Security Issues in RAN and possible solutions

Jagdeep Walia

Network Solutions, Ericsson

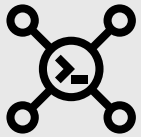
Why has security become important?

Dependency on mobile networks

Large part of the society use these networks for most aspects of their lives and businesses

Critical infrastructure

Regulatory requirements



New deployment scenarios and use-cases

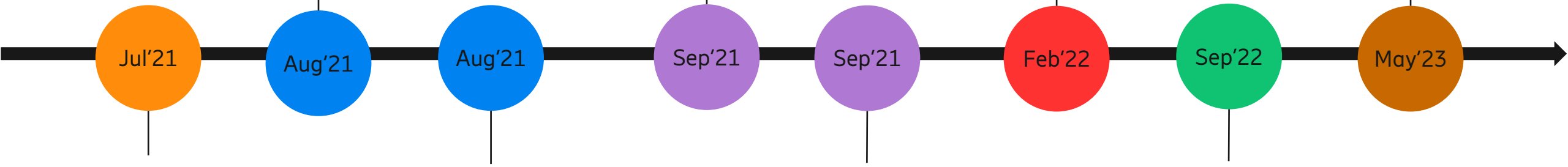
Traditional, centralized, distributed, hybrid types of deployments

New attack vectors

Ever-changing threat landscape

More advanced hackers, constant increase of cyber-attacks in public networks

Recent major Telco incidents



CNT

Ecuador's state-owned Corporacion Nacional de Telecomunicaciones (CNT) suffers from a ransomware attack that disrupts business operations, the payment portal, and customer support.

T-Mobile USA

T-Mobile discloses a data breach resulting in the loss of personal details for more than 50 million people. By exploiting an unprotected and exposed router, the threat actor managed to get access to information such as customer names, Social Security numbers and birth dates.

VoIP Unlimited

UK-based VoIP Unlimited suffers from a sophisticated DDoS attack attached to a large ransom demand, causing intermittent or total loss of internet connectivity services. Other UK telcos were also targeted in the ransomware DDoS-campaign, allegedly conducted by Revil.

Syniverse

US telecommunications company Syniverse reveals as intrusion, potentially going on for 5 years in their networks. Even if the investigation did not find any evidence, the company does not exclude the possibility of data exfiltration.

Roshan

Recorded Future's Insikt Group reveals that suspected Chinese-state sponsored threat actors have been exfiltrating gigabytes of data from the corporate mail server of major Afghan telecom provider Roshan over the past year.

Vodafone, Portugal

Vodafone Portugal was a target by cyberattack that caused network-wide damage and disruption. The threat actor intentionally destructed network functions, including redundant systems. Services were unavailable for 4-5 days.

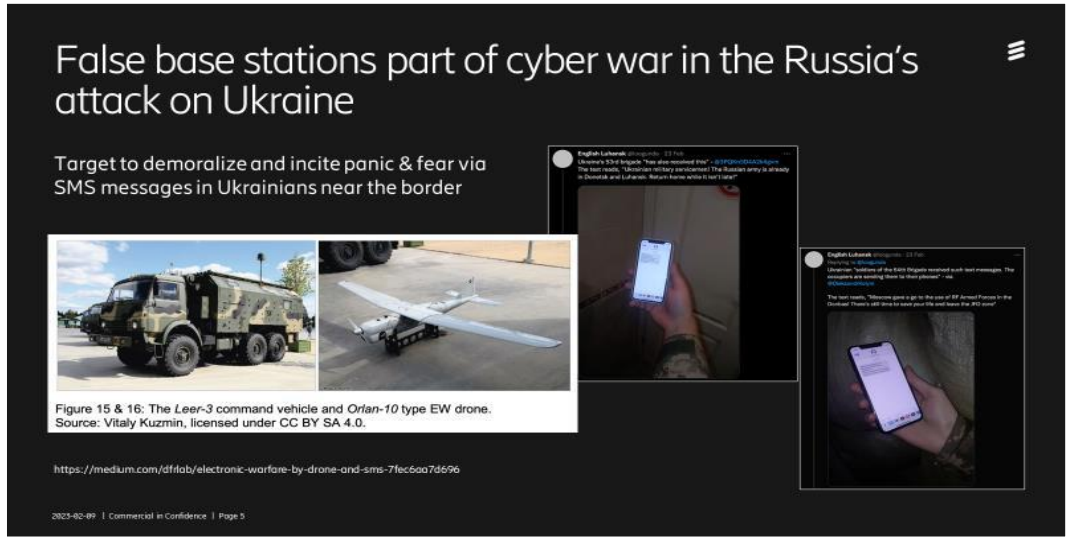
Optus

Optus disclosed a data breach resulting the unauthorized access of current and former customers' information. By exploiting an BSS API vulnerability, the threat actor managed to get access to information such as customer names, Social Security numbers and birth dates, passport pictures, drivers license, etc.

T-Mobile, USA

T-Mobile disclosed the second data breach of 2023 after discovering that attackers had access to the personal information of hundreds of customers for more than a month, starting late February 2023.

Examples of mobile network air interface attacks

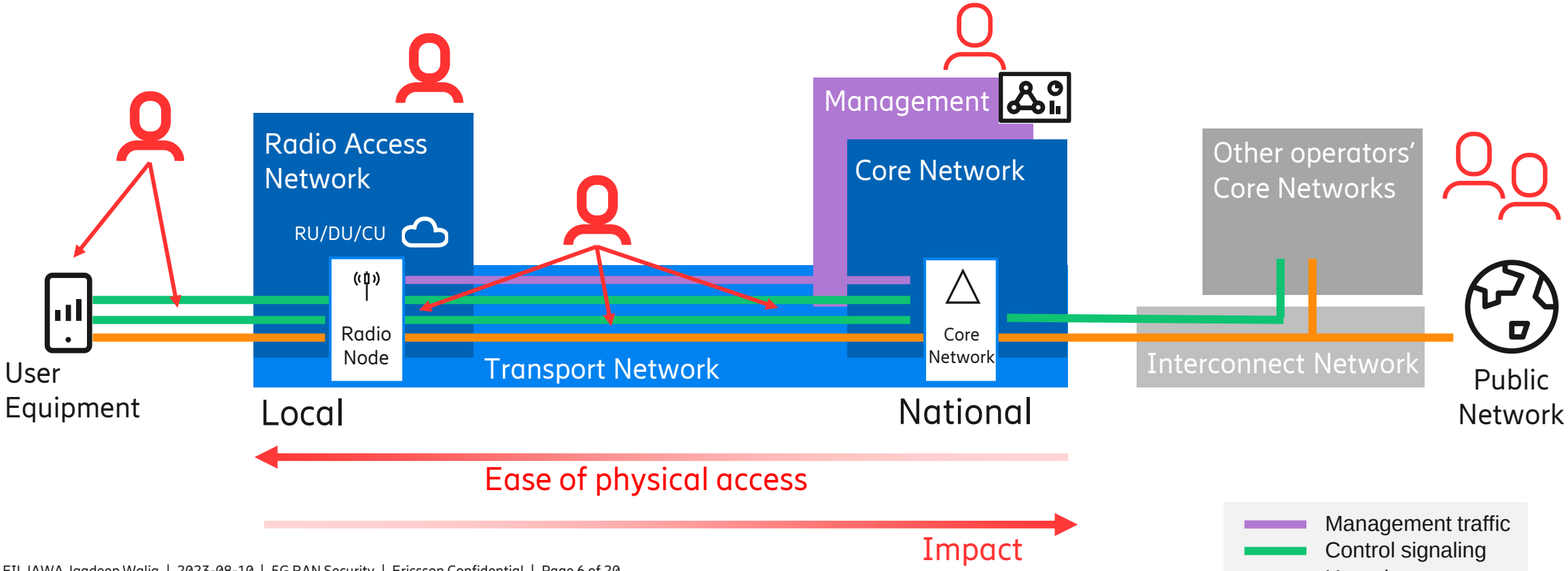


Access networks are at risk

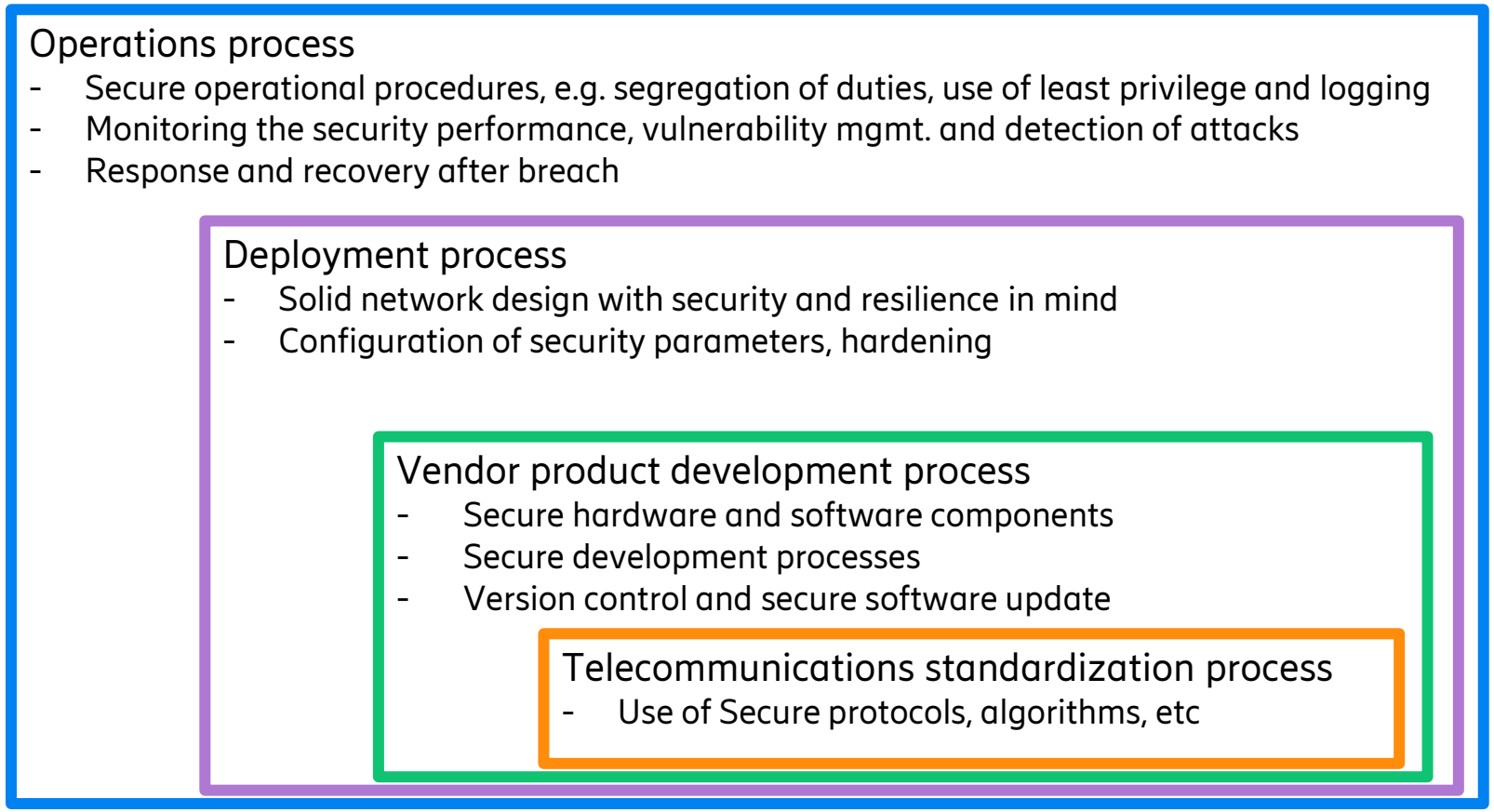
- Access network infrastructure is more physically accessible than other parts of the network
- Largest attack surface in a mobile network
- Public (untrusted) locations or access networks can be particularly vulnerable

RAN security attacks and impact

- Man-in-the-middle attacks
- Identity spoofing
- Denial of service (DoS) attacks
- Eavesdropping
- Data/traffic modification
- Software/Image poisoning
- Physical attacks
- Insider attacks



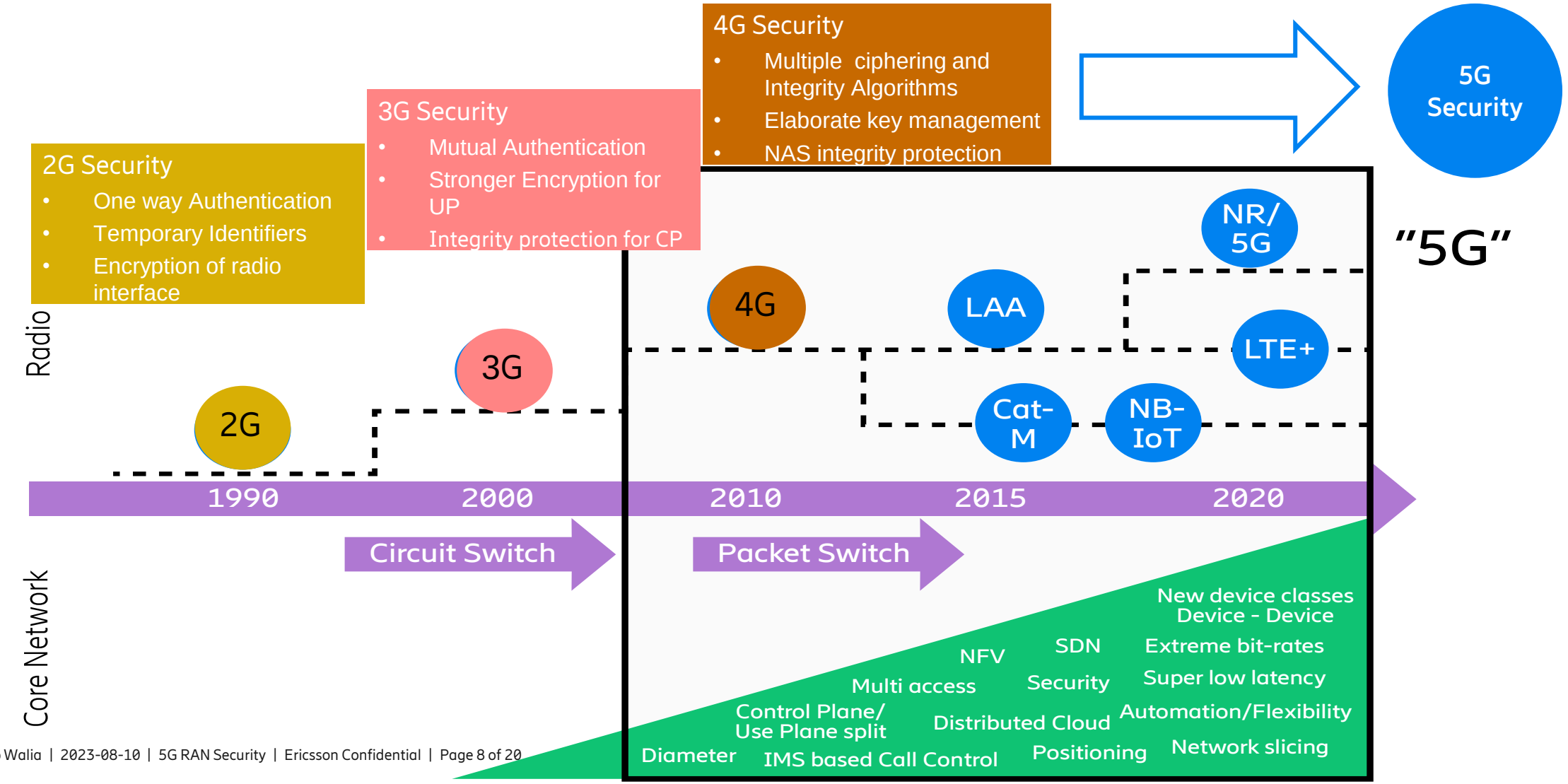
Ensuring network security requires mitigation on four levels



- Security status of deployed networks depends of four inter dependent levels.
- Holistic approach to security includes all four levels.
- Operators are in control of operations, deployment and integrator and vendor selection.
- Vendors are in control of their product development and sourcing decisions (component suppliers).
- Standards are set in a multi stakeholder fashion.

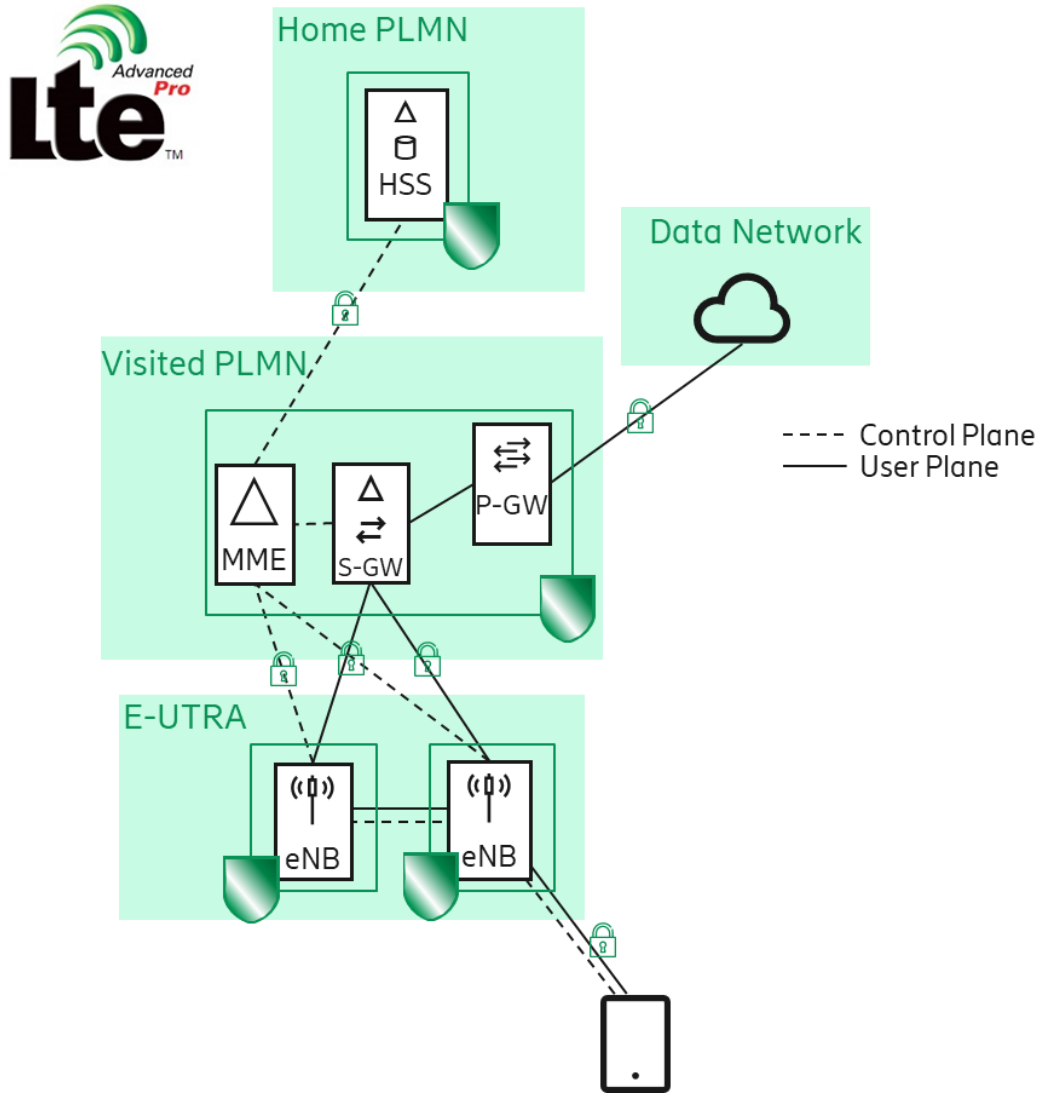
Security Evolution in Mobile networks

Increased level of security with each new G



Key existing Security challenges addressed by 5G

- **4G Vulnerabilities**
  - IMSI sent unencrypted in some cases over radio -> IMSI catchers
  - Fake base stations -> track users, eavesdropping
  - User plane on radio interface is not integrity protected –> data injection/modification
  - No protection for secured exchange to UE capabilities -> 2G/3G Downgrade Attack



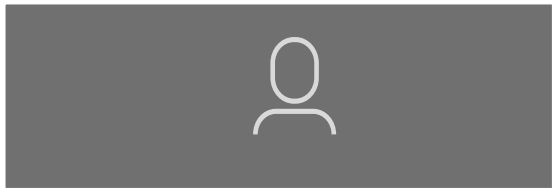
3GPP standard security improvements introduced in 5G

Integrity protection of user plane

- Integrity protection of user plane mandatory on UE and gNB
- Use is optional and under the control of the operator

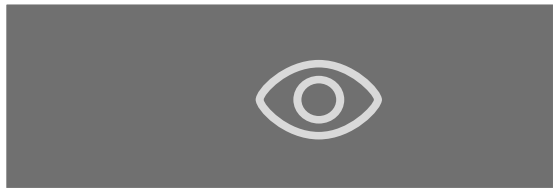
Enhanced subscriber privacy

- Mechanism for encrypting long term subscriber identifiers
- RRC UE capability transfer protection
- False base station detection



Protection of RAN-CN interfaces (transport)

- DTLS over SCTP support in addition to IPsec



Others

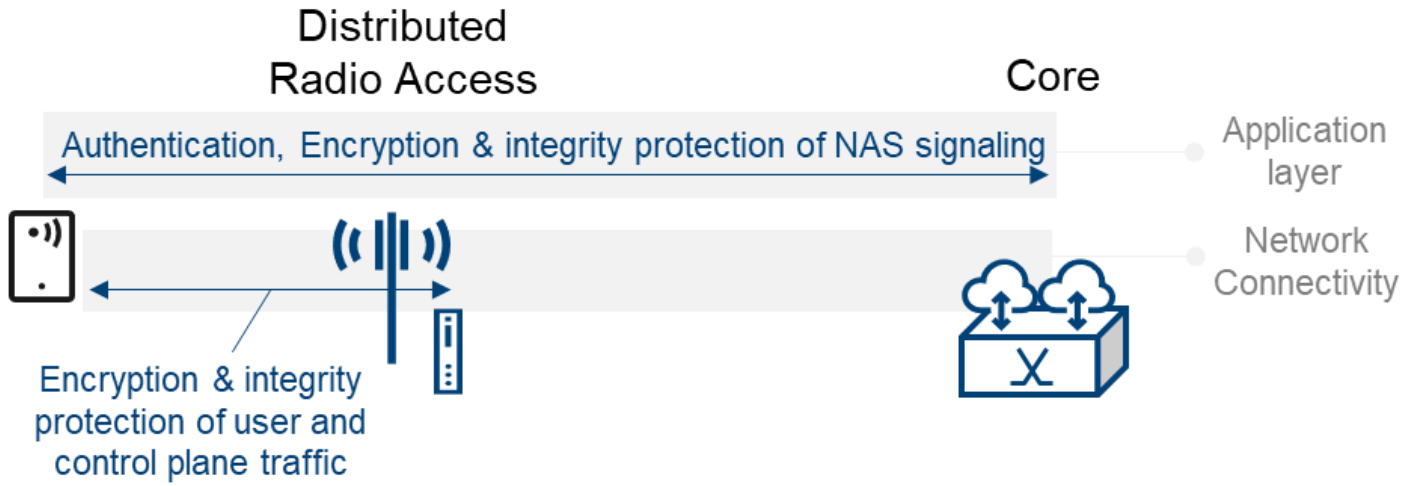
- Use of 256 bit algorithms
- Security assurance specification for 5G nodes

5G - Air interface

- Device authentication is done by the Core network
- The air interface is protected by encryption and integrity protection
  - Encryption of UP and CP (NEA1, NEA2, NEA3, NEA0)
  - Integrity protection of CP (NIA1, NIA2, NIA3) – Null is only supported under certain circumstances

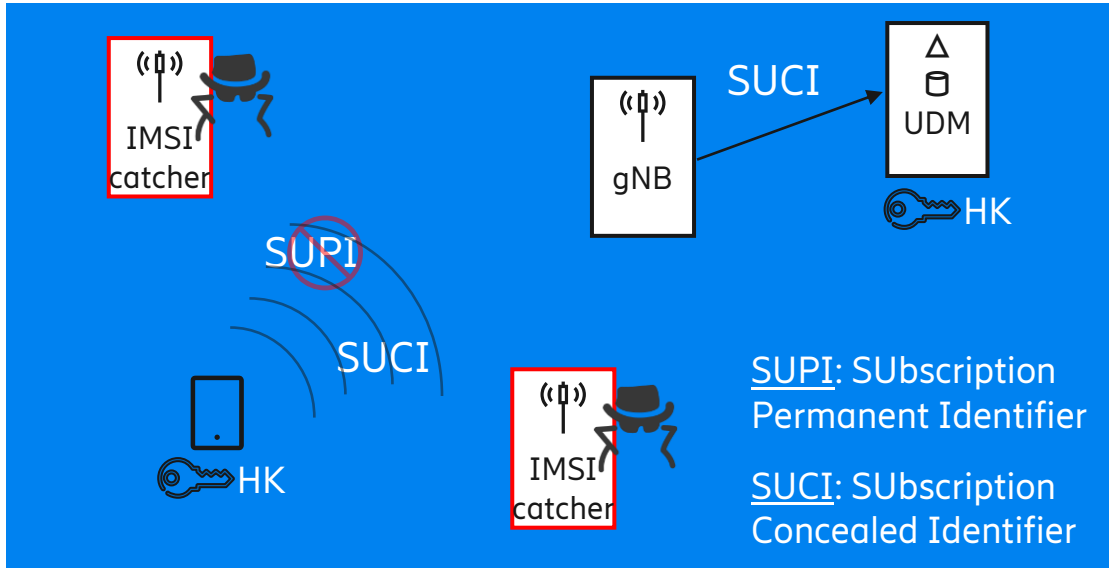
New with 5G SA

- Integrity protection of UP traffic
  - Integrity protection of UP (NIA1, NIA2, NIA3, NIA0)



NEA1/NIA1= SNOW 3G
NEA2/NIA2= AES
NEA3/NIA3= ZUC
NEA0/NIA0= Null (no encryption/integrity)

Enhanced Subscriber Privacy

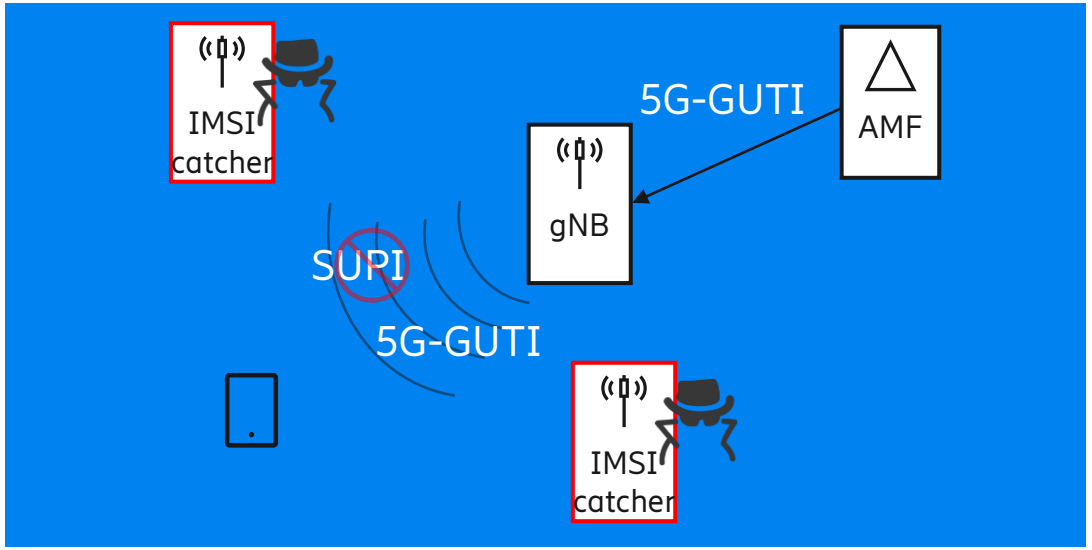


SUPI can be concealed over-the-air

An operator has the option to provision a public encryption key (Home Public Key) which will be used by the UE to encrypt the SUPI. This makes the IMSI catcher attacks impractical.

SUPI no longer used for paging

There is no SUPI-based paging in a 5G System. For paging only the 5G-GUTI is used which is a temporary identifier, thus mitigating UE tracking.

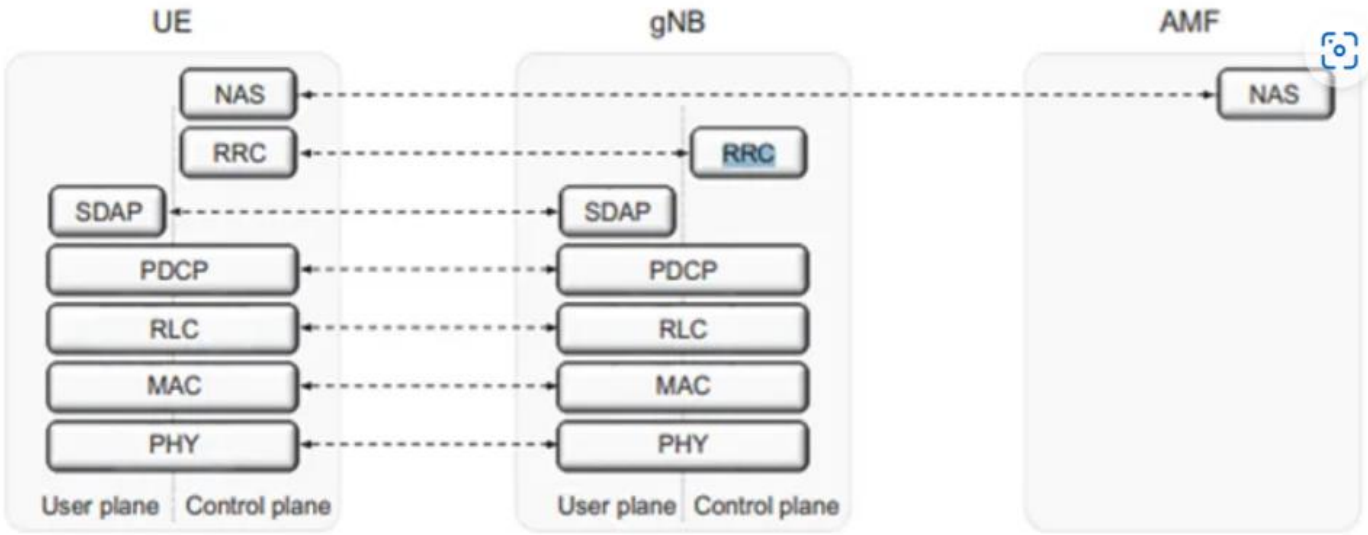


UE Radio capability Transfer protection

- UE capability is a RRC signaling mechanism by which UE can inform its capabilities to gNB (e.g. supported frequency bands, EN-DC support, MIMO, Subcarrier Spacing etc)
- Device Radio capabilities should be accessed only after establishing security.

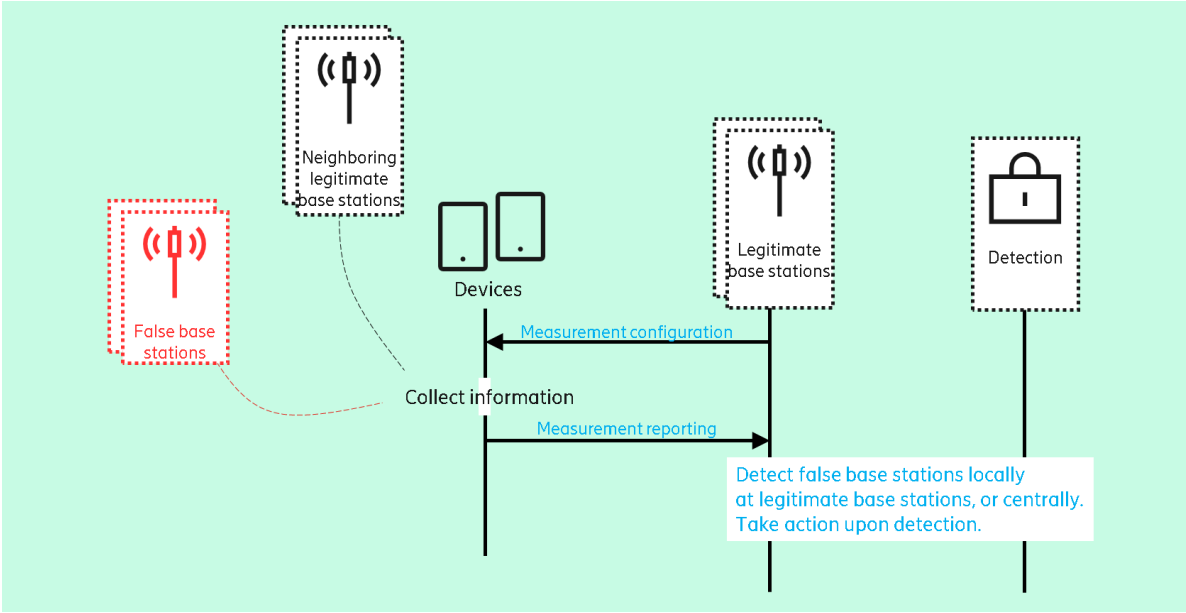
New with 5G SA

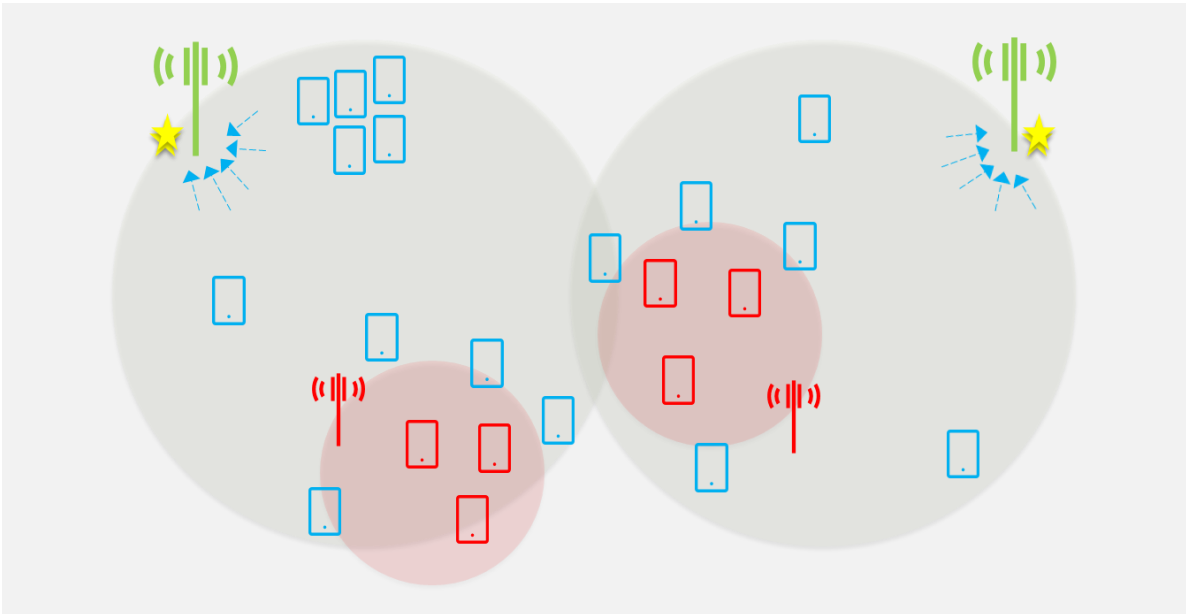
- The network runs the *RRC UECapabilityEnquiry* procedure only after AS security has been activated.



False base station detection

- Device-assisted
  - Radio measurements are done by existing (many many) devices on field.
  - Measurements could be done in connected mode and idle mode.
- Network-based
  - Actual detection is done in the network by analysing radio measurements received from the devices on field and information in the network.

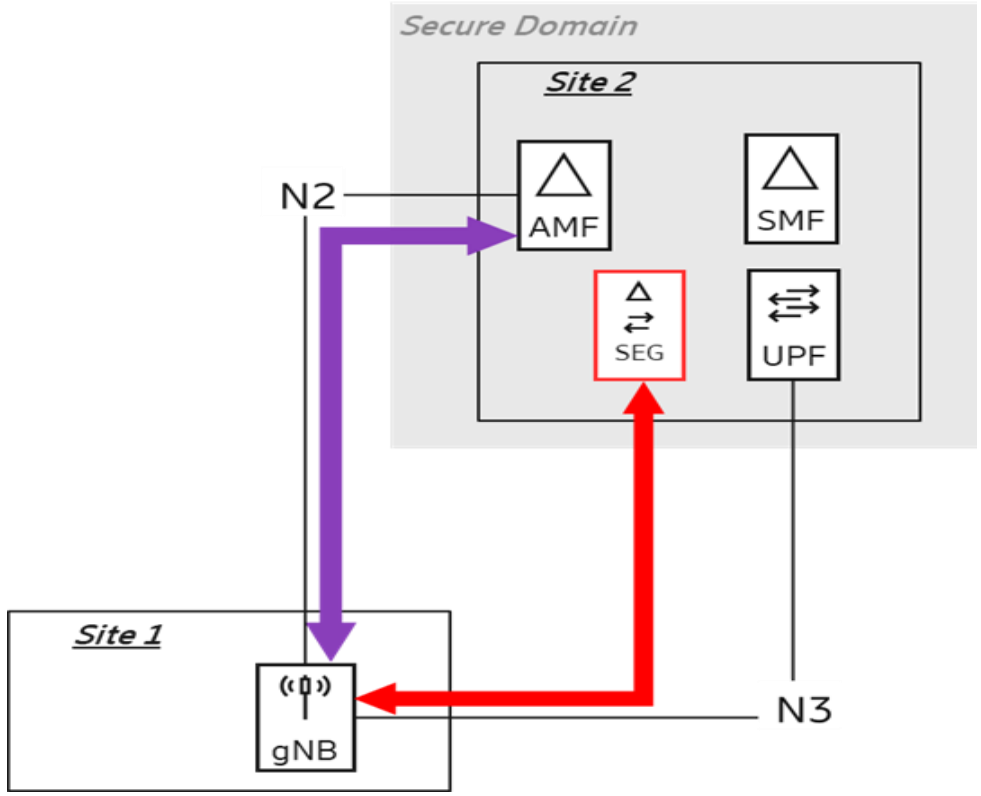




Transport protection

Includes protection for data in transit:
- Use of IPsec across interface (N2,N3 & Xn)

New with 5G SA
- Use of DTLS in addition to IPsec across interfaces (N2, Xn)
- DTLS provides:
  - Mutual authentication based on certificates
  - Ensures the confidentiality and integrity of data in transit
  - Easier to implement



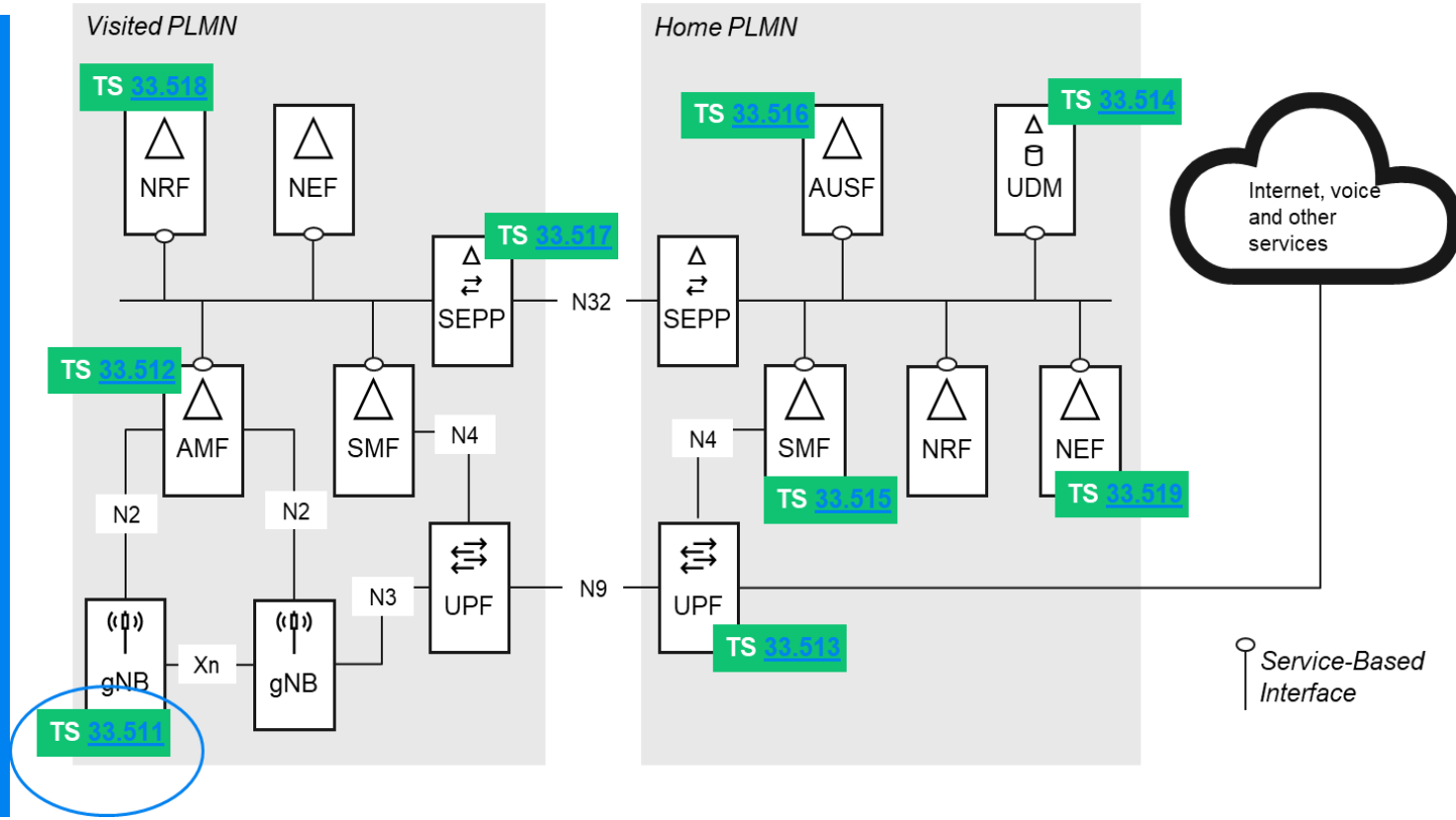
Use of 256 bit Encryption

- 3GPP has mentioned use of 256 bit algorithm for 5G.
- New 256-bit algorithms may be needed e.g. better performance and cost-effectiveness in virtualized environments, 3GPP has asked ETSI SAGE to analyze new 256-bit algorithms for 5G.
- ETSI SAGE has chosen three algorithms i.e. AES 256, SNOW 5G and ZUC 256, 3GPP will have a Rel-19 study to discuss if and how to include the new algorithms in 5G.

- Current 5g networks uses exactly the same algorithms used in 4G i.e. 128 bit since there are no weaknesses and they offer good enough performance when implemented in hardware.

5G Security Assurance

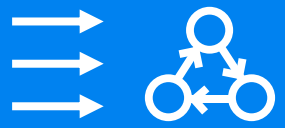
- Security assurance is a means to ensure that network equipment meets security requirements and is implemented following secure development and product lifecycle processes
- Co-operation to specify security assurance scheme (in GSMA) and security test specifications (in 3GPP) for 5G system.



SUMMARY

Increased focus on security due to:

- Evolving threat landscape
- Critical infrastructure that will carry massive amount of devices
- Network evolution (Cloud/containers/several actors etc)



Building trustworthy/secured networks/services depends on all layers:

- Mobile network standardization
- Secure product implementation,
- Secure network deployment
- Secure operations

Key security improvements include:

- Enhanced subscriber Privacy
- Protection of RAN-CN interfaces (transport)
- Integrity Protection of UP
- Security Assurance

https://www.ericsson.com/en/security

4G vs 5G Security

S.no	Function	4G	5G
1	Access Agnostic Authentication	Non Access Agnostic	Unified Authentication
2	Authentication Credentials	Only AKA credentials	AKA credentials or Certificate for IOT/Private Networks (Optional, informative Annexure
3	Authentication Protocol	EPS-AKA over 4G NAS	5G=AKA over 5G NAS or EPA- AKA'/EAP-TLS over 5G NAS
4	Security Protocol for Authentication credentials	UICC	UICC or Non removable UICC
5	Home control for Authentication	Not Supported	Supported (Home PLMN involved in Authentication and holds the key)
6	Integrity protection for UP Traffic	Not Supported	Supported(Optional to use)
7	Initial NAS protection	No	Yes
8	Subscription identity protection	IMSI is not protected if there is no security context	SUPI is always protected using Asymmetric cryptography
9	Network Domain Security	IPSec (Point to Point Architecture)	TLS/Application Layer Protection(SBA)