RSAConference2019
San Francisco | March 4–8 | Moscone Center


SESSION ID: IDY-F01

# 4G to 5G Evolution: In-Depth Security Perspective

**Dr. Anand R. Prasad**

Chief Information Security Officer
Rakuten Mobile Network
@AnandRPrasad2

# Objectives

- Introduction
- 4G security and issues
- 5G security details and virtualization considerations
- 5G security next steps
- Apply and Summary

RSAConference2019

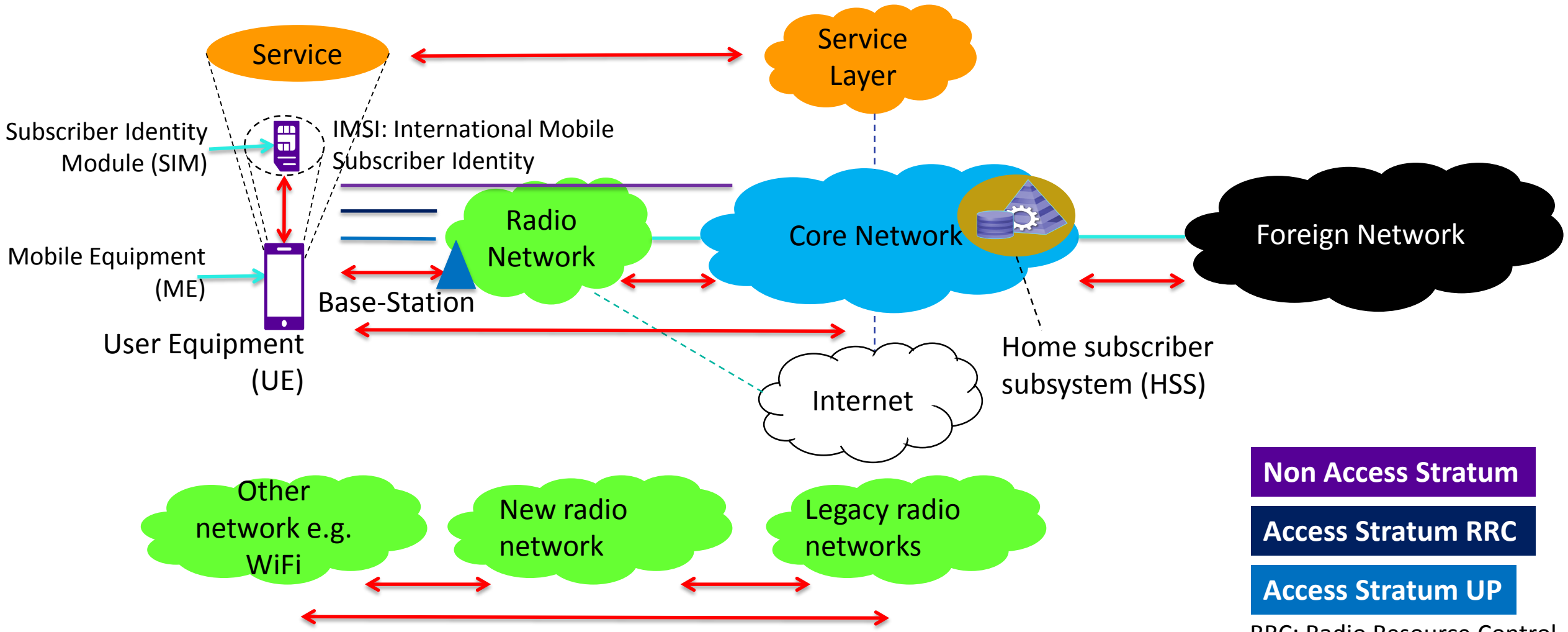
# Introduction

# 3GPP and Specifications Timeline

- 3GPP is the mobile communications specifications group
- 3GPP SA3 is the working group that develops mobile communications security specifications


| | | | | | |
|---|---|---|---|---|---|
| **Specification** | TS 33.102 | TS 33.401 & 402 | TS 33.401 | TS 33.501 | TS 33.501 + ? |
| **Release** | Release 3 | Release 8 | Release 15 | Release 15 | Release 16 |
| **Year** | 2000 | 2009 | 2017 | 2018 | 2019 |

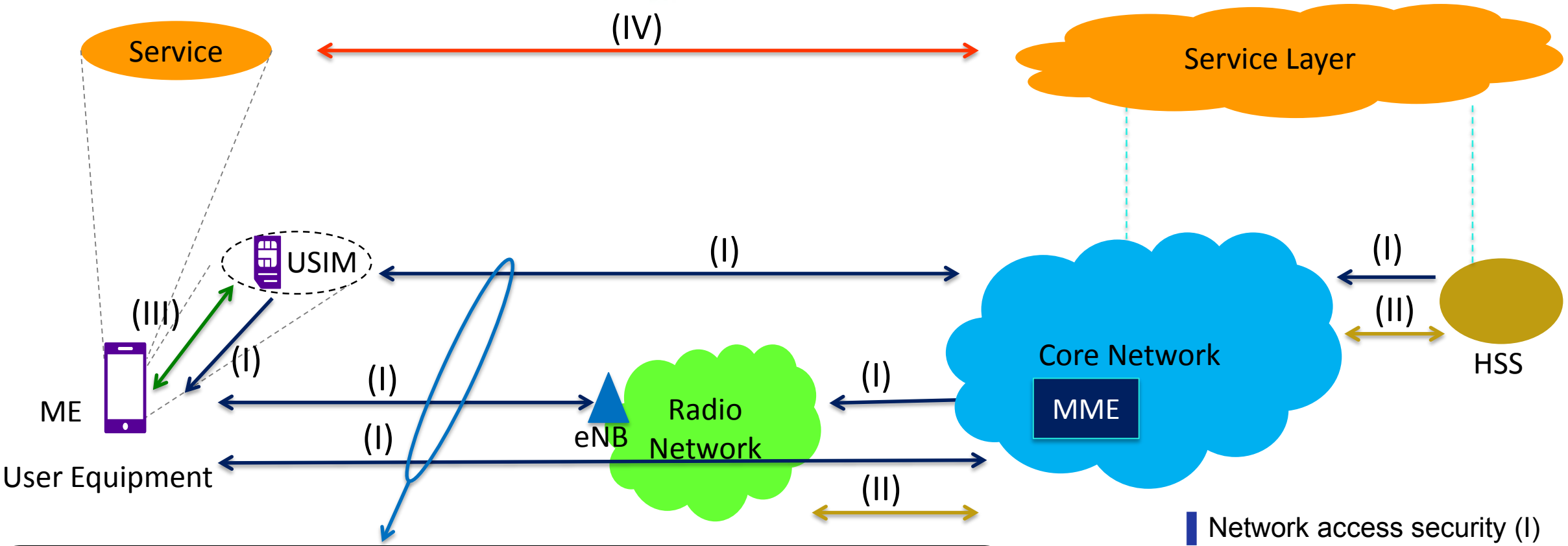
# Mobile Network Security – Introduction



RSAConference2019

# 4G Security and Issues

# 4G Security: Architecture




- Mutual authentication
- Integrity for control plane
- Confidentiality optional for both control and user planes
- Privacy provisioned by temporary identity

- Network access security (I)
- Network domain security (II)
- User domain security (III)
- Application domain security (IV)
- Visibility and configurability of security (V)

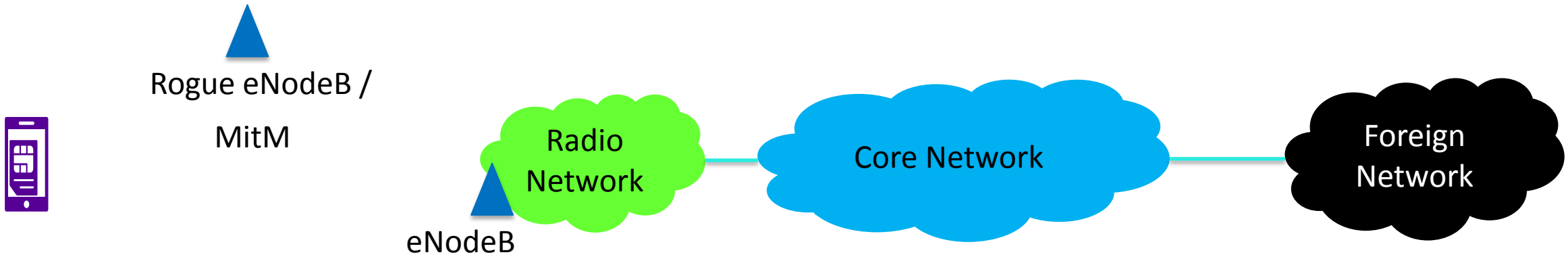


USIM: Universal Subscriber Identity Module; ME: Mobile Equipment; MME: Mobility Management Entity; HSS: Home Subscriber Subsystem

# Potential Threats on 4G

- IMSI in clear
- Temporary identity not changed
- No UP integrity protection
- Bid-down to GSM

Interconnect threats due to SS7 & Diameter

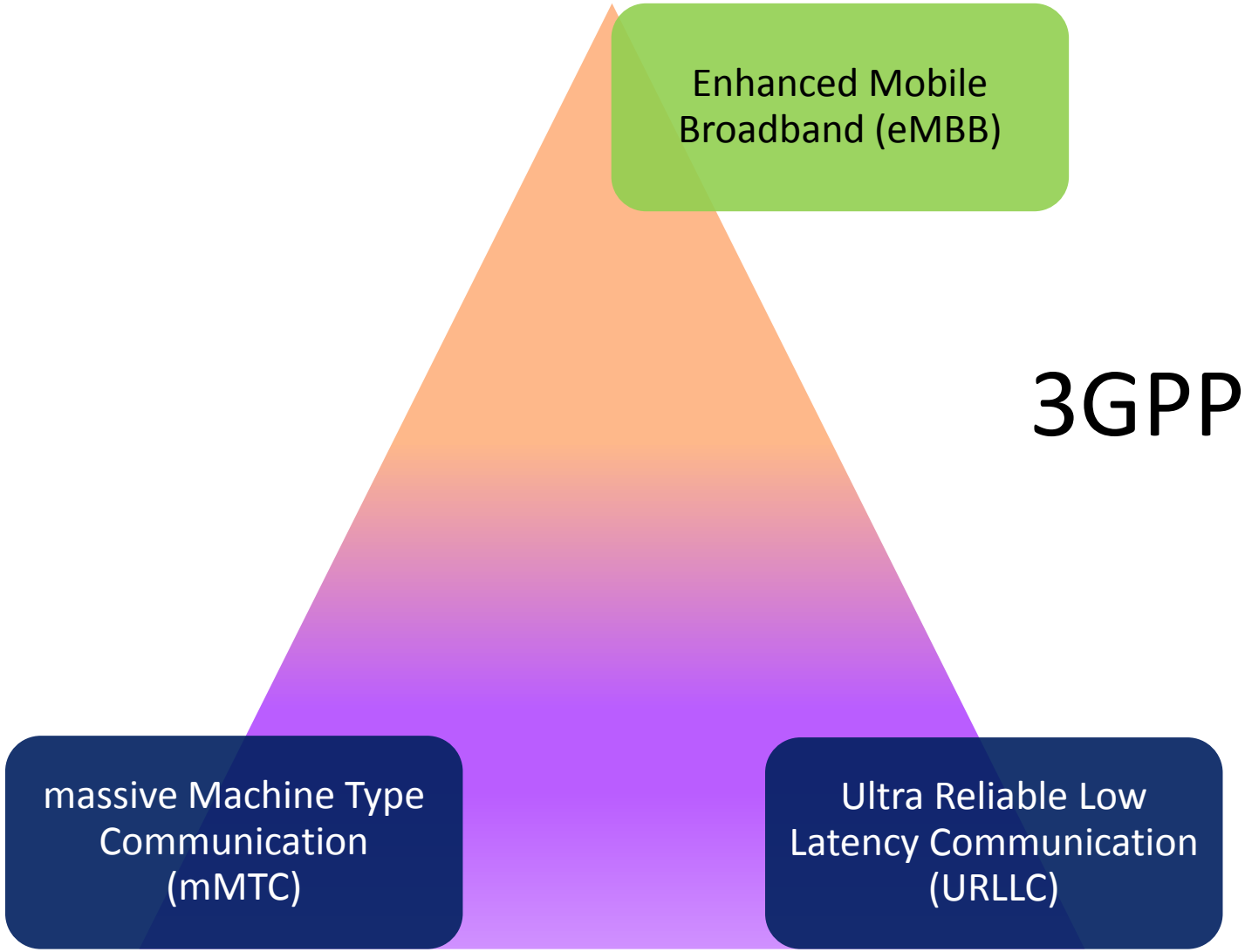


RSAConference2019

# 5G Security

# 3GPP 5G Specification Phases

Phase 1

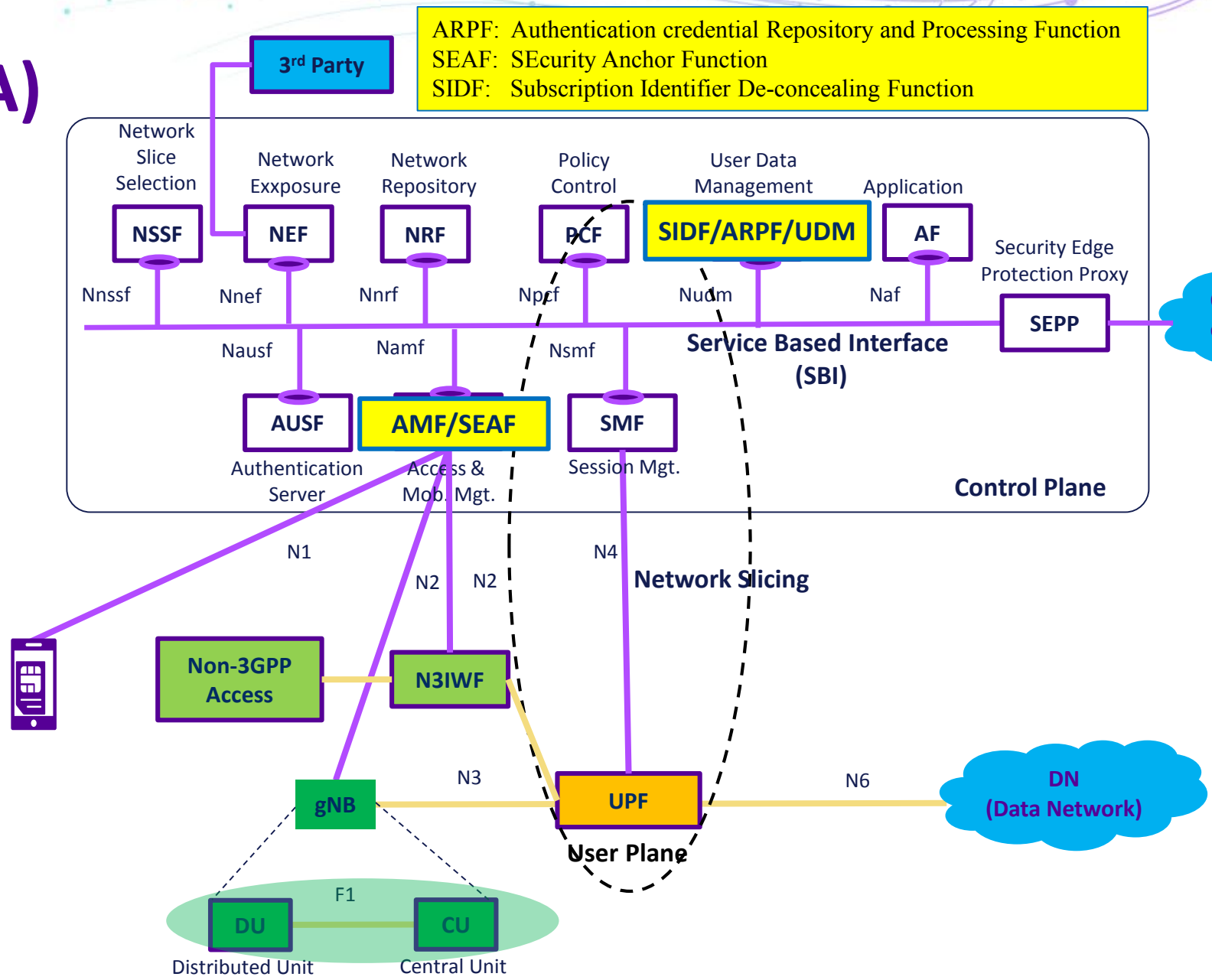



Phase 2

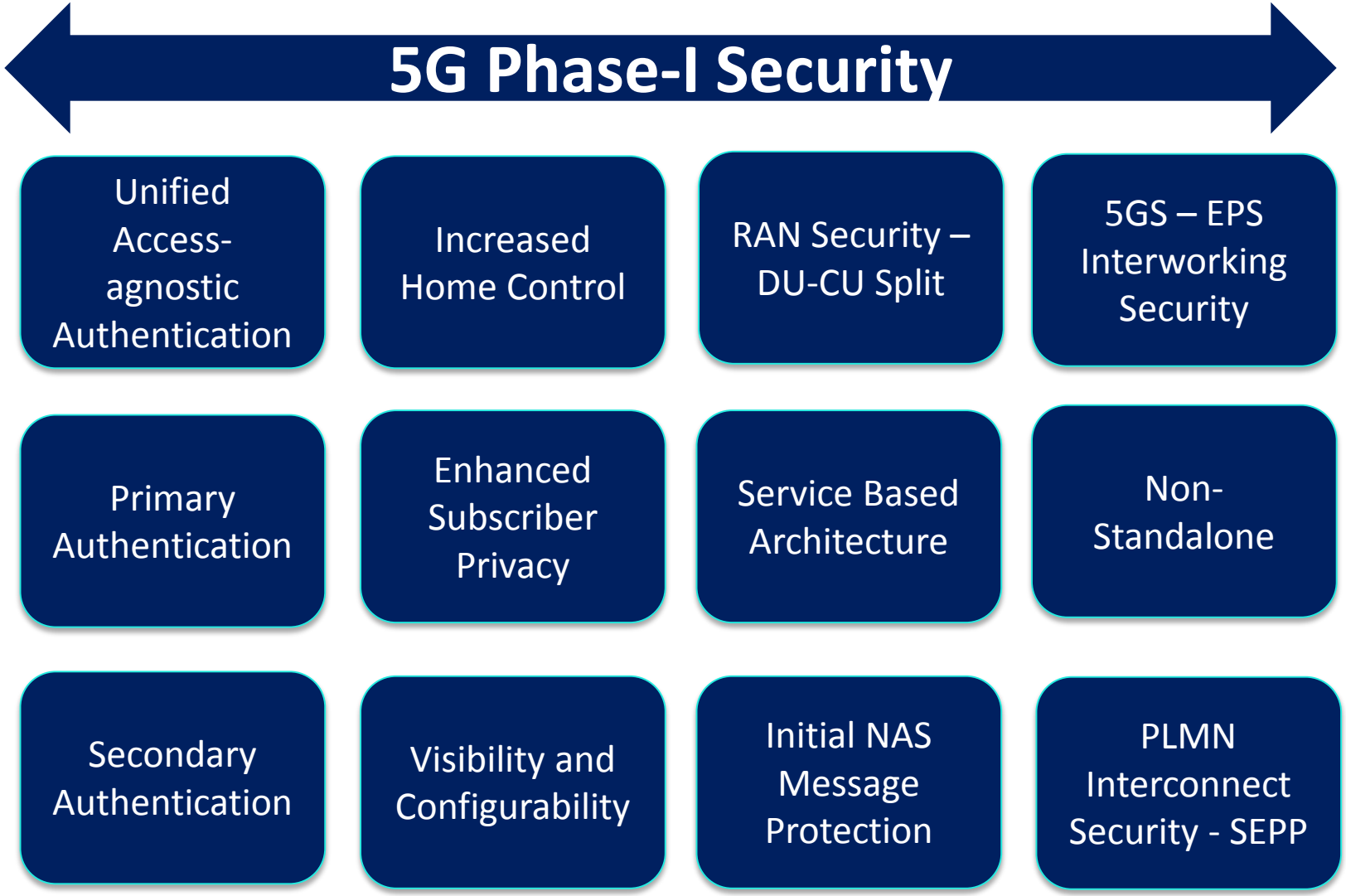
3GPP phase based 5G specification

# Service Based Architecture (SBA)

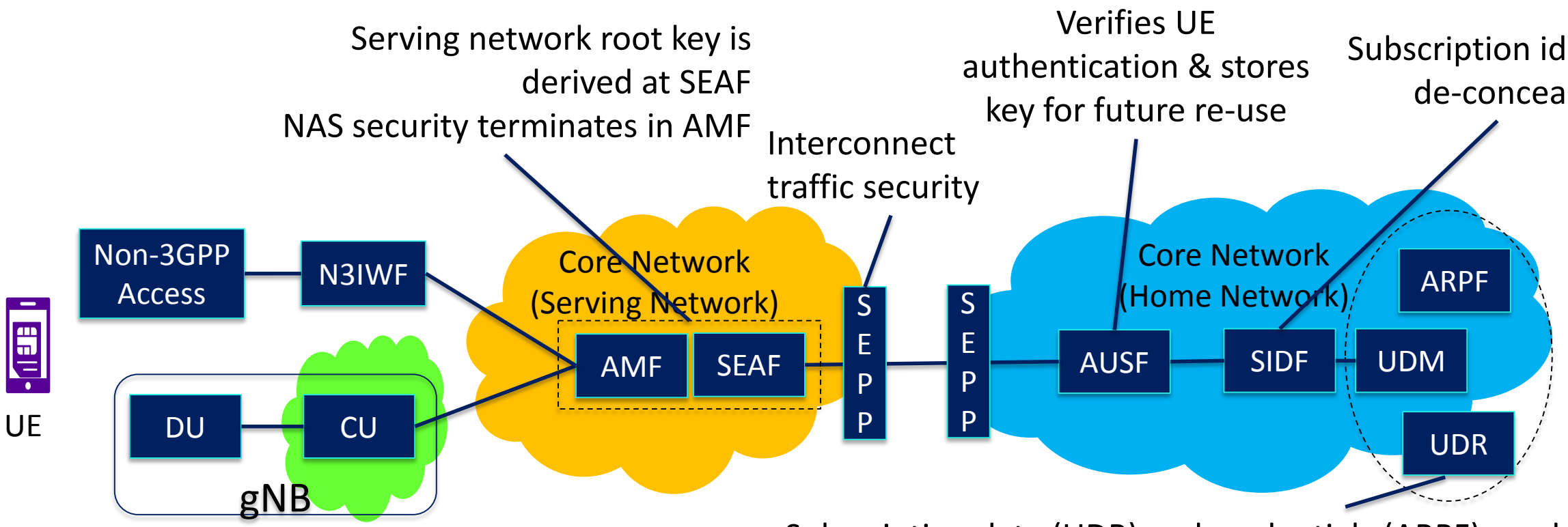
SBA and network slicing bring cloud and NFV technologies to mobile network



# Overview of 5G Phase-I Security



# Security Functions in 5G Architecture




AS terminates at CU & N3IWF
No security function is performed at DU

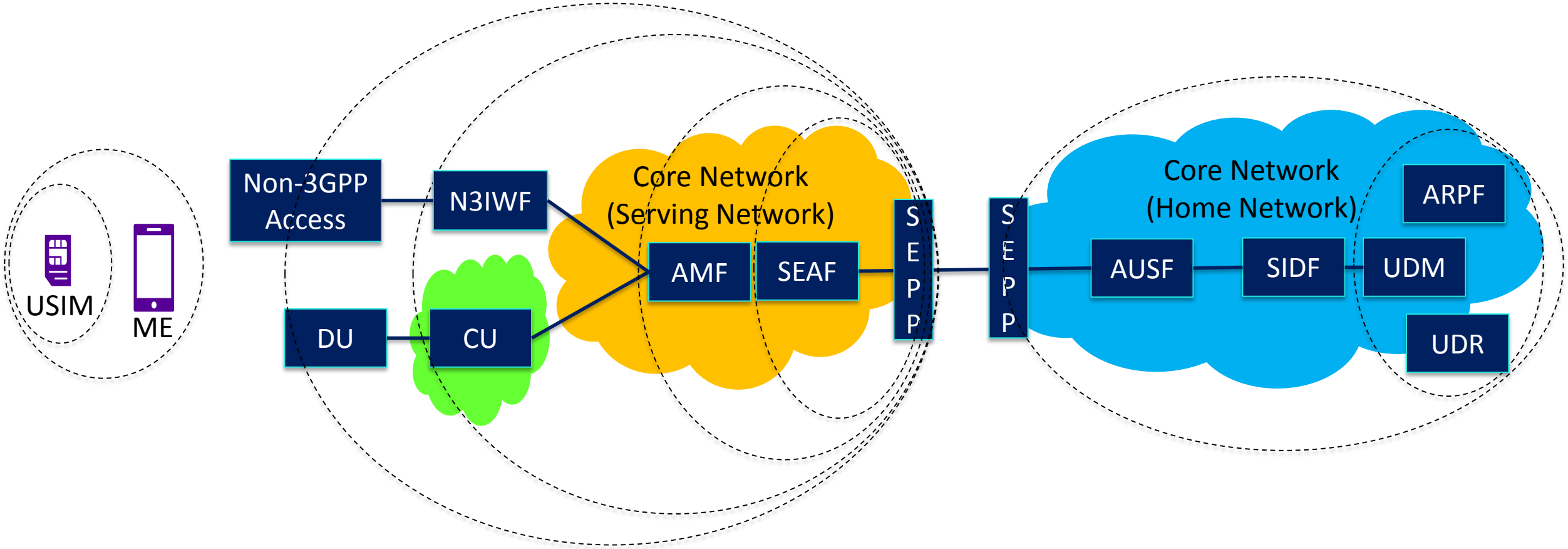
Subscription data (UDR) and credentials (ARPF) used by UDM for authentication credential generation, user identification etc.

AMF: Access Management Function
ARPF: Authentication credential Repository & Processing Function
AUSF: AUthentication Server Function
CU: Central Unit
DU: Distributed Unit
N3IWF: Non-3GPP Inter Working Function

SEAF: SEcurity Anchor Function
SEPP: SEcurity Protection Proxy
SIDF: Subscription Identifier De-concealing Function
UDM: Unified Data Management
UDR: Unified Data Repository
UE: User Equipment

Rakuten

# Trust-Model




AMF: Access Management Function
ARPF: Authentication credential Repository & Processing Function
AUSF: AUthentication Server Function
CU: Central Unit
DU: Distributed Unit
ME: Mobile Equipment
USIM: Universal Subscriber Identity Module

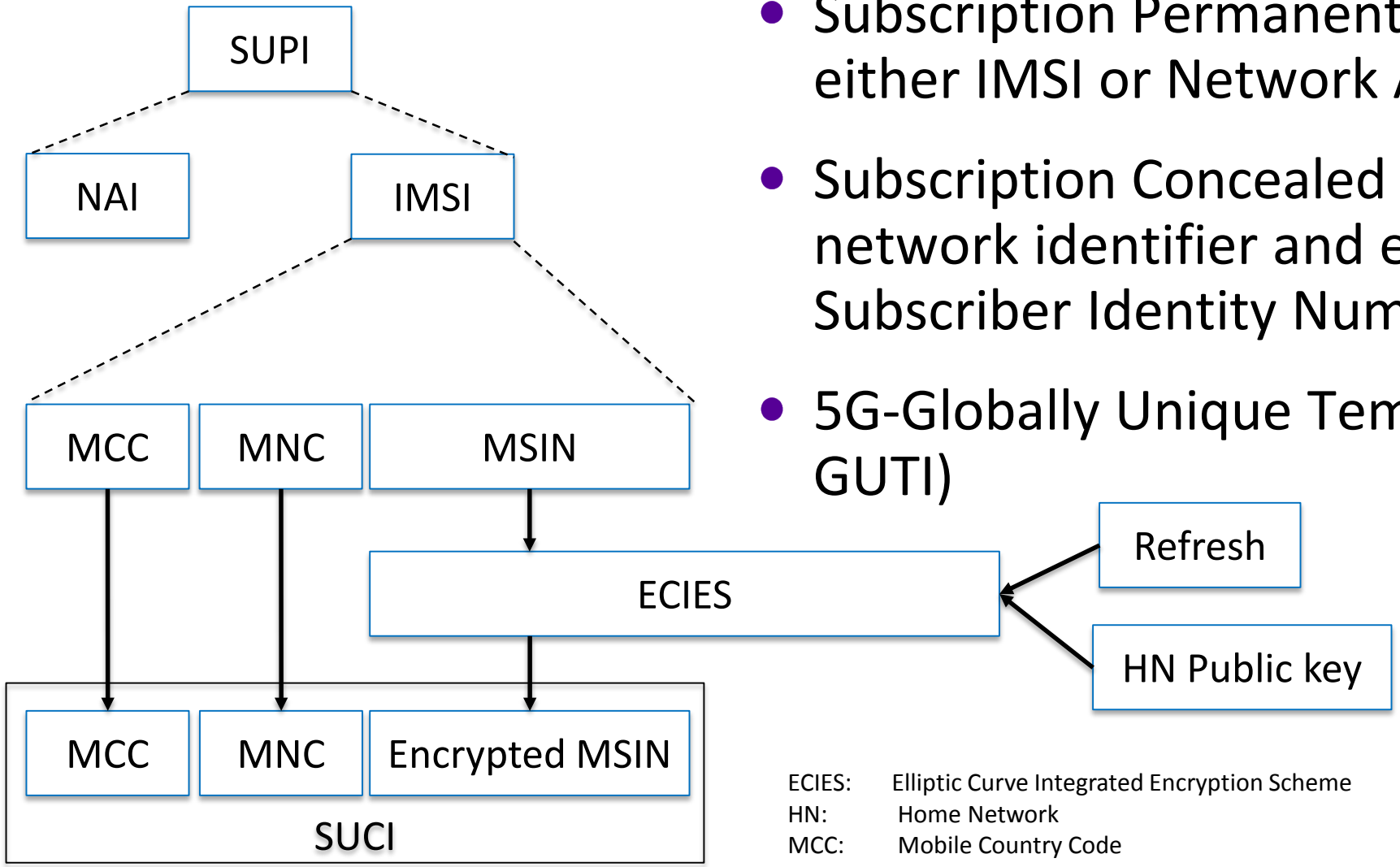
N3IWF: Non-3GPP Inter Working Function
SEAF: SEcurity Anchor Function
SEPP: SEcurity Protection Proxy
SIDF: Subscription Identifier De-concealing Function
UDM: Unified Data Management
UDR: Unified Data Repository
UE: User Equipment



Rakuten

RSAConference2019

# Identities

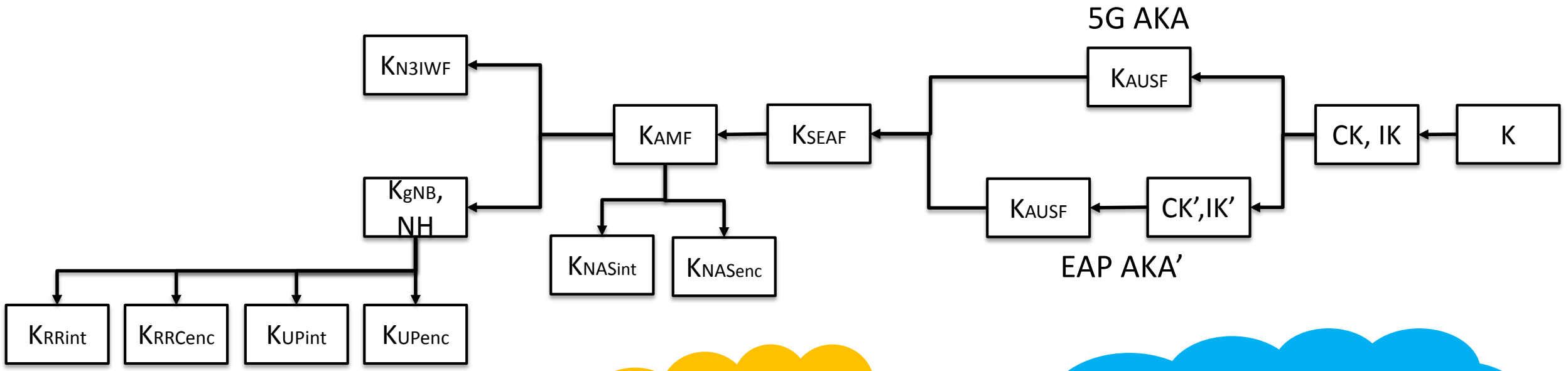


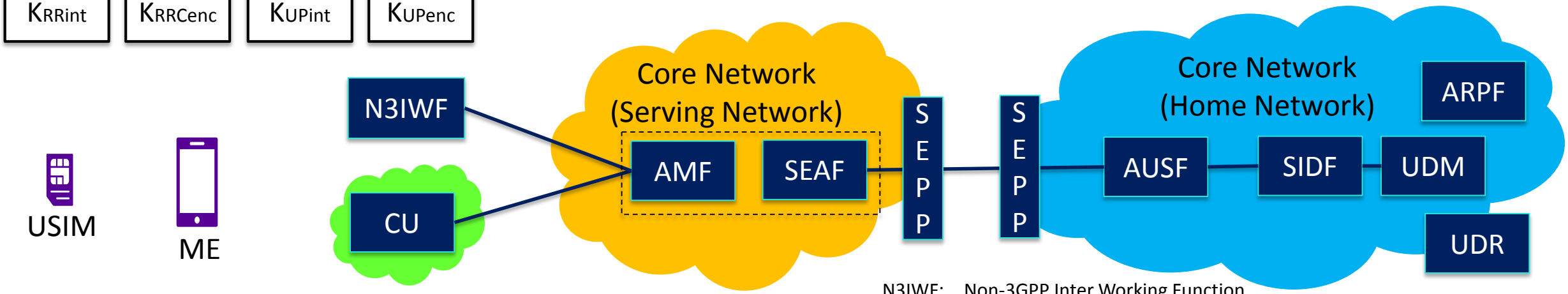

- Subscription Permanent Identifier (SUPI) can be either IMSI or Network Access Identifier (NAI)
- Subscription Concealed Identifier (SUCI) is home network identifier and encrypted Mobile Subscriber Identity Number (MSIN)
- 5G-Globally Unique Temporary UE Identity (5G-GUTI)

ECIES: Elliptic Curve Integrated Encryption Scheme
HN: Home Network
MCC: Mobile Country Code
MNC: Mobile Network Code

Rakuten

# Key Hierarchy



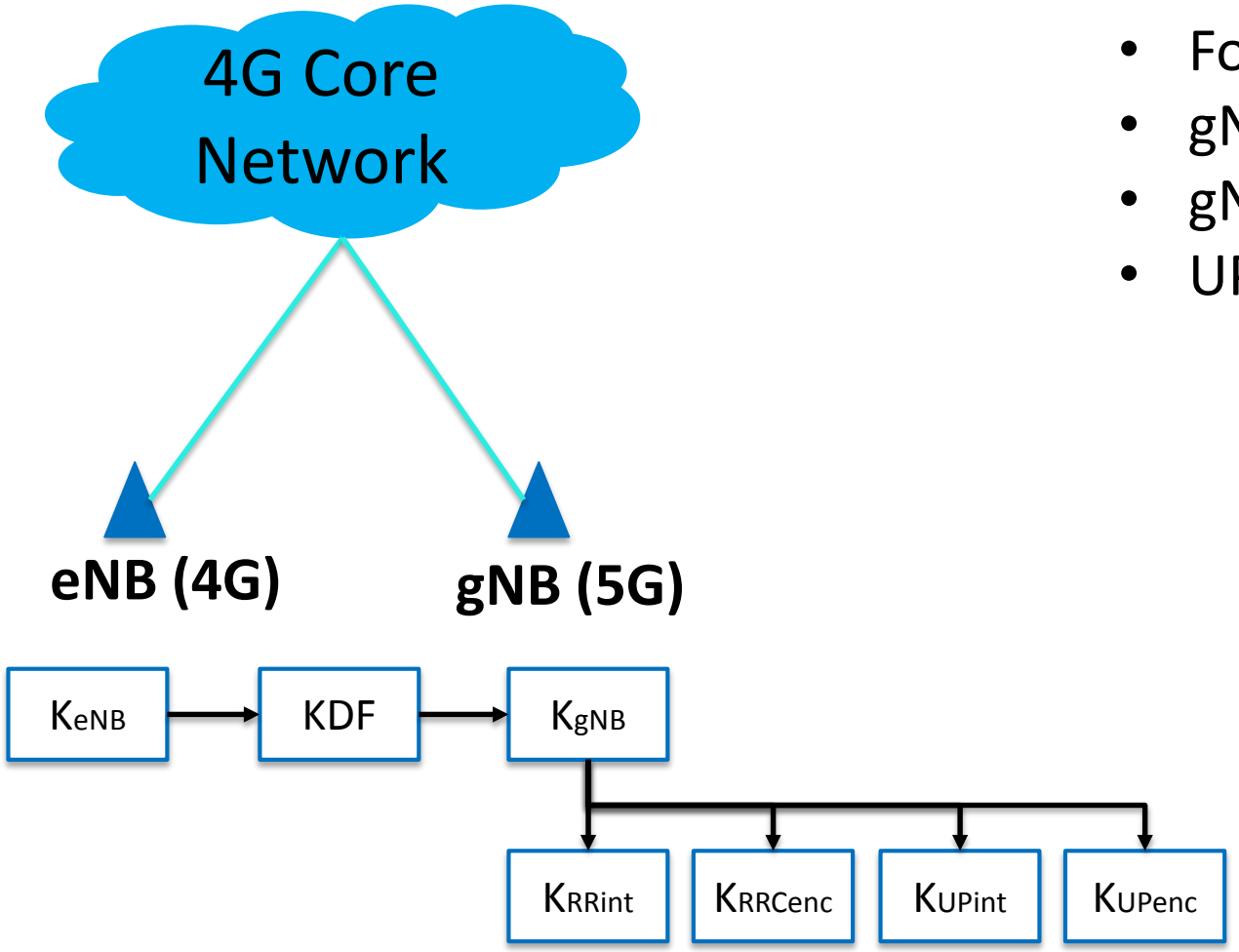

K | Rest

AMF: Access Management Function
ARPF: Authentication credential Repository & Processing Function
AUSF: AUthentication Server Function
CU: Central Unit
ME: Mobile Equipment
USIM: Universal Subscriber Identity Module

N3IWF: Non-3GPP Inter Working Function
SEAF: SEcurity Anchor Function
SEPP: SEcurity Protection Proxy
SIDF: Subscription Identifier De-concealing Function
UDM: Unified Data Management
UDR: Unified Data Repository
UE: User Equipment

Rakuten

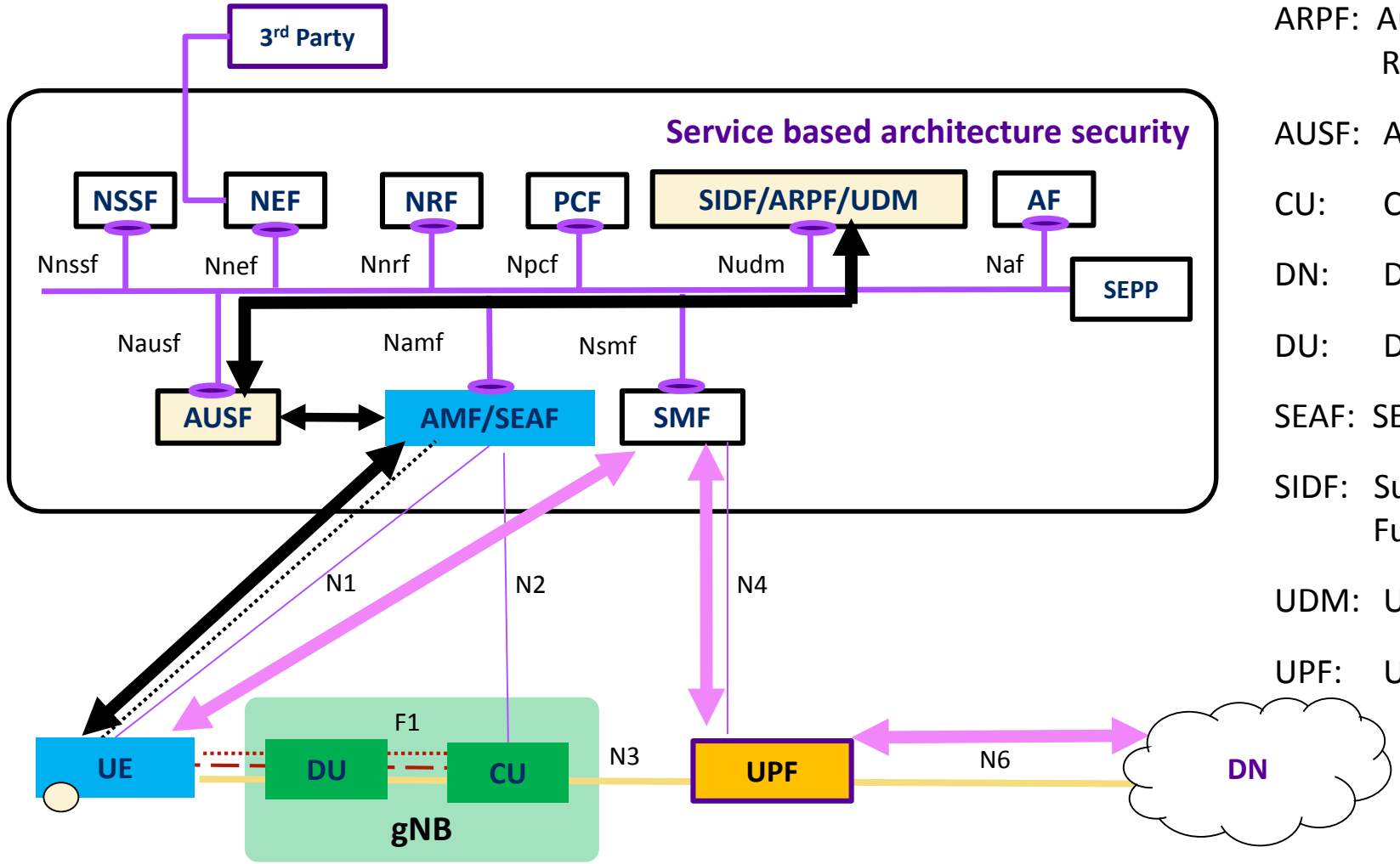
# Non-Standalone (NSA) Security




- For fast availability of 5G
- gNB connected to existing 4G core network
- gNB (5G) keys are derived from eNB (4G) key
- UP integrity protection not available

KDF: Key Derivation Function

# Security Associations




ARPF: Authentication credential Repository and Processing Function

AUSF: AUthentication Function

CU: Central Unit

DN: Data Network

DU: Distributed Unit

SEAF: SEcurity Anchor Function

SIDF: Subscription Identifier De-concealing Function

UDM: Unified Data Management

UPF: User Plane Function

Primary authentication

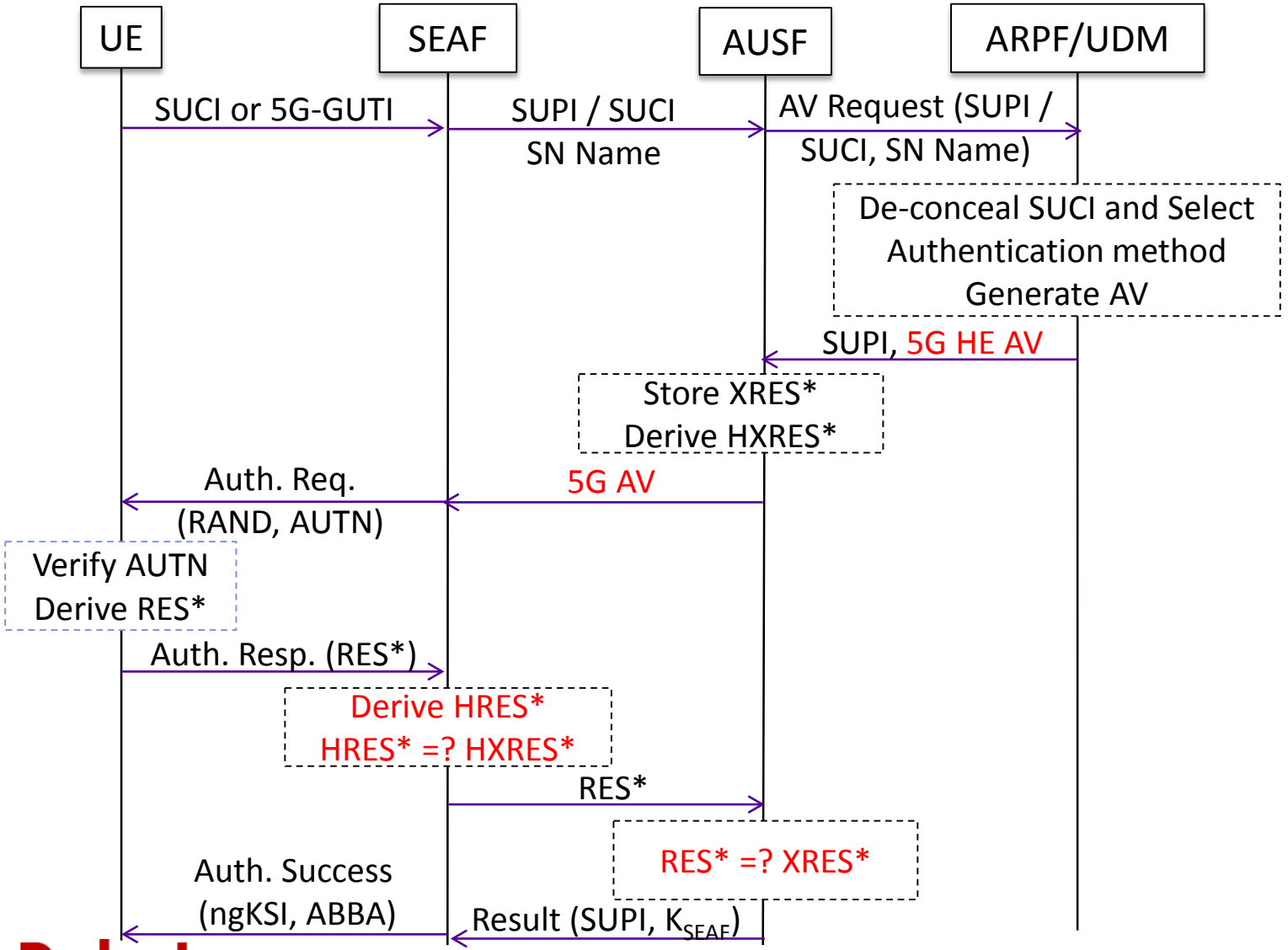
Secondary authentication

NAS Confidentiality/Integrity

RRC Confidentiality/Integrity

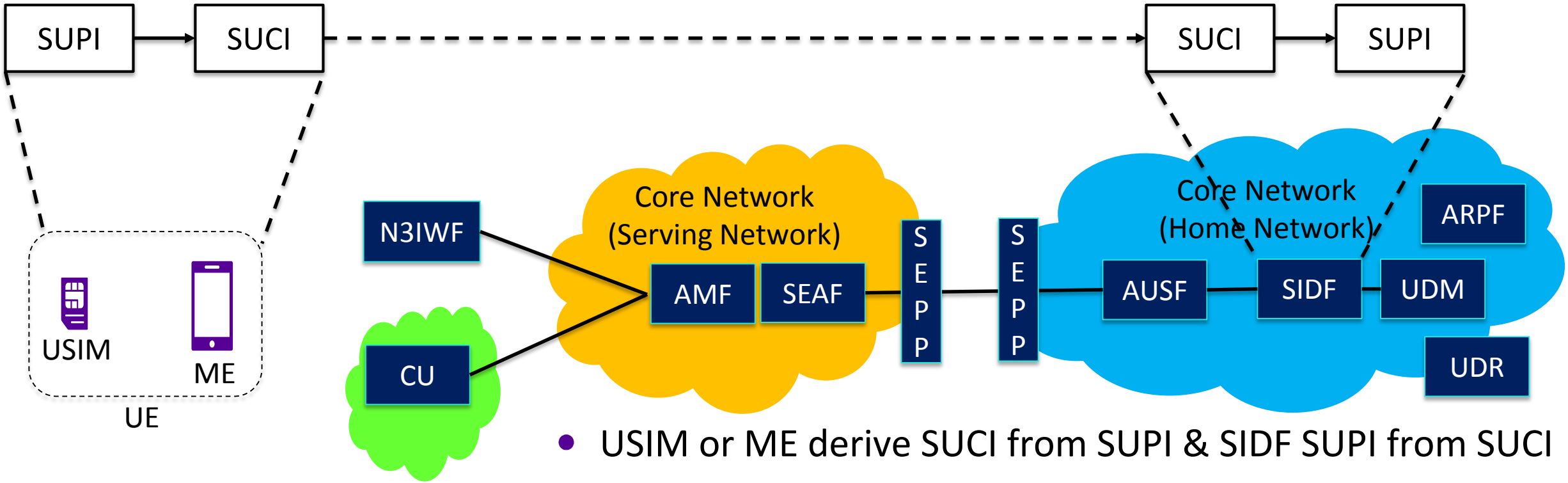
UP Confidentiality/Integrity

# Primary Authentication based on 5G AKA




- 5G Home Environment Authentication Vector (HE AV):
  (RAND, AUTN, (X)RES*, KAUSF)
  - (X)RES* = KDF (CK|IK, (X)RES)
- 5G Authentication Vector:
  (RAND, AUTN, HXRES*, KSEAF)
  - H(X)RES* = KDF (RAND, (X)RES*)
- ME derives RES* from RES & CK,IK
- $K_{SEAF}$ is bound to the serving network name (SN-name)
- ngKSI: Key Set Identifier in 5G
- ABBA: Anti-Bidding down Between Architectures parameter provides protection against bidding down of security features from higher to a lower release

# Enhanced Subscriber Privacy




- USIM or ME derive SUCI from SUPI & SIDF SUPI from SUCI
- Home Network Public Key is stored in USIM

AMF: Access Management Function
ARPF: Authentication credential Repository & Processing Function
AUSF: AUthentication Server Function
CU: Central Unit
DU: Distributed Unit
ME: Mobile Equipment
N3IWF: Non 3GPP Inter Working Function

SEAF: SEcurity Anchor Function
SEPP: SEcurity Protection Proxy
SIDF: Subscription Identifier De-concealing Function
UDM: Unified Data Management
UDR: Unified Data Repository
UE: User Equipment
USIM: Universal Subscriber Identity Module

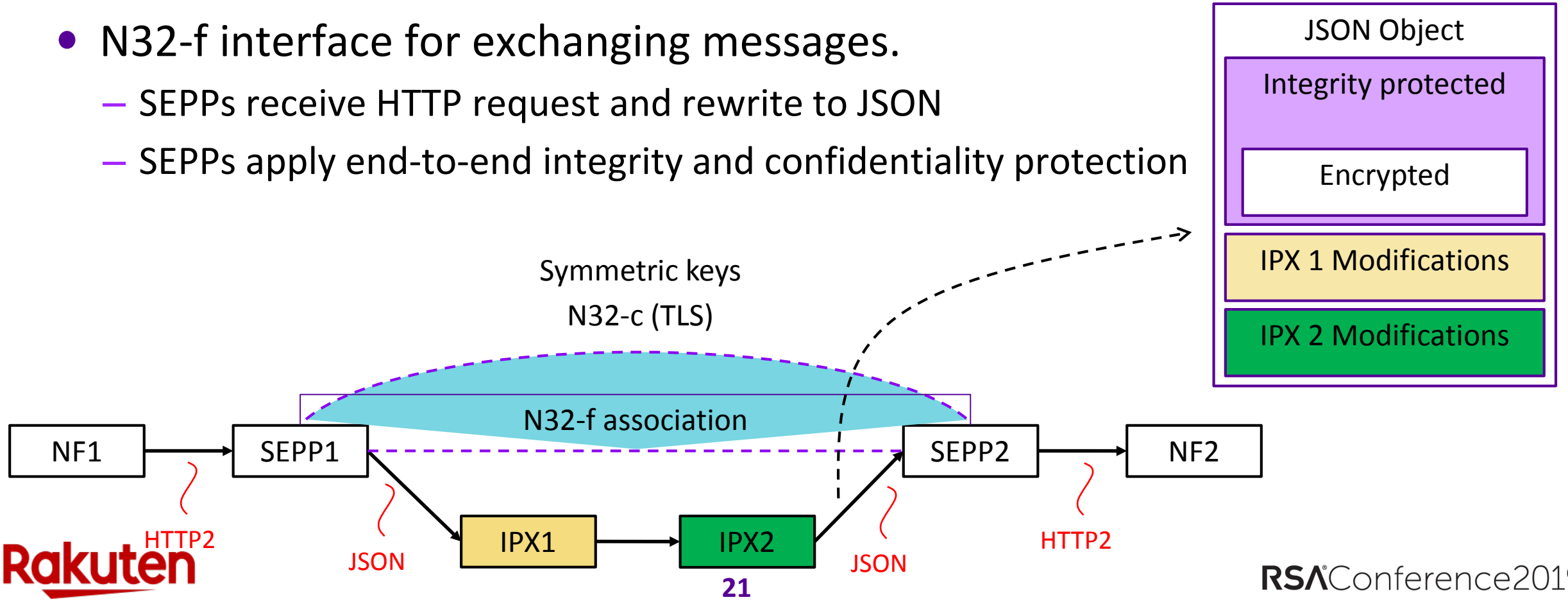


Rakuten

RSAConference2019

# Interconnect Security

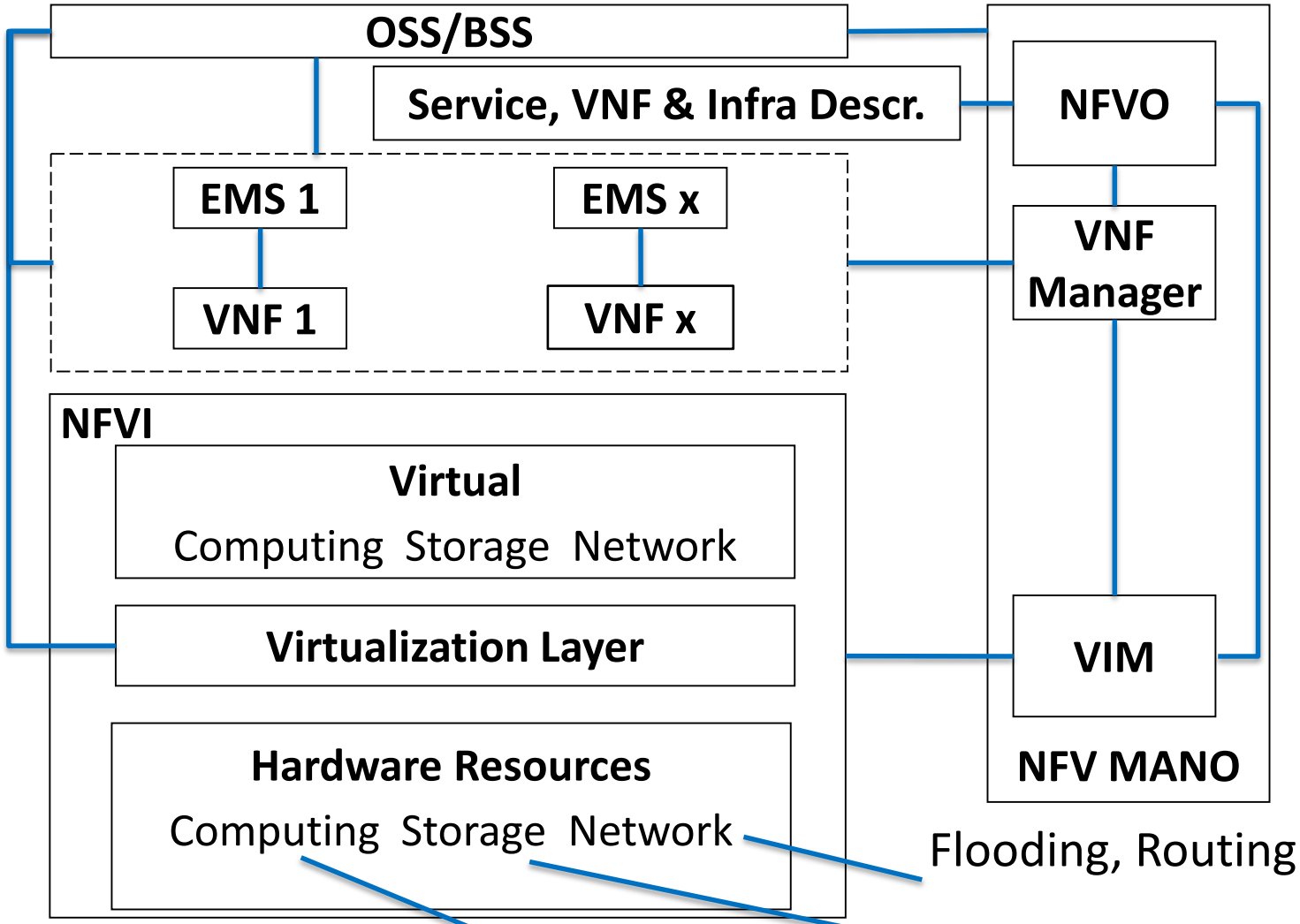
- N32-c interface for capability and policy negotiation between Security Protection Proxies (SEPPs)
- N32-f interface for exchanging messages.
  - SEPPs receive HTTP request and rewrite to JSON
  - SEPPs apply end-to-end integrity and confidentiality protection



RSAConference2019

# Virtualization Security

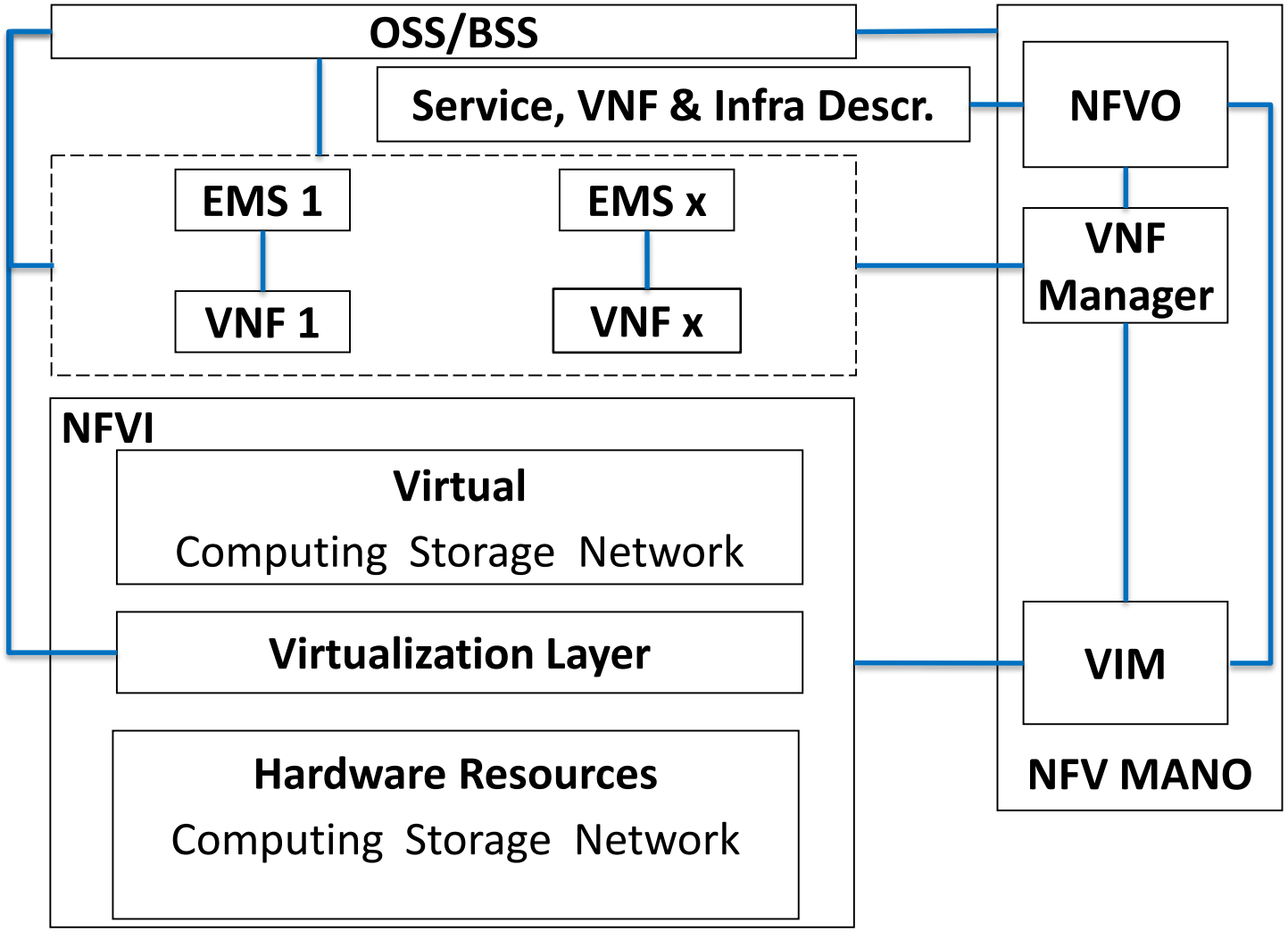
# Threats – Summary




- Data manipulation
- Privilege misuse
- Package modification
- Rogue VNF
- Malicious code or tenant
- Configuration modification
- Resource allocation issues
- Image tampering
- Catalogue information exploit
- Uploading malicious images

Rakuten

# Mitigation – Summary




- Secure boot and chain of trust
- Remote attestation
- Secure crash
- Security assurance, signing and verification of image
- VNF isolation
- Tenant and administrator isolation

RSAConference2019

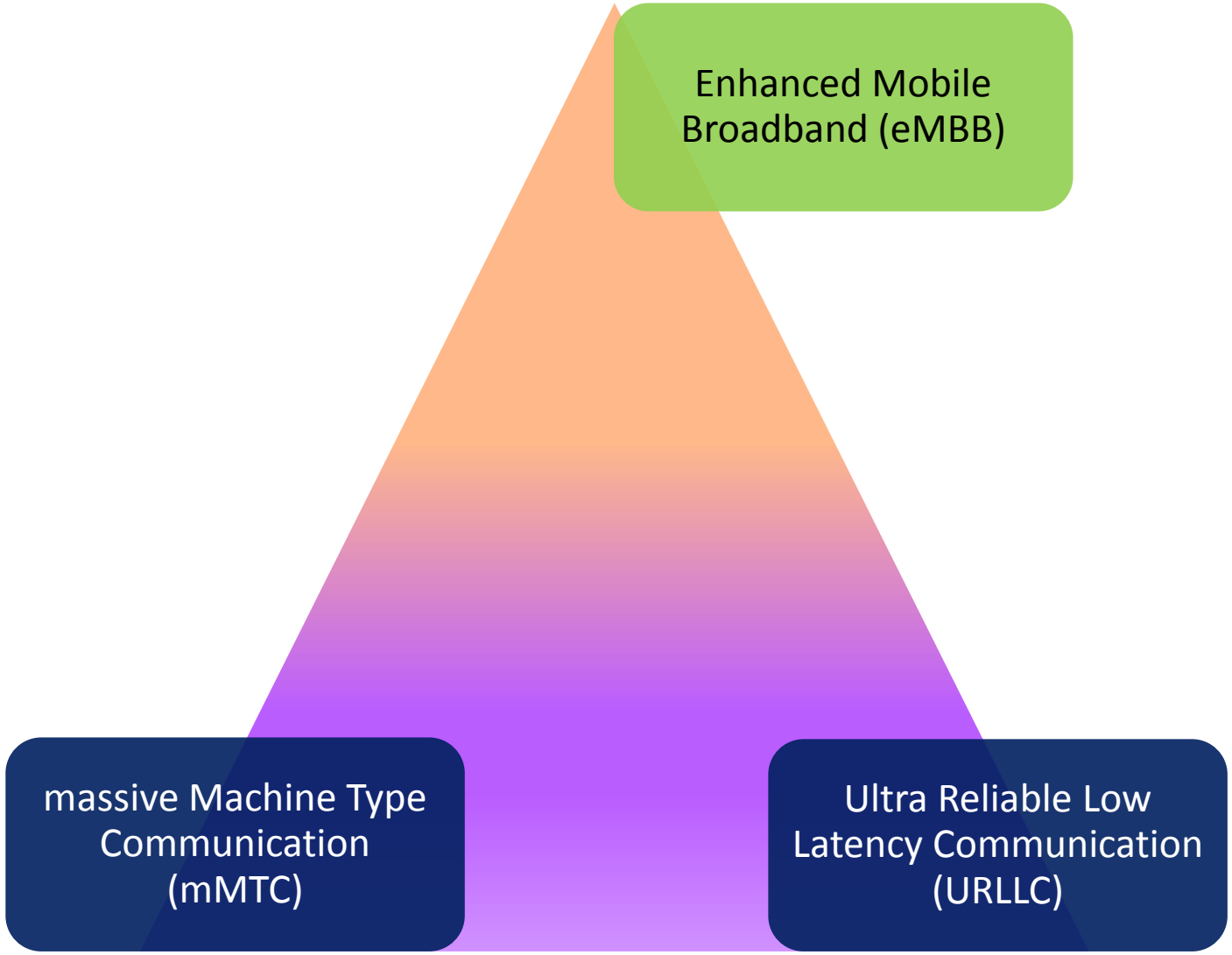
# 5G Security Next Steps

# 3GPP 5G Phase-2 Security

- Long-term key update
- 256 bits keys usage
- Security Assurance
- Network slicing security
- Location services security
- Security for 5G URLLC
- Security for Vertical & LAN Services

Phase 1

Phase 2



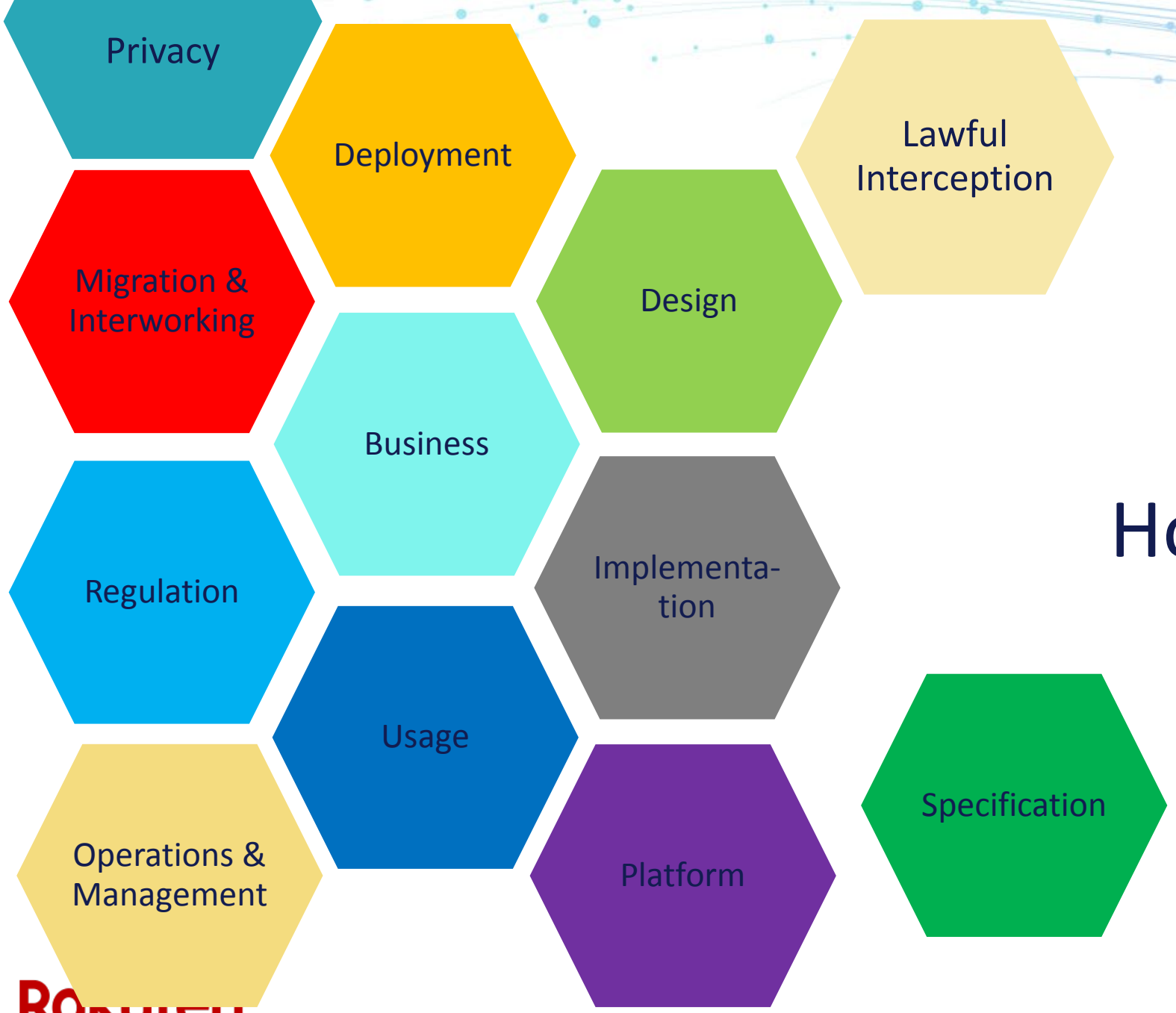

Rakuten

RSAConference2019

# Apply

# Apply

- Service providers (mobile operators, IT, digitization – IoT etc.)
  - Understand your organization's connectivity needs and security requirements
  - Map the requirements to 5G and virtualization
  - Develop appropriate management and automated control mechanisms
- Vendors
  - Verify 5G products security assurance requirements from 3GPP
  - Optimize implementation for virtualization
  - Consider security based on changing customer network architecture




# Holistic security from first step

RSAConference2019

# Summary

# Summary

- 4G security and issues
- 5G security and how 4G security issue are mitigated
- 5G security details and virtualization considerations
- 5G security next steps

# References


- Journal of ICT Standardization, River Publishers, https://www.riverpublishers.com/journal.php?j=JICTS
  - 5G non-standard aspects, vol 5 issue 3
  - 3GPP 5G specifications, vol 6 issue 1
- 3GPP SA3 specifications: http://www.3gpp.org/DynaReport/33-series.htm
  - 3GPP TS 33.401, “Technical Specification Group Services and System Aspects: 3GPP System Architecture Evolution (SAE) Security architecture”, Release 15, v 15.3.0, March. 2018.
  - 3GPP TS 33.501, “Security architecture and procedures for 5G system”, Release 15, v 15.0.0, March 2018.
- Ravishankar Borgaonkar, Altaf Shaik, N. Asokan, ValAeri Niemi, Jean-Pierre Seifert, *LTE and IMSI catcher myths*, https://www.blackhat.com/docs/eu-15/materials/eu-15-Borgaonkar-LTE-And-IMSI-Catcher-Myths.pdf
- David Rupprecht, Katharina Kohls, Thorsten Holz, and Christina Pöpper, *Breaking LTE on Layer Two*, https://alter-attack.net/
- Ravishankar Borgaonkar, Lucca Hirschi, Shinjo Park, and Altaf Shaik, *New Privacy Threat on 3G, 4G, and Upcoming 5G AKA Protocols*, https://eprint.iacr.org/2018/1175.pdf
- Tobias Engel. (December 2014). "SS7: Locate. Track. Manipulate", http://berlin.ccc.de/~tobias/31c3-ss7-locate-track-manipulate.pdf
- GSMA RIFS: "Diameter Roaming Security - Proposed Permanent Reference Document".

RSAConference2019

# Questions?

**Anand R. Prasad <anand@ieee.org>**

**@AnandRPrasad2**

**https://jp.linkedin.com/in/arprasad**