – 5G Security Architecture, clause 5.2.2.

Motivation: Certain services rely on protected message transfer. Establishment of secure connections should not depend on mobile device capability alone.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-29/1.3

Req 30	5GC networks must support confidentiality protection algorithms NEA1 (SNOW 3G) and NEA2 (AES) for User Plane, and for NAS and RRC (AS) Signalling Plane.

The 3GPP standard [11], clause 5.2.2 requires that both algorithms must be supported. This requirement emphasizes that both algorithms must always be supported, even if some vendors try to implement only one of them. Either of the algorithms can be used. NEA2 should be set as preferred algorithm in the network because it has been tested more extensively. The number of tests cases with NEA1 has been reduced in official conformance tests.

Ciphering of emergency calls depends on successful authentication (see [11] clause 10). NULL algorithm (NEA0) is only allowed to unauthenticated emergency calls.

Note: On the network side, User Plane and AS security terminate in the ng-eNodeB/gNodeB, NAS signalling security terminates in the AMF. Therefore, both elements must be checked independently for compliance.

Motivation: 5GC was designed with two security algorithms from the start to allow quick migration in case one algorithm is broken. Unlike UMTS, but similar to GSM, the 5GC security algorithms are implemented in the base stations and the AMF. Having two algorithms supported in each base station avoids massive cost for HW swap in case of an algorithm change.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-30/1.3

4.5. General ciphering requirements

Req 31	Networks must support 128-bit cipher keys (Kc128) for GSM and GPRS.

At minimum, it must be possible to upgrade new network elements and mobile devices remotely without HW change to support Kc128.

Note: On the network side, Kc128 support impacts the Base Station Subsystem (BSS), MSC, and SGSN. 128-bit keys and algorithms can and have to co-exist with their 64-bit variants as long as some subscribers still hold legacy SIM cards because they can only provide 64-bit keys. A USIM is needed to provide 128-bit keys.

Reference: [2] 3GPP TS 33.102 – 3G Security Architecture, clause 6.8.1.1.

Motivation: Kc128 support is required to enable the A5/4 and GEA4 ciphering algorithms in order to prevent the key recovery attack against a GEA1.

For this requirement the following threats are relevant:
- Unauthorized access to the system
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Disruption of availability
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-31/1.3

5. Other security requirements for mobile networks

Req 32	BSS with GERAN radio must implement layer 2 fill bits randomisation in uplink and downlink.

The requirement was introduced in 3GPP Rel-9 as standard feature into [9], clause 5.2, but it must be implemented in any new mobile device and into existing BSS (the effort is small), independent of their 3GPP release.

Motivation: Motivation: This function removes known plaintext from 2G radio frames and makes cryptographic attacks more difficult

For this requirement the following threats are relevant:
- Unauthorized access or tapping of data
- Unauthorized modification of data
- Unauthorized use of services or resources
- Denial of executed activities
- Unnoticeable feasible attacks
- Attacks motivated and facilitated by information disclosure or visible security weaknesses

For this requirement the following warranty objectives are relevant:

ID: 3.38-32/1.3

6. References

No.	Title
[1]	3GPP TR 21.905 - Vocabulary for 3GPP Specifications
[2]	3GPP TS 33.102 – 3G Security Architecture, rel. 15
[3]	3GPP TS 33.401 – EPS Security Architecture, rel. 17
[4]	3GPP TS 33.234 – WLAN interworking security, rel. 13
[5]	3GPP TS 33.402 – EPS and security aspects of non-3GPP accesses, rel. 15
[6]	3GPP TS 24.008 – Mobile radio interface Layer 3 specification; Core network protocols, rel. 17
[7]	3GPP TS 22.101 – Service Principles, rel. 17
[8]	3GPP TS 31.102 – Universal Subscriber Identity Module (USIM) application, rel. 17
[9]	3GPP TS 44.006 – Mobile Station - Base Station System (MS - BSS) interface, data link layer, rel. 9
[10]	3GPP TS 43.020 – Security related network functions
[11]	3GPP TS 33.501 – 5G Security Architecture, rel. 17
[12]	3GPP TS 23.003 – Numbering, addressing and identification, rel. 17
[13]	DT Technik GmbH – VoLTE 1.5 Emergency Call Solution Design

All 3GPP specifications can be downloaded at http://www.3gpp.org/ftp/Specs/latest/
Reference [13] can be downloaded at yam-united__VoLTE_1.5_emergency-call

7. Annex: A5/1 attack countermeasures

In recent years there have been several reports on practicability of attacks against GSM networks, and proof of concept attacks are quite advanced.
The attack consists of three main parts: capturing the radio signals, finding the target in the captured traffic, and finding the cipher key to decrypt the target's messages. While the long-term countermeasure is migration of networks and terminals to the stronger A5/3 ciphering algorithm, there are other countermeasures that should be taken as long as A5/1 must still be supported. They can prevent any of the attack steps, or at least make them more difficult, or they limit the effectiveness of the attack.

- More **frequent authentication** (see Req 2) reduces the usefulness of the attack. Every authentication run generates a new key, so that previously broken keys would become useless to an attacker who would have to try the key search process again. This will, however, increase average call setup time and HLR load.
- **Randomising the padding** bits (Req 32) will reduce known plaintext from radio frames and make the attack more difficult.
- A similar effect can be achieved by **requesting terminals to send their IMEISV** in the Cipher Mode Complete message. This is a standardised feature, which will also make contents of the message less predictable.
- More **frequent reallocation of the TMSI** (Req 13, Req 14, Req 15) will make finding and tracking specific targets more difficult.
- An optimised use of **frequency hopping** (both baseband and synthesized) will make it more difficult for an attacker to capture radio signals and crack a target's key.

More detailed information can be provided on request.

For example, a table showing two sample configurations for re-authentication parameters in NSN Rel-4 MSC. One set of values is the default with a good compromise between security and call setup latency/network load. The second set of values is for networks with evidence that attacks are performed. The values for this case are tuned to ensure maximum billing integrity.