RSAConference2022
San Francisco & Digital | June 6 – 9

TRANSFORM

SESSION ID: **TECH-R05**

How to Secure Private 5G Networks

Srinivasan Balasubramanian

Distinguished Member, CTO Office Head of Standards & IP
srini@celona.io
@celona

Disclaimer

Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

Introduction

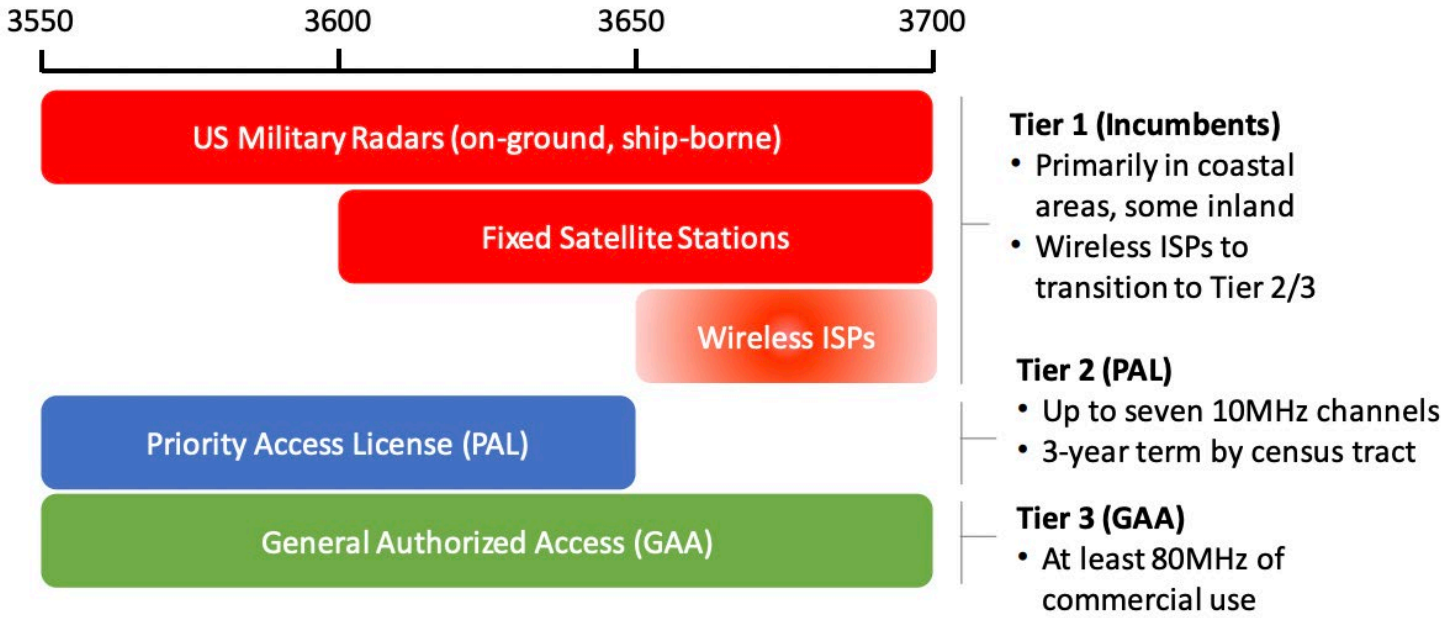
- A guide to bringing enterprise IT and cellular communications onto a common platform or infrastructure.
- Topics:
  - Shared spectrum for private networks
  - Zero Trust Architecture (ZTA)
  - ZT in 5G
  - Mobile Security and Network Access Control
  - Inter application, function, node security
- Appendix
  - 3GPP Architecture and Security Framework
  - SEVEN TENETS OF THE NIST ZERO TRUST ARCHITECTURE
  - References

RSAConference2022

Shared spectrum for private networks

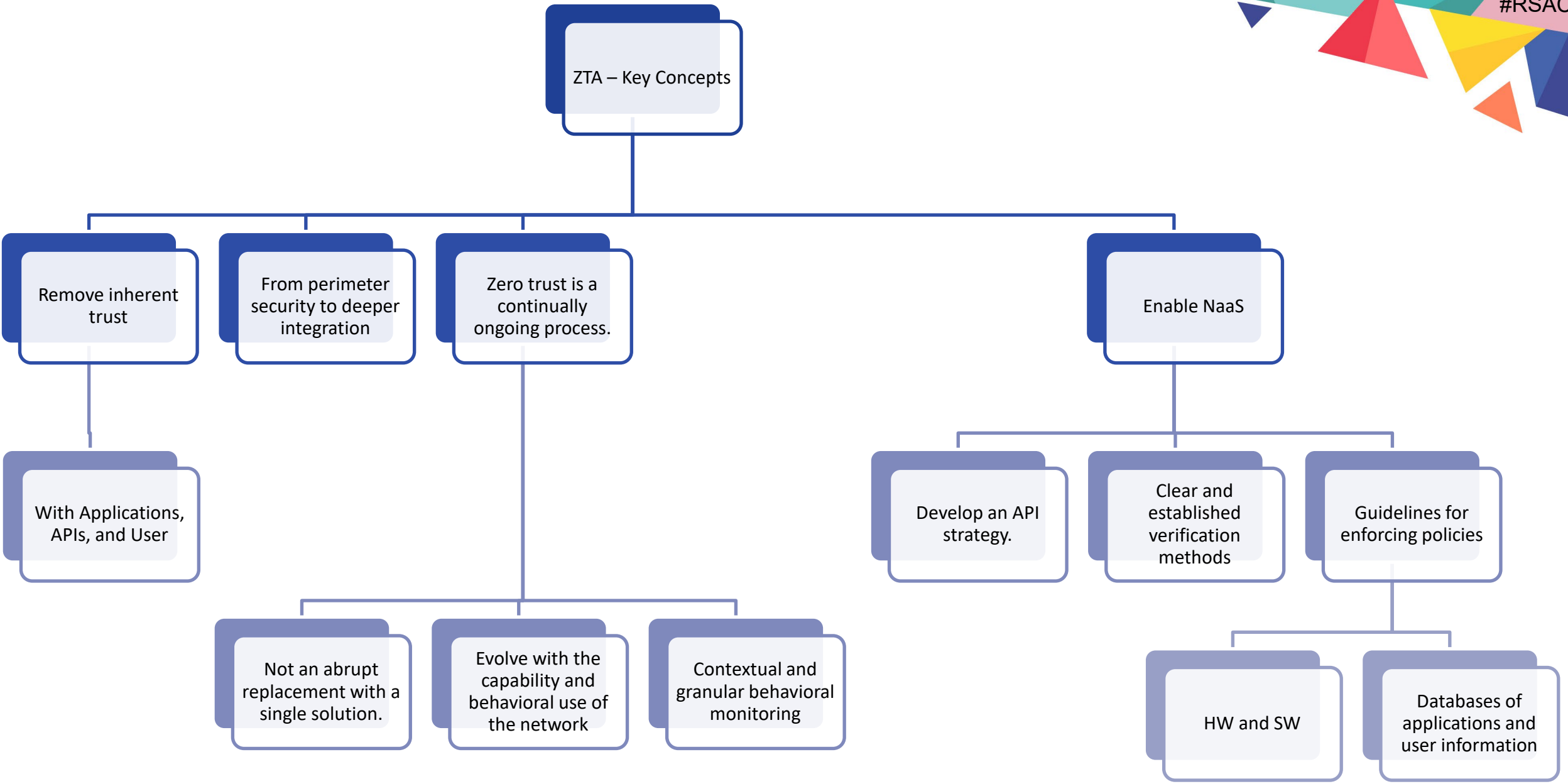
Shared spectrum for private networks

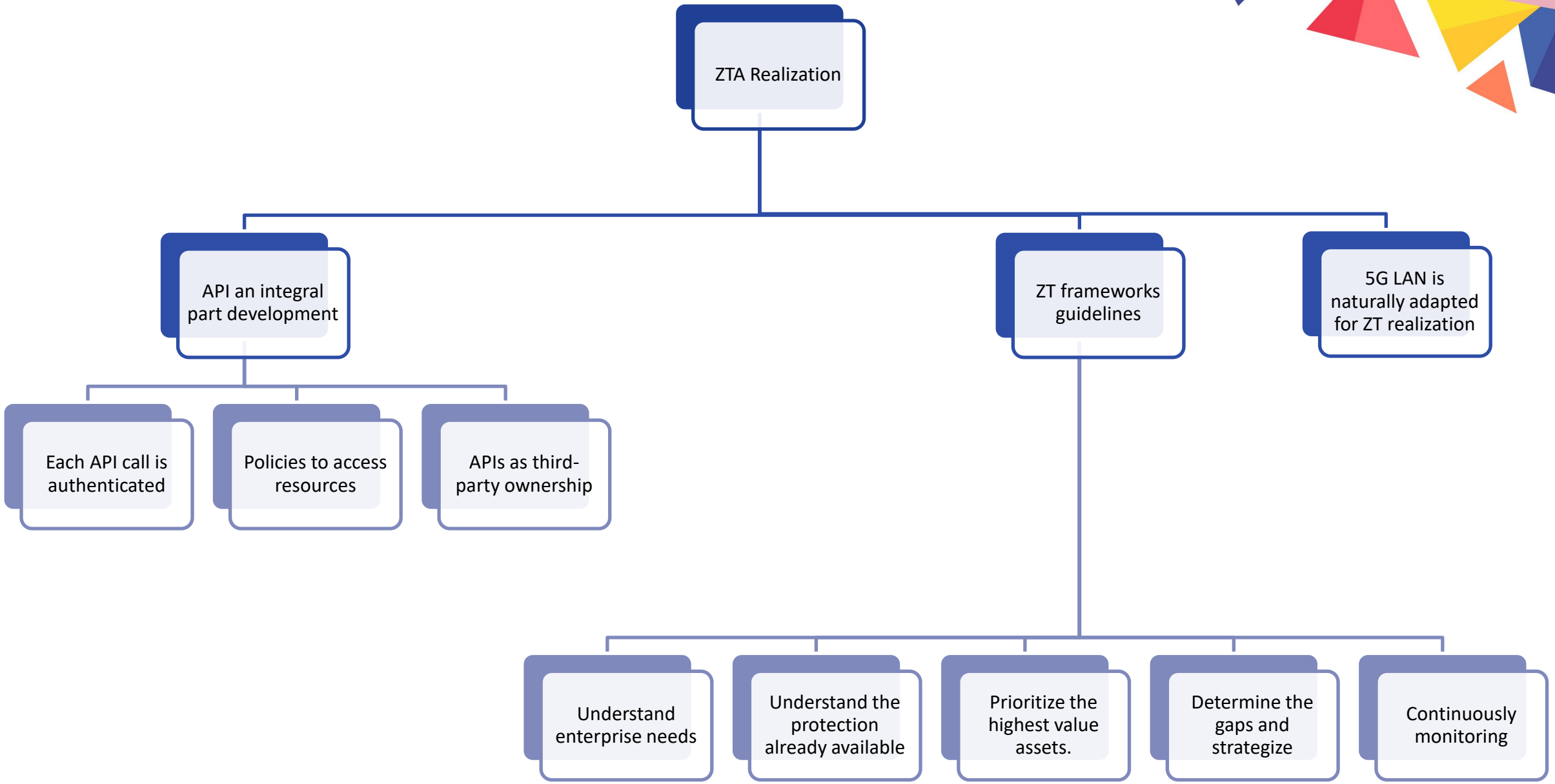
- Citizens Broadband Radio Service (CBRS) is band 48 operating in the mid band spectrum : 150MHz;
- Spectrum allocation coordinated through a central entity: Spectrum Access System (SAS)
- Allows for regular LTE / NR devices to camp on enterprise networks
- Model being considered for in other bands: 3.1GHz to 3.45GHz; 6GHz;
- Approach being used across the globe – both static and dynamic methods



RSAConference2022

Zero Trust Architecture (ZTA)

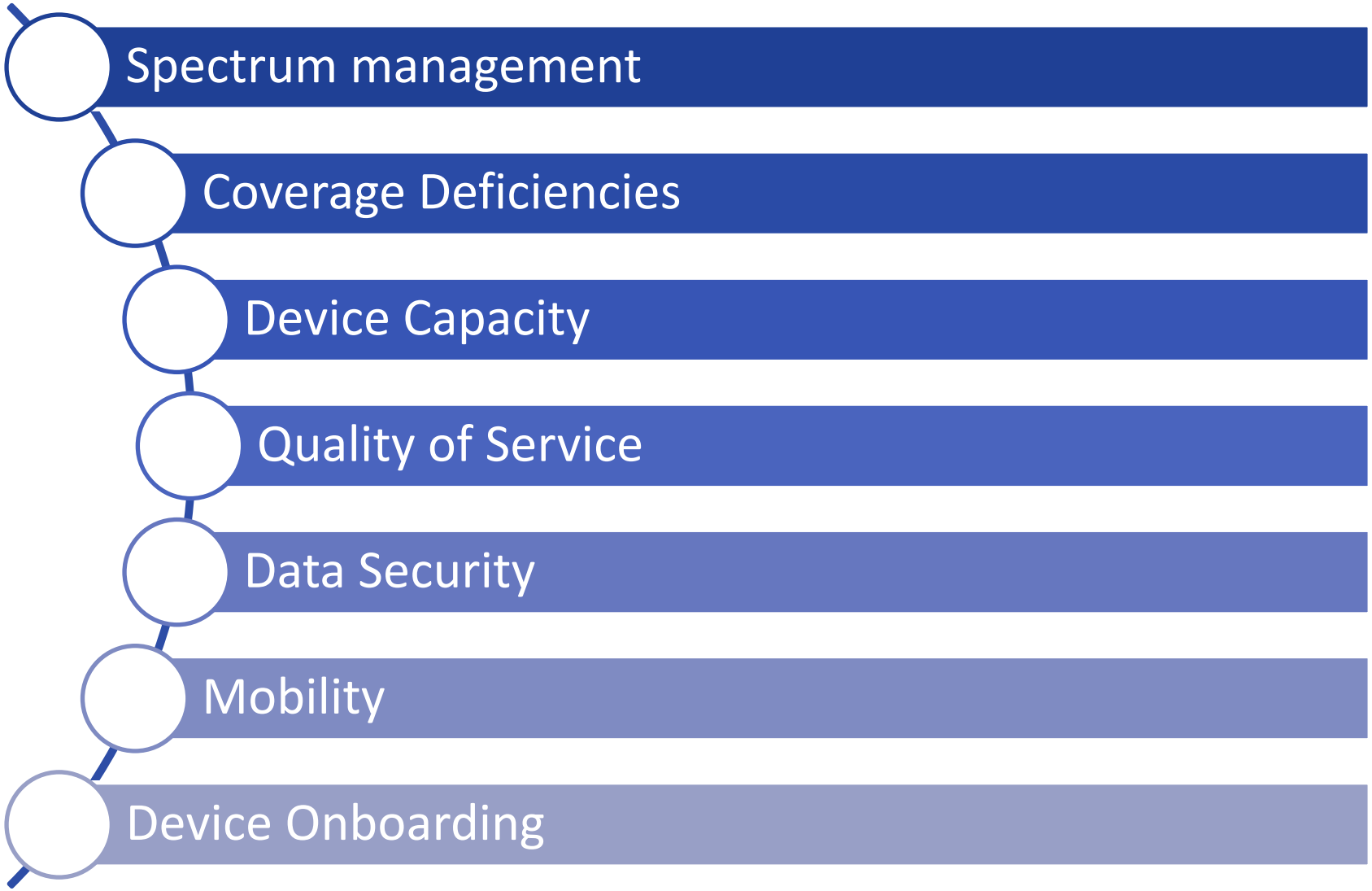

ZTA – Key Concepts
Remove inherent trust
From perimeter security to deeper integration
Zero trust is a continually ongoing process.
Enable NaaS
With Applications, APIs, and User
Not an abrupt replacement with a single solution.
Evolve with the capability and behavioral use of the network
Contextual and granular behavioral monitoring
Develop an API strategy.
Clear and established verification methods
Guidelines for enforcing policies
HW and SW
Databases of applications and user information


ZTA Realization
API an integral part development
Each API call is authenticated
Policies to access resources
APIs as third-party ownership
ZT frameworks guidelines
5G LAN is naturally adapted for ZT realization
Understand enterprise needs
Understand the protection already available
Prioritize the highest value assets.
Determine the gaps and strategize
Continuously monitoring

RSAConference2022

ZT in 5G

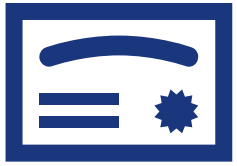
Key challenges addressed by 5GLAN



What is 5GLAN

RAT Choice

- Carefully choose wireless technology or risk of dealing with performance, reliability and security issues.

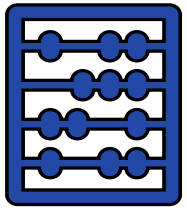


Simplicity

- Combining conventional wireless LANs with advanced LTE/5G NR technology, supporting seamless wireless connectivity

IT-friendly

- Overlay atop existing enterprise networks, fully integrated that includes indoor and outdoor small cell access points



Flexible

- Easy to use alternative to traditional wireless systems that are cost effective

Need for ZT early on

Threat vectors

- Remains the same
  - Network, Users, Email, Applications (Web or Cloud), Remote access nodes, Mobile devices, Data in motion and at rest (enterprise data)

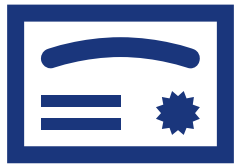
Increased exposure

- Multiple technologies with different security levels;
- Multi-Access Edge (MEC)
- The disaggregated nature of 5G with Service Based Architecture
- Newer services enabled through LTE/5G NR
- Network exposure functions (NEFs) and interfaces create a larger attack surface

Support Your Zero Trust Strategy with 5G LAN

Strong Device Identification

- Known, fixed endpoint identification supports authentication and asset management

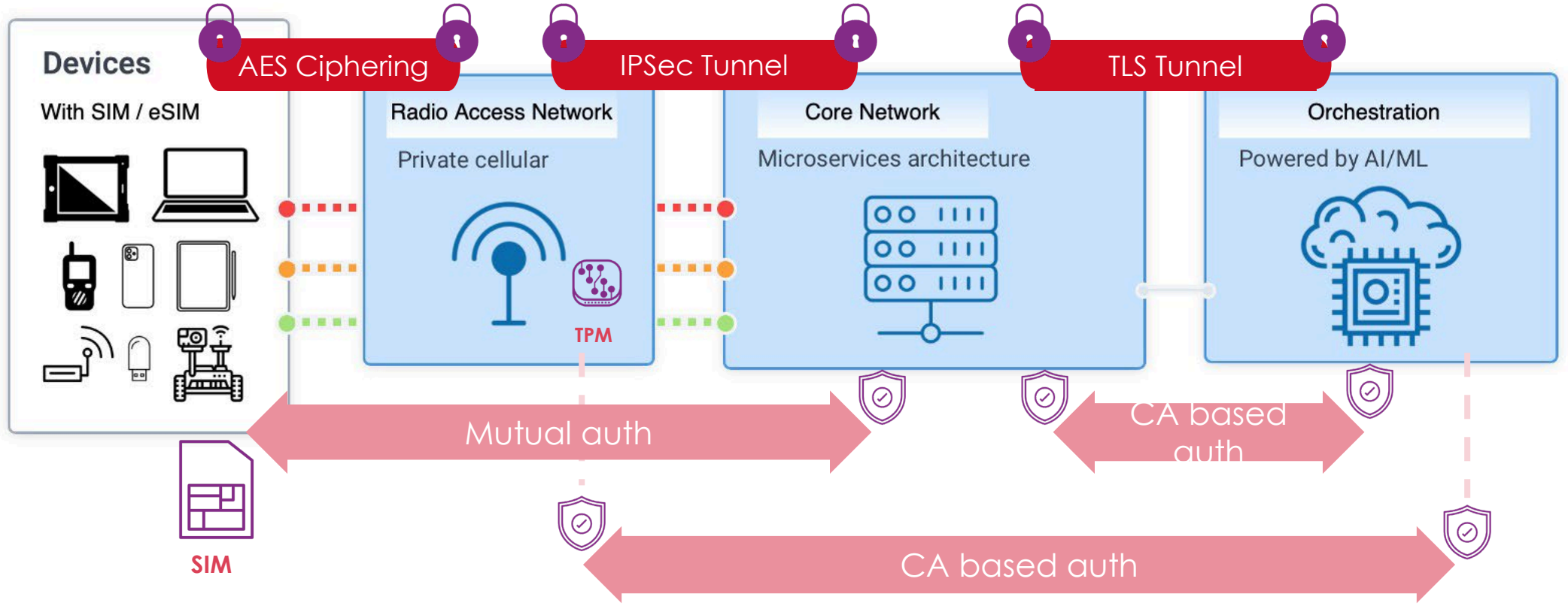


Mutual Authentication

- Between endpoints and 5G LAN, plus infrastructure components to one another

End-to-End Encryption

- Over the air, through the 5G LAN, enterprise LAN, and to any private or public cloud



The 5G LAN infrastructure includes strong mutual authentication and encryption along the full data path, wireless and wired.

Network segmentation as a ZT realization with 5GLAN

Segmentation

- Segment over the air and through public and private networks

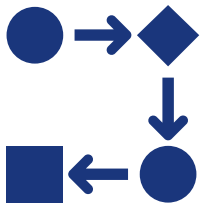
Quality of Service

- Guarantee availability and SLAs for critical applications

Extensible Architecture

- Native microservices based platform with APIs for extensibility and integrations

Maintain Data Privacy

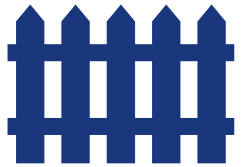


Data Path Control for Privacy and Compliance

Enterprise data stays 100% under your control, alleviating privacy concerns of public 5G and private solutions from MNOs.

Privacy Promise

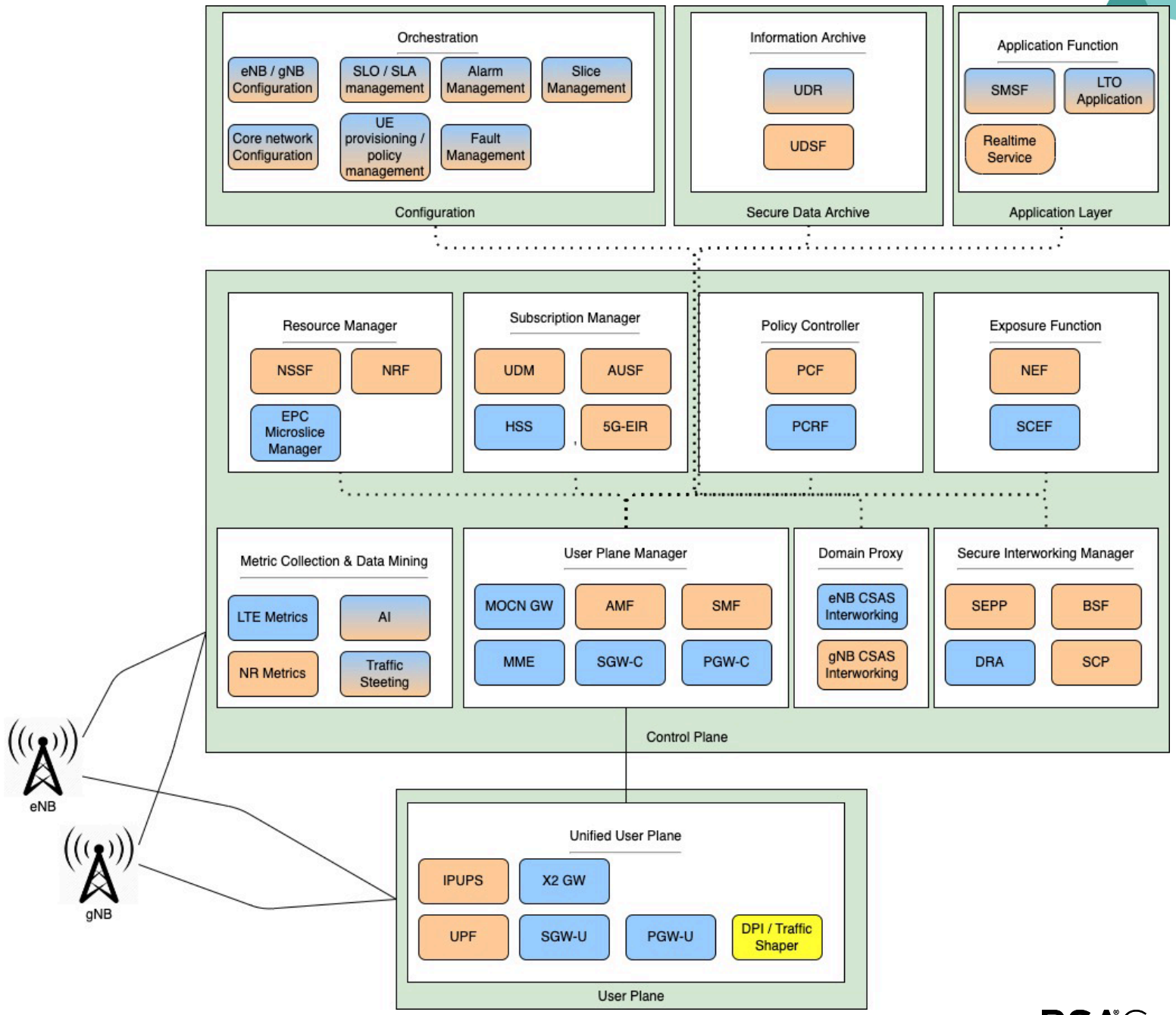
Never have access to data payloads and does not sell, share, or monetize any client or meta data.



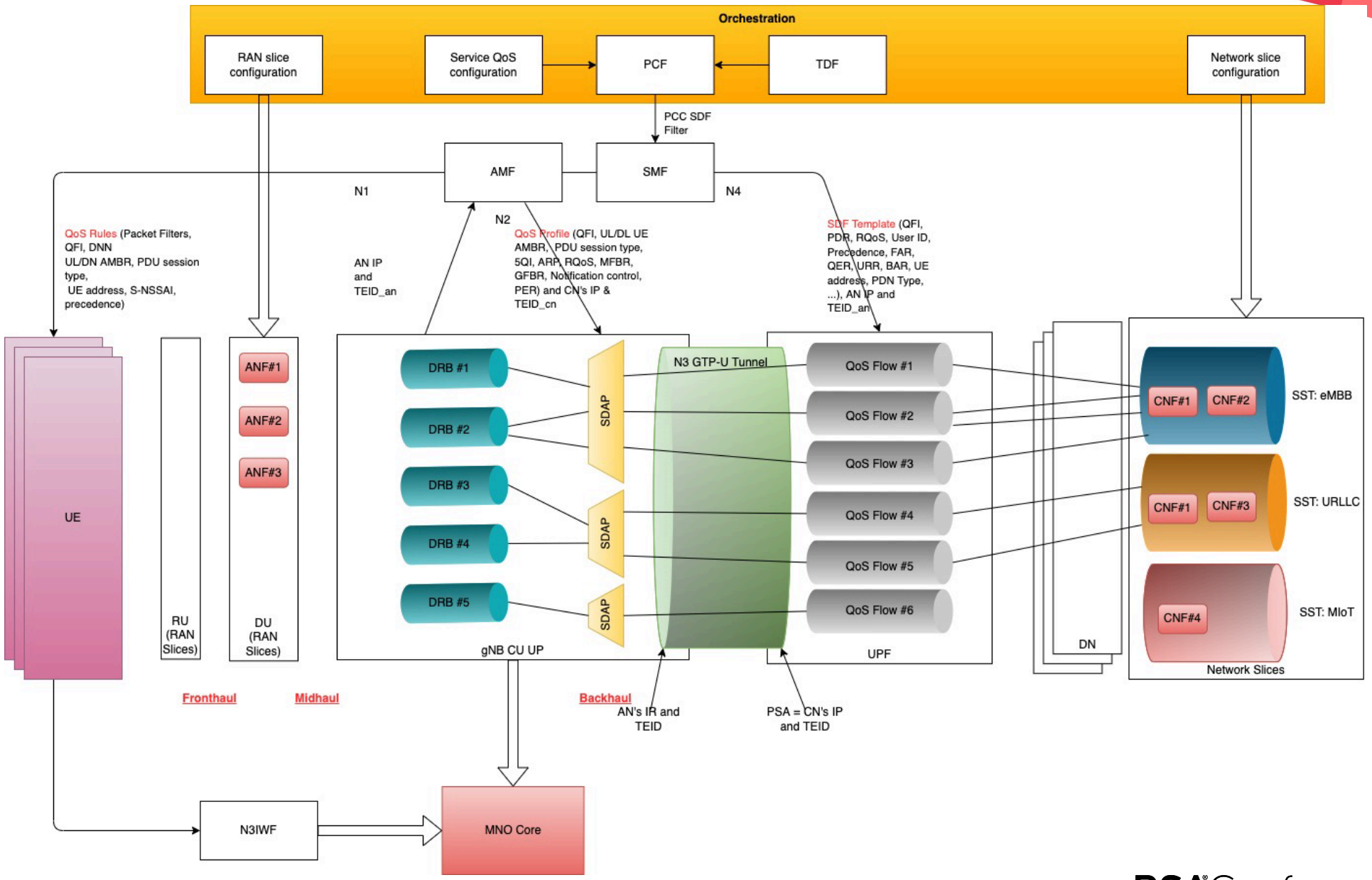
Preserved Privacy with Neutral Host Networks

For organizations pursuing NHN, private connections are segregated and secured from public connections.

ZT with SBA use in 5GC



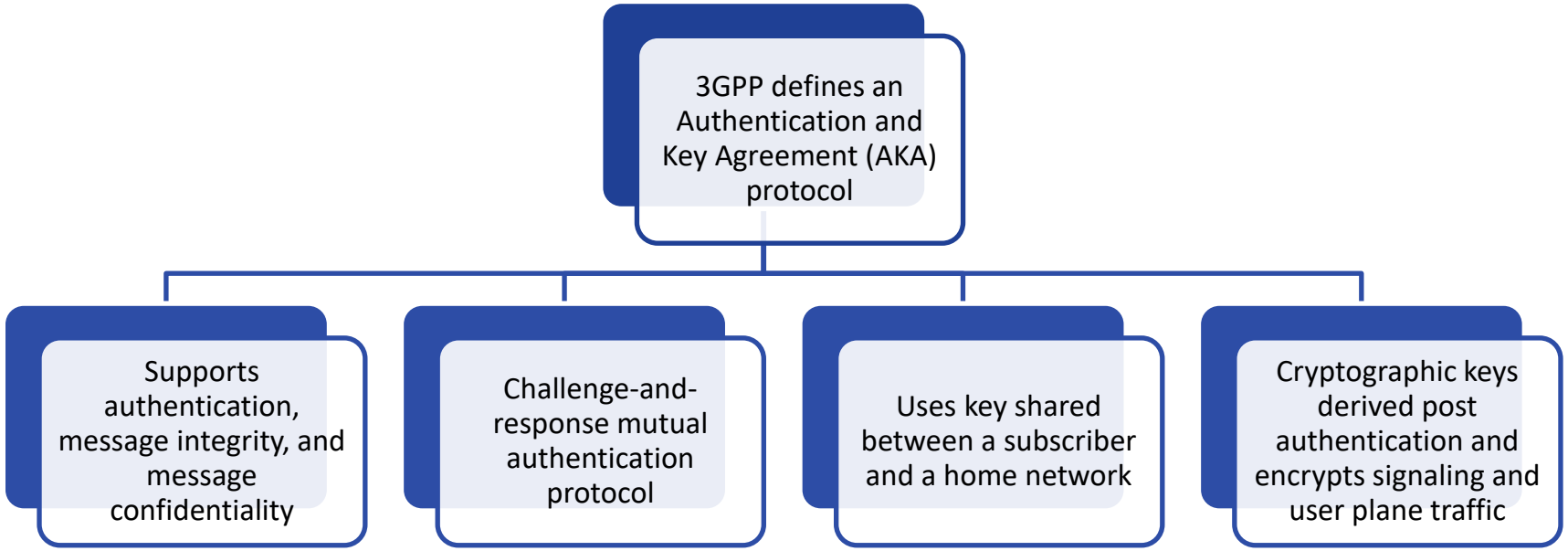
ZT with CUPS


Orchestration
RAN slice configuration
Service QoS configuration
PCF
TDF
Network slice configuration
PCC SDF Filter
AMF
SMF
N1
N2
N4
QoS Rules (Packet Filters, QFI, DNN UL/DN AMBR, PDU session type, UE address, S-NSSAI, precedence)
AN IP and TEID_an
QoS Profile (QFI, UL/DL UE AMBR, PDU session type, 5QI, ARP, RQoS, MFBR, GFBR, Notification control, PER) and CN's IP & TEID_cn
SDF Template (QFI, PDR, RQoS, User ID, Precedence, FAR, QER, URR, BAR, UE address, PDN Type, ...), AN IP and TEID_an
UE
RU (RAN Slices)
DU (RAN Slices)
ANF#1
ANF#2
ANF#3
DRB #1
DRB #2
DRB #3
DRB #4
DRB #5
SDAP
SDAP
SDAP
gNB CU UP
N3 GTP-U Tunnel
QoS Flow #1
QoS Flow #2
QoS Flow #3
QoS Flow #4
QoS Flow #5
QoS Flow #6
UPF
DN
CNF#1
CNF#2
SST: eMBB
CNF#1
CNF#3
SST: URLLC
CNF#4
SST: MIoT
Network Slices
Fronthaul
Midhaul
Backhaul
AN's IR and TEID
PSA = CN's IP and TEID
N3IWF
MNO Core

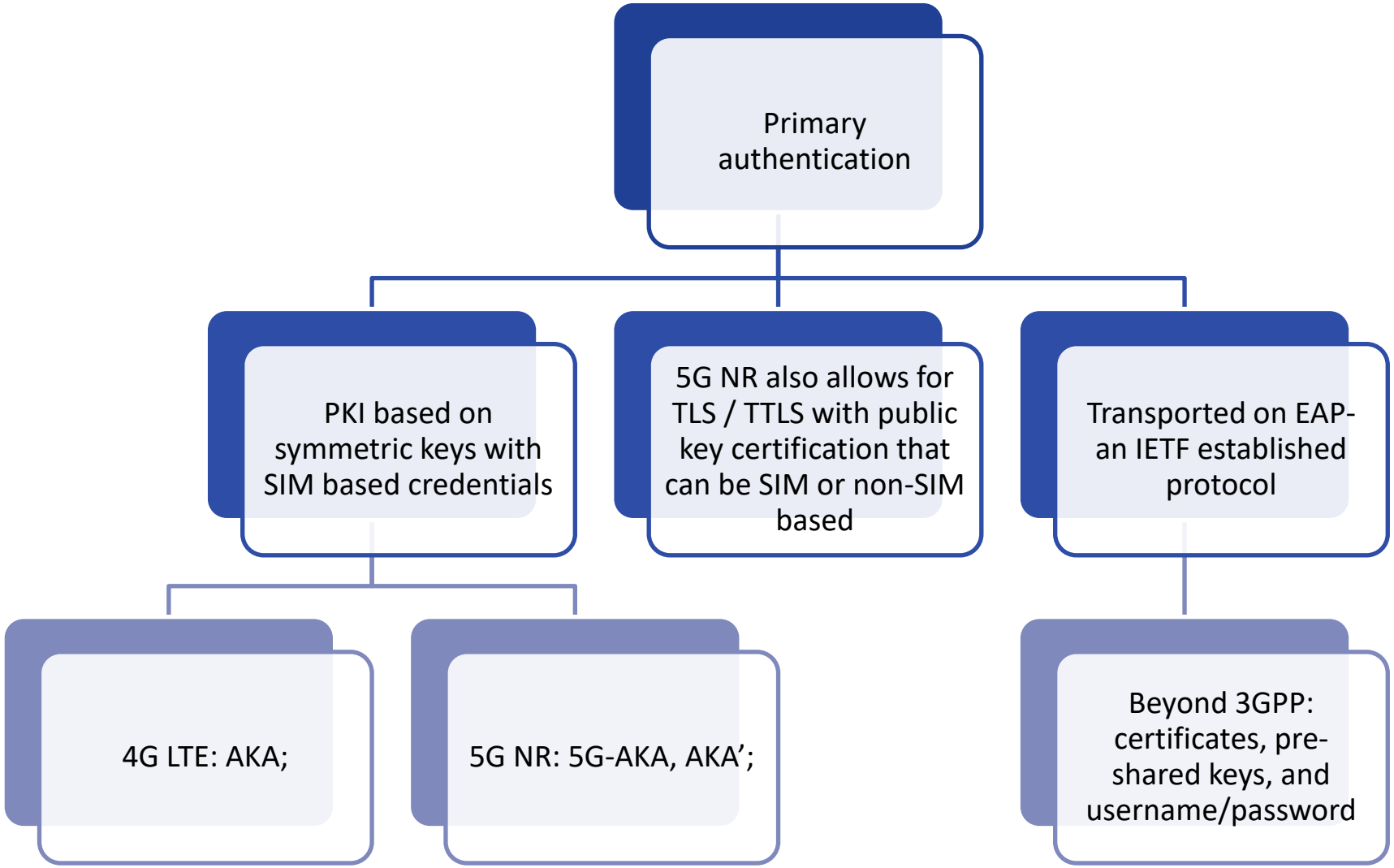
RSAConference2022

Mobile Security and Network Access Control

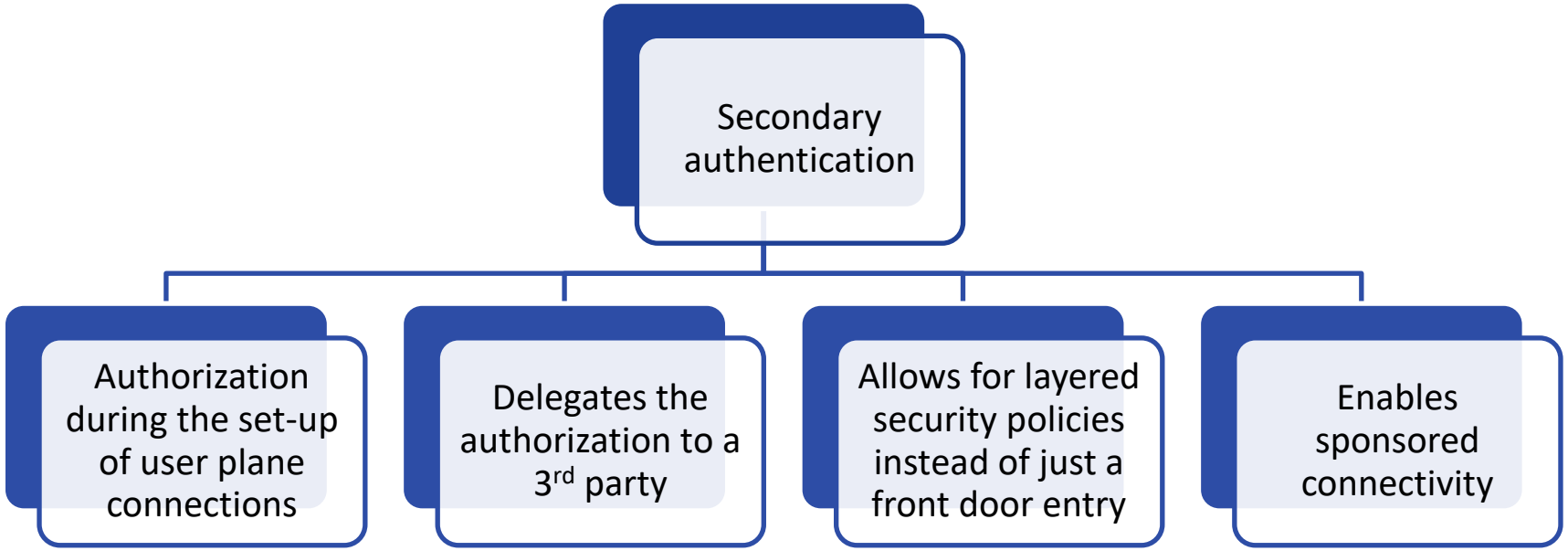
3GPP Authentication Protocol



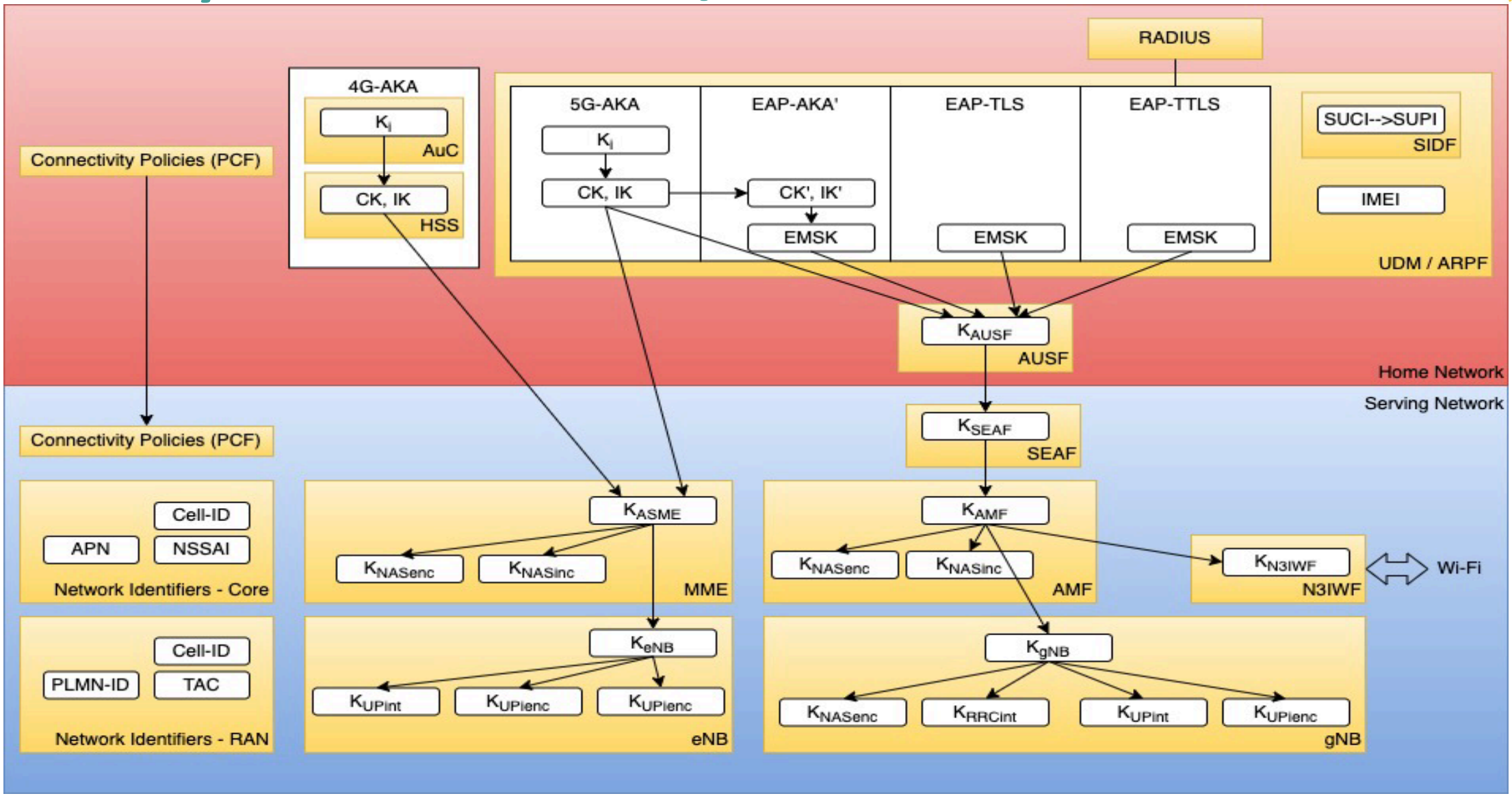
Primary User Authentication



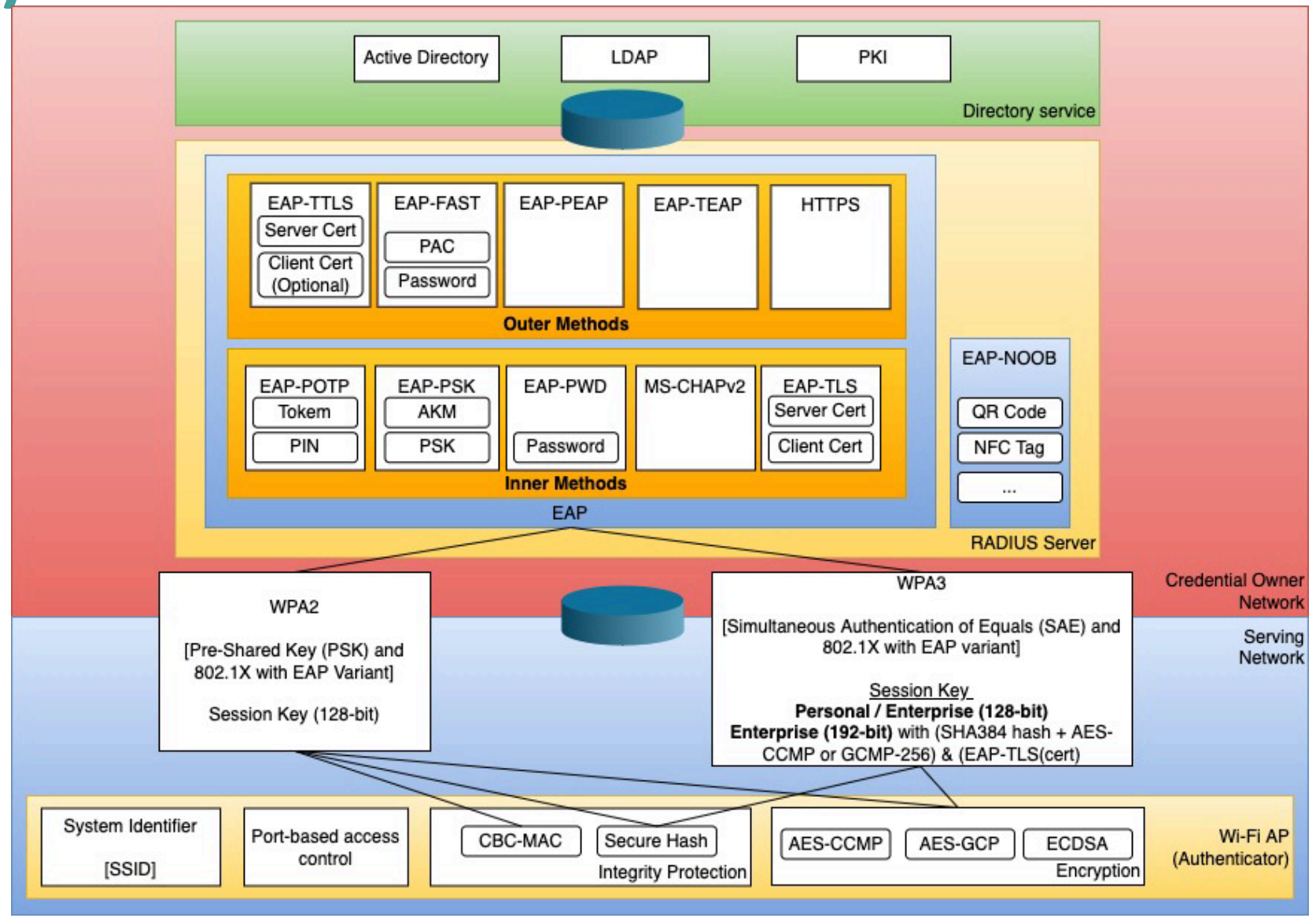
Secondary User Authentication



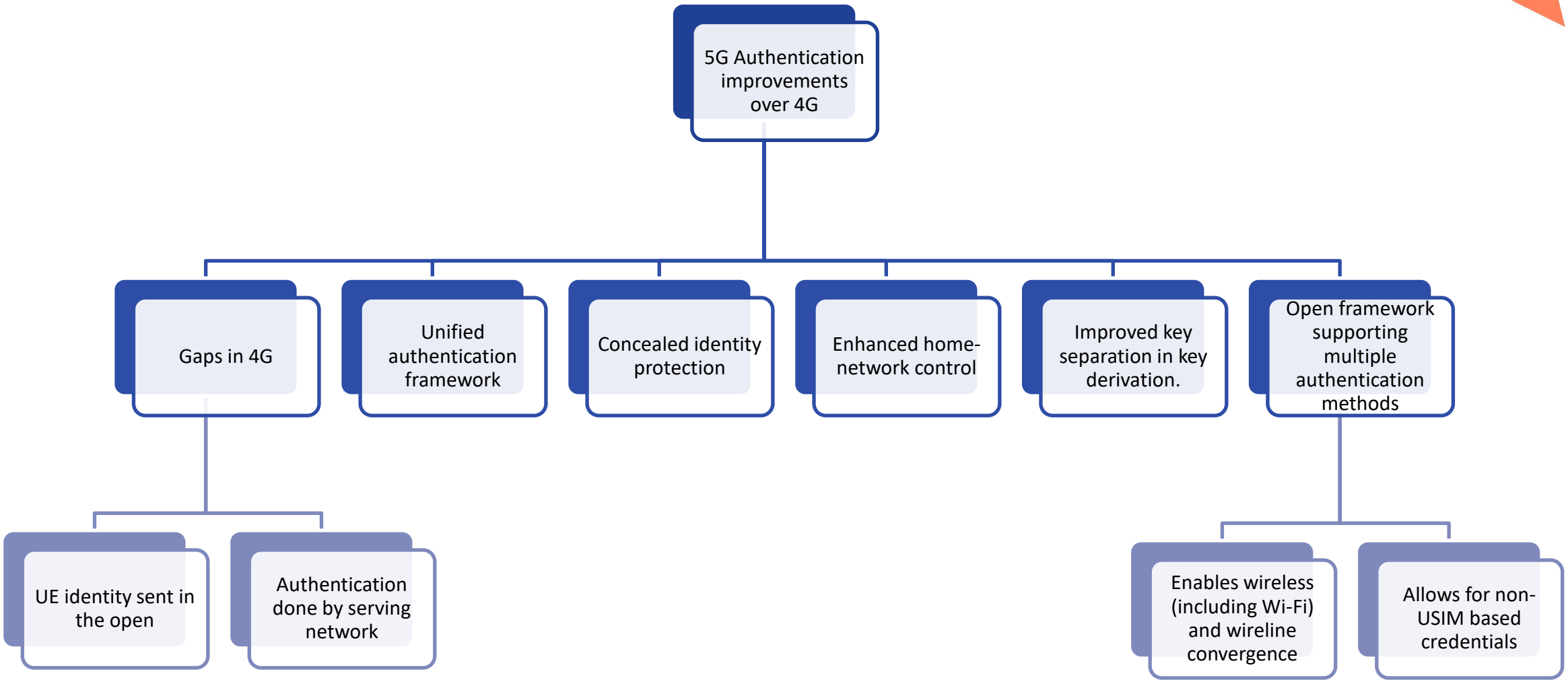
Security Framework – 4G / 5G



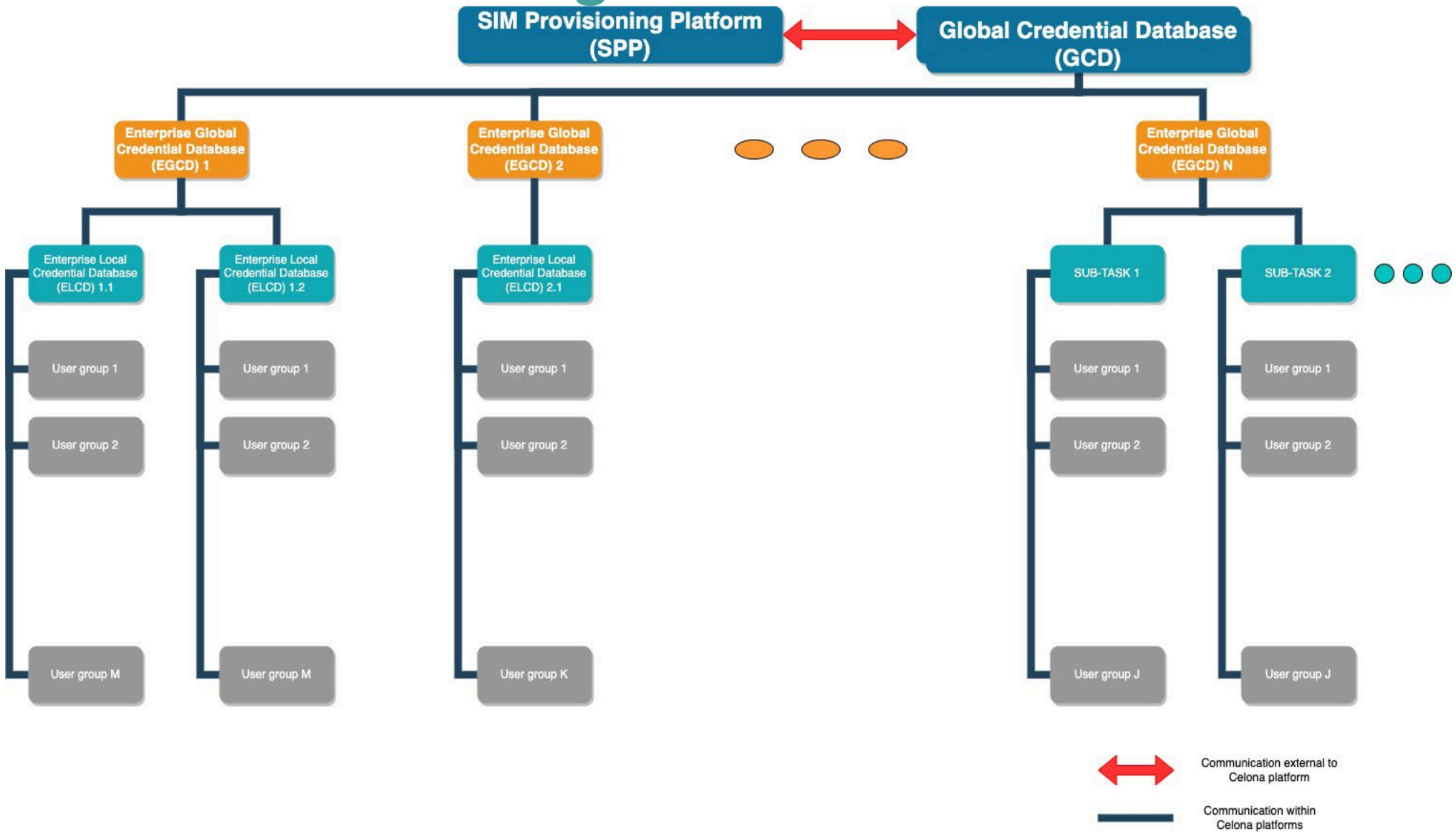
Security Framework – Wi-Fi



5G authentication improvements over 4G



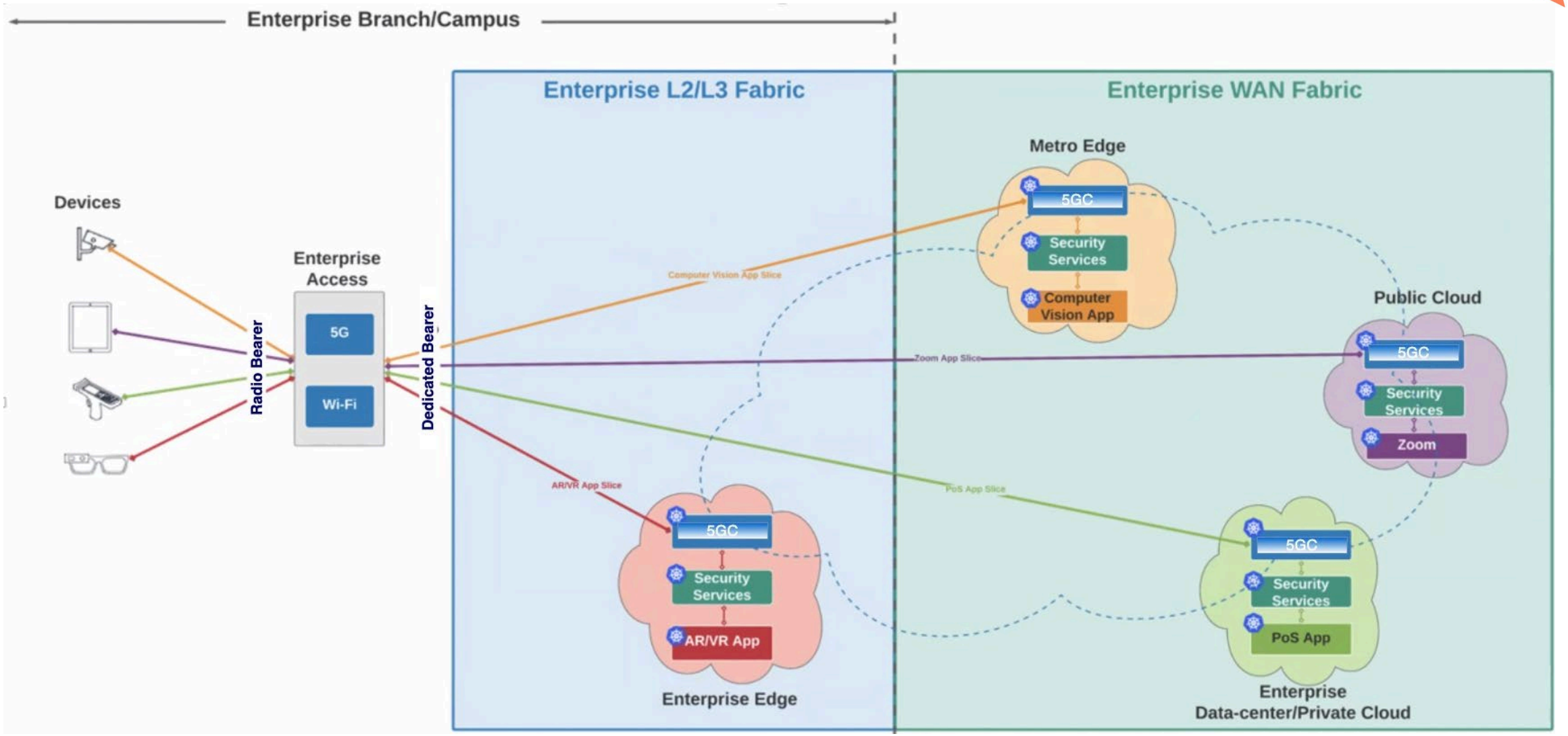
Device credential management



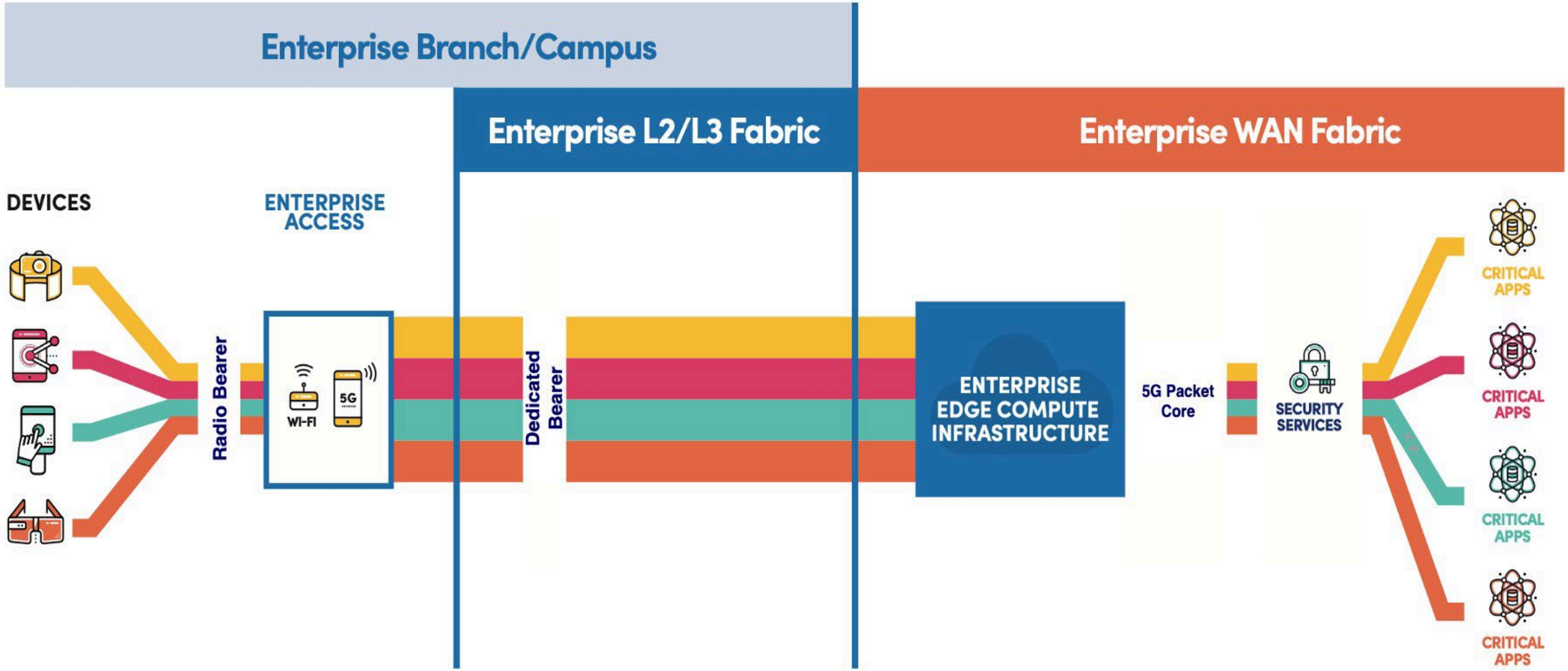
RSAConference2022

Inter application, function, node security

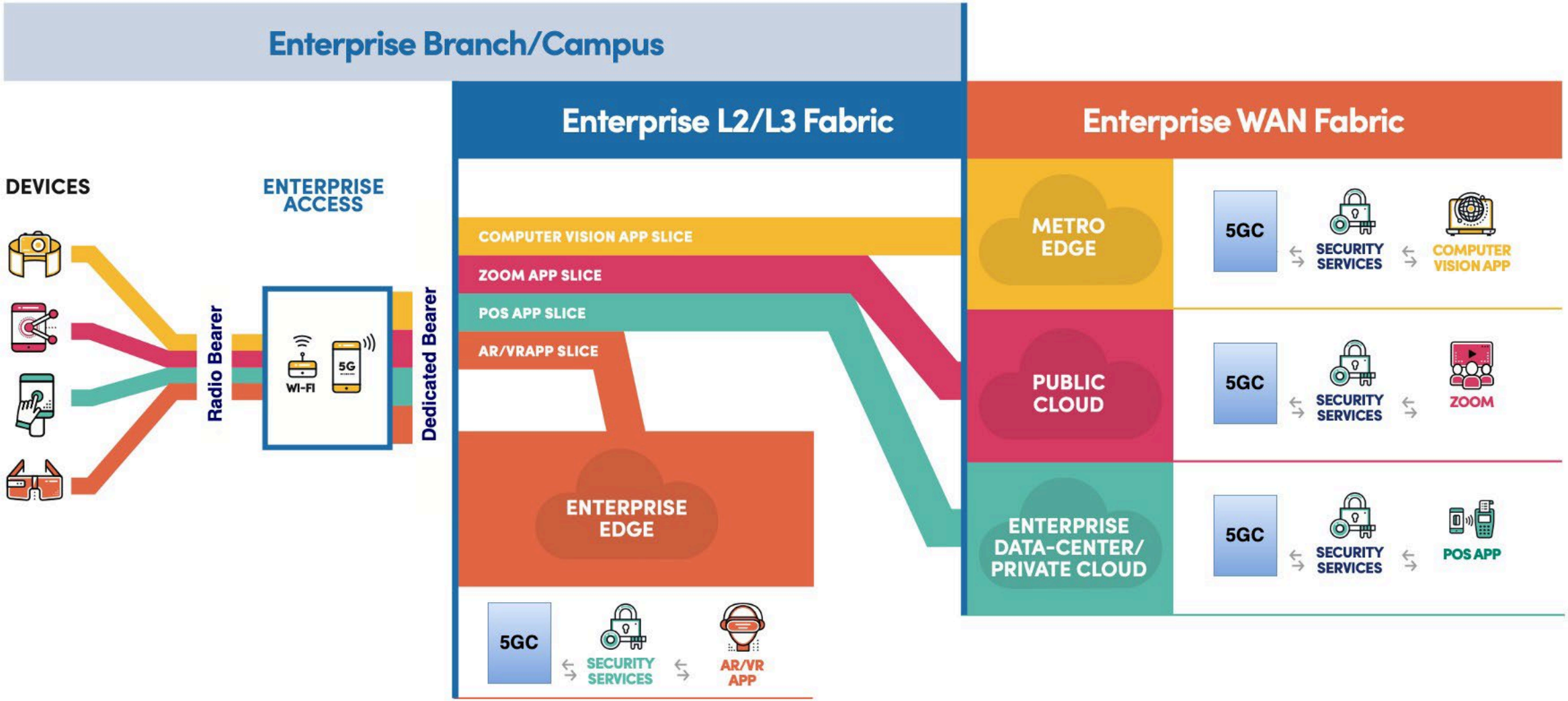
Service Based Architecture



Edgeless


Enterprise Branch/Campus
Enterprise L2/L3 Fabric
Enterprise WAN Fabric
DEVICES
ENTERPRISE ACCESS
Radio Bearer
WI-FI
5G
Dedicated Bearer
ENTERPRISE EDGE COMPUTE INFRASTRUCTURE
5G Packet Core
SECURITY SERVICES
CRITICAL APPS
CRITICAL APPS
CRITICAL APPS
CRITICAL APPS

Edge Compute and Multi Cloud



How to apply what we went over today

- Determining the service needs of the enterprise
  - Identify the required SLO of the different services
  - Identify the resources that need to be protected
  - Identify user groups and the isolation of access and information exchange
  - Identify the inbound and outbound roaming and secure accesses required
- Determining the capability of individual RAT
  - Find the right RAT that will meet the current and future needs of the enterprise
- Identify the threat vectors in the system
- Design the network to meet the SLO of the different services while addressing the threat vectors

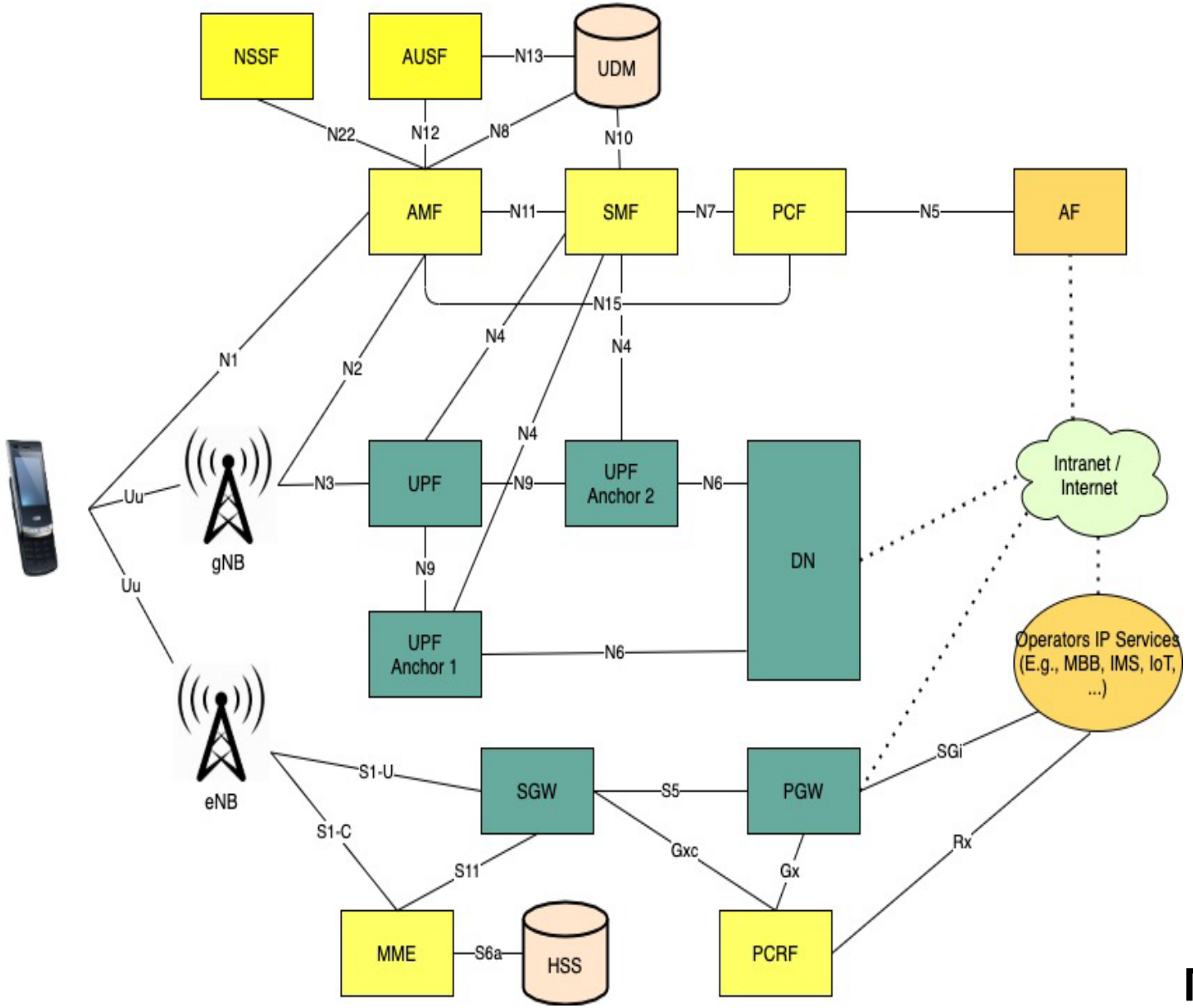
RSAConference2022

Appendix

RSAConference2022

3GPP Architecture and Security Framework

4G / 5G Network Architecture



4G and 5G Authentication summary view

		Entities located in			Message Format		Trust Model	UE Identity		SN Identity	Authentication vector generated by	Authentication of UE decided by	HN informaed of UE authenticatiom n	Anchor key heirarchy
		UE (User Equipment)	SN (Serving Network)	HN (Home Network)	UE <--> SN	SN <--> HN		UE --> SN	SN --> HN					
4G Authentication	EPS-AKA	USIM	MME	HSS	NAS	Diameter	Shared symmetric key	IMSI / GUTI	IMSI	SN Id (MCC / MNC)	HSS	MME	No	K_i -> CK+IK -> K_{ASME}
5G Authentication	5G-AKA'		SEAF	AUSF / UDM / ARPF / SIDF	NAS	HTTP based web APIs		SUCI/5G-GUTI	SUCI / SUPI	SN Name (5G: MCC/MNC)	UDM / ARPF	SEAF & AUSF	Yes	K_i -> CK+IK -> KASME -> KSEAF
	EAP-AKA'				NAS|EAP						UDM / ARPF	AUSF	Yes	K_i -> CK+IK -> CK'+IK' -> EMSK -> K_{SEAF}
	EAP-TLS	USIM/Non-USIM			NAS|EAP		Public key certificate				N/A	AUSF	Yes	EMSK -> K_{AUSF} -> K_{SEAF}

RSAConference2022

SEVEN TENETS OF THE NIST ZERO TRUST ARCHITECTURE

SEVEN TENETS OF THE NIST ZERO TRUST ARCHITECTURE

- All data sources and computing services are considered resources.
- All communication is secured regardless of network location.
- Access to individual enterprise resources is granted on a per-session basis.
- Access to resources is determined by dynamic policy and may include other behavioral and environmental attributes.
- The enterprise monitors and measures the integrity and security posture of all owned and associated assets.
- All resource authentication and authorization are dynamic and strictly enforced before access is allowed.
- The enterprise collects as much information as possible about the current state of assets, network infrastructure, and communications and uses it to improve its security posture.

RSAConference2022

References

IETF References

- Internet Engineering Task Force, “Improved Extensible Authentication Protocol Method for 3rd Generation Authentication and Key Agreement (EAP-AKA'),” Request for Comments (RFC) 5448 (May 2009).
- Internet Engineering Task Force, “Extensible Authentication Protocol (EAP),” Request for Comments (RFC) 3748 (June 2004).
- Internet Engineering Task Force, “The EAP-TLS Authentication Protocol,” Request for Comments (RFC) 5216 (March 2008).

3GPP Specification References

- 3GPP, “3GPP System Architecture Evolution (SAE)—Security Architecture” (Release 15), technical specification (TS) 33.401, v15.2.0 (September 2018).
- 3GPP, “Security Architecture and Procedures for 5G System” (Release 15), technical specification (TS) 33.501, v15.5.0 (September 2018).
  - provides additional authentication methods using EAP framework
- 23.502
- 38.331
- 31.102
  - outlines characteristics of USIM application
- 31.103 ISIM
- TR 33.899
  - secure storage and processing can be UICC and Smart Secure Platform (SSP)
- TR 31.890 allows for legacy UICC to be used for 5G access.

GSMA References

- eSIM: The What and How of Remote SIM Provisioning. GSMA paper
- ISO/IEC 7816 smart card standard.
- SGP.21 V2.2
- SPG.22 V2.2.2

Conference Paper References

- Zhenhua Li, Weiwei Wang, Christo Wilson, Jian Chen, Chen Qian, Taeho Jung, Lan Zhang, Kebin Liu, Xiangyang Li, and Yunhao Liu, “FBS-Radar: Uncovering Fake Base Stations at Scale in the Wild,” Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2017).
- Altaf Shaik, Ravishankar Borgaonkar, N. Asokan, Valtteri Niemi, and Jean-Pierre Seifert, “Practical Attacks Against Privacy and Availability in 4G/LTE Mobile Communication Systems,” Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (Feburary 2016).
- Byeongdo Hong, Sangwook Bae, and Yongdae Kim, “GUTI Reallocation Demystified: Cellular Location Tracking with Changing Temporary Identifier,” Proceedings of the Internet Society Symposium on Network and Distributed System Security (NDSS) (February 2018).
- David Basin, Jannik Dreier, Lucca Hirschi, Saša Radomirovic, Ralf Sasse, and Vincent Stettler, “A Formal Analysis of 5G Authentication,” Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security (CCS '18) (October 2018).