Qualcomm @QCOMResearch NDSS 2023 March 2023

5G Security and Privacy

Gavin Horn
Senior Director, Wireless R&D
Qualcomm Technologies, Inc.

Soo Bum Lee
Principal Engineer, Wireless R&D
Qualcomm Technologies, Inc.

5G Accelerating Globally

225+
Operators with 5G commercially deployed

275+
Additional operators investing in 5G

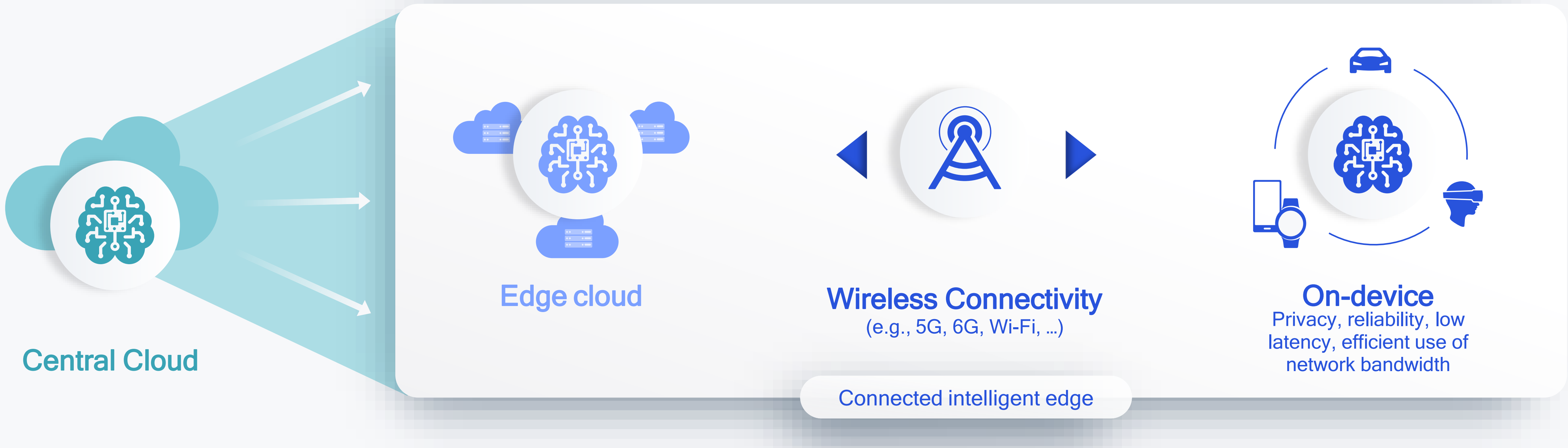
1B+
5G connections by 2023 – 2 years faster than 4G

5B+
5G smartphones to ship between 2020 and 2025

1,490+
5G designs launched or in development

Sources – 5G commercial networks, operators investing in 5G: GSA, Sep ‘22. 2023 5G connection projections: average of ABI (Sep ‘21), Ericsson (Jun ‘21) and GSMA Intelligence (Sep ‘21). 5G cumulative smartphone shipments: average of CCS Insight (Sept ‘21), Counterpoint Research (Dec ’21), IDC (Nov ‘21), Strategy Analytics (Oct ‘21); Launched / announced devices: GSA, Sep ’22.

To scale efficiently, AI processing is expanding towards the edge


Central Cloud
Edge cloud
Wireless Connectivity
(e.g., 5G, 6G, Wi-Fi, …)
On-device
Privacy, reliability, low latency, efficient use of network bandwidth
Connected intelligent edge

Qualcomm is leading the realization of the connected intelligent edge

Convergence of:

Wireless connectivity
Efficient computing
Distributed AI

Unleashing massive amount of data to fuel our digital future

Connected intelligent edge expansion

leading to greater threat surface

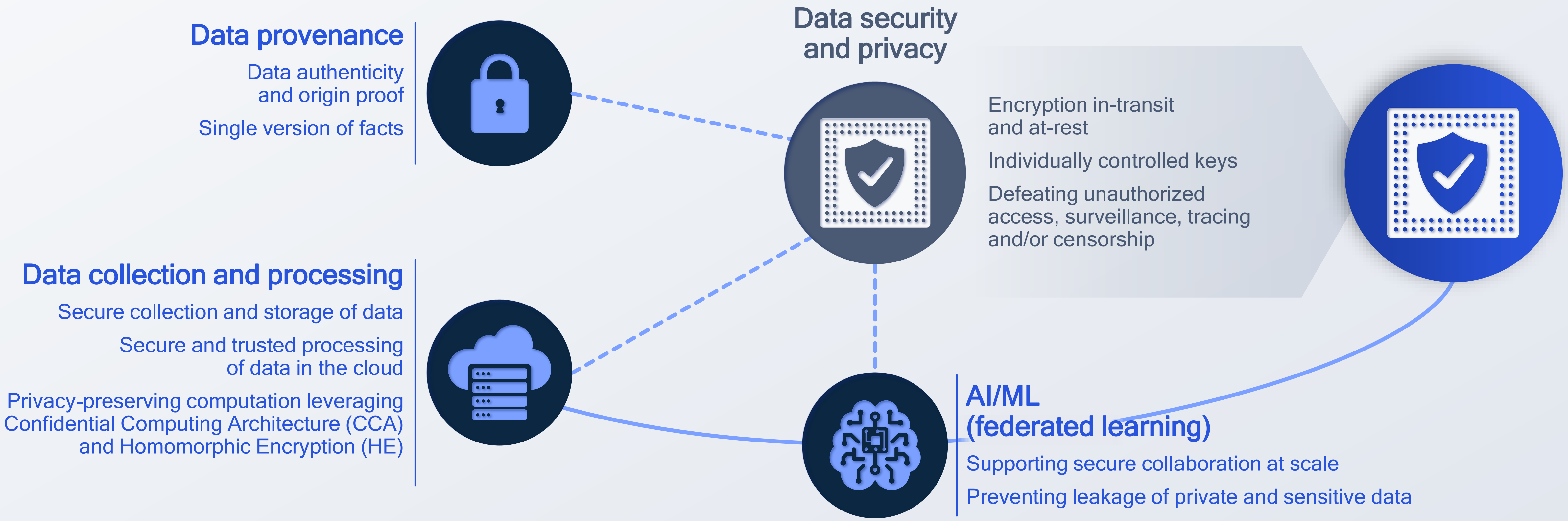
in the end-to-end system

More devices are connected across different deployments
(i.e., public and private networks)

Networks are becoming more disaggregated with increasing number of interfaces

5G system continues to evolve to address growing **security** and **privacy needs**

Protecting data – the most valuable asset in the digital world



Data provenance

Data authenticity and origin proof

Single version of facts

Data security and privacy

Encryption in-transit and at-rest

Individually controlled keys

Defeating unauthorized access, surveillance, tracing and/or censorship

Data collection and processing

Secure collection and storage of data

Secure and trusted processing of data in the cloud

Privacy-preserving computation leveraging Confidential Computing Architecture (CCA) and Homomorphic Encryption (HE)

AI/ML (federated learning)

Supporting secure collaboration at scale

Preventing leakage of private and sensitive data

Data is exposed to various security and privacy threats

In transit | At rest in local and/or remote storage | In use (processing) | In access | For validation

5G System strives for resilient communication

End-to-end approach to provide comprehensive system security and privacy

Communication Resiliency

Privacy

Data encryption on all levels

Security

Integrity, reliability, and protection of networks, devices, applications, and services

Identity

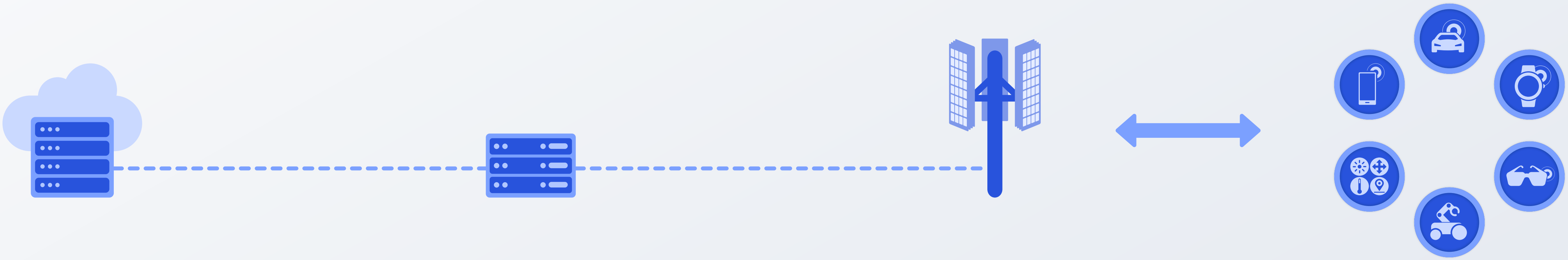
Encrypted long-term subscriber identifiers

Trust

Mutual authentication and authorization

Robustness

Attack detection and confinement, and sustained operations



Application Threats

App server vulnerabilities

Application vulnerabilities

API vulnerabilities

IoT vulnerabilities

Core Network Threats

DoS[1] & DDoS[2] attacks

Sniffing

API vulnerabilities

Roaming partner vulnerabilities

Improper access control

IoT vulnerabilities

Radio Network Threats

Jamming

MitM[3] attack

Rogue nodes

User privacy

Eavesdropping

DoS attacks

Device Threats

Malware

Sensor susceptibility

API vulnerabilities

Bots DDoS

Firmware hacks

Device tampering

Why resilient communication requires an end-to-end solution

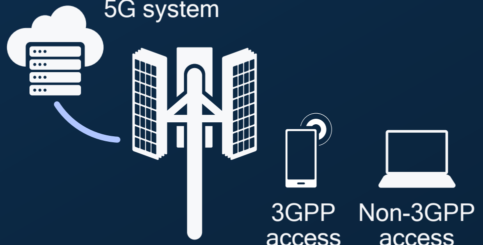
An end-to-end security approach is required to provide wide-ranging protection to the dynamic attack surface

[1] Denial of Service; [2] Distributed Denial of Service; [3] Men in the Middle

5G

Delivering enhanced level of wireless security

Built on the proven, solid security foundation of 4G LTE



Flexible framework

To support new devices, use cases, and deployments

Unified authentication for 3GPP/non-3GPP devices

Security anchor function

Network slicing

Tighter security

To expand protection and increase flexibility

User-plane integrity protection

Lower trust in serving networks

Subscription credentials in secure HW element

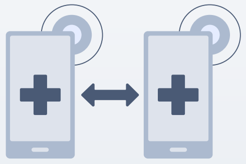
Enhanced privacy

To eliminate communication of unprotected device-specific info

Ciphered user and device specific information

Providing a flexible framework to secure a wide range of deployments

Sidelink



Secure group member and service discovery

Flexible configuration of security and privacy per application

V2X

Sidelink groupcast and broadcast security

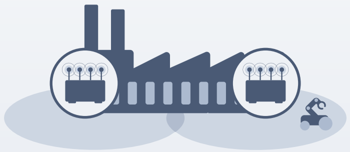
Sidelink unicast security including bearer layer security and privacy

Edge

End-to-end security between the device and edge server

Support for server-authenticated TLS

Private Networks



As another layer of security, 5G network slicing can be leveraged to provide traffic segregation between various business

Device onboarding support

IoT

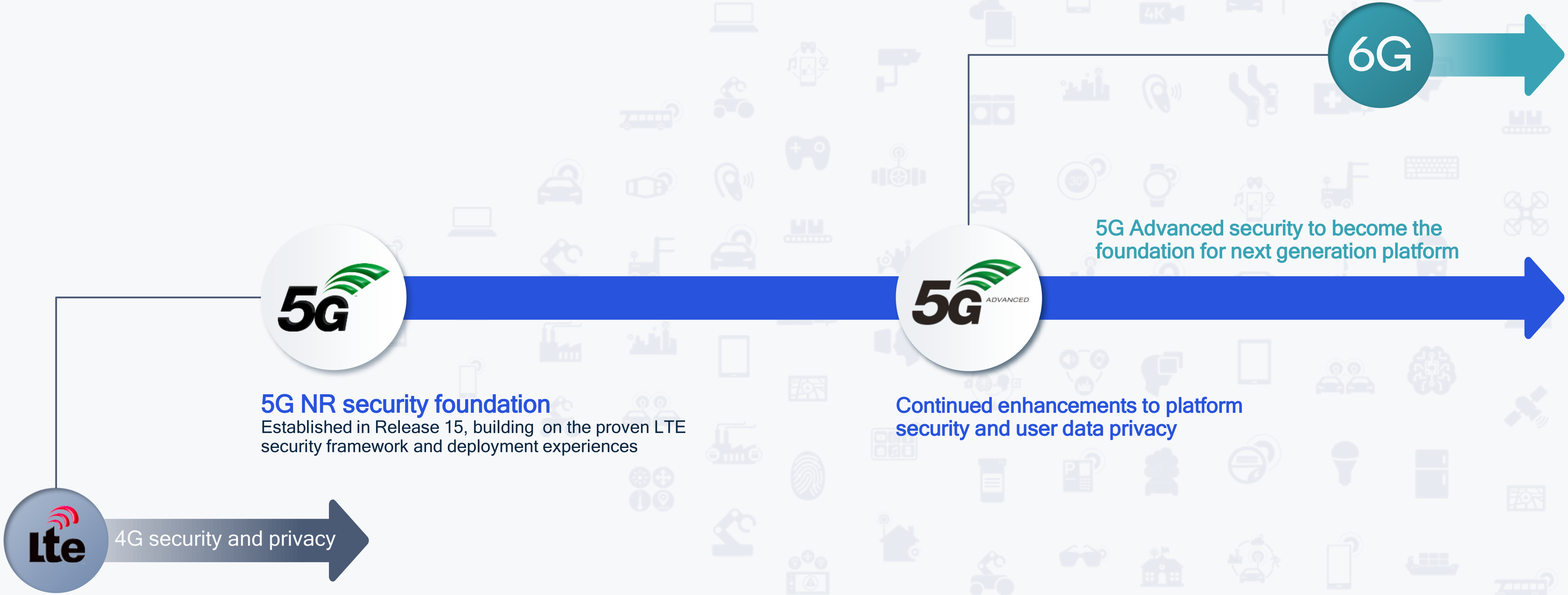
Control and user planes security optimizations to support massive IoT

5G System modeled as a bridge in Time Sensitive networks (TSN) to support private networks in IIoT

Secure credentials and identifiers

Secure transport in both radio and core networks

Flexible policy frameworks and security monitoring



5G Advanced security to become the foundation for next generation platform

5G NR security foundation

Established in Release 15, building on the proven LTE security framework and deployment experiences

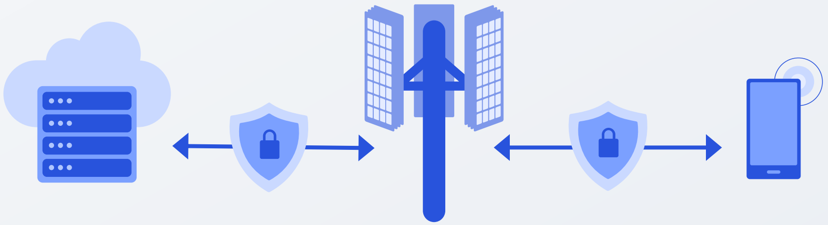
Continued enhancements to platform security and user data privacy

4G security and privacy

Continued evolution to strengthen the mobile security foundation

5G Security

Release 15



5G security foundation

Release 15

Focusing on end-to-end system security for eMBB use cases (e.g., smartphones)

Flexible, unified, and strong subscriber authentication

Supporting

- Various mutual authentication protocols (i.e., 5G-AKA[1], EAP-AKA’, and EAP-TLS[2]) and non-SIM authentication for non-public networks and IoT devices
- Unified procedures for 3GPP and non-3GPP access
- Secondary authentication and authorization for data network access

Enhanced subscriber privacy

Providing encryption for long-term subscriber identifiers via Subscription Concealed Identifier (SUCI)

Secure service-based architecture (SBA)

Supporting TLS 1.2/1.3 to protect transport layer communication and OAuth[3] 2.0 to ensure service access only to authorized network functions

Secure roaming interconnects

Introducing SEPP[4] at the application layer to provide communication protection in interconnect networks

User-plane integrity

Introduced for 5G NR standalone with the flexibility of reduced data rate

3GPP Release 15 established the security foundation for 5G

1 Authentication and Key Agreement; 2 Extensible Authentication Protocol - Transport Layer Security; 3 Open Authorization; 4 Security Edge Protection Proxy

5G Security

Release 16

5G security foundation

Release 16

Enhancing security for non-public networks, IoT, commercial use cases and beyond

Use case-specific security enhancements

Ensuring security and privacy for cellular IoT, V2X, URLLC services, and integrated access backhaul (IAB)

Specific network slice authentication and authorization

Providing separate authentication and authorization per network slice

Secure non-public networks

5G private networks provide security and privacy on dedicated resources that are independently managed

Inter-PLMN user plane security

The role of the User-Plane Function (UPF) is expanded to include traffic protection with a common firewall between two roaming PLMNs

Full-rate user plane integrity protection

No rate limitation allowing a receiver to determine that received messages are not tampered with by an attacker

Secure industrial IoT

Expanding TSN[1] support for time synchronization and time-sensitive communications (TSC) for applications, along with the corresponding security mechanisms (i.e., secure interfaces, authentication and authorization)

Improving 5G system resiliency for broader devices, use cases, verticals

[1] Time Sensitive Networking

5G Security

Release 17

5G security enhancements

Release 17

Improving security for sidelink, drones and broadcast systems

Secure unicast, multicast and broadcast applications

Protecting both user and control planes

Secure proximity-based services

Providing security for sidelink communications (i.e., security for direct discovery, direct communications, and relay communications)

User consent framework

Establishing a framework for privacy control of user data collected by the network

Security for drones

Ensuring security and privacy for unmanned aerial systems (UAS)

Improved edge security

Supporting security between UE and AF

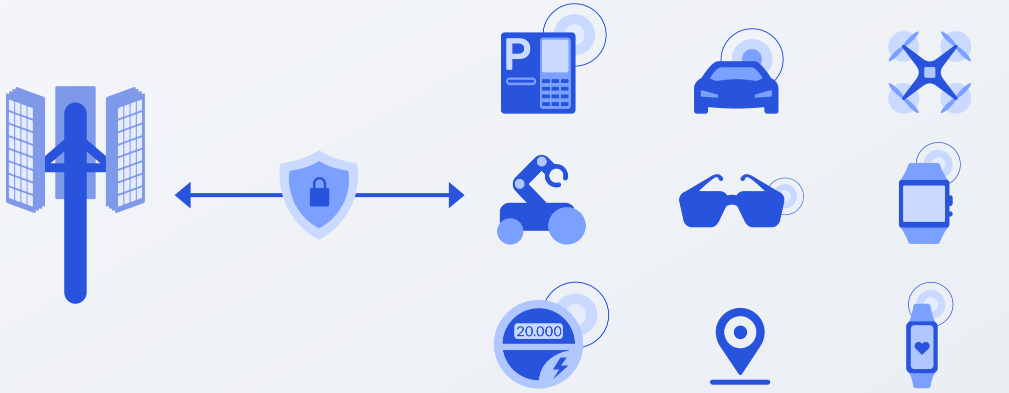
Secure enablers for network automation (eNA)

Securing data collection and analytics for network automation – including AI/ML

Strengthening system security for new 5G communication modes

5G Security

Release 18+



5G advanced security enhancements

Release 18+

Expanding to new devices, use cases, deployments

Sidelink positioning and ranging security

Protecting both user and control planes

AI/ML security

Securing AI/ML model and data to ensure the robustness of AI/ML in 5G system

Security enhancements against false base stations

Continued efforts from Rel-16 to identify and address potential threats from false base station

Identity privacy

Securing data collection and analytics for network automation - including AI/ML

Personal IoT network security

Securing access to a personal IoT network and its communication

Continued enhancements for new use cases & deployments this decade

And establishing the security foundation for next-generation mobile platform

Key longer-term research vectors enabling the path towards 6G

AI-native E2E communications

Scalable network architecture

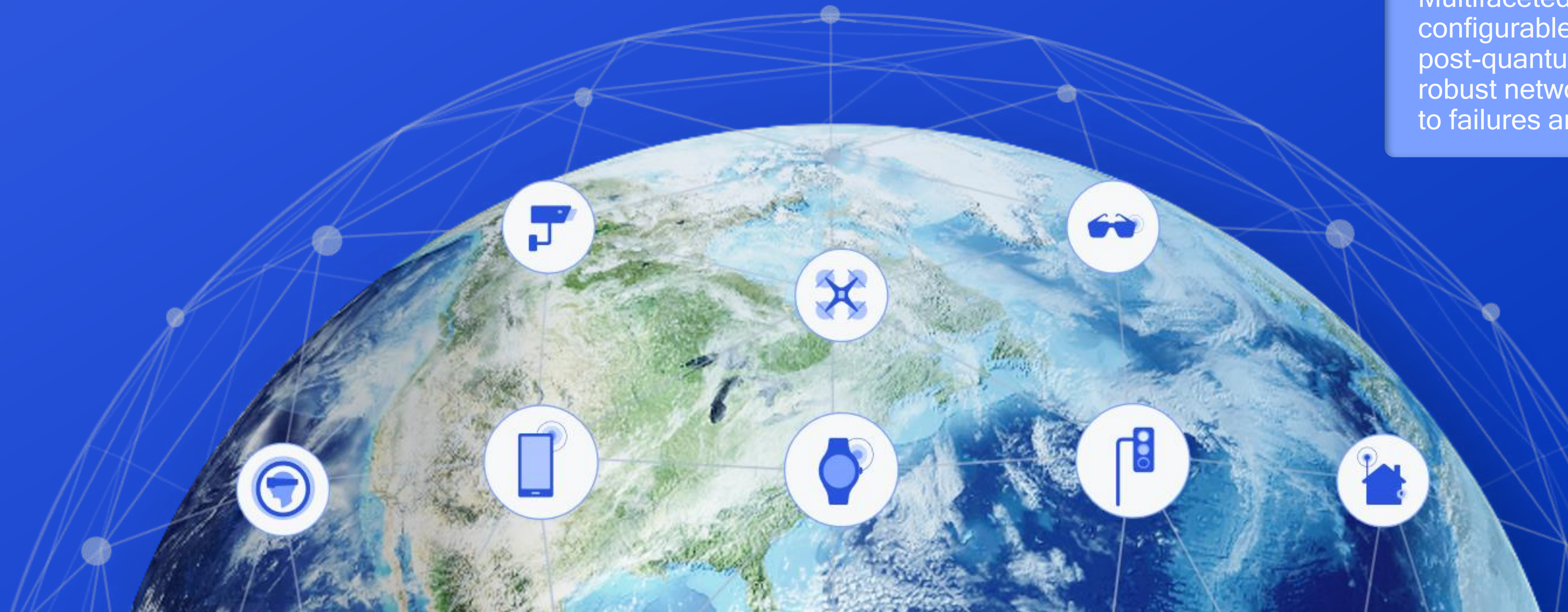
Expanding into new spectrum bands

Merging of worlds

Air interface innovations

Communications resiliency

Multifaceted trust and configurable security, post-quantum security, robust networks tolerant to failures and attacks



Our research focus in 6G communications resiliency across all layers

A continuous end-to-end approach to system security and data privacy

Native security

Security across all layers

Service adaptive security

Cloud-native security architecture

Post-quantum security

Post-quantum crypto algorithms

Quantum security (QKD, QRNG)

Data security and privacy

AI/ML security

Confidential computing

Homomorphic encryption

Robust trust

Multifaceted trust

Zero-trust architecture

Verifiable root of trust

Other key research areas

- Jamming resilience
- Generative adversarial network
- Ultra secure communication
- Web 3.0
- Differential privacy
- Remote attestation
- Secure multi-party computation
- Blockchain
- Confidential computing architecture
- Physical layer security
- Data ownership structure/ management
- Secure device onboarding
- Deep fake protection
- Homomorphic encryption

Zero-trust security is at the core of a resilient system

Zero trust security model

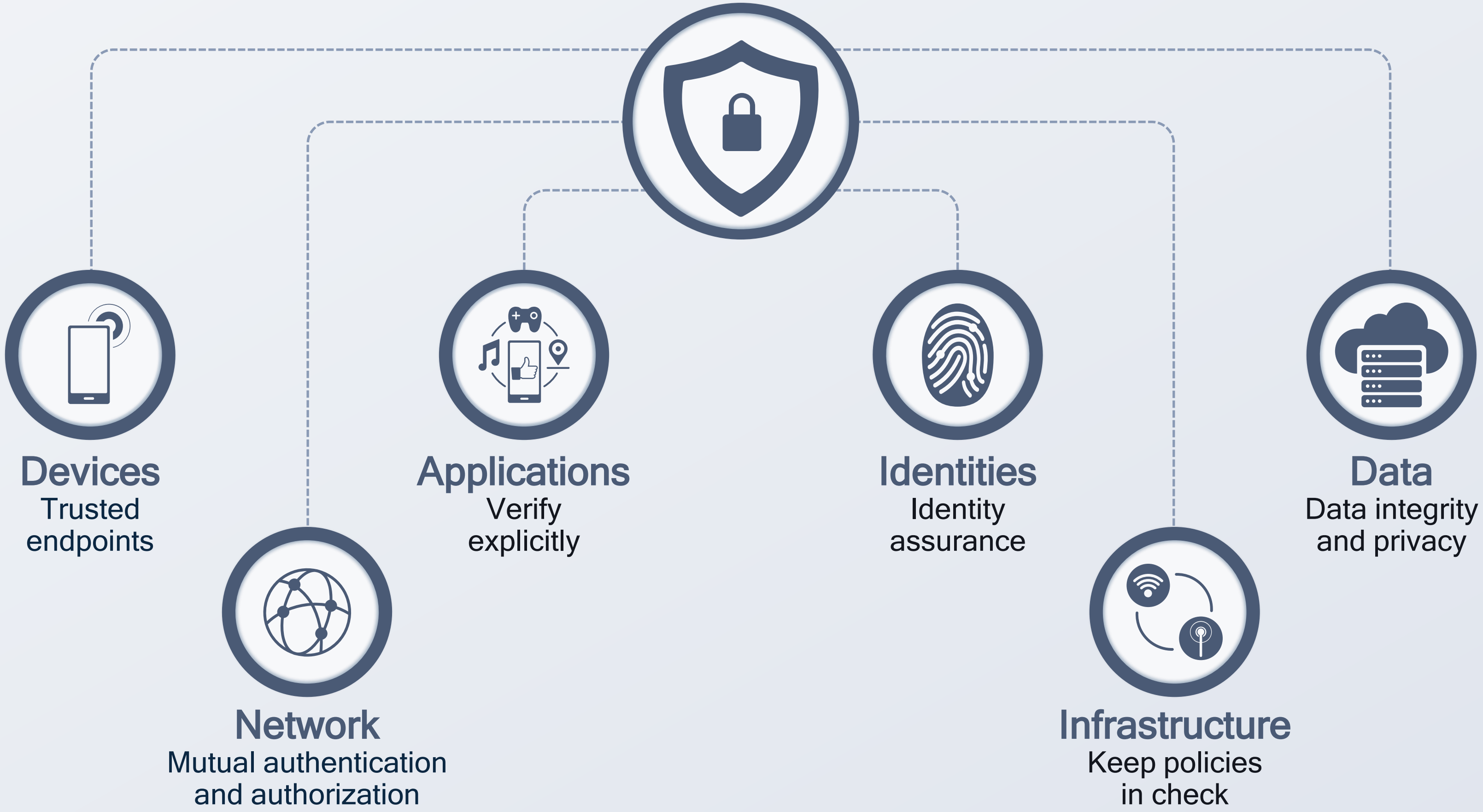
moves defenses from static, network-based perimeters to focus on users, assets, and resources

“Never trust, always verify”

approach to security, both inside and outside of the network

Zero Trust Security Model

Built on web protocols utilizing virtualization, containerization, and cloud-based platforms


Devices
Trusted endpoints

Network
Mutual authentication and authorization

Applications
Verify explicitly

Identities
Identity assurance

Infrastructure
Keep policies in check

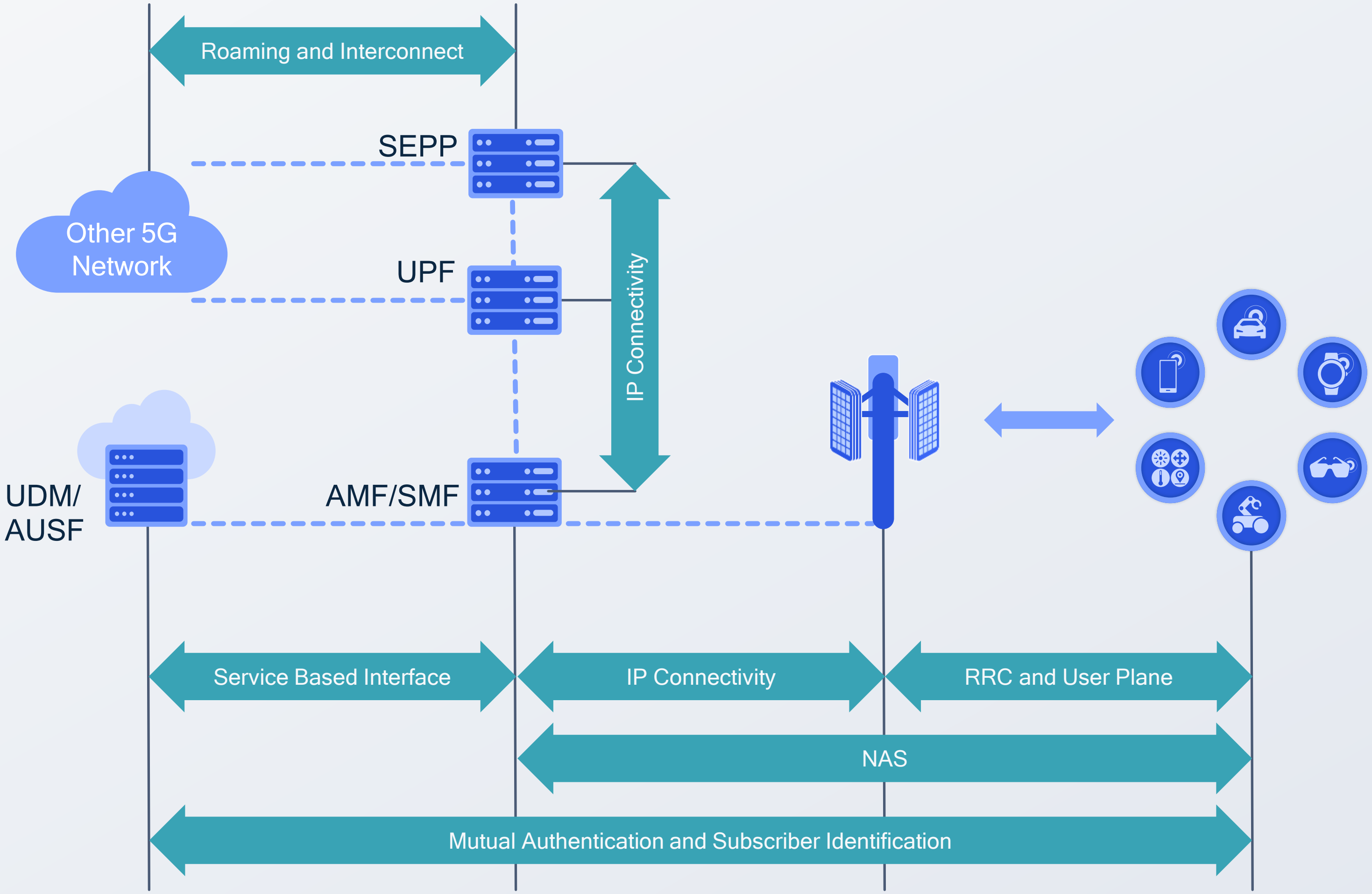
Data
Data integrity and privacy

5G security provides compatibility with zero-trust principles

Zero-trust principles	5G Security
All data sources and computing services are considered resources	The 5G network (i.e., UEs, RAN, transport, core, applications, and services) comprises of assets and data sources
All communication is secured regardless of network location	Secure communications in 5G include TLS, IPSec, SUCI, and user plane integrity protection
Access to individual [operator] resources is granted on a per-session basis	Authentication and key agreements using 5G-AKA, EAP-AKA', or EAP-TLS. Network slice specific authentication and authorization, secondary A&A for data network access, fine-grained authorization using OAuth in the service-based architecture
Access to resources is determined by dynamic policy	The PCF[1] feeds the AMF[2] with access and mobility policies that affect UE authorization to access 5G network resources. The NRF[3] grant access tokens to network functions for service access
Operator monitors and measures the integrity and security posture of all owned and associated assets	NWDAF[4] incorporates standard interfaces from the service-based architecture to collect data and evaluate systems in terms of compliance with security policy rules
All resource authentication and authorization are dynamic and strictly enforced before access is allowed	OAuth 2.0 token-based authorization for any network function that wants to communicate with another one
Operator collects information about the current state of assets, network infrastructure and communications and uses it to improve its security posture	Leverage continuous diagnostic and mitigation (CDM) systems as defined by NIST, and have a GSMA NESAS compliant supply chain risk management (SCRM)

1 Policy Control Function; 2 Access & Mobility Management Function; 3 Network Repository Function; 4 Network Data Analytics Function

5G provides a zero-trust architecture to secure connectivity at scale



End-to-End Security Considerations

Mutual Authentication between device and network

Encryption and Integrity Checking

- Signaling: NAS and RRC
- User plane

Protecting the Subscriber Identity:

- SUCI: IMSI encryption

Protecting the 5G SBA

HTTP/TLS: mutual authentication and data encryption

OAuth 2.0: client authorization by service provider

Securing AN to CN Communication:

IPSec

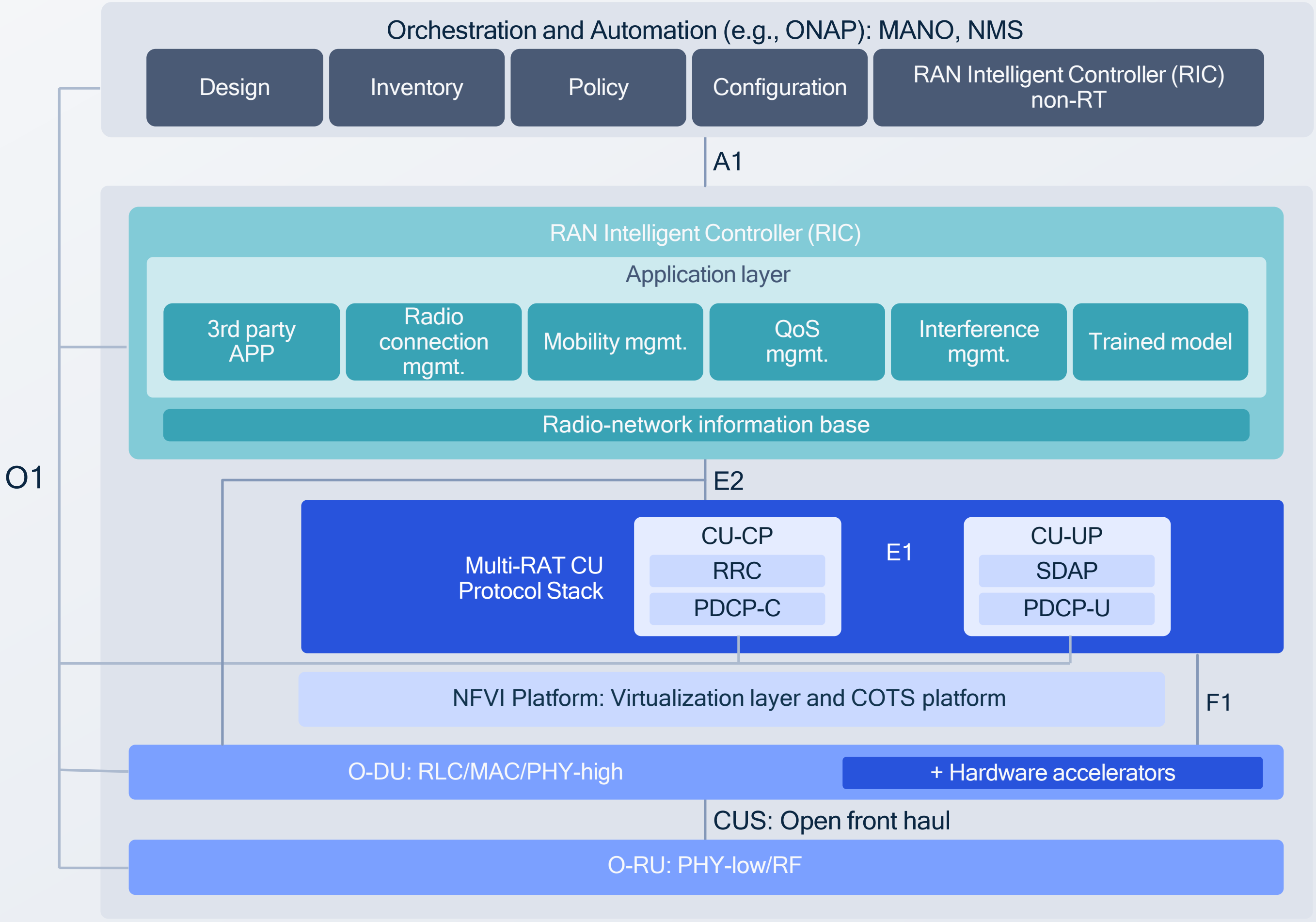
Roaming Security

Security Edge Protection Proxy

PRINS: signaling security

IPUPS: user plane security

Transparency and openness of O-RAN pave the way to a more secure cellular system



O-RAN's disaggregated architecture brings many security benefits such as agility, adaptability, and resiliency

Interface Security

Standards-defined security mechanisms on all interfaces

Software Security

Self-certification encompassing code testing, verification, and signing

Software Bill of Material (SBOM) to secure SW supply chain and lifecycle management

Zero-Trust Model

Endpoints are authenticated, authorized, and continuously validated to be granted or keep access to resources

Learn more:

Thank you

Qualcomm

Follow us on:

For more information, visit us at:
qualcomm.com & qualcomm.com/blog

Nothing in these materials is an offer to sell any of the components or devices referenced herein.

References in this presentation to “Qualcomm” may mean Qualcomm Incorporated, Qualcomm Technologies, Inc., and/or other subsidiaries or business units within the Qualcomm corporate structure, as applicable. Qualcomm Incorporated includes our licensing business, QTL, and the vast majority of our patent portfolio. Qualcomm Technologies, Inc., a subsidiary of Qualcomm Incorporated, operates, along with its subsidiaries, substantially all of our engineering, research and development functions, and substantially all of our products and services businesses, including our QCT semiconductor business.