5G SECURITY STANDARDIZATION

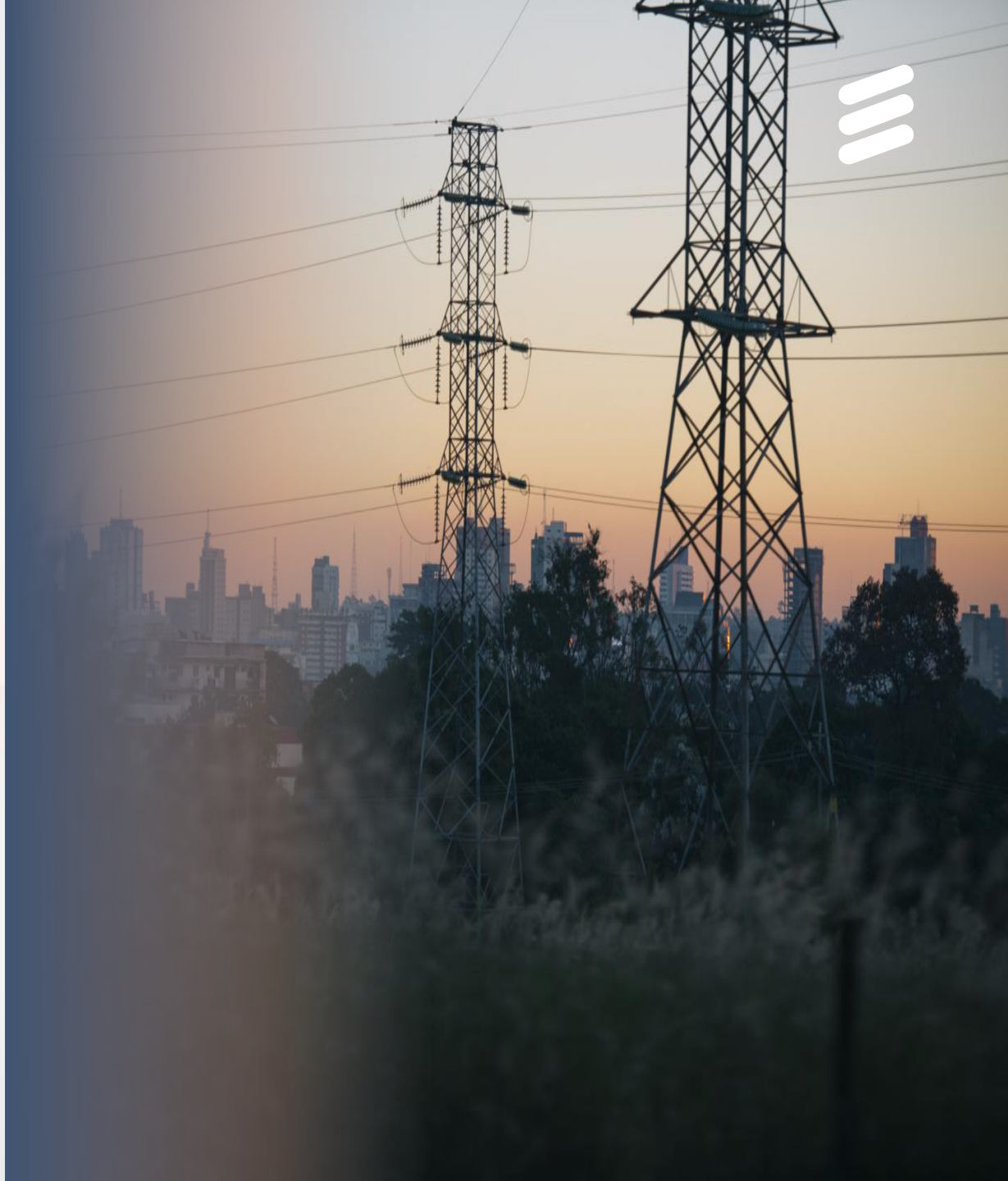
ERICSSON

SICS SECURITY DAY 2016

Karl Norrman, Master Researcher, Security
Ericsson Research, 2016-05-11

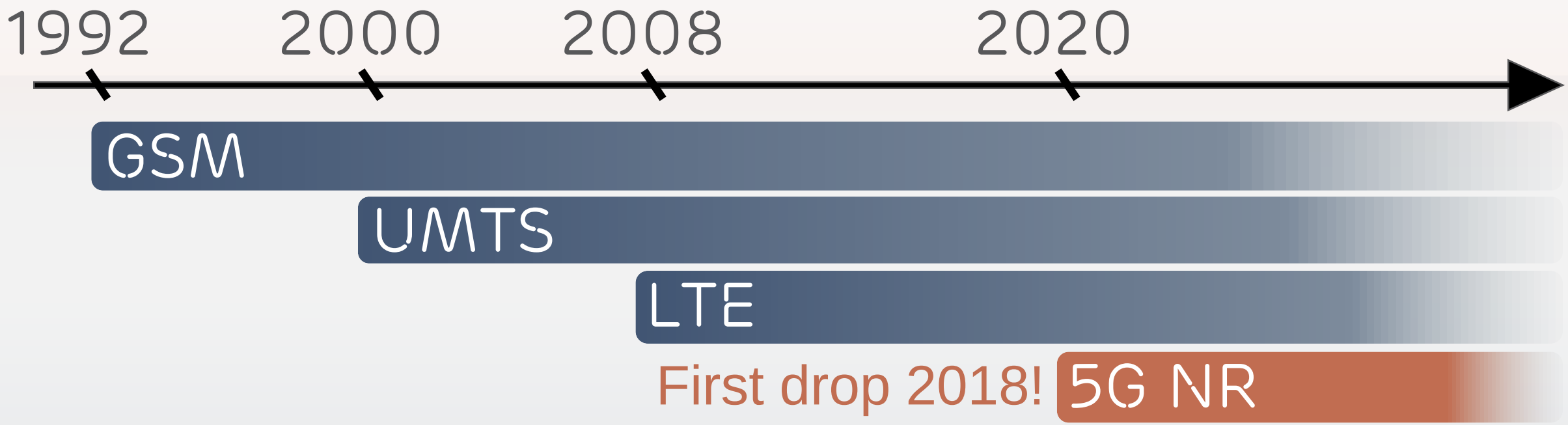
OUTLINE

- Who standardizes 5G radio?
- 3GPP organization and what the working groups do
- Current work status
- Some hot security topics
  - Multi-radio integration
  - Authentication
  - Security termination points
  - Privacy
  - Cloudified implementations
- Conclusions



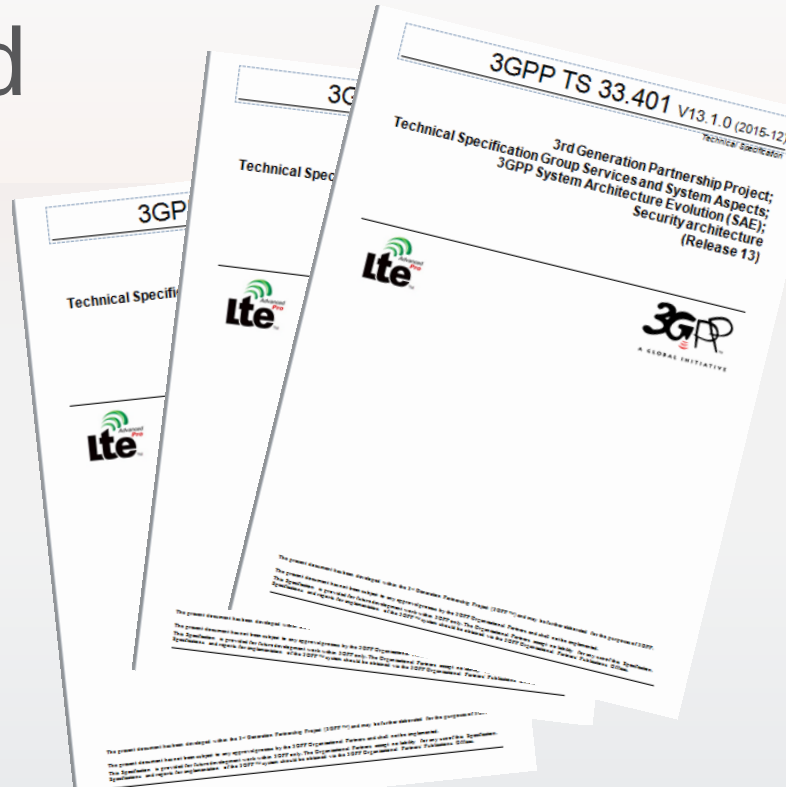
WHAT IS 3GPP?

- Standardization body for mobile networks
- Vendors, operators and regulators from all over the world
- Specifying a new 5G radio and core network for IMT-2020



WHAT IS 3GPP?

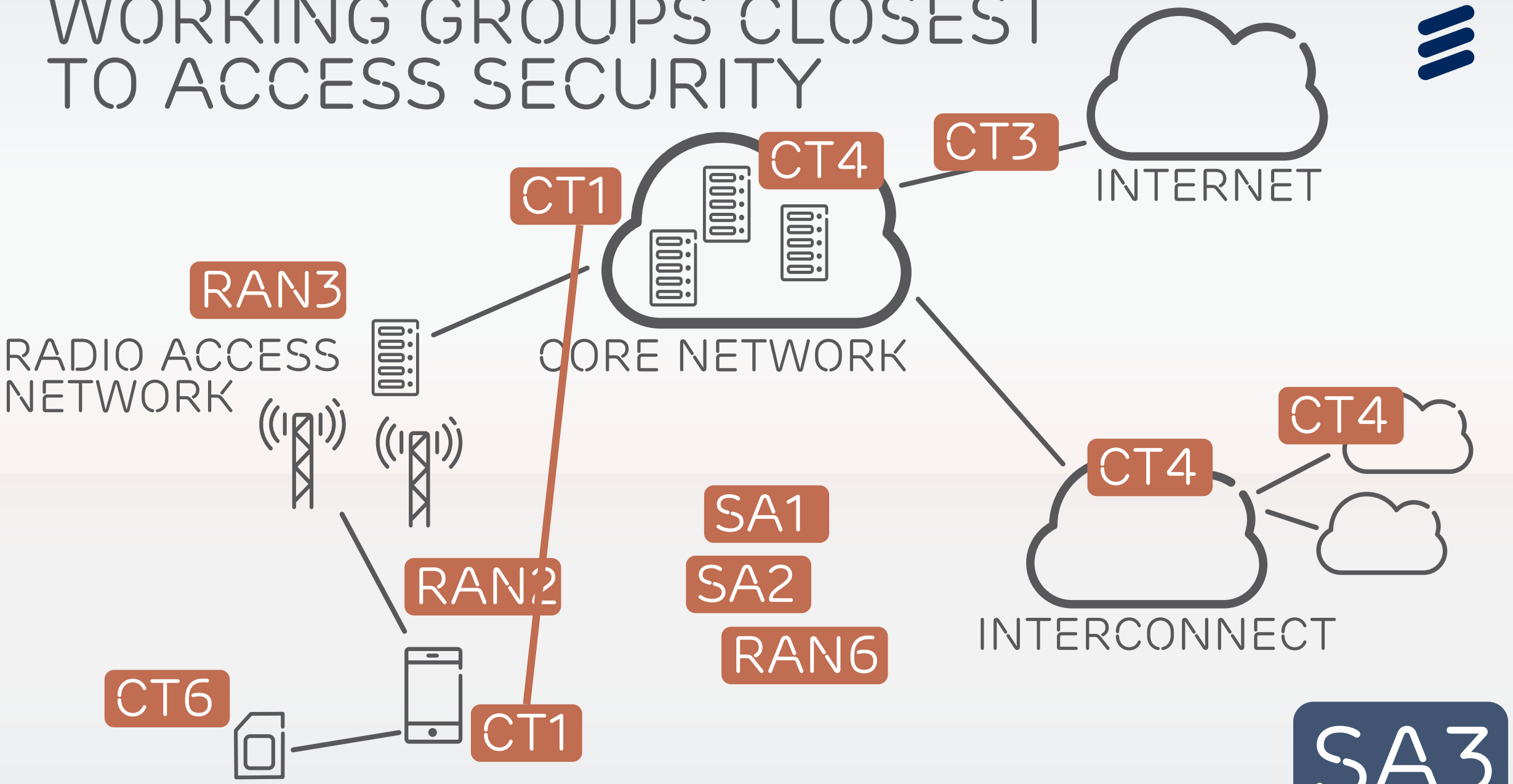
- Why? – interoperability and security
- Architecture, protocols, algorithms and implementations
- Technical Reports and Specifications



3GPP WORKING GROUPS AND ORGANIZATION

RAN Radio Access Networks	CT Core NW & Terminals	SA Services & System
RAN1 Radio Layer 1	CT1 CN – Terminal	SA1 Requirements
RAN2 Radio Layer 2,RRC	CT2 → CT1	SA2 Architecture
RAN3 Access Network	CT3 Interworking ext NWs	SA3 **SECURITY**
RAN4 Performance	CT4 CN – CN	SA4 Multimedia
RAN5 Conformance testing	CT5 → OMA	SA5 OAM
RAN6 Legacy (GSM) Radio	CT6 Smartcards (SIM)	SA6 Mission critical apps

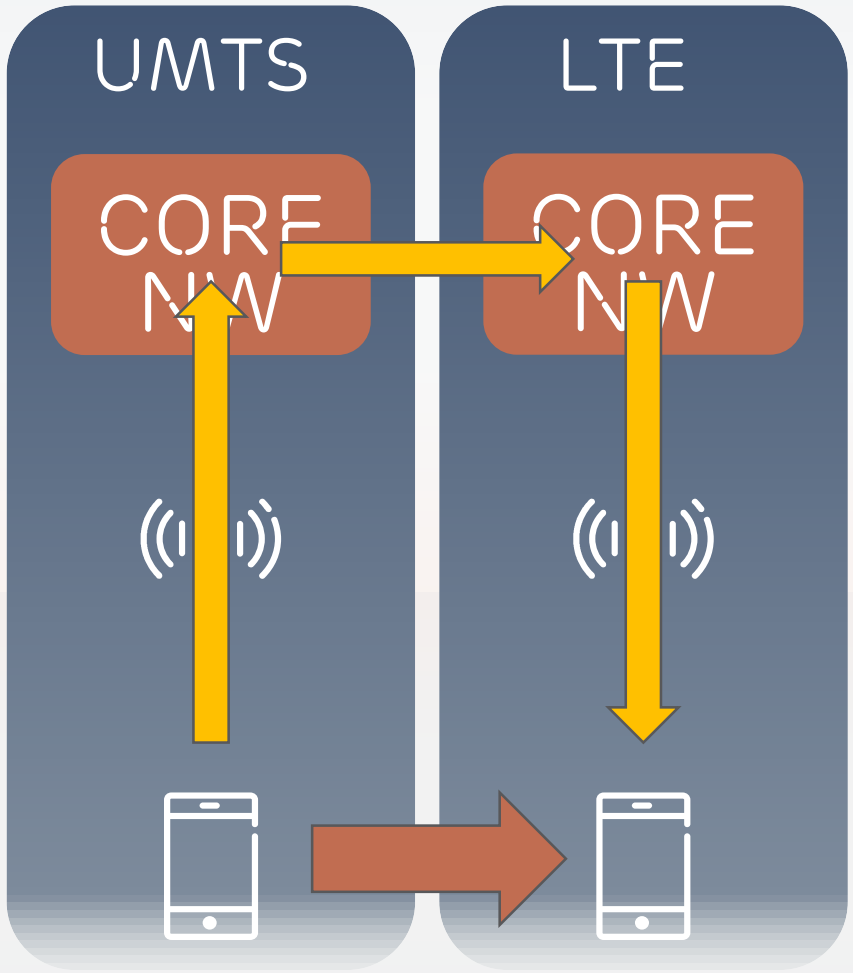
WORKING GROUPS CLOSEST TO ACCESS SECURITY



ONGOING 5G WORK
(CLOSEST TO SECURITY)

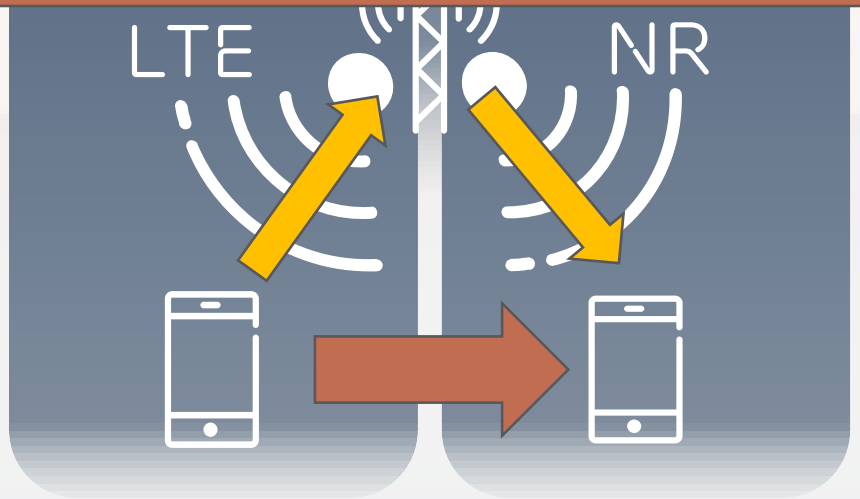
- SA1 (Requirements):
  - TR 22.861 Massive Internet of Things
  - TR 22.862 Critical Communications
  - TR 22.863 Enhanced Mobile Broadband
  - TR 22.864 Network Operation
- SA2 (Architecture):
  - TR 23.799 Study on Architecture for Next Generation System
- SA3 (Security):
  - TR 33.899 Study on the security aspects of the next generation system
- RP (RAN plenary):
  - TR 38.913 Study on Scenarios and Requirements for Next Generation Access Technologies
- RAN3 (Radio Network Architecture):
  - TR 38.801 Study on New Radio Access Technology; Radio Access Architecture and Interfaces

MULTI RADIO INTEGRATION



LOOSER INTEGRATION
(USED TODAY)

Potential positive effects on security:
- No core network required (for IRAT mobility)
- Single security context
- Maybe not even need for implicit authentication
- If common control plane and PDCP:
  - Simultaneous multi-connectivity “easy”
- and more…



TIGHT INTEGRATION
(LTE AND NR)

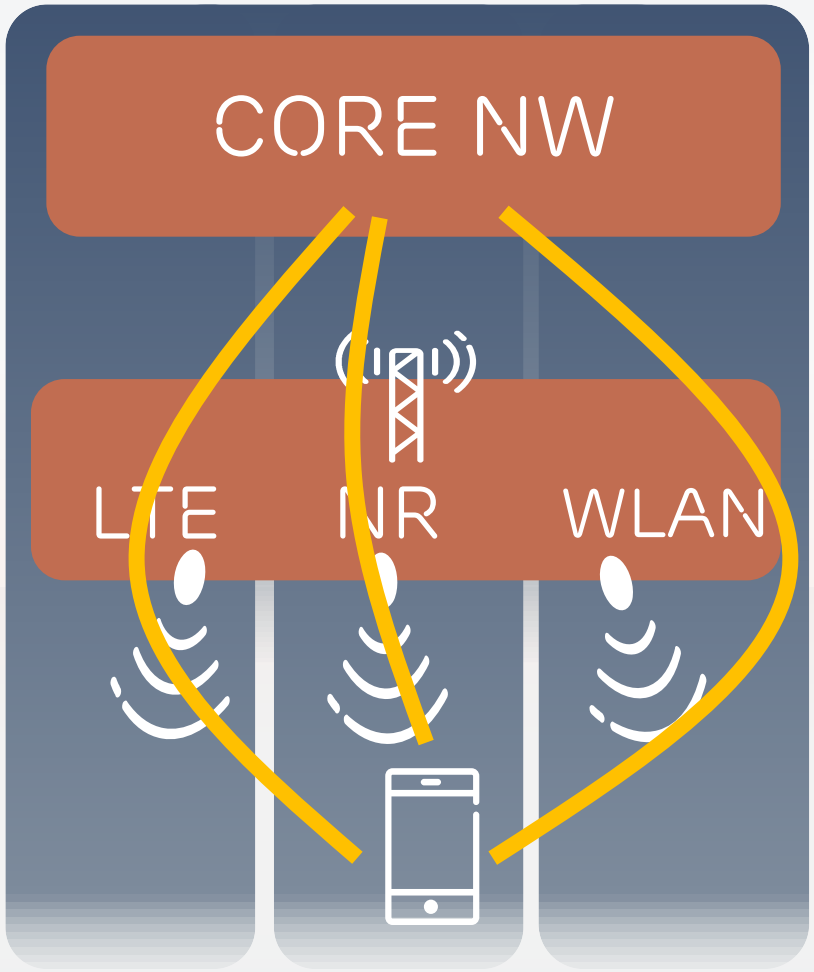
AUTHENTICATION FRAMEWORK

Potential benefits for security:

- Core NW may not need to be aware of which access used
- No need for additional IKEv2+IPsec tunneling
- If generic enough: other types of credentials than USIM
- Can jack in existing credentials (e.g., corporate certs)
- …

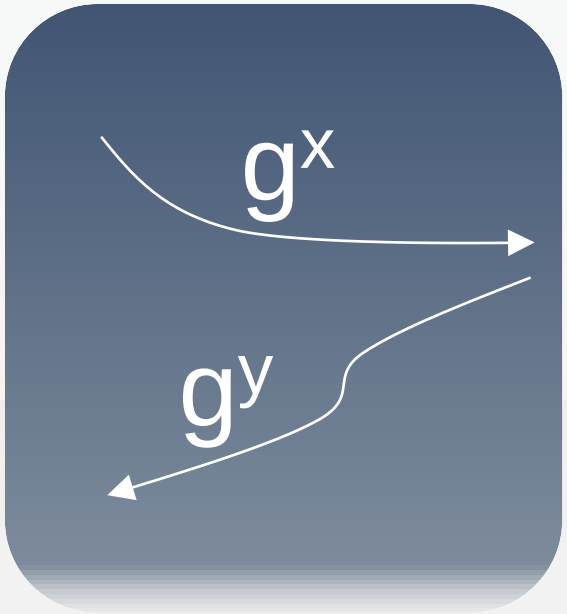
- Candidate framework is EAP or something modelled on similar principles

- Regardless of what happens USIMs will remain an option



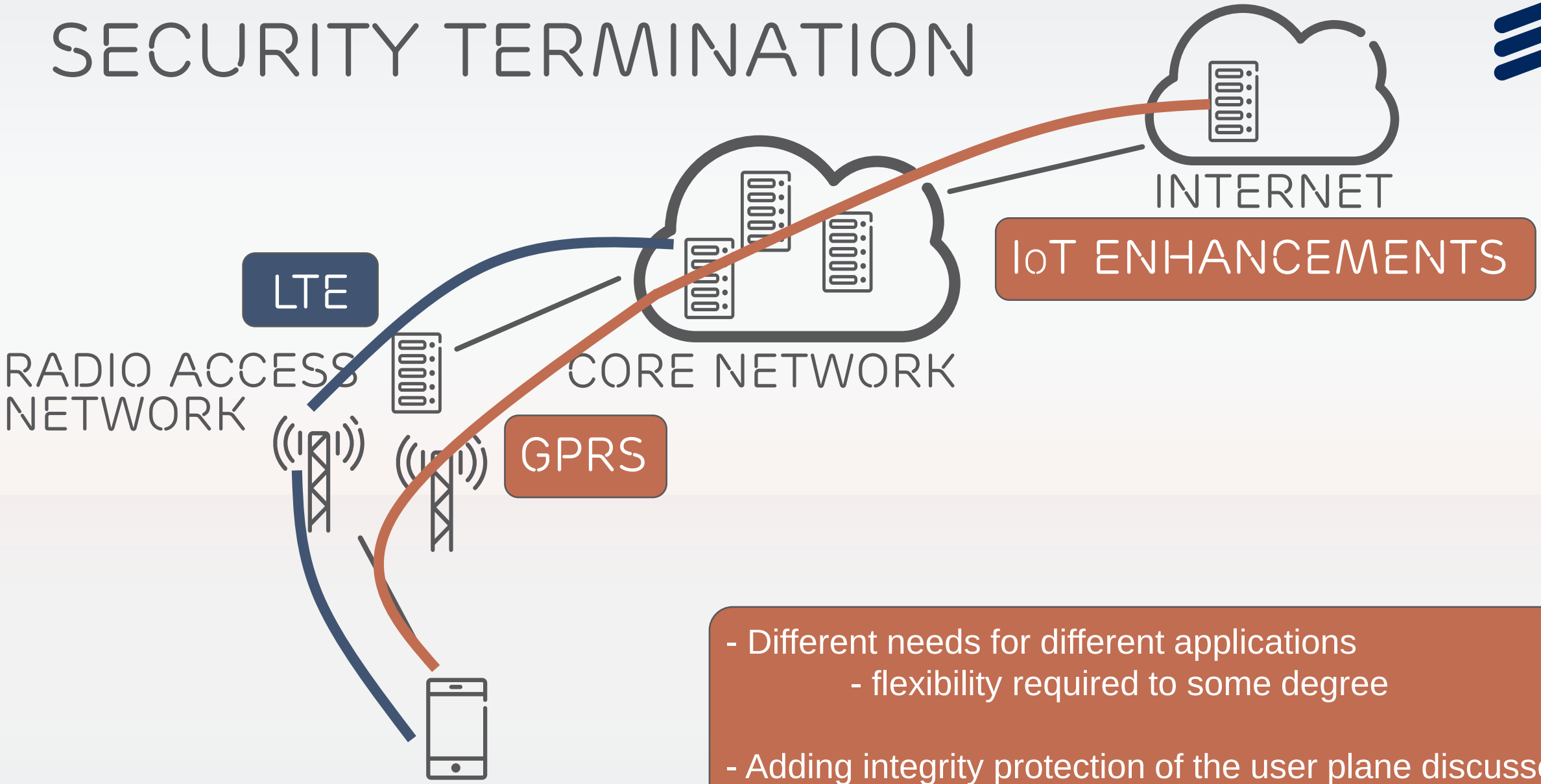
5G AUTHENTICATION FRAMEWORK

AUTHENTICATION ENHANCEMENTS



- After “SIM heist”: reduce effects of compromised long-term keys
  - PFS (only help previous session keys at compromise)
  - DH exchange: forces MITM attacks on authentication run
  - Include DH not only at authentication
  - Different options on the table. What is the cost in terms of processing and transmission overhead?

SECURITY TERMINATION



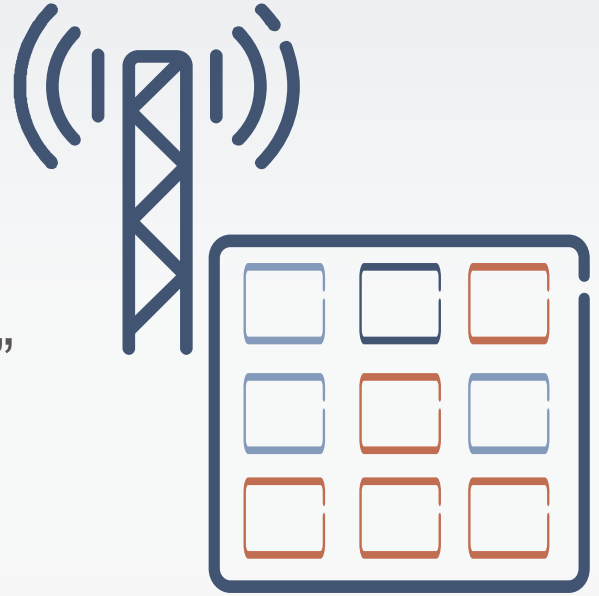
- Different needs for different applications
  - flexibility required to some degree

- Adding integrity protection of the user plane discussed

PRIVACY

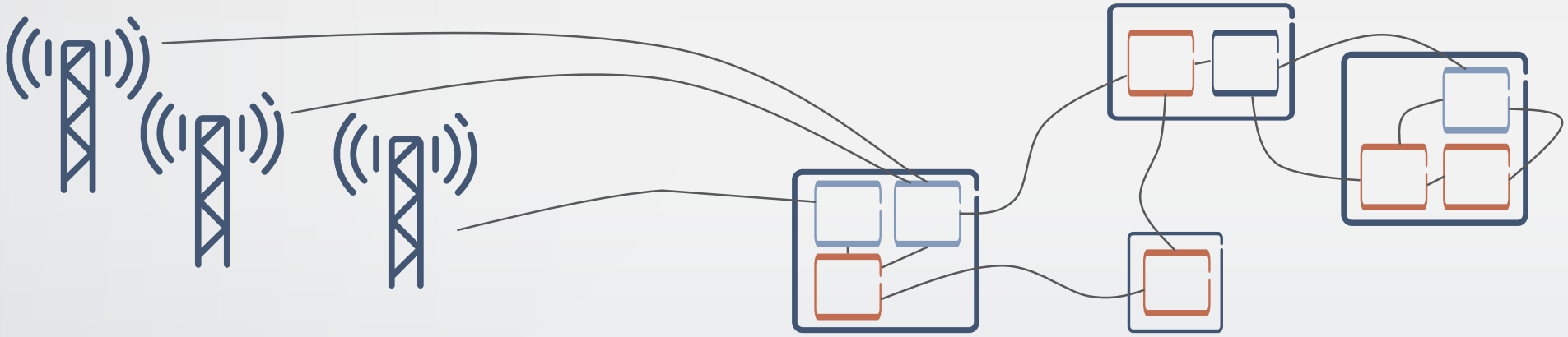
- Protection against IMSI catchers
- Increased concerns on privacy in general
- Topic was hot in mid-90s, 2000 and 2007
  - Hope that IMSI protection and other privacy functions will be improved for 5G

CLOUD
(IN THE MOST GENERIC SENSE OF THE WORD)



- Moving away from “one-function == one-physical box”

- E.g., radio base station can be virtualized
  - Antennas remain physical, but all other functions can be divided into parts and distributed



CLOUD

- Dynamic nature:
  - Discover need for additional (virtual) resource
  - Deploy resource
  - Monitor system behavior
  - Decommission resource when no longer needed

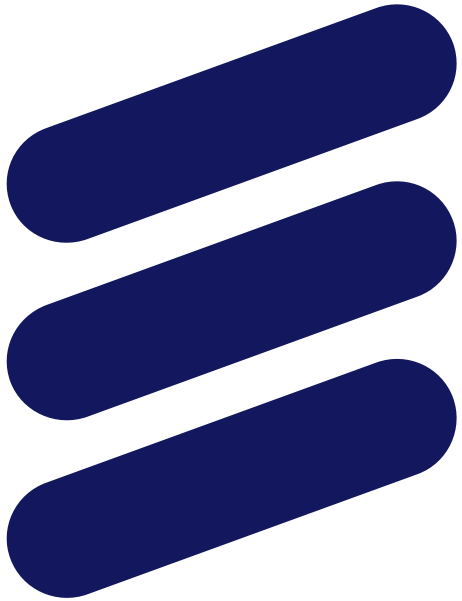
- Need to verify that platform is secure before deployment
- Need to verify whether resource should connect to other resources securely etc
- Management and control of resources even more complex than today

CLOUD

- Although largely an implementation issue, *may* require standardization:
  - Security Assurance requirements (a' la SECAM) may be needed
  - For interoperability of inter-function protection
  - Authentication of HW to SW and vice versa may be needed
  - …
- Should it be standardized at all? Is 3GPP the right place to do it? ETSI NFV? Both or somewhere else?
  - Open question…

CONCLUSIONS

- NR security work just starting up in 3GPP
- Many security features have been studied in other contexts before
- Many security features that were not included in LTE are being brought up again
- A lot of hard work required and many very good ideas, but so far few unexpected topics that impact security have been brought up
- Cloudified implementations – Changes the fabric, but what are implications for standardization?



ERICSSON