

5G mobile radio network security challenges and opportunities

3GPP compliant zero trust security

NOKIA



Wireless communication is inherently vulnerable and needs specific protection against interception and tampering. To secure user communication, encryption has been used on the radio interface ever since GSM — the second generation of mobile networks.

The security architecture was significantly enhanced in the following two generations of mobile networks, UMTS (3G) and LTE (4G). The industry has not encountered any major flaws in LTE security concepts since they were specified 10 years ago.

We are now in the era of a new mobile network generation, 5G, and the question that arises is: Are new security concepts required? The answer is yes. In this White Paper, we will focus on 5G security enhancements.



Visit Nokia Threat Intelligence Center

5G security drivers

While LTE was designed primarily to support the mobile broadband use case, that is enabling broadband access to the Internet, 5G targets in addition a variety of advanced use cases with a wide range of specific requirements.

These include support for a massive density of mobile devices or the need for ultra-low latency communications. New use cases, such as vehicular traffic control or industrial automation, place the highest demands on the reliability of the network.

With some of the use cases that 5G enables, human safety and even human lives can depend on the availability and integrity of the network service.

To support each use case in a comprehensive way, security concepts will also need to be more flexible and adapt to the requirements. For example, security mechanisms used for ultra-low latency, mission-critical applications may not be suitable for massive Internet of Things (IoT) deployments where mobile devices are inexpensive sensors that consume a very small amount of energy and transmit data only occasionally.

Other 5G security drivers include the emergence of new types of cyber attacks and threats. This White Paper does not describe such threats in more detail.

Nokia Threat Intelligence Center develops detection rules for malware infections in mobile networks, and publishes related security notes and research papers.



5G security standardization

The 3rd Generation Partnership Project (3GPP) is a consortium of standards bodies that develop protocols for mobile telecommunications. It is the main standardization organization for 5G mobile networks and has in the past specified UMTS and LTE. In the context of 3GPP, release studies are being carried out on all important aspects in different specification groups, particularly in the Radio Access Network (RAN) and Service and System Aspects (SA) groups. This work is captured in various technical reports.

For 5G, 3GPP has specified a comprehensive set of potential requirements, including security, for what it calls the “next generation system”. As 5G is an evolution of the 4G systems, its security architecture is designed to integrate 4G equivalent security, while the reassessment of other security threats has led to further security enhancements.

In 3GPP, the technical specification group SA3 concentrates on security work. The group is currently responsible for defining requirements for 5G security and privacy as well as specifying the related technology architecture and protocols, including which cryptographic algorithms to use and how.

The group has discussed numerous contributions on next generation security. Its recent study captures key issues of different security areas, including architectural aspects, authentication, security context and key management, as well as subscriber privacy and network slicing security. Solutions proposed for a variety of key security issues have also been captured.

5G is immune to identity thefts



Legacy radio technologies allowed transmission of plain text mobile subscriber identity (IMSI). In 5G, the new encrypted Subscriber Concealed Identifier (SUCI) makes connections more secure and immune to IMSI catching.

Nokia zero trust architecture and procedures

There is no such thing as a perfectly secure system. There are many ways how attackers may try to compromise a communication network that stores valuable, constantly updated data, so it is important to identify and address the various threats that can impact the network at any stage of the communication chain.

Nokia zero trust is a strategic and holistic approach to cyber security that secures an organization by reducing the need to rely on trust – which means that it continuously validates every stage of a digital interaction, addressing all threats.

The Nokia zero trust architecture is based on 3GPP standardized identification, authentication, ciphering and integrity protection and covers all mobile radio access network elements.

For end-to-end security, Nokia offers a comprehensive, real-time security operations and security monitoring management system, which covers radio access, transport and core network domains.

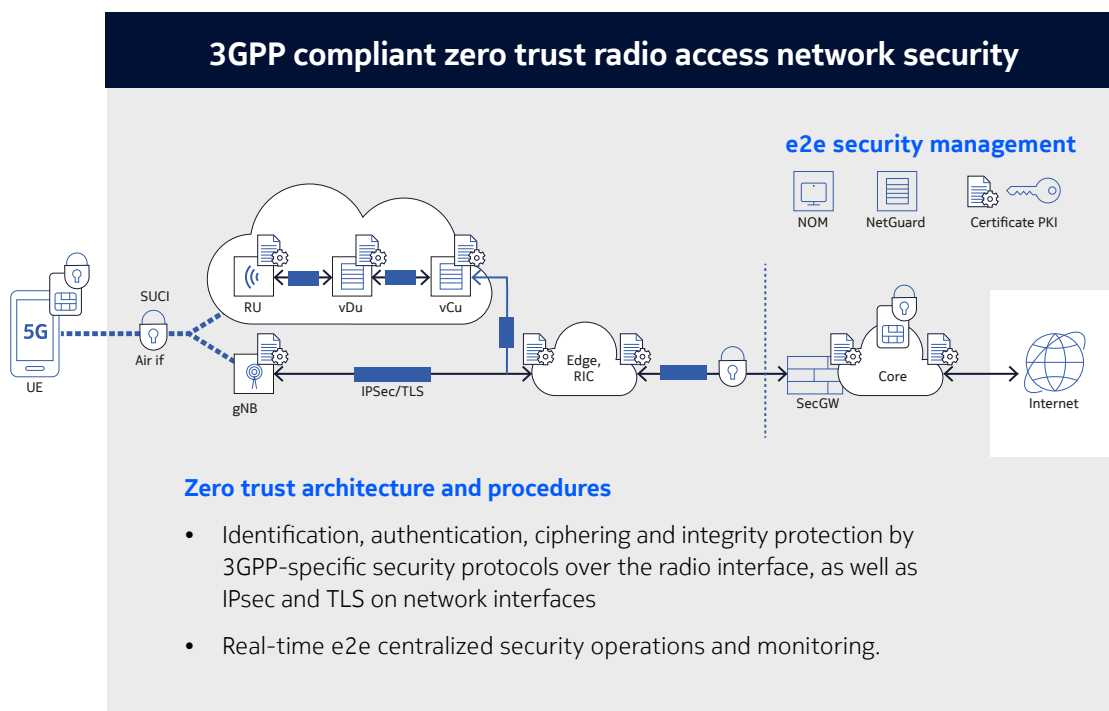


Figure 3. Nokia 5G radio access zero trust architecture and procedures

Value of Nokia zero trust 5G security

5G network operators need a robust and comprehensive security architecture and processes that encompass all traffic across signaling, data and application layers. The unique Nokia 5G zero trust architecture provides the following key benefits:

- Zero trust robust architecture and procedures against advanced threats and attacks, based on 3GPP standards
- Enables shift from reactive to proactive security measures with centralized end-to-end security management system for radio access, transport and core networks
- Reduces mean time to analysis, detection and resolution with real-time security operations and monitoring, which minimizes average cost of data breaches
- Ensures compliance with regulatory or country-specific legislation, reducing risk for possible penalties.

Conclusion



The evolution of mobile communication networks to support advanced use cases has opened the door for new types of cyber threats.

Investing in 5G security proactively helps avoid unexpected costs that arise when reactively countering attacks or when insufficiently protected high-value data becomes compromised.

The zero trust approach to 5G security architecture design and procedures aims to protect subscribers, devices and their communications, as well as the integrity of the network itself in all use case scenarios.

Abbreviations

3GPP	Third Generation Partnership Project
GSM	Global System for Telecommunications (2G)
IMSI	International Mobile Subscriber Identity
LTE	Long Term Evolution (4G)
PKI	Public Key Infrastructure
RAN	Radio Access Network
SUCI	Subscription Concealed Identifier
UMTS	Universal Mobile Telephone System (3G)

References

1. 3GPP TR 22.261, "Service requirements for next generation new services and markets", (work in progress). Available at <http://www.3gpp.org/DynaReport/22261.htm>
2. 3GPP TR 22.861, "Feasibility Study on New Services and Markets Technology Enablers – Network Operation". Available at <http://www.3gpp.org/DynaReport/22861.htm>
3. 3GPP TR 23.799, "Study on Architecture for Next Generation System", (work in progress). Available at <http://www.3gpp.org/DynaReport/23799.htm>
4. 3GPP TR 33.821: "Rationale and track of security decisions in Long Term Evolved (LTE) RAN/ 3GPP System Architecture Evolution (SAE)". Available at http://www.3gpp.org/ftp/Specs/archive/33_series/33.821/33821-900.zip
5. 3GPP TR33.899, "Study on the security aspects of the next generation system", (work in progress). Available at <http://www.3gpp.org/DynaReport/33899.htm>



Visit Nokia Cyber security page to find out more about our end-to-end security solutions

Nokia OYJ
Karakaari 7
02610 Espoo
Finland

Tel. +358 (0) 10 44 88 000

CID: 212519

nokia.com

NOKIA

At Nokia, we create technology that helps the world act together.

As a B2B technology innovation leader, we are pioneering the future where networks meet cloud to realize the full potential of digital in every industry.

Through networks that sense, think and act, we work with our customers and partners to create the digital services and applications of the future.

Nokia is a registered trademark of Nokia Corporation. Other product and company names mentioned herein may be trademarks or trade names of their respective owners.

© 20XX Nokia