Reinforced access stratum security for 6G

White paper

Mobile networks are essential for fostering inclusive and sustainable global economic growth. Achieving this requires networks that are trustworthy, secure, and resilient. Network security is achieved through a comprehensive approach that begins with research and standardization. Nokia is a strong advocate of open and global security standards as this adheres to the confidence in the reliability of the specified security features. For many years, Nokia has been at the forefront of researching and standardizing innovative, secure and resilient algorithms and protocols. As of now, security standardization for 5G has reached a high level of maturity, and research on 6G security is already underway. Building upon the robust foundation established by advanced 5G security features, 6G security will harness the advancements from ongoing pre-standardization efforts in quantum-safe networks, including Post Quantum Cryptography (PQC), privacy-enhancing technologies, zero trust and cloud-native architectures, secure API exposure, security for AI, and AI for security.

The ongoing research in 6G security is closely intertwined with the development of 6G systems and architectures, emphasizing a 'secure by design' approach. These developments also encompass lower-layer security considerations detailed in this paper. This integrated approach ensures that 6G networks will embody state-of-the-art security principles. At Nokia, we have been working on how to ensure native security for medium access control layer in 6G. LTE/4G and 5G have put encryption and integrity protection for the radio interface into the upper part of the layer two (L2) radio protocol stack, leaving lower layers such as the medium access control (MAC) layer without cryptographic protection due to the perceived low risk of applicable threats at the time. Attacks against the unprotected lower layers, however, have been figured out by security researchers over the years. It is imperative to ensure protection of the lower layer control procedures such as MAC control elements (CEs).

Contents

Introduction

Cryptographic protection of traffic on the radio interface is one of the most important security requirements for mobile networks. Securing user plane (UP) traffic protects the content of the data (i.e., it is more difficult to attack the content), and securing control plane (CP) traffic protects the integrity of operational procedures and metadata (i.e., it is more difficult to eavesdrop or harm maintenance of the traffic). 2G/GSM specified the use of encryption as an essential mechanism to ensure the confidentiality of the user traffic, which was voice at that time. Encryption was also specified for GPRS.

With 3G/UMTS, mutual authentication between user equipment (UE) and network was introduced, and building on that, integrity protection for signalling traffic. This is essential to prevent attackers from impersonating subscribers or, more impactful, impersonating the network itself.

With 4G, separate security associations were introduced for the access stratum (AS), which covers the radio interface between UE and base station, and the non-access stratum (NAS), which covers the signalling between UE and core network. This ensures that the highly sensitive NAS signalling is safe even in case the base station has been successfully compromised by attackers.

These sound security principles were maintained in 5G. It brought additional security enhancements, in particular, for the protection of the subscriber identity and the secure interworking of different mobile networks in the support of roaming. However, this paper focuses only on reinforced AS security design.

In 4G and 5G, encryption and integrity protection for the signalling traffic on the radio interface is specified. It is performed in a protocol layer in the upper part of the radio protocol stack, the Packet Data Convergence Protocol (PDCP), thus avoiding the need to do crypto processing under the stringent real-time requirements applying to the lower layers. Consequently, lower layers such as the MAC layer are not cryptographically protected.

At that time, the risk of attacks against the lower layers was considered low. Over the years, however, more and more impactful attacks against the unprotected lower layers have been figured out by security researchers. As we have discussed in the white paper "A novel approach to radio protocols design for 6G" [1], it is envisioned that the MAC layer will solely handle more control procedures in 6G. And because superior security and trustworthiness are key values of 6G, MAC-level security will be imperative as 6G networks become available from 2030 onwards [2] and are expected to be available for a long time.

In the following, we give a more detailed descriptions of today's AS security mechanisms. We show how the lack of protection at the MAC layer could be exploited by attackers, and we propose a solution that extends AS security to the MAC layer.

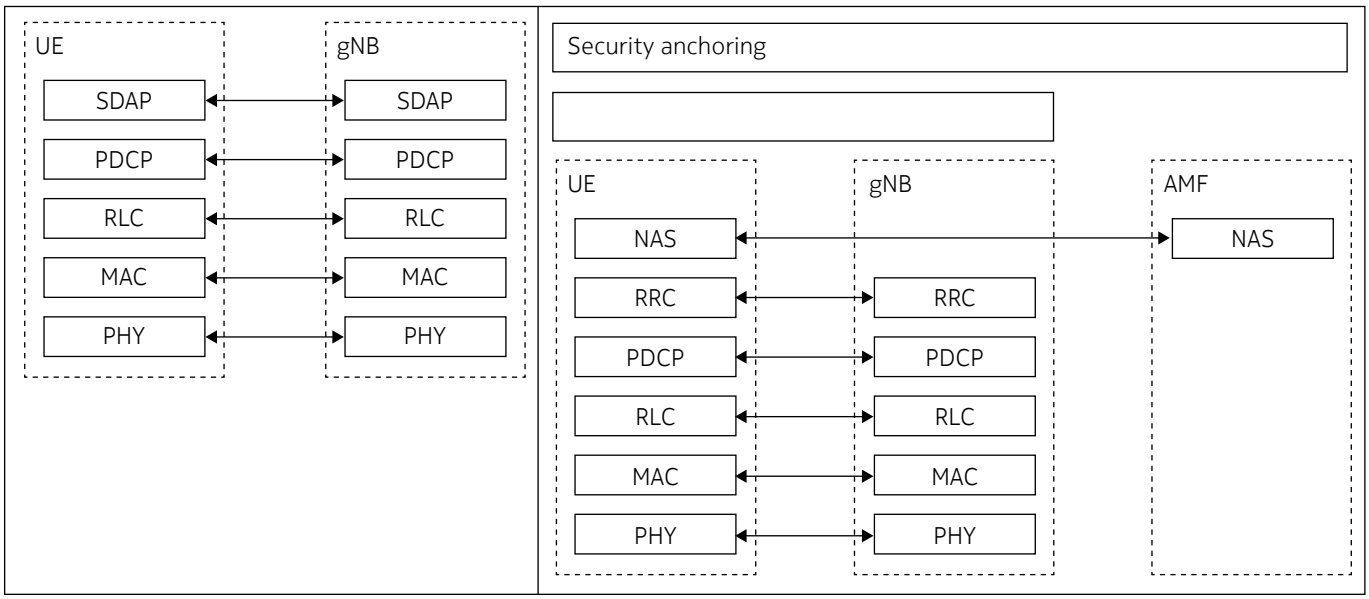
Security for 6G

AS security principles in 5G

AS security mechanisms as specified by 3GPP in 5G provide sound cryptographic protection of CP and UP traffic between UE and base station (i.e., the gNB, as the base station is called in 5G). AS security is independent of the way authentication and key agreement between UE and network are executed and the way the NAS is secured. For establishing AS security, the gNB receives the UE's security capabilities (i.e., the crypto algorithms the UE supports) and a key K_{gNB} from the core network. The gNB selects the crypto algorithms to be used, applies a key derivation function to derive from K_{gNB} four different keys to encrypt/integrity protect the CP and the UP, and triggers activation of AS security by sending the Radio Resource Control (RRC) protocol message SecurityModeCommand (SMC), which informs the UE about the selected algorithms and the activation of security. The UE independently derives the same keys as the gNB and replies with the RRC message SecurityModeComplete. This establishes security for the SRB1 (the Signalling Radio Bearer 1 that is used for exchanging RRC messages), thus all subsequent RRC messages are protected. All other radio bearers are subsequently taken into use with protection enabled. Note that use of protection is not mandated for data radio bearers, and, in particular, integrity protection may not be applied, so as to reduce the computational effort at both the UE and the gNB.

AS security is maintained in all AS mobility procedures, in particular handover, connection re-establishment, suspend-resume, or secondary gNB addition. Figure 1 shows the radio protocol stack for the UP (left) and CP (right). UP packets such as IP packets are encapsulated in Service Data Access Protocol (SDAP) packets, which in turn are passed to the Packet Data Convergence Protocol (PDCP) layer. In the CP, NAS messages (carrying signalling between the UE and the access and mobility management function (AMF) in the core network) are encapsulated within RRC messages and are passed to the PDCP layer. For both UP and CP, the PDCP performs the encryption and integrity protection as needed and passes the protected PDCP protocol data unit (PDU) to the lower layers. On the receiving side, the lower layers pass PDCP PDUs to the PDCP layer, which performs decryption and verifies integrity before passing the PDCP payload to the higher layers.

Figure 1. Radio interface protocol stacks: UP (left) and CP (right)

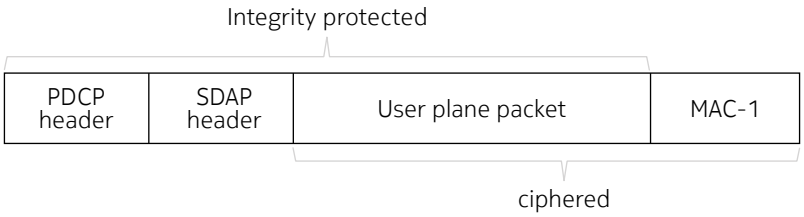


PDCP security

For each radio bearer in the UE and gNB, there is a dedicated PDCP entity that is configured to apply integrity protection, encryption, or both. In case of SRB1, the PDCP entity starts without protection, and during the SMC procedure, the PDCP entity is reconfigured to apply protection. PDCP entities for the other radio bearers are instantiated with configurable protection. In the PDCP packets themselves, there is no indication whether encryption has been applied—the receiving PDCP entity must be properly configured to apply decryption or not.

The PDCP PDU with protection comprises a header with the sequence number, a payload (the SDU) and the message authorization code for integrity (MAC-I). Integrity protection covers the PDCP header and the PDCP payload. Integrity protection is applied first, and subsequently the PDCP payload and the MAC-I are ciphered. The SDAP protocol layer is, however, exempt from ciphering, i.e., SDAP headers and SDAP control PDUs are not ciphered. The PDCP also uses control packets that do not carry higher layer payloads; these are transmitted without protection. The protected PDCP PDU is visualized in Figure 2.

Figure 2. Protected PDCP PDU carrying a UP packet



Three crypto algorithm pairs (each pair consisting of an encryption algorithm and an integrity protection algorithm) are specified, based on SNOW3G, AES, and ZUC ciphers. Encryption operates in all three cases in stream cipher mode, i.e., a cipherstream is generated for each message (i.e., RRC message or UP packet) and then XORed with the message, resulting in the encrypted message. The receiving PDCP entity generates the same cipherstream and XORs the encrypted message with the cipherstream, resulting in the original message.

It is an essential security requirement that each cipherstream is different from any other cipherstream generated with the same key. Unique input is thus required for the generation of each cipherstream, which is composed of the message counter maintained by the PDCP entity, a unique ID of the respective radio bearer, and a direction bit (different for uplink and downlink). Integrity protection involves the sending PDCP entity walking through the message and using all its content to compute a MAC-I, and the receiving PDCP entity doing the same and verifying that the computed MAC-I equals the MAC-I received from the sender for this message. 3GPP Release 19 will aim to have 256-bit confidentiality and integrity algorithms for the air interface and introduce authenticated encryption with associated data (AEAD) mode, as discussed in the Nokia Bell Labs white paper "Security and trust in the 6G era" [3].

Absence of security on the MAC layer

On the MAC layer, control information can be exchanged over the radio interface using so called MAC control elements (CEs). This way, lower layer control tasks can be performed quickly without the involvement of higher layer signalling like the RRC or entities further up in the network like the CU.

4G put encryption and integrity protection on the PDCP layer. The 3GPP Technical Report TR 33.821 [4] describes the "Rationale and track of security decisions in LTE/SAE" and considers the threat of attacks against the lower layers. For example, the threat to falsify or forge a MAC layer buffer status report (BSR) message is recognized. It is suggested that this attack is difficult to mount and only limited denial of service (DoS) can be achieved, with no severe impact. In general, providing encryption for the MAC layer is considered, but it is concluded that this is not required.

This decision may have been reasonable at the time the 4G security architecture was designed. In hindsight, sticking to this decision and design in 5G could be questioned, as in the meantime, more and more security research work has been published disclosing meaningful attacks against the lower layer control communications. Further, quantum computing may pose more threats than were foreseen earlier, which illustrates that security aspects will need to evolve in 6G, as discussed in [3].

As a simple example, the timing advance information conveyed in one MAC CE allows attackers to determine the distance of a victim UE to the base station, and this can be combined with further attack techniques to exactly localize the UE within a cell. On the sophisticated end of the attack spectrum, an attack has been described that observes the MAC CEs containing the "activation bitmap" indicating the cells to be used in a carrier aggregation configuration. Although the transmitted carrier aggregation configuration is encrypted and not known to the attackers, it was possible to identify walking paths taken by victim subscribers on a campus with a certain accuracy solely based on monitoring the cell activation MAC CEs. This second example shows that a quite surprising amount of relevant information may be drawn from seemingly unsensitive information in MAC CEs. This calls for preventative security and should be a warning against forgoing protection in cases where information appears not sensitive, and no obvious ways to exploit the information are (yet) known.

Currently we do not assume that the overall commercial operation of 5G networks is seriously endangered by not protecting the lower layers of the 5G radio protocol stack. However, attacks tend to become more impactful, and attack tools become more available and convenient to use. Moreover, 6G is envisioned to carry ever more communication for critical services such as infrastructure, so if 6G is envisioned to handle more control procedures such as cell changes by the MAC layer, potential attacks could become more impactful. Therefore, it is imperative that 6G includes mechanisms for strong protection of MAC CEs to reinforce the overall 6G security.

Mechanisms of the physical layer contributing to security

Exploiting the lack of protection on the MAC layer requires attackers or, respectively, their tools, to take into account the physical layer mechanisms. These mechanisms do not comprise cryptographic protection, but some of them still can pose an obstacle to attackers, as discussed in the following.

The MAC layer passes each MAC PDU, which may comprise MAC CEs as well as higher layer PDUs, as a so-called "transport block" to the physical layer. Several operations are applied to the transport block before transmission over the air. In particular, bits containing a cyclic redundancy check (CRC) are appended, where for certain physical channels, namely the physical downlink control channel (PDCCH), the UE's temporary cell level identifier, called C-RNTI (Cell Radio Network Temporary Identifier), is among the inputs to the computation of the CRC. A CRC is unlike a MAC-I; it does not provide protection against

targeted attacks that try to modify the content of a message, or insert faked messages, because it can be computed without knowledge of a secret key.

Furthermore, the transport block is scrambled by XORing it with a scrambling sequence, where the C-RNTI may be used as one of the inputs to generate the scrambling sequence. The C-RNTI of a UE cannot easily be protected against being uncovered by attackers, so it cannot prevent attackers from generating the correct descrambling sequence. Other input to generate the scrambling sequence is also not secret but available to attackers. There is one exception: in 5G NR, a 16-bit "scrambling ID" is among the inputs, and the network could select this parameter individually and unpredictably for each UE and transmit it to the UE in an encrypted RRC message. This way, attackers would face an obstacle in creating the right descrambling sequence. However, it must be noted that scrambling with a secret 16-bit scrambling ID must not be mistaken for encryption. Encryption would require a significantly longer key as well as the creation of a cryptographically strong random sequence instead of a scrambling sequence and using a different random sequence for every message protected with the same key.

Improved MAC security in 6G

While the detailed protocol stack structure for 6G is still under discussion and expected to have some differences with 5G (see [1]), we assume that in addition to the RRC protocol, lower layer control messages such as MAC CEs today will still exist in 6G. For ease of understanding, we use the current names RRC and MAC for these two different layers. Obviously, RRC messages will need protection, which is already provided today, but, as argued above, we also aim to protect MAC CEs.

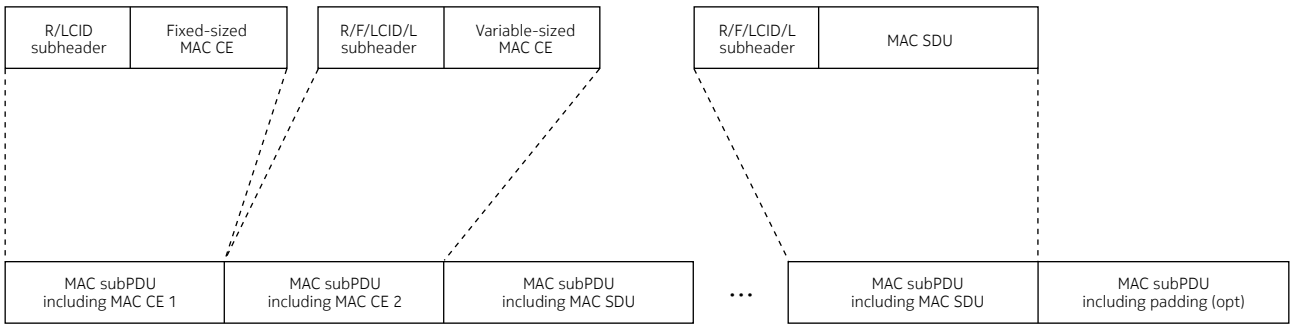
When aiming for a solution that requires only limited changes to the current approach, one may think of re-using protection mechanisms as today for RRC and adding cryptographic protection on the MAC layer for the MAC CEs, or at least for those MAC CEs that are sensitive. In an alternative approach, cryptographic protection of the CP could be moved from the PDCP layer down to the MAC layer, so MAC CEs and all PDUs of higher layers in the CP stack, up to RRC, are cryptographically protected by the MAC layer.

Note that these considerations do not involve the UP. Today, UP packets can be fully protected by the PDCP, and we see no specific threat in using unprotected lower layer headers. In 6G, this approach might be adopted, or alternatively, new approaches may be taken for UP security. So, it is favourable to avoid tying together 6G CP and UP security mechanisms at this time, thus not narrowing down the options for a potential evolution of UP security in 6G.

Today, a MAC PDU—the protocol data unit exchanged between the MAC layers of sender and receiver—may consists of several MAC subPDUs, each of which either carries a MAC CE or a MAC SDU holding a higher layer PDU. Such a higher layer PDU may include an RRC message, encapsulated into a PDCP PDU, which is in turn encapsulated into a radio link control (RLC) PDU or a UP packet (also encapsulated in the PDUs of the applicable protocol layers).

Figure 3 below is taken from 3GPP Technical Specification TS 38.321 [5] and shows an example of the MAC PDU structure for 5G, illustrating how a MAC PDU is constructed.

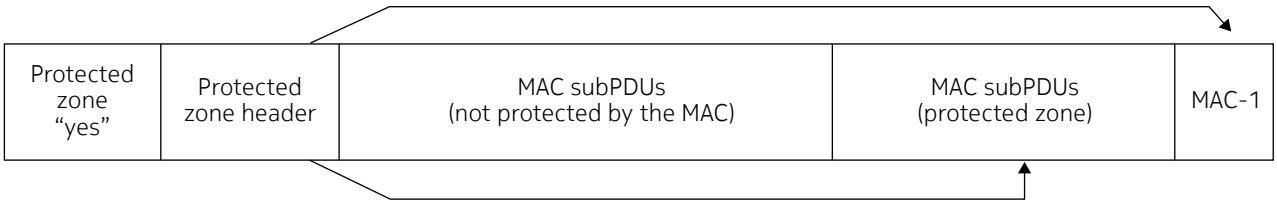
Figure 3. MAC PDU structure in 5G [5]



MAC CEs are typically put into one block ("MAC subPDU") within the MAC PDU, at the beginning (if it is a downlink PDU) or at the end (if it is an uplink PDU). So cryptographical protection could be applied to exactly this part. Generalizing this idea somewhat, each MAC PDU may include what we call a "protected zone". A header field would be added to the MAC PDU, with an indication of whether a protected zone is contained in this PDU, and, if so, additional header fields would indicate the location and size of it. Moreover, a counter would be included providing a unique value to be used as part of an initialization vector for the crypto algorithms. Finally, a field allowing the transmission of a MAC-I would be added.

Figure 4 gives an example of the format of the MAC PDU supporting a protected zone (other choices for the format are obviously possible):

Figure 4. Example structure of a MAC PDU with protected zone

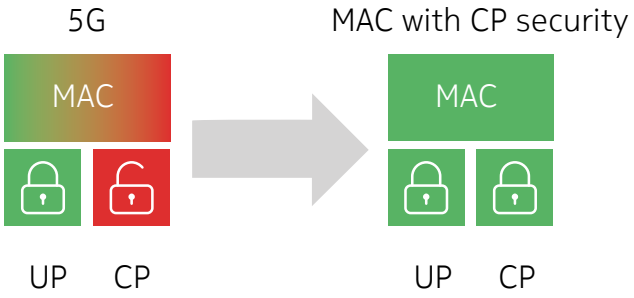


With this, the solid cryptographic principles taken in the PDCP today can be adopted for the protection provided in the MAC layer. The same algorithms can be used as in the PDCP, where the counter and a direction bit can provide unique input for generating the cipherstream. Keys for encryption and integrity protection can be derived from the KgNB in the same way as the keys used by the PDCP today, simply defining additional constants as input into the key derivation function. The approach is also open for future evolution of cryptographic algorithms (as studied by 3GPP for 5G Advanced), e.g., 256bit algorithms. As well, authenticated encryption providing encryption as well as integrity protection in a single algorithm can be adopted. UE security capabilities with respect to MAC layer security can be specified, allowing network and UE to flexibly negotiate the algorithms to be used in a session.

This approach is flexible concerning what information is protected on the MAC layer, i.e., what is put into the protected zone. For example, not all MAC CEs may be considered sensitive, and only sensitive ones would be transmitted in a protected zone. On the other hand, this approach also allows transmission of MAC subPDUs containing RRC messages within protected zones of MAC PDUs, thus shifting the CP protection from PDCP down to the MAC layer.

It should be noted that most MAC PDUs may contain only MAC subPDUs carrying UP traffic. All these PDUs would not be affected by the proposed MAC layer protection and would not burden the MAC layer with additional operations compared to today. This is advantageous, as the MAC layer operation is subject to real-time requirements. For example, receiving a certain piece of information in a certain timeslot may trigger a specific reaction due in a specified subsequent timeslot. To enable the MAC layer to perform the operations for encryption and integrity protection clearly requires adequate computing resources to be available to the MAC layer. Restricting MAC layer protection to the CP, or even to sensitive MAC CEs only, limits the additional compute burden making MAC real-time requirements more easily achievable while still improving the security. This would allow future MAC security to be further reinforced compared to the 5G MAC security, as illustrated in a simplified fashion in Figure 5.

Figure 5. Simplified illustration of MAC with further reinforced security



Conclusion

As 6G will evolve over a long time, the security threats faced will also evolve (e.g., quantum computing threats as discussed in [3]). The means to protect radio communication over the 6G air interface will, therefore, also have to evolve. Not protecting the lower layers of the radio protocol stack, in particular MAC control elements, would leave a security gap. Even though the gap is probably not yet actively exploited in today's 4G and 5G networks, it would be prudent to close it to achieve the superior security and trustworthiness goals of 6G. The solutions detailed in this white paper leverage the sound cryptographical procedures specified in 5G for protecting not only higher layer signalling, but also the sensitive control communication on the MAC layer. Adopting this solution in future 6G security standards would improve the security of the air interface, which can reinforce the overall system security and ensure critical communications are secured.

References

1. Nokia, “A novel approach to radio protocols design in 6G,” Nokia white paper, 2023. Online: https://onestore.nokia.com/asset/213456
2. Bertenyi, B., “6G standardization is beginning: here’s why you should care,” Nokia blog post, Mar 2024. Online: https://www.nokia.com/about-us/newsroom/articles/6g-standardization-is-beginning-heres-why-you-should-care/
3. Kanugovi, S., Montag, M., Viswanathan, H. and Ziegler, V., “Security and trust in the 6G era,” Nokia Bell Labs white paper, Aug 2021. Online: https://www.bell-labs.com/institute/white-papers/security-and-trust-6g-era/
4. 3GPP, “TR33.821: Rationale and track of security decisions in Long Term Evolution (LTE) RAN / 3GPP System Architecture Evolution (SAE),” 3GPP Technical Report, Version 9, 2009. Online: https://www.3gpp.org/ftp/Specs/archive/33_series/33.821/33821-900.zip
5. 3GPP, “TR38.321: NR; Medium Access Control (MAC) protocol specification,” 3GPP Technical Report, Rel. 18.1, Apr 2024. Online: https://www.3gpp.org/ftp/Specs/archive/38_series/38.321/38321-i10.zip

Abbreviations

AEAD	Authenticated Encryption with Associated Data
AES	Advanced Encryption Standard
AMF	Access & Mobility Management Function
AS	Access Stratum
BSR	Buffer Status Report
CA	Carrier Aggregation
CE	Control Element
CP	Control Plane
CRC	Cyclic Redundancy Check
C-RNTI	Cell Radio Network Temporary Identifier
DC	Dual Connectivity
DoS	Denial of Service
DRB	Data Radio Bearer
gNB	5G Node-B
GPRS	GSM Packet Radio System
IP	Internet Protocol
L2	Layer Two (OSI model)
LTE	Long Term Evolution (4G)
MAC	Medium Access Control

MAC-I	Message Authorization Code for Integrity
NAS	Non-Access Stratum
PDCCH	Physical Downlink Control Channel
PDCP	Packet Data Convergence Protocol
PDSCH	Physical Downlink Shared Channel
PDU	Protocol Data Unit
PHY	Physical Layer
RLC	Radio Link Control
RRC	Radio Resource Control
SDAP	Service Data Adaptation Protocol
SDU	Service Data Unit
SMC	Security Mode Command
SNOW3G	Not an abbreviation, but the name of a member of the family of SNOW stream cipher algorithms
SRB	Signalling Radio Bearer
UE	User Equipment
UP	User Plane
XOR	eXclusive OR
ZUC	A stream cipher algorithm named after Zu Chongzhi (fifth-century Chinese mathematician)

Nokia OYJ
Karakaari 7
02610 Espoo
Finland
Tel. +358 (0) 10 44 88 000

Document code: CID214078 (August)