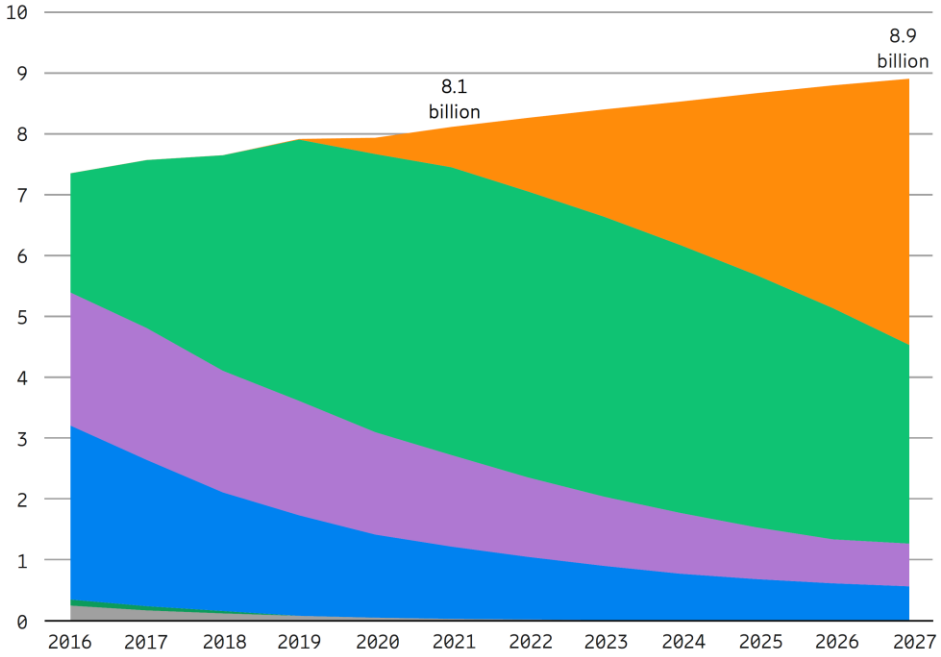
Computer Security Capstone

Supplementary: 5G Security

Chi-Yu Li

National Yang Ming Chiao Tung University

Mobile Subscriptions



5G subscriptions are forecast to reach 4.4 billion in 2027.

4.4bn

- 5G
- LTE (4G)
- WCDMA/HSPA (3G)
- GSM/EDGE-only (2G)
- TD-SCDMA (3G)
- CDMA-only (2G/3G)

[1] GSA (October 2021).
[2] A 5G subscription is counted as such when associated with a device that supports New Radio (NR), as specified in 3GPP Release 15, and is connected to a 5G-enabled network.
[3] Mainly CDMA2000 EVDO, TD-SCDMA and Mobile WiMAX.

Source: Ericsson Mobility Report, Nov. 2021

Various Requirements to 5G

Low-power, low-complexity devices such as smart meters and environment sensors

Deep coverage
To reach challenging locations

Ultra-low energy
10+ years of battery life

Strong security
e.g., Health / government / financial trusted

Ultra-high reliability
< 10^{-5} per 1 millisecond

Ultra-low complexity
10s of bits per second

Ultra-low latency
As low as 1 millisecond

Can't-fail services like V2V communication and factory automation

Ultra-high density
1 million nodes per km^2

Extreme capacity
10 Tbps per km^2

Next wave of consumer devices

Extreme user mobility
Up to 500 km/h

Extreme data rates
Multi-Gbps peak rates;
100+ Mbps user experienced rates

Deep awareness
Discovery and optimization

Source: Ana Schafer, "Enhanced Mobile Broadband – 5G Innovation for consumers," Qualcomm developer network, 2019.

How to Deliver eMBB?

- Needs: higher throughput, lower latency, greater capacity, better uniformity and complete mobility
- Communication technologies
  - Massive MIMO
  - More spectrum sharing
  - mmWave
  - Gigabit LTE
  - Device-centric mobility

How to Deliver MCC?

- Needs: faster than humans can think; failure is not an option

- Enhanced ultra-reliable, low-latency communication (eURLLC)
  - Scalable slot duration down to 125 us
  - Efficient multiplexing with scheduled traffic
  - Spectrum sharing allows for more-predictable QoS
  - Redundant links to mission-critical devices with multi-connectivity

How to Deliver Massive IoT?

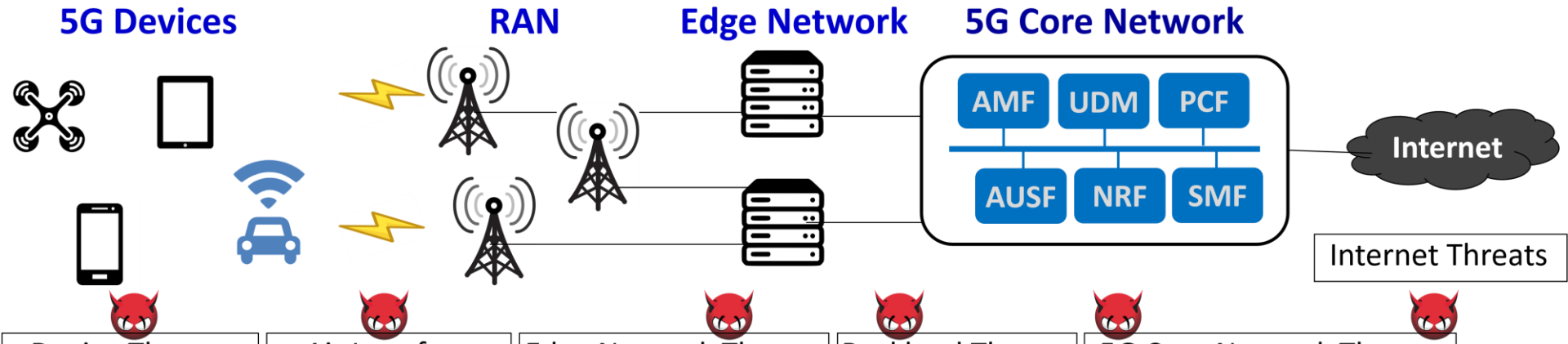
- Needs: more efficiently connect the wide variety of IoT devices and services

- Communication technologies
  - Upon the foundation of NB-IoT
  - More efficient uplink transmission scheme for IoT with RSMA
  - WAN-managed multi-hop mesh to extend network coverage

5G Revolution

- Service-based Core: delivering multi-network slicing, multi-level of services and multi-connectivity network capabilities
  - Based on virtualization and SDN
  - flexibility, agility and economics of scale
- Addressing many threats faced in today's 4G/3G/2G
  - E.g., new mutual authentication capabilities
- However, adopting new network technologies introduces new potential threats
  - Increasing attack surface

Security in 5G: Threats Everywhere



Device Threats
- Bots
- DDoS
- MitM Attacks
- Firmware Hacks
- Device Tempering
- Malware
- Sensor Susceptibility

Air Interface Threats
- Jamming
- MitM Attacks
- Eavesdropping

Edge Network Threats
- MEC server vulnerabilities
- Rouge Nodes
- Authentication Issues
- Side Channel Attacks
- Improper Access Control

Backhaul Threats
- DDoS Attacks
- Control and user plane sniffing
- MEC Backhaul Sniffing
- Flow modification attacks

5G Core Network Threats
- Software issues
- API vulnerabilities
- Networking Slicing issues
- DoS and DDoS attacks
- Improper Access Control
- Virtualization issues

5G Security Highlights

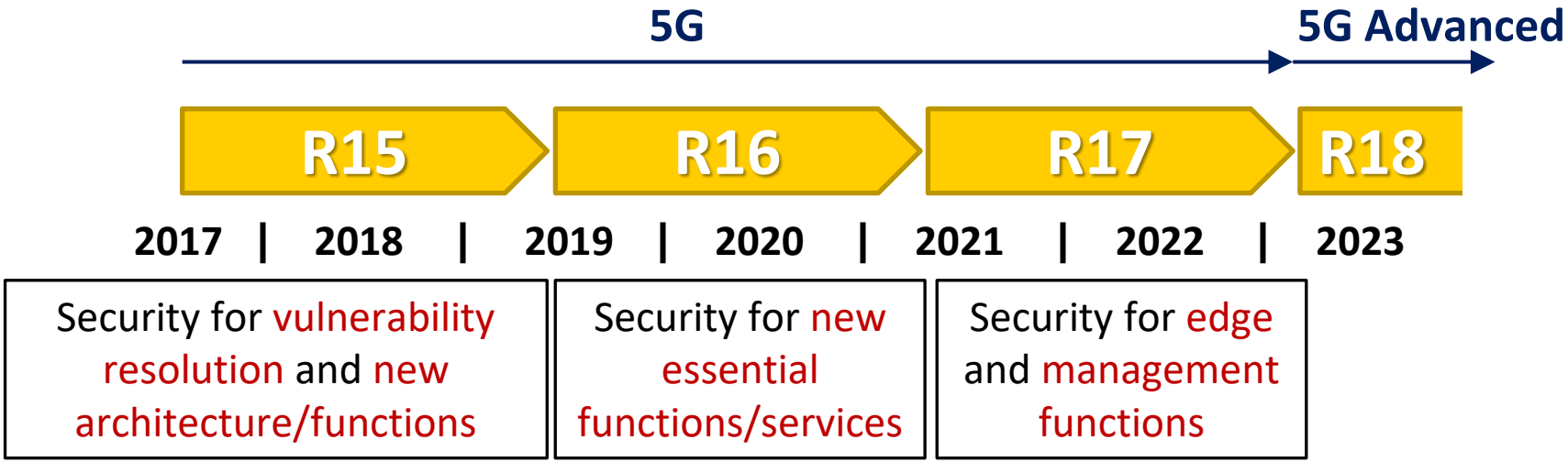
- New attack surface: changes from legacy cellular
  - Inter-working between multiple technologies and multiple generations, even non-trusted environments
  - User device proliferation
  - Moving intelligence from the core to the edge of networks
  - Network virtualization
  - Shift from telecom network protocols to IP-based protocols
  - Convergence of multiple technologies
  - More open platform/technology stacks with software from more vendors

5G Security Highlights (cont.)

- New attack surface: new innovations and verticals
  - Cloud RAN, vRAN, O-RAN
  - Service based core network architecture
  - SDN, NFV, network slicing, etc.
  - Cloud and edge computing
  - Limits of standards-specified protection

5G Security Evolution

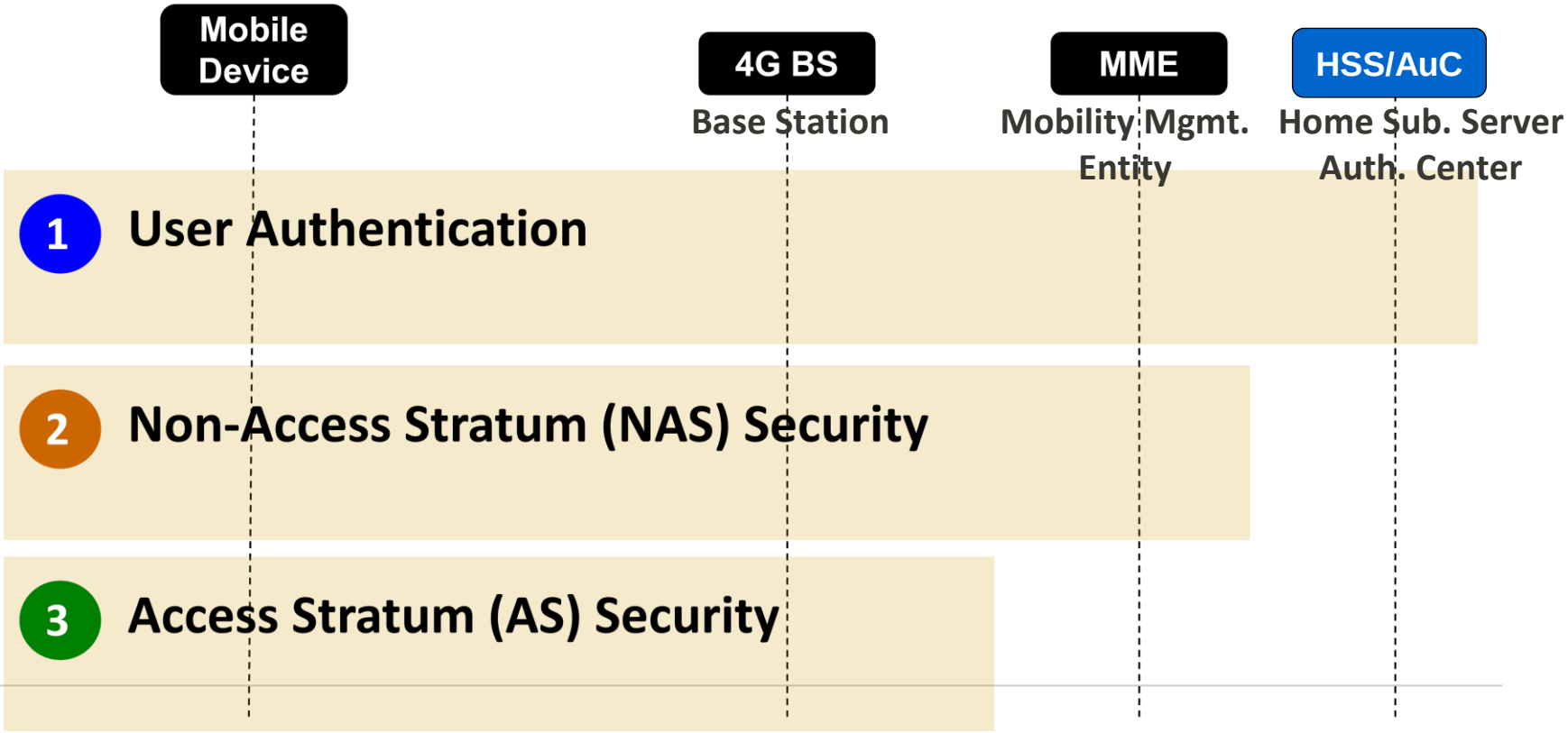
- Main document: 3GPP TS 33.501
  - Security architecture and procedures for 5G system



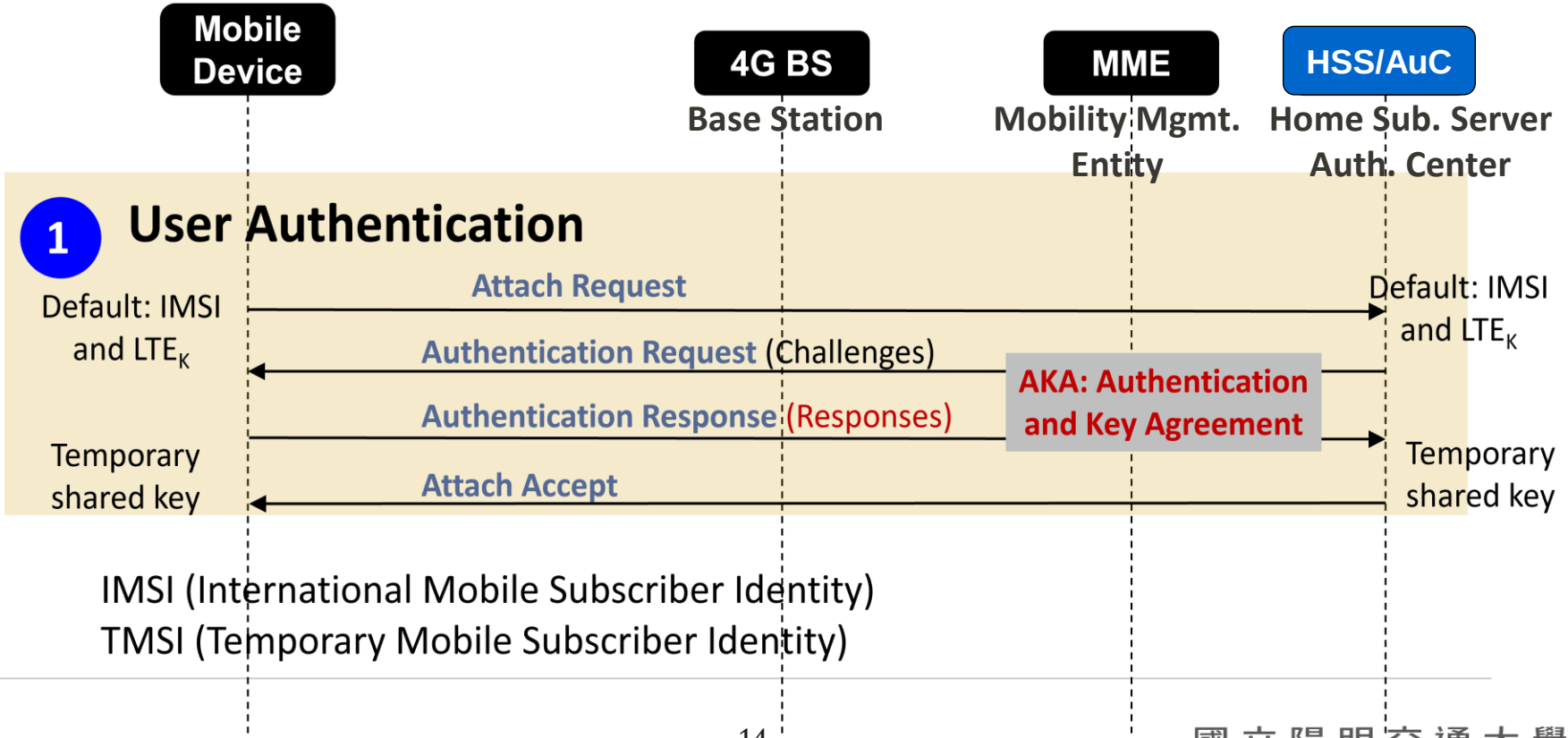
5G Security in 3GPP R15

- Security for vulnerability resolution from legacy security
  - **Subscriber ID privacy**: ID is never disclosed over the air
  - **Increased home control**: Home network makes final auth. decision
  - **Security edge protection proxy (SEPP)**: security between two networks

Legacy 4G Security

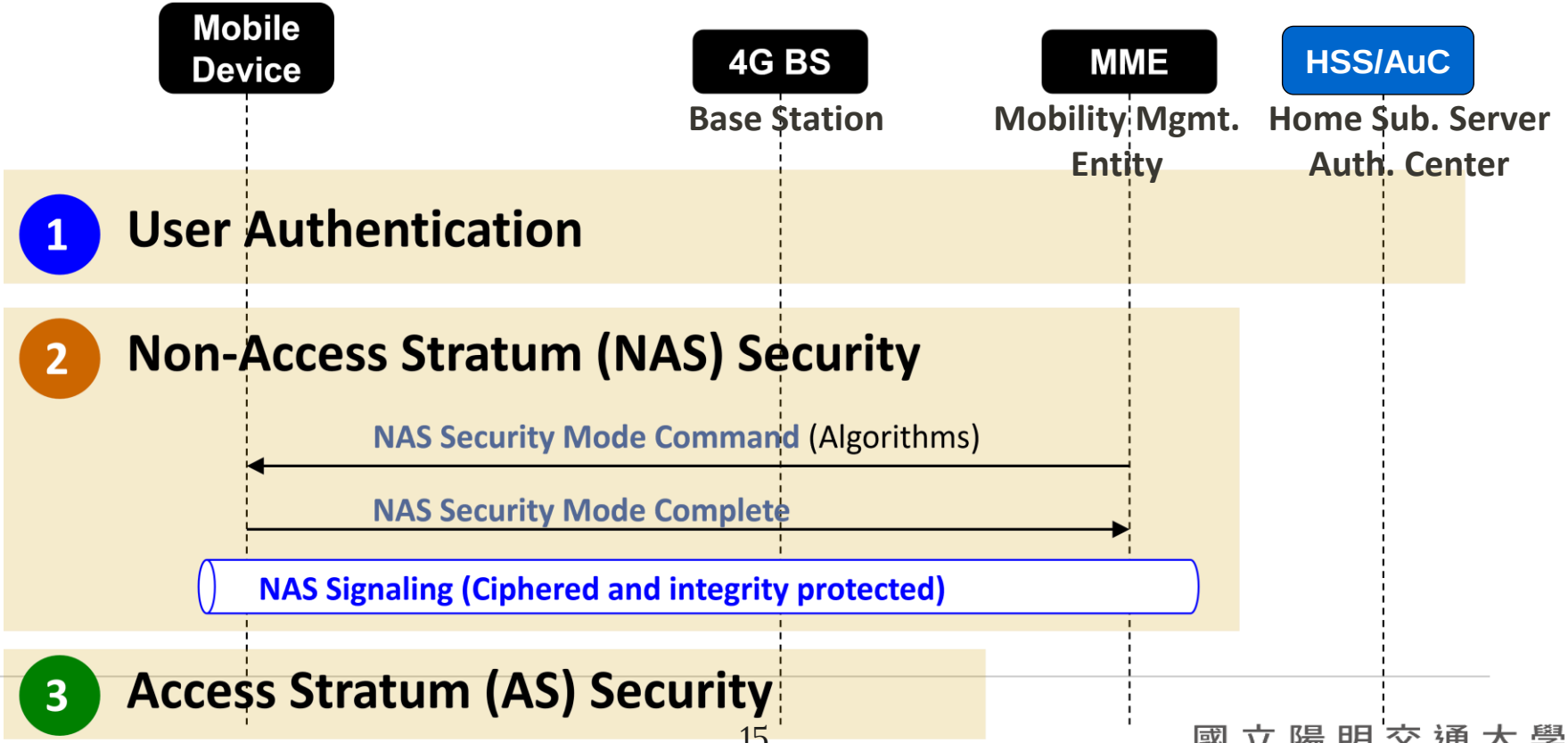


Legacy 4G Security (Cont.)

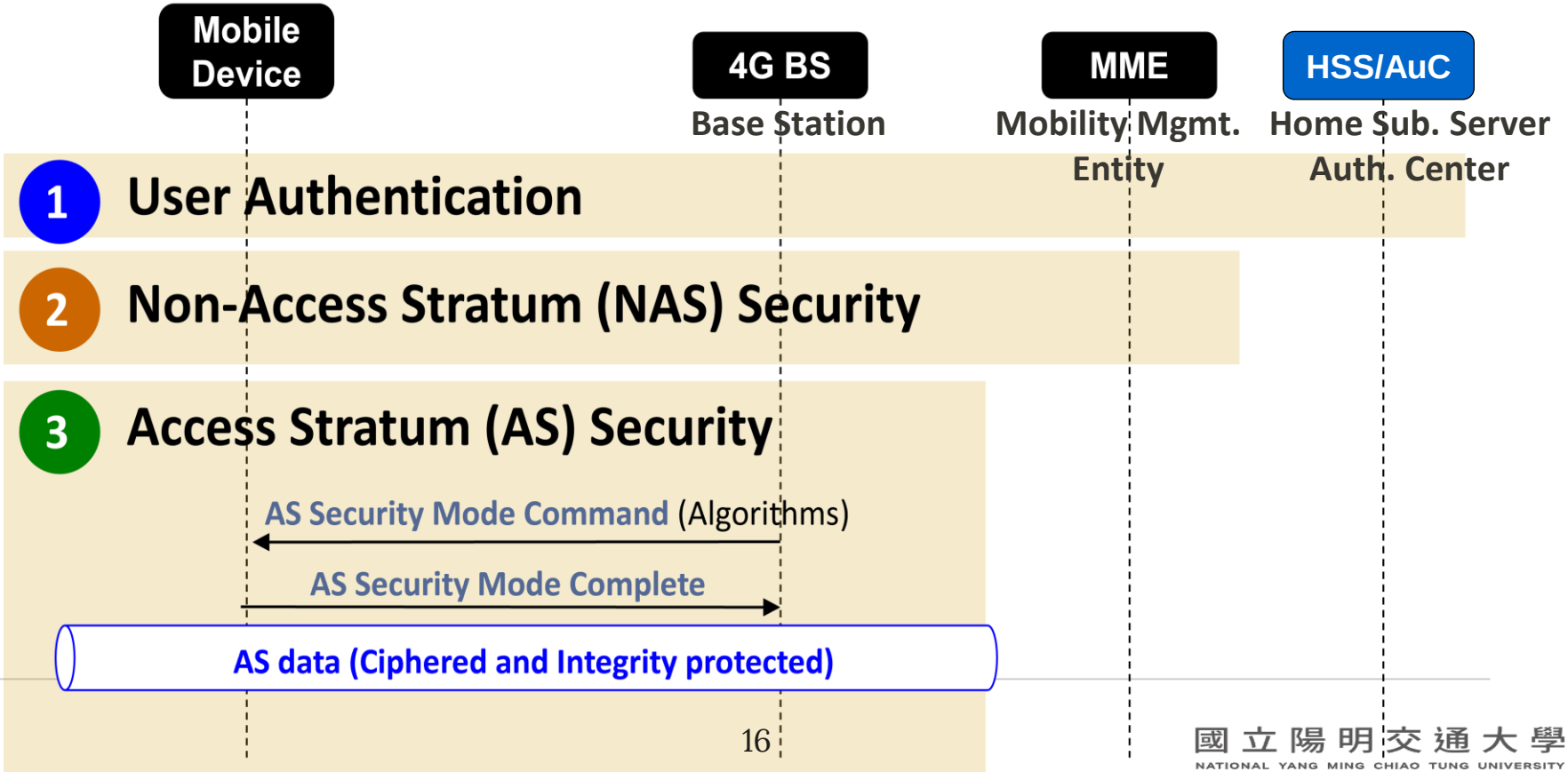


IMSI (International Mobile Subscriber Identity)
TMSI (Temporary Mobile Subscriber Identity)

Legacy 4G Security (Cont.)

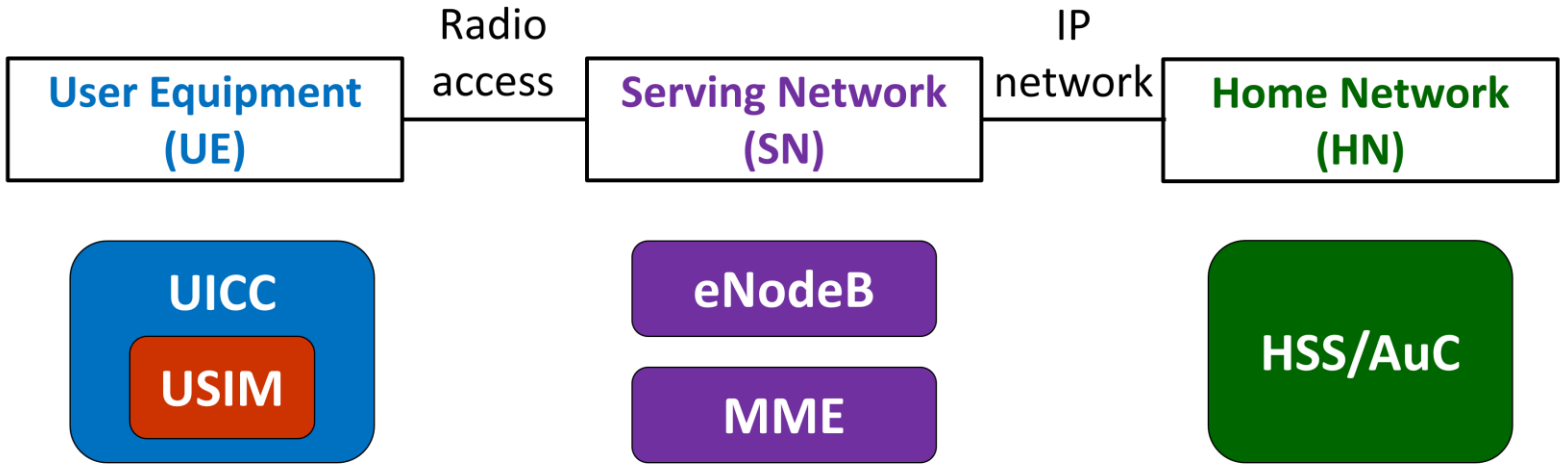


Legacy 4G Security (Cont.)



4G Authentication Framework

- **EPS-AKA**: EPS-Authentication and Key Agreement

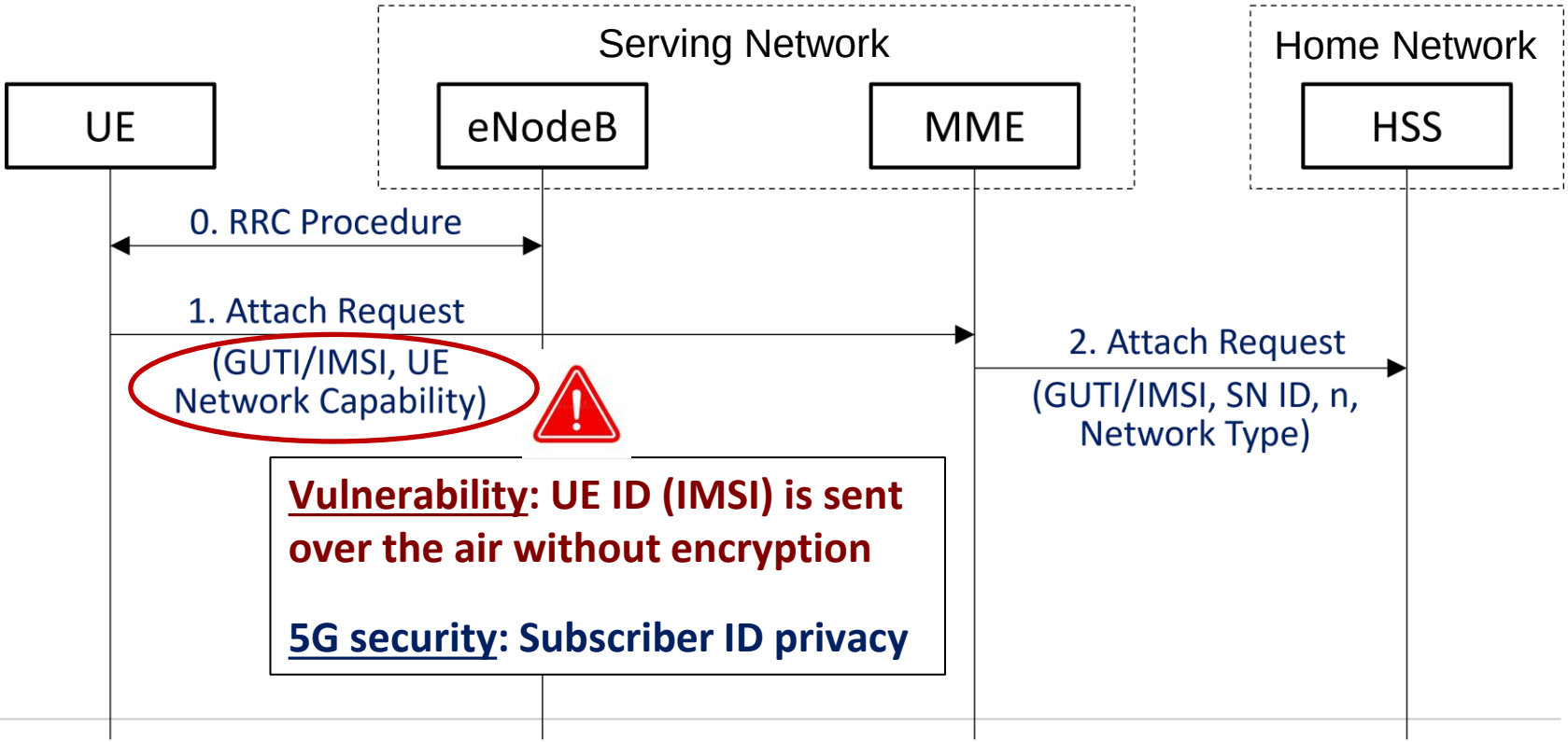


UICC (Universal Integrated Circuit Card)
USIM (Universal Subscriber Identity Module)
- storing a cryptographic key shared with the HN

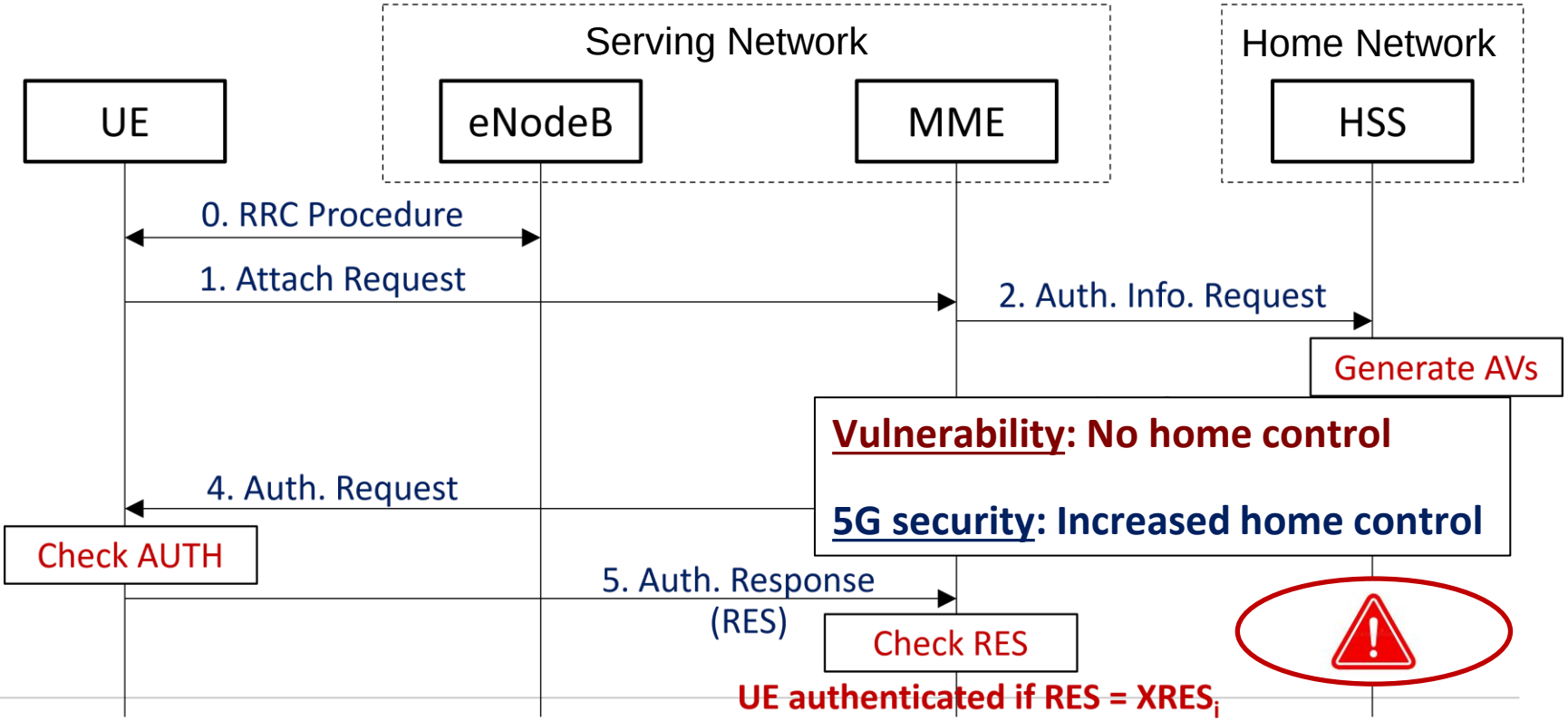
eNodeB (Evolved NodeB)
MME (Mobility Management Entity)

HSS (Home Subscriber Server)
- Storing user credentials
- Authenticating UE

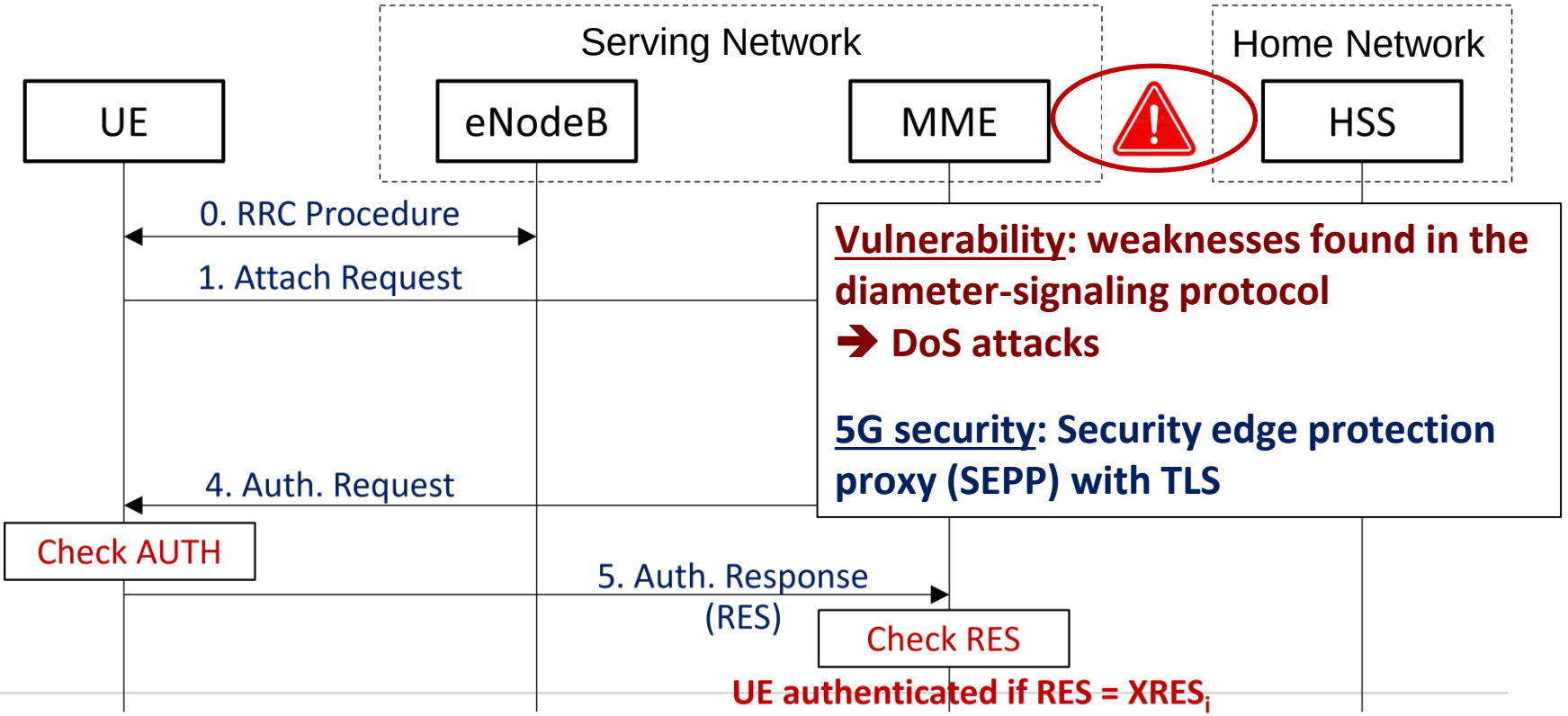
4G EPS-AKA Procedure



4G EPS-AKA Procedure (cont.)



4G EPS-AKA Procedure (cont.)



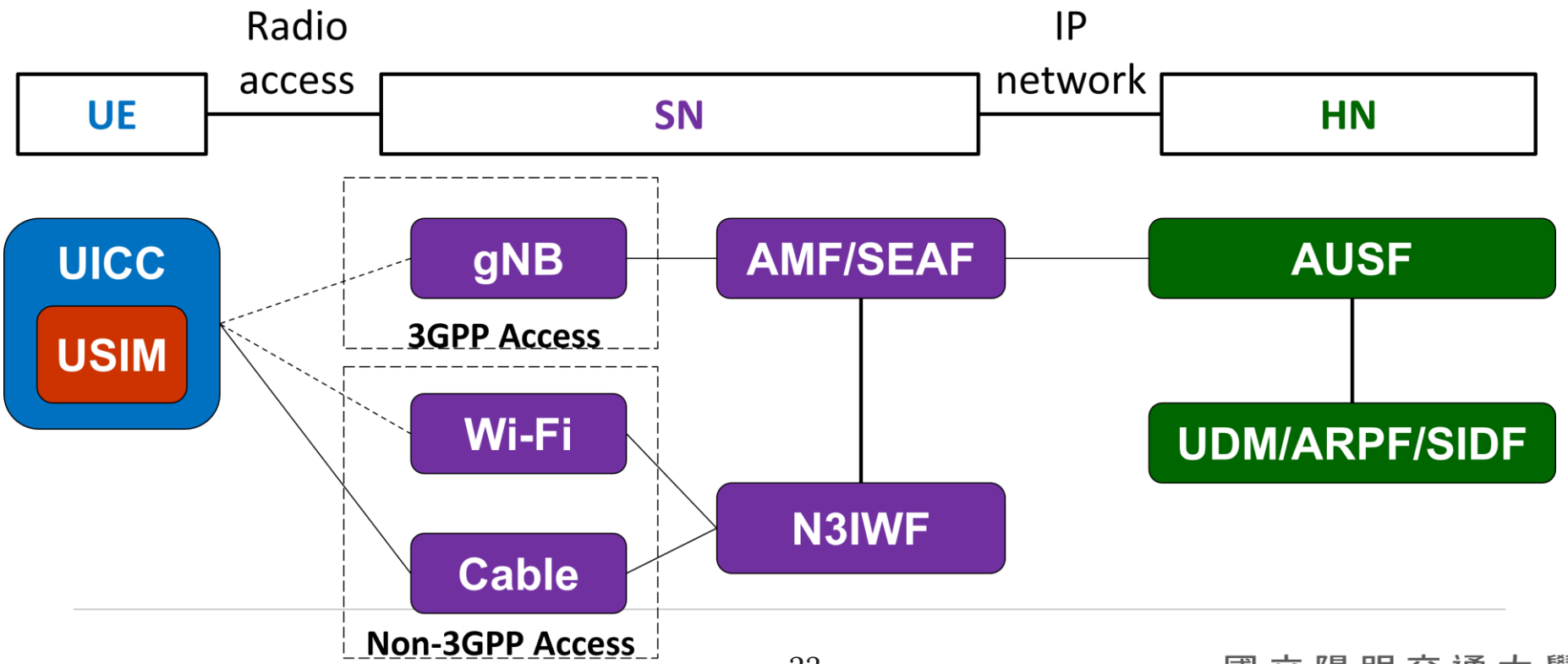
5G Security in 3GPP R15

- Security for vulnerability resolution from legacy security
  - **Subscriber ID privacy**: ID is never disclosed over the air
  - **Increased home control**: Home network makes final auth. decision
  - **Security edge protection proxy (SEPP)**: security between two networks
- Security for new architecture and functions
  - **Unified authentication framework**: 3GPP and non-3GPP access networks
  - **Service based architecture (SBA) security**

5G Unified Auth. Framework

- Three authentication methods
  - **5G-AKA** & **EAP-AKA'**
    - Trust model: shared symmetric key
  - **EAP-TLS**
    - Limited use cases: private networks and IoT environments
    - Trust model: public key certificate
- Why EAP (Extensible Authentication Protocol)?
  - Allowing the use of different types of credentials besides the ones commonly used in mobile networks

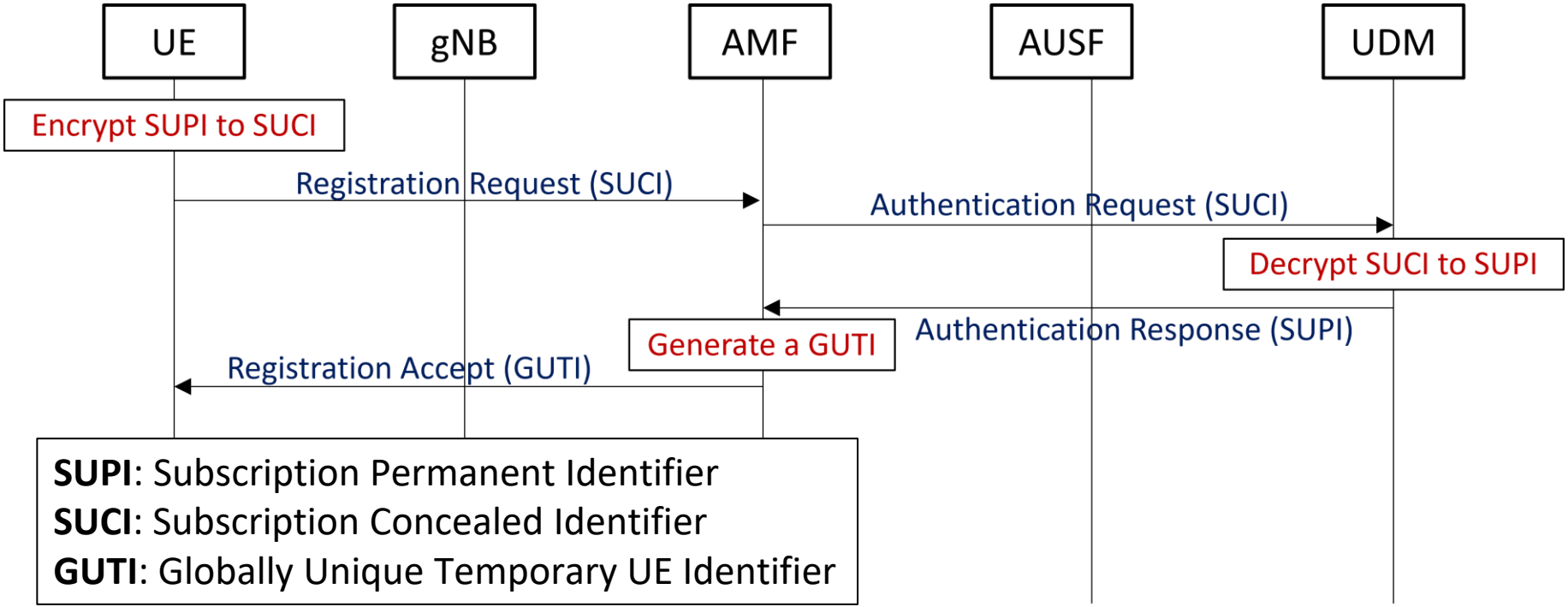
5G Unified Auth. Framework



5G Subscriber ID Privacy

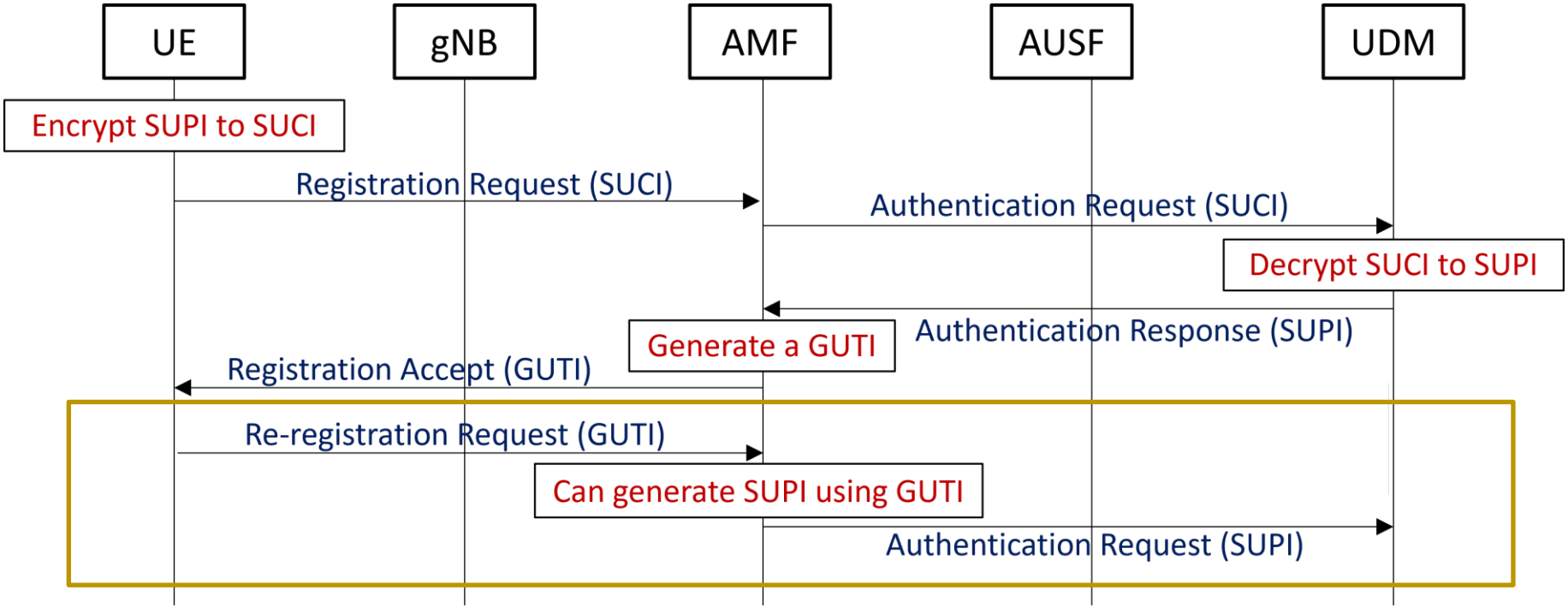
- **SUPI**: Subscription Permanent Identifier
- **SUCI**: Subscription Concealed Identifier
- **GUTI**: Globally Unique Temporary UE Identifier

5G Subscriber ID Privacy

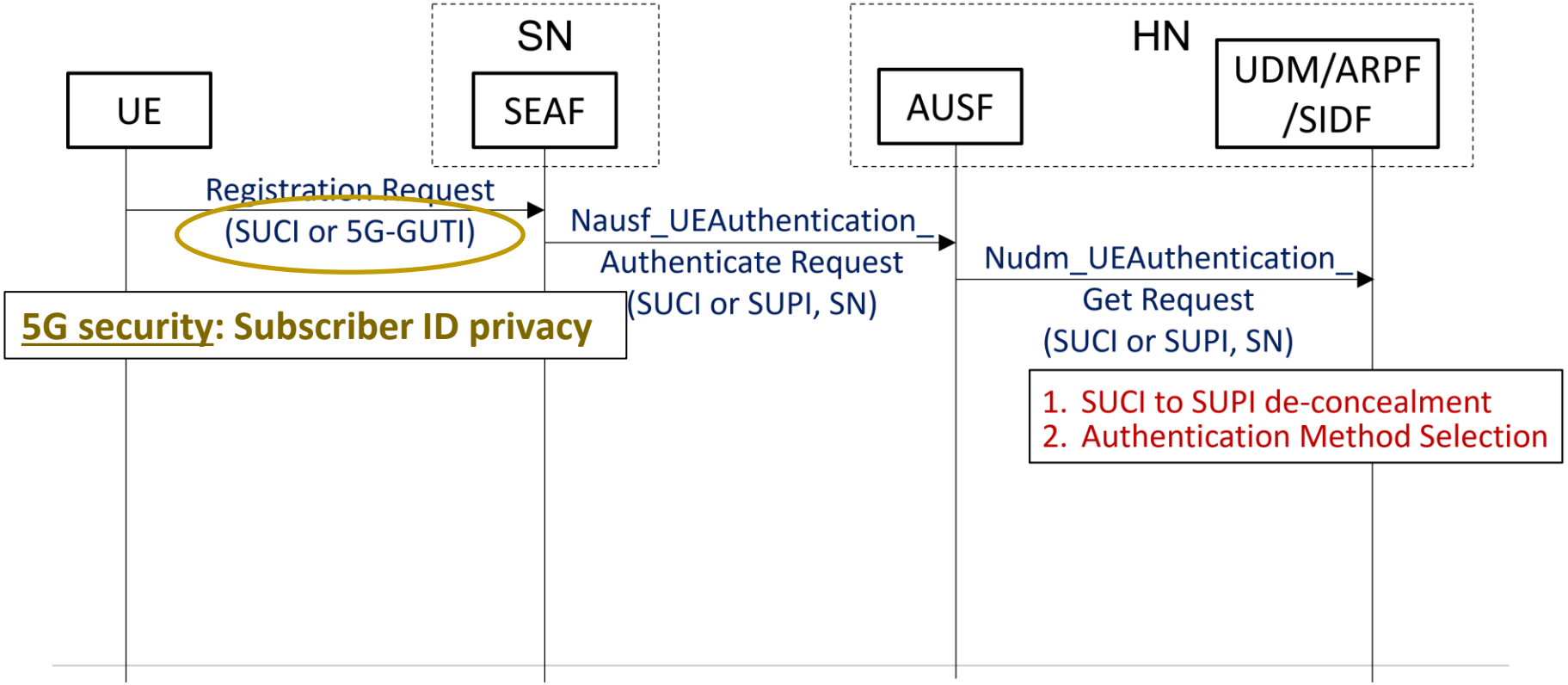


SUPI: Subscription Permanent Identifier
SUCI: Subscription Concealed Identifier
GUTI: Globally Unique Temporary UE Identifier

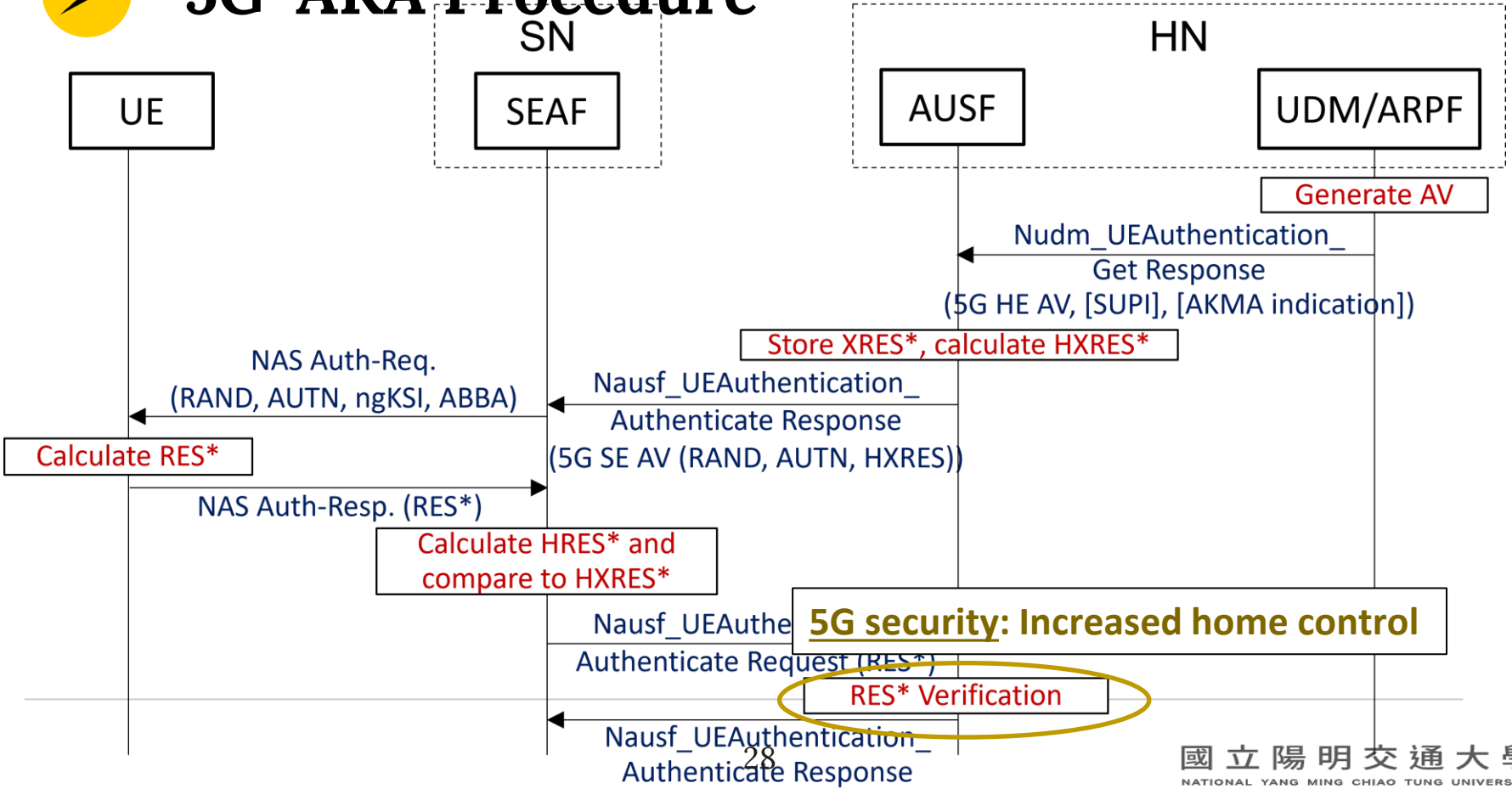
5G Subscriber ID Privacy



5G-AKA Procedure



5G-AKA Procedure



5G Security in 3GPP R15

- Security for vulnerability resolution from legacy security
  - **Subscriber ID privacy**: ID is never disclosed over the air
  - **Increased home control**: Home network makes final auth. decision
  - **Security edge protection proxy (SEPP)**: security between two networks

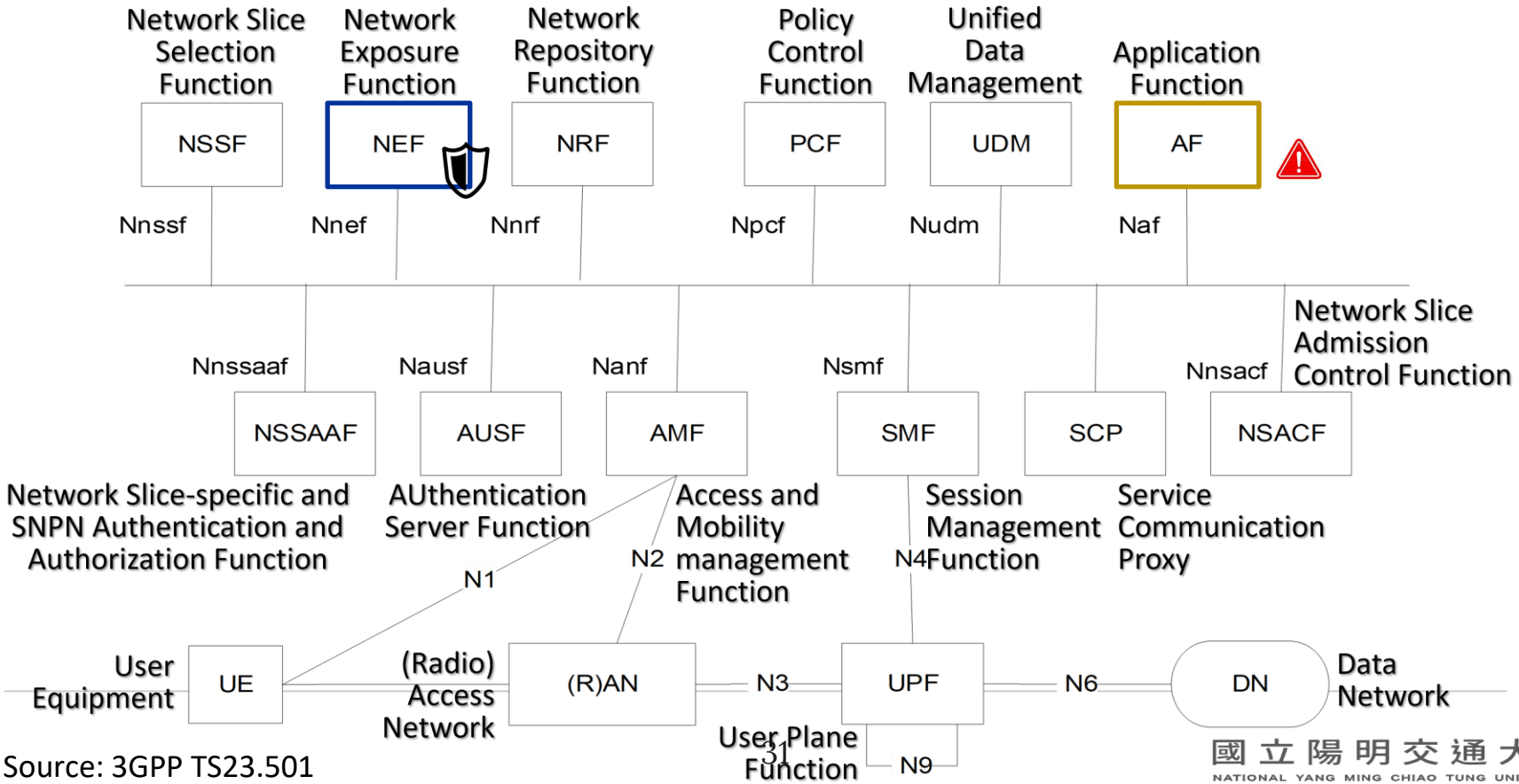
- Security for new architecture and functions
  - **Unified authentication framework**: 3GPP and non-3GPP access networks
  - **Service based architecture (SBA) security**

5G Security in 3GPP R15

- Security for vulnerability resolution from legacy security
  - **Subscriber ID privacy**: ID is never disclosed over the air
  - **Increased home control**: Home network makes final auth. decision
  - **Security edge protection proxy (SEPP)**: security between two networks

- Security for new architecture and functions
  - **Unified authentication framework**: 3GPP and non-3GPP access networks
  - **Service based architecture (SBA) security**

5G SBA (Service-based Architecture)



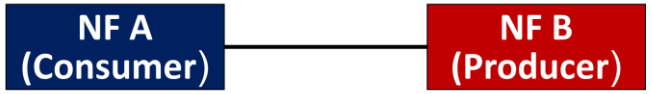
Source: 3GPP TS23.501

Why 5G SBA?

- **Updating production network**: loosely-coupled services
- **Extensibility**: light-weighted service-based interface
- **Modularity and Reusability**: easily invoked by other services
- **Openness**: easily exposed to external users

5G SBA: NFs Security

- Direct communication
  - Transport-layer protection (e.g., TLS)
  - Token-based authorization (OAuth 2.0)



Discovery of NF B by local configuration or via NRF

- Indirection communication via SCP
  - Implicit authentication
  - Token-based authorization (OAuth 2.0)

Direct discovery or delegation of discovery to SCP

5G Security in 3GPP R16

- Security for new essential functions and services
  - Network slices
  - Non-3GPP access
  - Non-public network
  - Time Sensitive Communications (TSC) service
  - Integrated Access and Backhaul (IAB)
  - Ultra-Reliable and Low Latency Communications (URLLC) service

5G Security in 3GPP R17

- Security for edge and management functions
  - Edge computing
  - Multicast/broadcast service
  - Message service for Massive IoT (MIoT)
  - Network Data Analytics Function (NWDAF)

Certifications/Audit Enhancement

- NESAS (Network Equipment Security Assurance Scheme) jointly defined by GSMA and 3GPP
  - Security evaluation of mobile network equipment
- Benefits for vendors
  - Accreditation from the world's leading mobile industry representative body
  - Offers a uniform approach to security audits
  - Avoding fragmentation of requirements in different markets
- Benefits for operators
  - Rigorous security standard requiring a high level of vendor commitment
  - Peace of mind for appropriate security measures and practices
  - No need to spend money and time conducting individual vendor audits

Conclusion

- 5G security designs from 3GPP standard
  - (R15) Security for vulnerability resolution and new architecture/functions
  - (R16) Security for new essential functions and services
  - (R17) Security for edge and management functions
- NESAS: Security for mobile network equipment
- However, any of design flaws, implementation bugs, and operation slips may cause security issues to a system
  - Especially for new architecture/functions/services

Conclusion (cont.)

- So, more security efforts are required beyond the designs
  - Threat prevention
  - Anomaly detection
  - Attack response
  - Loss recovery

Thanks for Your Attention!

Reference

- 3GPP TS 23.501, “System architecture for the 5G System (5GS).”
- 3GPP TS 33.501, “Security architecture and procedures for 5G system.”
- 3GPP TS 33.535, “Authentication and Key Management for Applications (AKMA) based on 3GPP credentials in the 5G System (5GS).”
- 3GPP TS 33.813, “Study on security aspects of network slicing enhancement.”
- “Ericsson Mobility Report,” Ericsson, Nov. 2021
- Ana Schafer, “Enhanced Mobile Broadband – 5G Innovation for consumers?” Qualcomm developer network, 2019
- “A Comparative Introduction to 4G and 5G Authentication,” CableLabs, 2019.
- “5G Security when Roaming - Part 2,” Mpirical, 2022. [Online]. Available: https://mpirical.com/blog/5g-security-when-roaming-part-2
- IETF RFC 6749, “The OAuth 2.0 Authorization Framework.”