OPEN AIR interface

First OAI Foundation U.S. Hands-on Workshop

17-19 November 2025

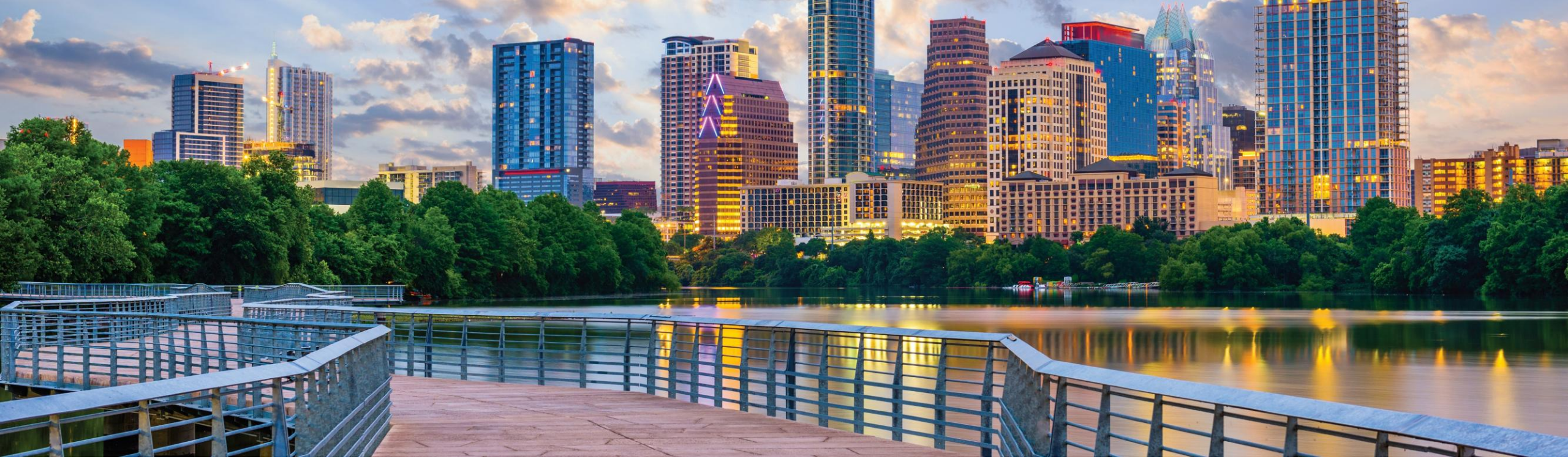
University of Texas at Austin

Understanding 5G NR security with OpenAirInterface

19/Nov/2025 | 14:00-17:00 | Avaya Auditorium

Hugo Marques
Assistant Professor
hugo@ipcb.pt

Luis Pereira
Chief of 5G/6G R&D
lpereira@allbesmart.pt

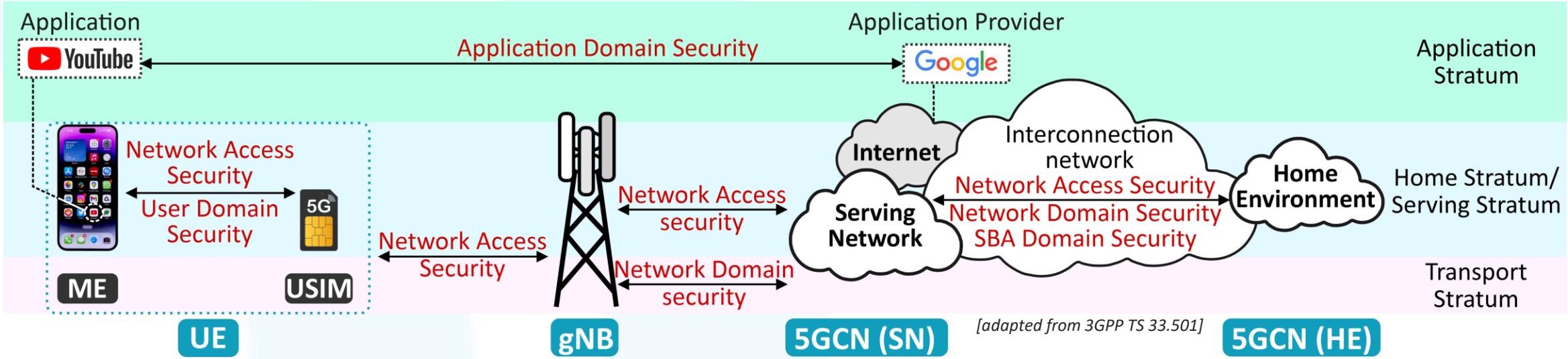


Introduction to the 3GPP Security Architecture

- 5G Security Architecture (simplified)
- 5G Radio Bearers, Signaling and User Data
- 5G Radio Bearers, Signaling and User Data
- 5G Security Algorithms
- 5G Key Hierarchy, Key Derivation, and Distribution Scheme
- 5G UE Authentication Procedure (5G AKA)

5G Security Architecture (simplified)

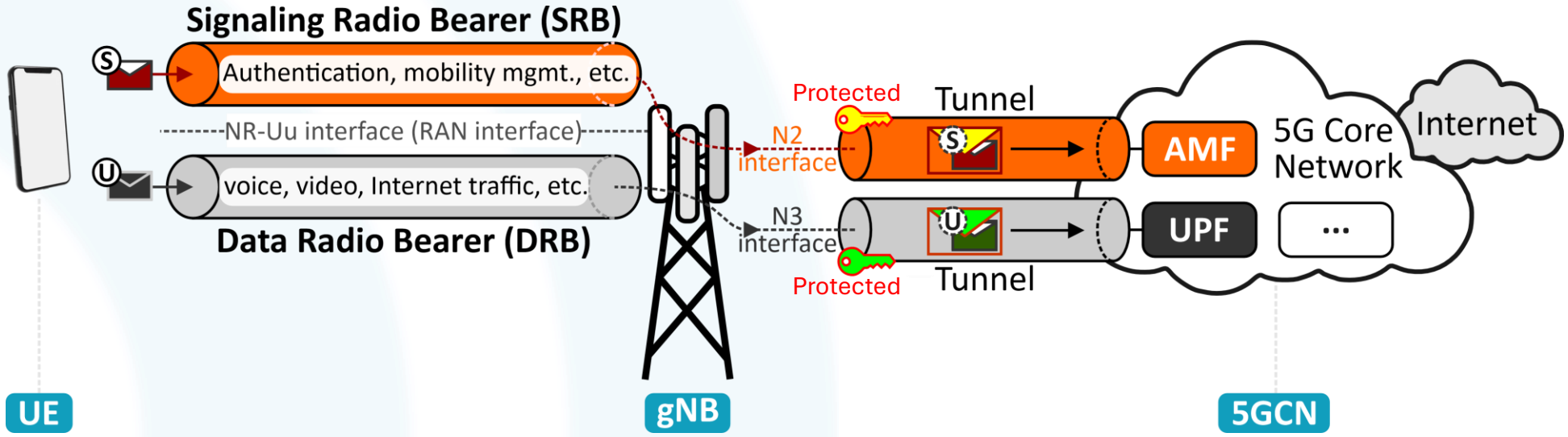
- Different security domains and *strata* are defined:
  - User Domain Security
  - Network Access Security
  - Network Domain Security
  - Software Based Architecture SBA Domain Security
  - Application Domain Security



[adapted from 3GPP TS 33.501]

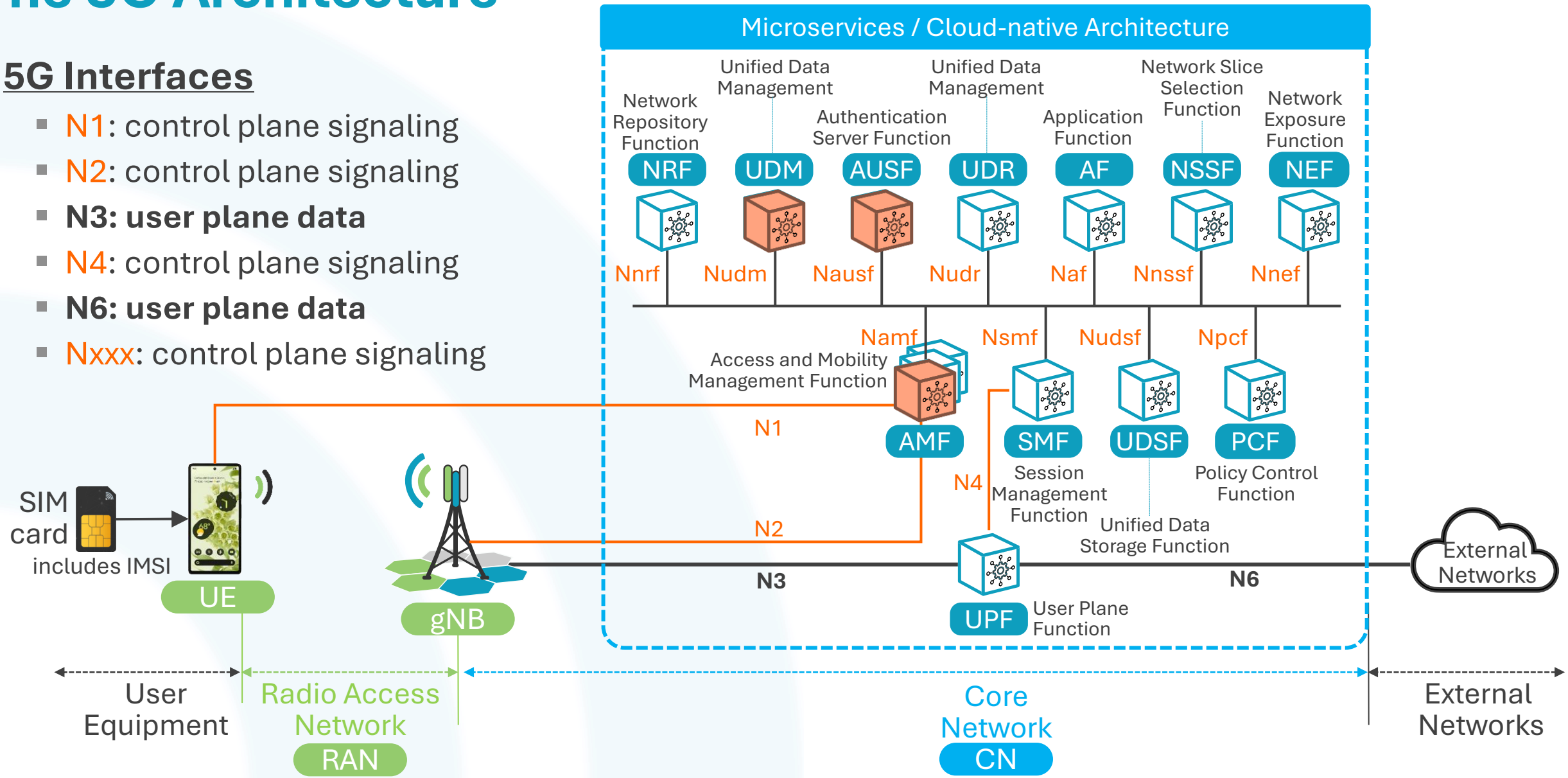
5G Radio Bearers, Signalling and User Data

- Communication between the UE and the access network has always relied on logical channels
- Starting from LTE 4G, these channels are clearly distinguished and categorized as follows:
  - ***Signalling Radio Bearers*** SRBs used exclusively for control plane signalling
  - ***Data Radio Bearers*** DRBs used for user plane data



The 5G Architecture

- **5G Interfaces**
  - N1: control plane signaling
  - N2: control plane signaling
  - **N3: user plane data**
  - N4: control plane signaling
  - **N6: user plane data**
  - Nxxx: control plane signaling



5G Security Algorithms

- Both NEA and NIA are used to secure communications over the SRBs and DRBs
  - NEA - *Encryption Algorithm for 5G*
  - NIA - *Integrity Algorithm for 5G*

5G Algorithm	Purpose	Security Operation Performed by:
NEA0	**Null encryption**	Not applicable
NEA1	Encryption	SNOW 3G *note: used for backward compatibi lity*
NEA2	Encryption	AES
NEA3	Encryption	ZUC
NIA0	**No integrity protection**	Not applicable
NIA1	Integrity Protection	SNOW 3G *note: used or backward compatibility*
NIA2	Integrity Protection	AES-CMAC Cipher-based Message Authentication Code
NIA3	Integrity Protection	ZUC

SRB	Purpose	Used Before or After Security Activation?	Security Services Provided
SRB0	RRC messages[1]	Before	**None**
SRB1	RRC messages & NAS messages	After	Authentication, Confidentiality and Integrity
SRB2	NAS messages only optimized	After	
SRB3	RRC messages for secondary gNB optional	After	

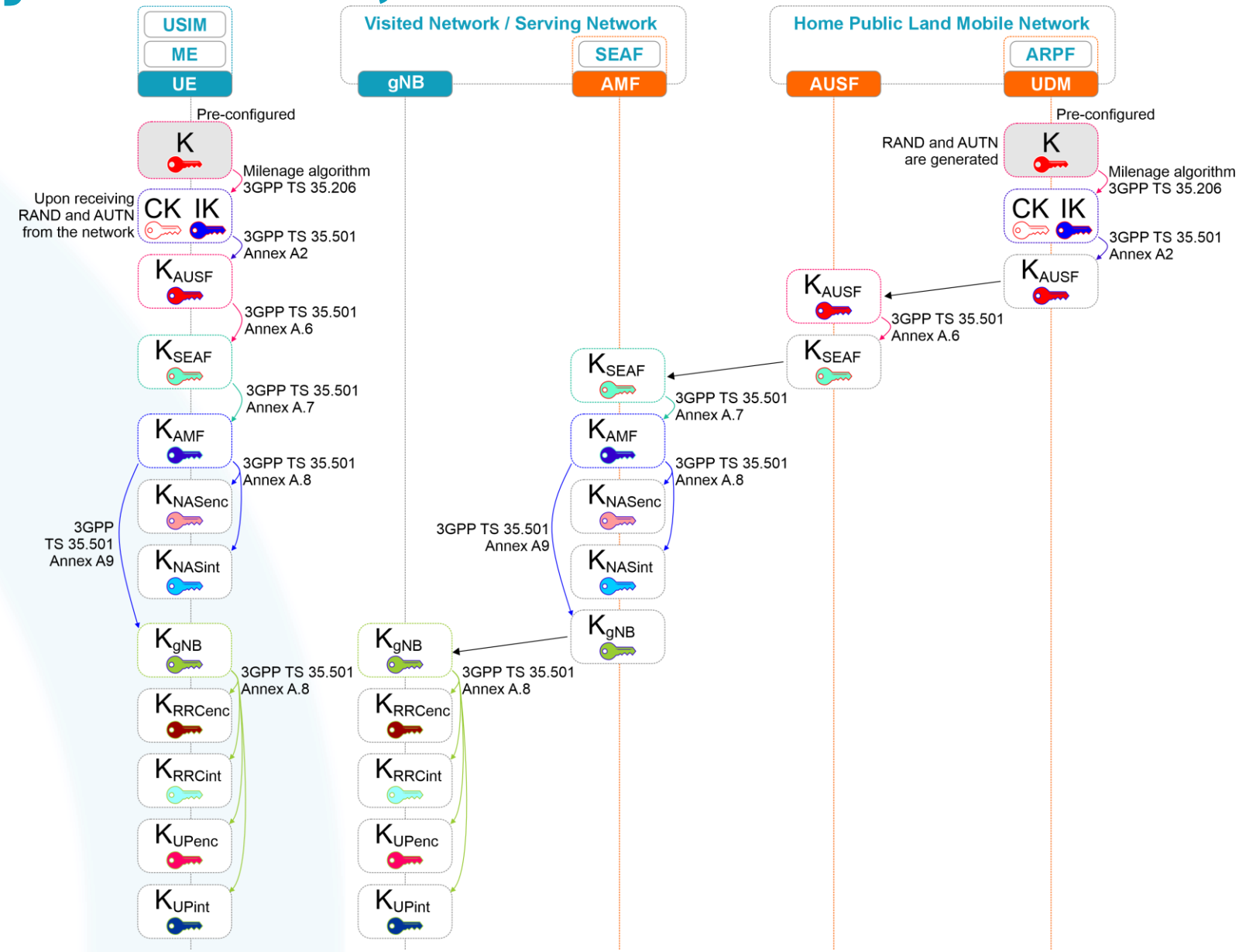
[1] SRB0 is specifically used for transmitting initial RRC messages before a security context has been established. Security procedures, such as the Security Mode Command and its corresponding response, are carried out over SRB0.

  - With the exception for SRB0, **all SRBs must use encryption and integrity protection**
  - DRBs, on the other hand, have some flexibility, where the network might opt for NEA0

5G Key Hierarchy, Key Derivation, and Distribution Scheme

Key	Key name
K	Root of Trust Key
CK and IK	Confidentiality and Integrity keys
K_{AUSF}	Home Environment Anchor Key
K_{SEAF}	Serving Environment Anchor Key
K_{AMF}	NAS Anchor Key
K_{NASenc}	NAS Encryption Key
K_{NASint}	NAS Integrity Key
K_{gNB}	RAN Key
K_{RRCenc}	RRC Encryption Key
K_{RRCenc}	RRC Integrity Key
K_{UPenc}	User Plane Encryption Key
K_{UPint}	User Plane Integrity Key

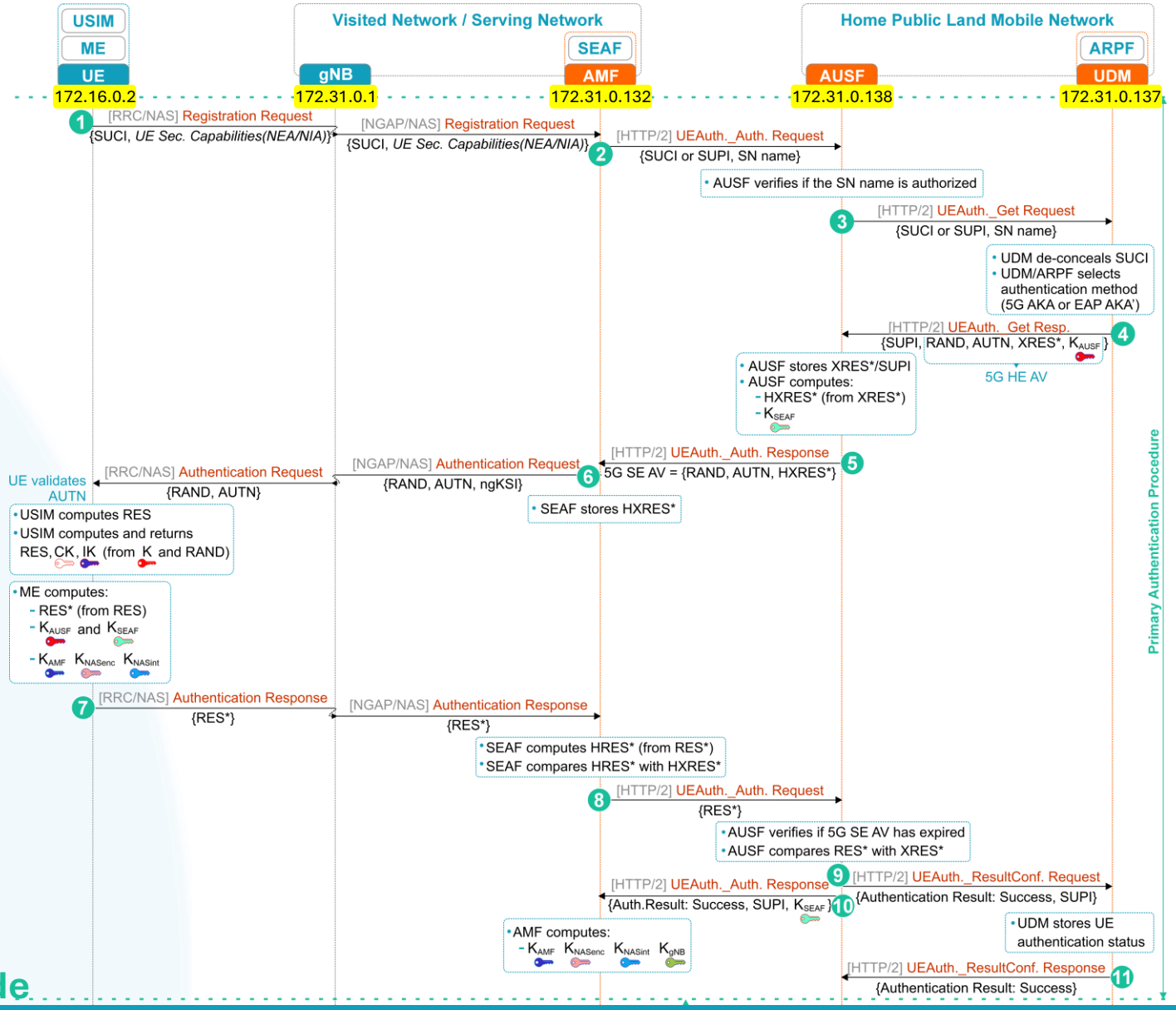
AMF: Anchor and Mobility Function
ARPF: Authentication credential Repository and Processing Function
AUSF: Authentication Server Function
SEAF: Security Anchor Function
UDM: Unified Data Management



5G UE Authentication Procedure (5G AKA) [1/2]

- Primary Authentication

1. Registration Request
2. UEAuthentication_Authenticate Request
3. UEAuthentication_Get Request
4. UEAuthentication_Get Response
5. UEAuthentication_Authenticate Response
6. NAS Authentication Request
7. NAS Authentication Response
8. UEAuthentication_Authenticate Request
9. UEAuthentication_ResultConfirmation Request
10. UEAuthentication_Authenticate Response
11. UEAuthentication_ResultConfirmation Response



Continues on next slide

5G UE Authentication Procedure (5G AKA) [2/2]

- NAS Security Context
  - 12 NAS Security Mode Command
  - 13 NAS Security Mode Complete
- AS Security Context
  - 14 Initial Context Setup Request
  - 15 Initial Context Setup Response
  - 16 AS Security Mode Command
  - 17 AS security mode complete