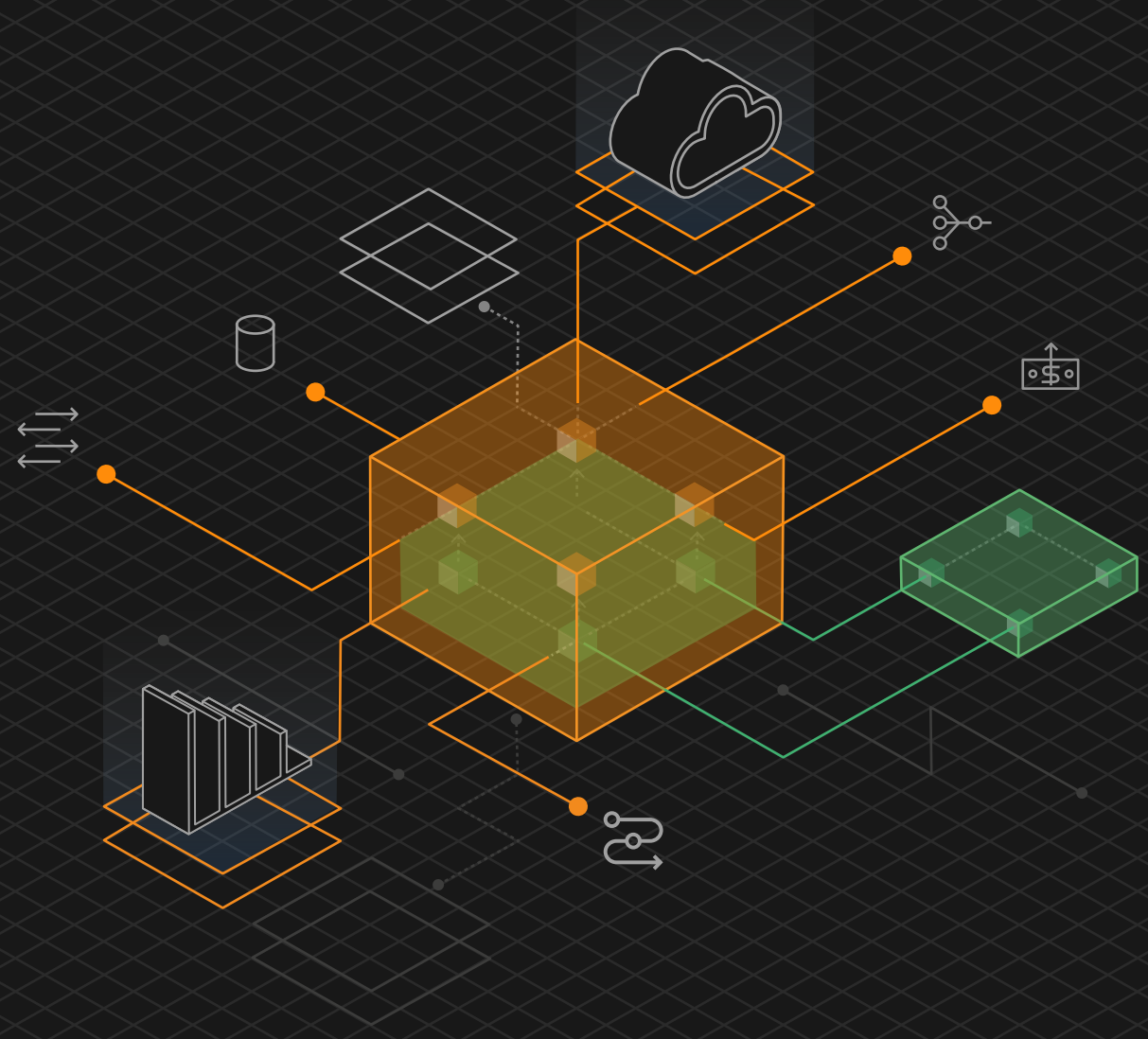
One core — the best of two worlds

Ericsson's dual-mode 5G Core solution



October 2020

Taking a dual-mode approach to core evolution

Ericsson's experience is now applied to 5G. We firmly believe in "one core" for multi-access and services, as well as what we call a "dual-mode 5G Core". But what do we mean by this?

5G has the potential to achieve up to 65 percent population coverage and 2.8 billion 5G subscriptions by the end of 2025. In the same period, mobile data traffic is expected to see a 25 percent compound annual growth rate (CAGR), with 45 percent of this being carried by 5G networks.

For over 140 years, Ericsson has been learning from each and every technology shift. Now, that vast knowledge is being applied to 5G, with a dual-mode 5G Core, for communications service providers (CSPs).

While optimizing the deployment of mobile broadband services, new business opportunities are to be addressed, including enhanced mobile broadband (eMBB), fixed wireless access (FWA), massive Internet of Things (IoT) and critical IoT with automotive vehicle-to-everything (V2X), manufacturing industries and other verticals.

For CSPs to maximize profitability and take advantage of the wide range of business opportunities, flexibility in balancing cost-optimized versus performance-optimized network deployment is crucial. New technologies including, but not limited to, 5G New Radio (NR) Standalone (SA), 5G Core (5GC), network slicing, automation and cloud native are required to meet the needs of an efficient, flexible and programmable network.

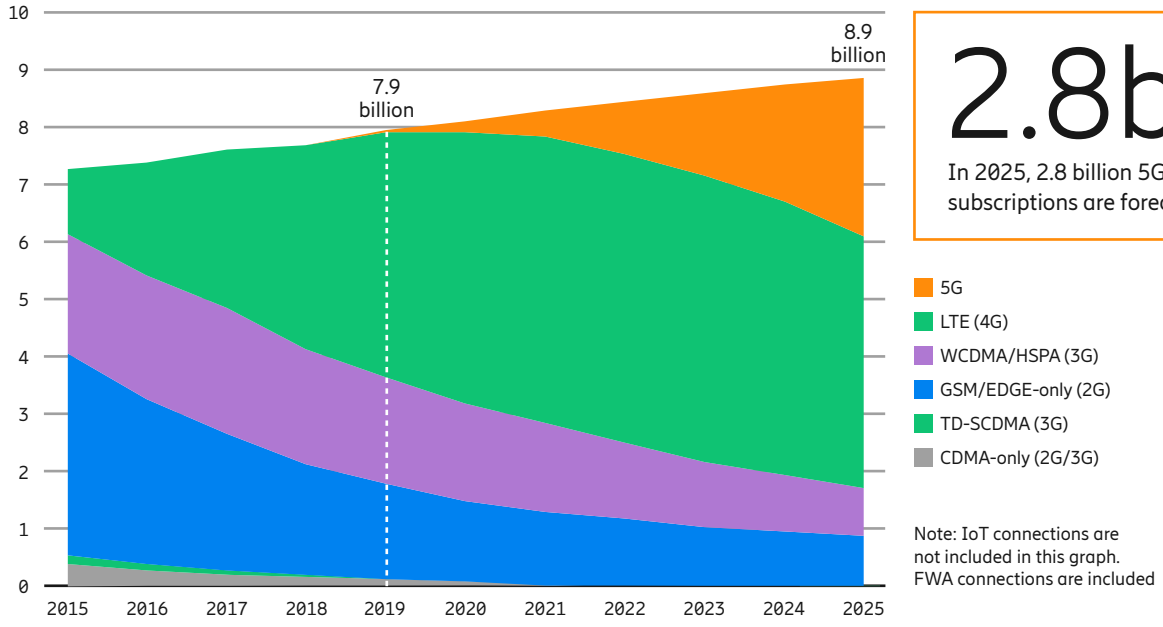
164EB

Mobile data traffic is predicted to reach 164 exabytes per month by the end of 2025.

45%

By 2025, 45 percent of mobile data traffic will be on 5G.

Figure 1: Mobile subscriptions by technology (billion)



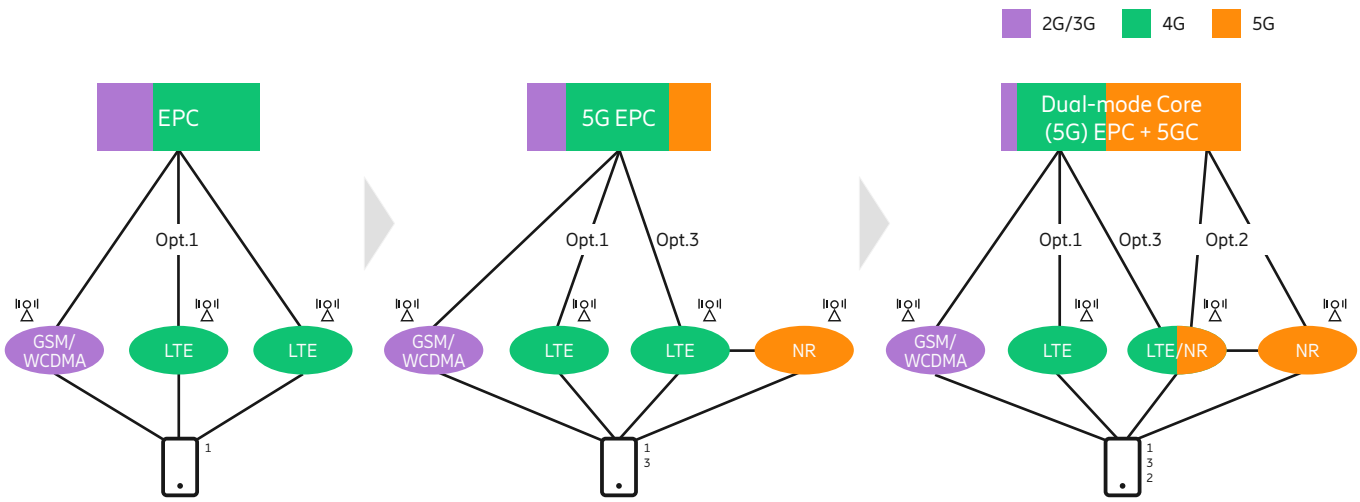
Note: IoT connections are not included in this graph. FWA connections are included

2.8bn

In 2025, 2.8 billion 5G subscriptions are forecast.

Source: Ericsson Mobility Report (June 2020)

Figure 2: Supporting gradual and flexible evolution to 5G



From a core perspective, there are two main steps to support 5G NR, as described in Figure 2. The first phase – NR Non-Standalone (NSA) – is based on an enhanced Evolved Packet Core (EPC), which Ericsson calls 5G EPC. The second phase – NR SA – is a new 5GC built on a service-based architecture (SBA). The timings and steps each CSP takes on the 5G journey will depend on market conditions and when it makes most business sense.[1] During this journey, Ericsson's dual-mode solution for 5G EPC and 5GC Network Functions (NFs) will support your current services, fast and flexible 5G introduction and smooth network evolution, at your own pace.

This paper focuses on Ericsson's dual-mode 5G Core solution and its products, including Packet Core, Subscriber Data Management (SDM), Policy and Signaling functions. These products consist entirely of microservice-based cloud native NFs that deliver 5GC and 5G EPC functionalities, including support for new SBA. The dual-mode 5G Core enables new network capabilities that allow you to release the full potential of new 5G-enabled use cases. This also secures a smooth migration from existing network capabilities.

Ericsson's dual-mode 5G Core supports 5G EPC and 5GC

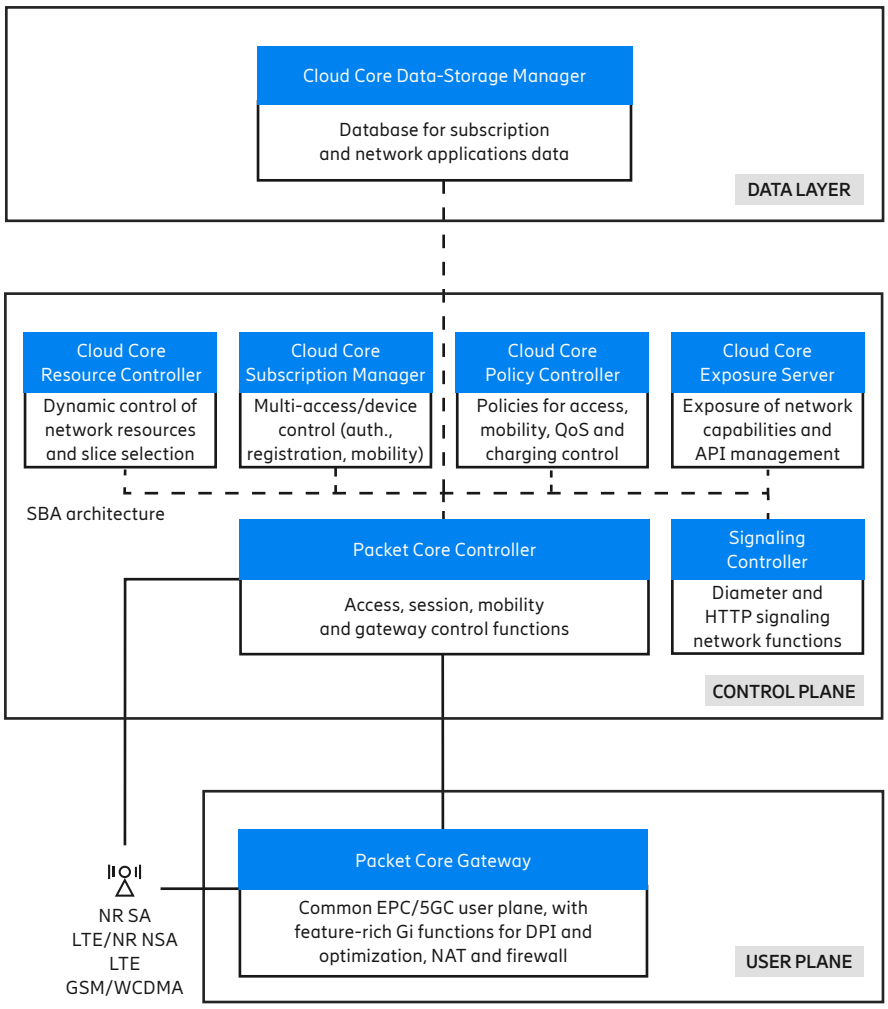
[1] Ericsson, Building a new world: Evolution from EPC to 5G Core

A cloud native and programmable solution

Ericsson's dual-mode 5G Core solution delivers cloud native applications that support EPC and 5GC 3GPP architectures.

This allows for a multi-access and programmable 5G Core solution, including support of 5G NR (NSA and SA) deployments, as well as all previous generations, in a single software platform for operational efficiency. It incorporates Ericsson's Cloud Packet Core, Cloud Unified Data Management (UDM) and Policy as well as Signaling Controller NFs in eight new, efficient products.

Figure 3: Ericsson's dual-mode 5G Core portfolio



Portfolio highlights:

- Single platform for (5G) EPC and 5GC functionalities
- Cloud native/microservices architecture
- Automated and simplified operation and maintenance (O&M)
- Network exposure capabilities for programmability
- High user plane (UP) performance and scalability
- Flexible allocation and control of network resources

Why 5GC is different

5GC is a new network architecture introduced in 3GPP Release 15.

The major difference, compared to EPC, is that 5GC's control plane (CP) functions interact in SBA. A key NF of SBA is the Network Repository Function (NRF), which provides NF service registration and discovery, enabling NFs to identify appropriate services in one another.

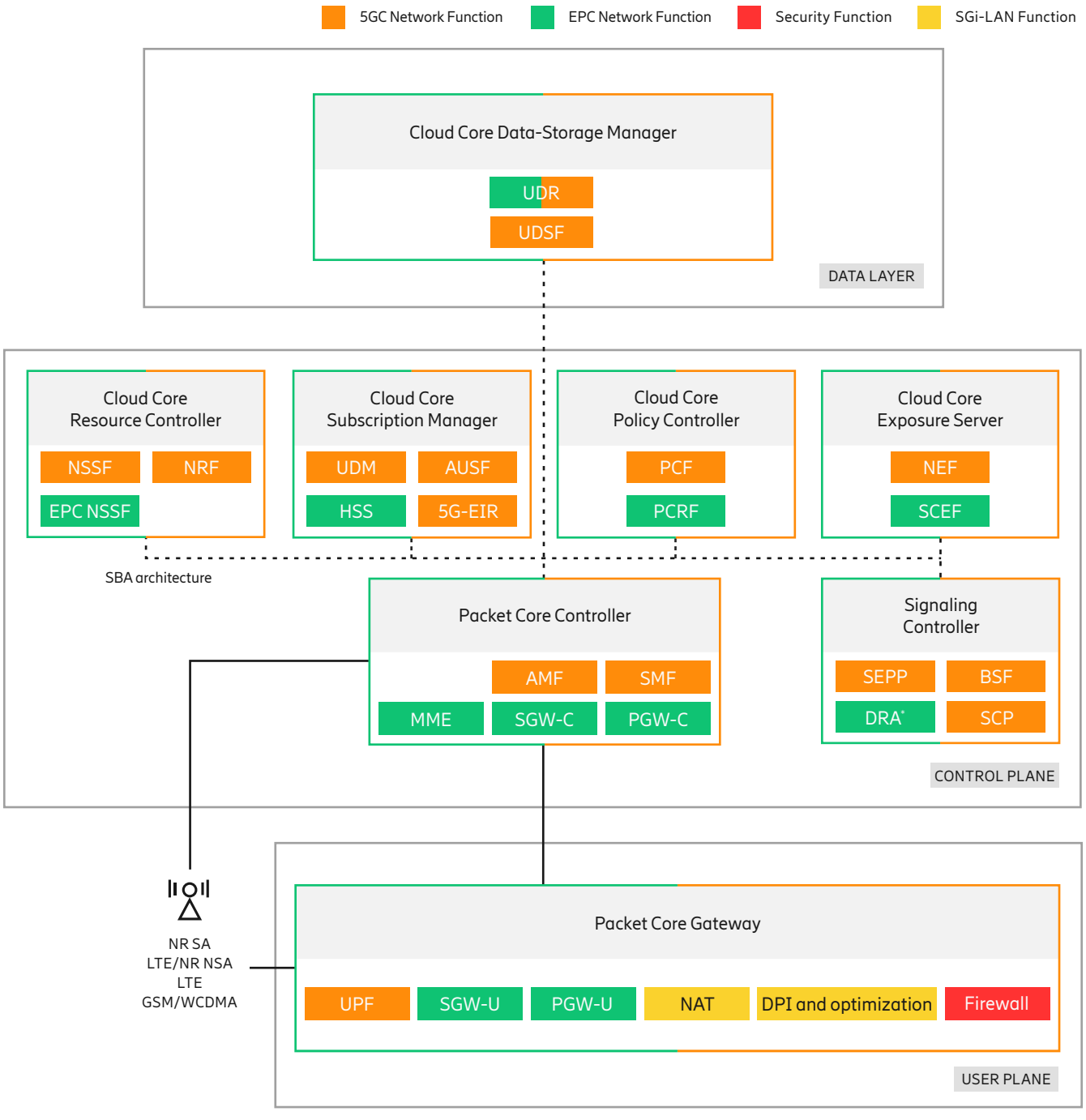
SBA principles apply to interfaces between CP functions within 5GC only, so interfaces toward Radio Access Network (RAN), user equipment or User Plane Functions (UPF – N1, N2, N3, N4, N6 and N9) are excluded. Leveraging the capabilities within SBA with common O&M interfaces across the complete portfolio shows estimated savings of up to 80 percent when adding new NFs, compared to the traditional way of building networks. Another major difference in 5GC's CP is the structure, with different functional separation of Access and Mobility Functions (AMF) and Session Management Functions (SMF). 5GC includes the separation of UP and CP functions of the gateway, an evolution of the gateway CP/UP separation (CUPS) that was introduced in EPC Release 14. 5GC also introduces a completely new protocol HTTP/2 as compared to Diameter in 4G to communicate between various NFs. 5GC-specific signaling functions include Service Communication Proxy (SCP), Binding Support Function (BSF) and Security Edge Protection Proxy (SEPP). Other changes include a separate Authentication Server and several new functions, such as the Network Slice Selection Function (NSSF) and Network Exposure Function (NEF).

Considering a CSP's concerns to protect investments made in their networks, Ericsson has designed a solution that allows full integration of new cloud native NFs with virtualized or physical NFs (VNFs and PNFs) in the same network, and offers different migration paths to bring all NFs into a fully cloud native, dual-mode 5G Core over time. This permits deployment flexibility, full interworking with legacy networks and a smooth evolution to 5GC.

Ericsson's dual-mode 5G Core solution is fully based on cloud native principles, with software architecture based on microservice technology. It ensures capacity, elasticity and agnosticity to underlying infrastructure, and high levels of orchestration and automation for operational efficiency. See the "Automated operations for speed and efficiency" section for more on Ericsson's cloud native design principles and microservice architecture.

5G is here and Ericsson's 5G Core will greatly help CSPs reap the benefits

Figure 4: Inside Ericsson's dual-mode 5G Core portfolio



* DA and DEA functions also supported

Dual-mode 5G Core NFs:

- 5G-EIR: 5G Equipment Identity Register
- AMF: Access and Mobility Management Function
- AUSF: Authentication Server Function
- BSF: Binding Support Function
- DPI and optimization: Deep Packet Inspection and TCP traffic and video optimization
- DRA: Diameter Routing Agent
- EPC NSSF: Evolved Packet Core Network Slice Selection Function
- Firewall: Integrated Security Functions
- HSS: Home Subscriber Server
- IPUPS: Inter-PLMN UPF Security
- MME: Mobility Management Entity
- NAT: Network Address Translation
- NEF: Network Exposure Function
- NRF: NF Repository Function
- NSSF: Network Slice Selection Function
- PCF: Policy Control Function
- PCRF: Policy and Charging Rules Function
- PGW-C: Packet Data Network Gateway – Control Plane
- PGW-U: Packet Data Network Gateway – User Plane
- SCEF: Service Capability Exposure Function
- SCP: Service Communication Proxy
- SEPP: Security Edge Protection Proxy
- SGW-C: Serving Gateway Control Plane
- SGW-U: Serving Gateway User Plane
- SMF: Session Management Function
- SMSF: Short Message Service Function
- UDM: Unified Data Management
- UDR: User Data Repository
- UDSF: Unstructured Data Storage Function
- UPF: User Plane Function

The products

Here, we look deeper into the products and how they can help evolve your network.

Packet Core Gateway
Packet Core Gateway provides a common UP with UPF, PGW-U, SGW-U and other Gi functions. It delivers advanced and highly efficient processing of data payload, including support for distributed deployment. It further supports tight interworking with an existing EPC.

The product provides high capacity with 193Gbps per dual-socket server, as well as 5G peak rates, such as individual peak rates of 20/10Gbps (downlink/uplink) per UE, in a loaded system without impacting individual user performance.

With scalable software architecture, the UP and CP scale independently to accommodate a range of services and associated traffic profiles. Topological scalability is also supported, where CP functions are centralized while the UP functions are widely distributed to support efficient traffic offload and low latency services.

It supports advanced payload, processing value-added traffic management functions based on intelligent traffic steering, in combination with service chaining and integration with the UPF as one managed solution. With internal service chaining for both Ericsson and Third-Party Products (3PP) value-added services, there is 30 percent less footprint, compared to traditional Gi-LAN deployments.

Examples of traffic management functions include deep-packet inspection, content insertion like header enrichment, content optimization and Transmission Control Protocol (TCP) optimization, comparable to an external TCP optimizer.

The Packet Core Gateway secures development of new services, at both distributed and centralized locations. It is also designed to be stateless with user data in a centralized database. This is key in providing superior high availability, session continuity, ISSUs and smooth scale in/out.

30%

An open and flexible UP with internal service chaining leads to 30 percent less footprint.

The integrated Packet Core Firewall is an all-in-one security offering, combining cloud native UP threat mitigation and advanced security functions. It addresses security use cases for UP deployments in MBB and IoT segments. Packet Core Firewall provides the best TCO compared to any other Packet Core security solution maintaining 5G latency and throughput.

Packet Core Controller
Packet Core Controller is efficient at controlling device network access, mobility and session management including 5GC capabilities with AMF and SMF.

It comes with complete support for EPC signaling with SGW-C, PGW-C and MME functions based on millions of lines of redesigned, industry-hardened code from Ericsson MME and SGW-C/PGW-C business logic. This is all to be fully cloud native with complete functionality for MBB, Voice over LTE and IoT.

The product also provides low risk and the best time to market (TTM) for 5GC deployments by supporting overlay deployments with a rich feature set in AMF and SMF, validated in leading Tier 1 operator trials.

Though optimized for 4G and 5G access, the Packet Core Controller supports 2G and 3G using Control User Plane Split (CUPS), and provides seamless services when outside of 4G and 5G coverage or for roaming.

Similar to how virtual EPC was successfully introduced with a virtual MME as part of a hybrid pool, the product can support the same model. This allows for a reliable method to introduce new cloud native MMEs into a network with geo-redundant pooling across Ericsson's container, virtual and physical MMEs, for capacity expansions and operational transformation in a low-risk way.

One major driver in 4G and 5G EPC for network evolution is CUPS. The product could be deployed as CUPS CP, integrated with existing native or virtual GW nodes deployed as UP.

To allow for more seamless mobility across EPC and 5GC, the PGW-C and SMF business logic is implemented as a combined service. This enables UEs to maintain IP address and session contexts for GW and Gi service chains, also in case of handovers between 5GC and EPC. Similar to the Packet Core Gateway, this product is designed to be stateless with user data in a centralized database.

Building on how most CSPs are deploying and operating their networks today, organization flexibility with access and mobility management, separated from IP service delivery, is supported. This is provided with one set/pool of instances for combined MME/AMF and other instances for SGW-C and PGW-C functionalities across EPC and 5GC. O&M of Northbound Interfaces (NBI) and information models are also unified for all underlying NFs to greatly improve ease of use and total cost of ownership (TCO).

The products that make up Ericsson's 5G Core can help evolve your network

Signaling Controller
Signaling Controller handles all the communication signaling between various 5G Core NFs. The product implements the 3GPP NFs such as SCP, BSF and SEPP in the SBA of the 5GC. The SCP function inside the product is a central element in the overall 5GC network which simplifies the network topology, aggregates signaling from all 5GC NFs, performs load balancing/distribution, signaling throttling, signaling prioritization, parameter harmonization, and handles signaling storms etc. The BSF function inside the product ensures various sessions belonging to a single subscriber originating on different interfaces are bound together and routed towards the same PCF. It is mandatory when there are two or more PCFs in the network to select from. It also enables 5G voice. The SEPP function connects to roaming partner networks and is mandatory to enable 5G roaming and security.

Signaling Controller also comes with complete support for Diameter-based signaling functions such as Diameter Agent (DA), Diameter Edge Agent (DEA), Diameter Routing Agents (DRA) and Server Lookup Function (SLF). Signaling Controller includes a Unified Signaling Firewall that secures networks across 2G/3G/4G/5G technologies. The product is designed on robustness principles and covers both the 4G and 5G signaling needs for CSPs. It implements the same logic and behavior across the Diameter and HTTP signaling domains.

Cloud Core Resource Controller
Cloud Core Resource Controller is the commercial realization of the NSSF and NRF functions in the 5GC.

The product provides control of network resources and services, securing awareness of the status and use toward the other NFs. Based on this, the Cloud Core Resource Controller can dynamically steer the UE's traffic from one slice to another to fulfill commercial service requirements and deliver the expected Quality of Experience (QoE).

The key role of NRF inside the product is to provide resource control in the network in an automated way, where resources include NFs and NF services. NRF maintains the NF profile of available NF instances and their supported services, received from NFs during registration. NRF functionality removes the need for network configuration every time a new NF is added or removed from the network, or every time NF capacity is updated due to scale-in or scale-out. NRF also provides key functionalities to improve robustness in the network due to its crucial role in 5GC architecture.

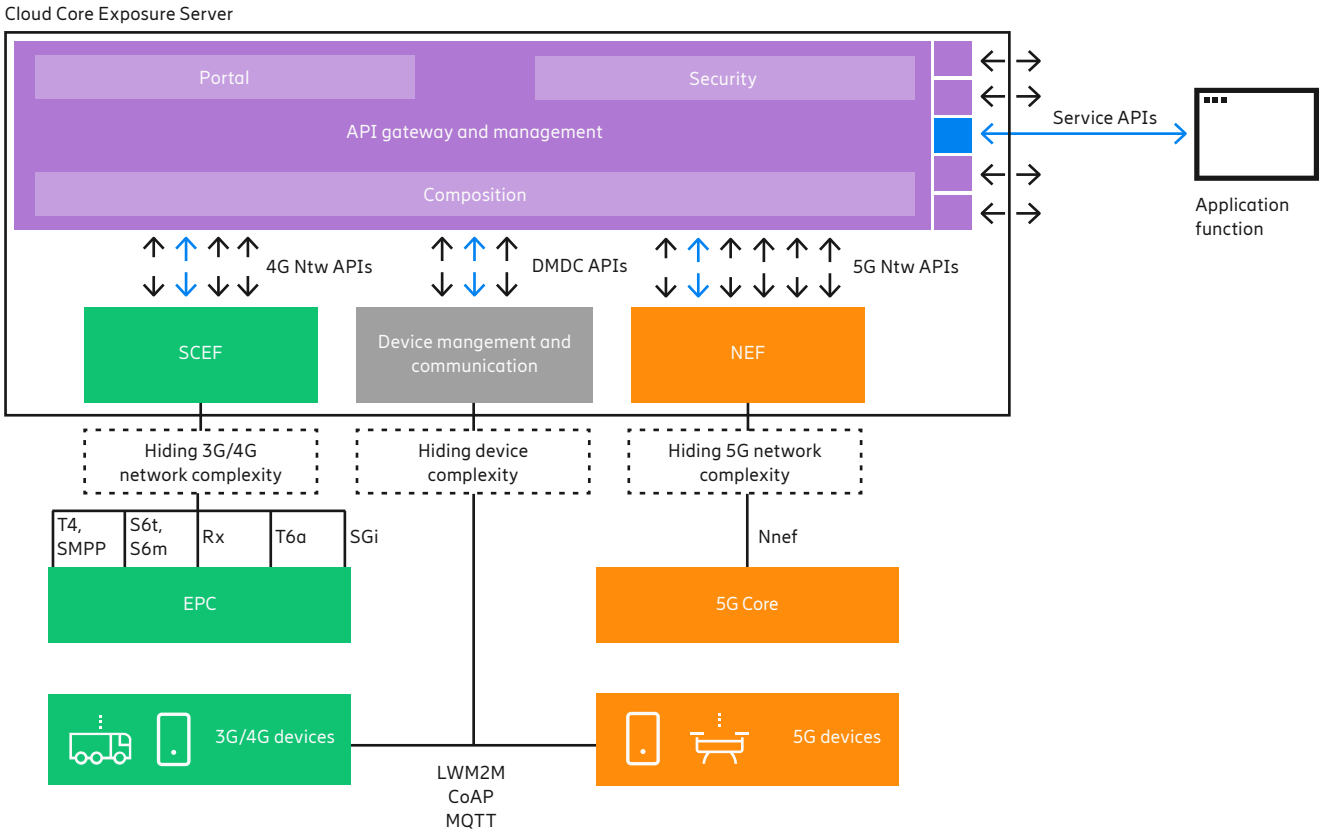
The key role of NSSF inside the product is to dynamically place a UE on the most suitable slice according to a CSP's defined policies. It provides policy-based realization of NSSF, enabling the implementation of CSP policies for network slicing in real-time, based on NSSF user and network context awareness.

The Cloud Core Resource Controller also supports a slice selection mechanism applicable to the 3G/4G network. This is called EPC NSSF and is based on Packet Gateway allocation.

Cloud Core Subscription Manager
Cloud Core Subscription Manager is the commercial realization of the UDM/Authentication Credential Repository and Processing Function (ARPF), AUSF functions in 5GC and evolves HSS-EPC, HSS-IP Multimedia Subsystem (IMS) and EIR functions in 3G and 4G core networks. It supports a dual-mode operation, with all 3G, 4G and 5G NFs in the same VNF, providing optimal and efficient interworking with existing HSS in the legacy domain.

The product handles identifiers, authentication, registration, mobility and subscription data management for multiple end-user devices. It executes access authentication of these devices connecting over 3G, 4G and 5G, and secures the radio-access type with the best quality at any time, harmonizing the service experience over the different access technologies (service continuity). The Cloud Core Subscription Manager also supports overload-protection mechanisms to secure high, resilient telco-grade performances.

Figure 5: Foster business innovation with network exposure capabilities



Cloud Core Policy Controller

Cloud Core Policy Controller provides the PCF function in 5GC and includes support for EPC (2G/3G/4G) networks with PCRF capabilities.

It offers a centralized policy control point for the new-generation core networks, providing the tools to dynamically optimize the service delivery settings to provide the best QoE. It offers all the cloud native advantages together with Ericsson's experience in policy with the main global operators.

The product takes policy control to a new dimension. User Experience (UX) is one of the key assets. Policy handling has been simplified and flexibility increased, allowing multiple configuration options. It is possible to deploy different flavors specialized in either session management or in user, access and mobility management.

The Cloud Core Policy Controller is a perfect fit for new networks, giving a fresh programmability dimension. Closed loops with artificial intelligence modules will allow fresh information flow from the UP, adapting the policies to the actual network behavior. All of this is complemented by the geographical redundant configuration for maximum resilience and robustness.

Cloud Core Exposure Server

Exposure Server is the commercial realization of the NEF function in the 5GC, as well as the evolution of SCEF in 3G and 4G core networks.

As seen in Figure 5, it is an exposure platform able to aggregate 4G and 5G network Application Programming Interfaces (APIs), enabled by SCEF and NEF, and to compose them for the creation and the secure exposure of advanced service APIs.

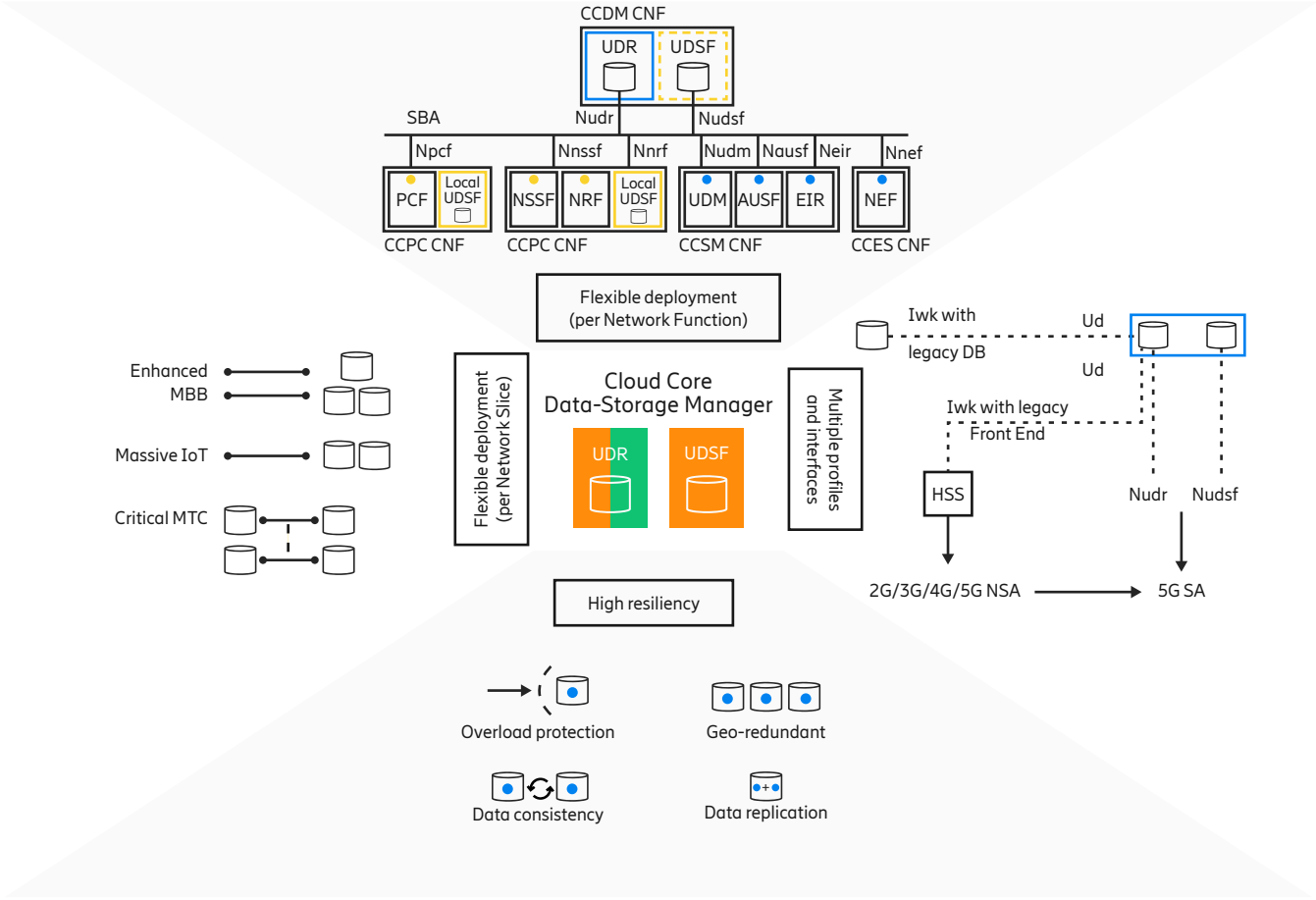
Service APIs can be designed around the concrete use cases that CSPs want to address in the market, enabling them to securely expose and monetize the 3G, 4G and 5G core network capabilities toward external parties.

The product supports the modular and flexible deployment of embedded or standalone NEF, SCEF and API Gateway and management modules, offering the CSPs maximum flexibility in designing their network exposure platform. With multi-layered and flexible security mechanisms, it also secures a CSP's network while exposing the capabilities and new business innovations to third parties. The product can also be used to expose network capabilities internally to the CSP's trusted domain.

The Cloud Core Exposure Server plays a key role in making a network really programmable, enabling more than a 4 percent increase in total revenue by Open Network APIs.[2]

[2] Ericsson, "5G Core programmability: an underestimated opportunity"

Figure 6: Highly resilient and flexible data storage, combining telco-grade and cloud native design



Cloud Core Data-Storage Manager
Cloud Core Data-Storage Manager is the commercial realization of the UDR and UDSF functions in the 5GC, including some key functionalities for interworking with 3G and 4G application front ends.

It stores subscriber and network control data, and user and service profiles for 5G NR as well as 2G, 3G and 4G access. It is based on UDR and UDSF NFs that allow flexible distribution of data storage points across different network slices and NFs, to address all the various needs for data centralization or distribution.

As described in Figure 6, this is a cloud native database, fulfilling the needs of cloud native deployments, but still coping with telco-grade characteristics.

The Cloud Core Data-Storage Manager addresses telco data repository needs (dynamicity, access speed and frequency, and data structure) in a cloud native environment, securing high-level telco-grade robustness based on unique protection mechanisms that are well consolidated and proven in the market, like overload protection.

To support smooth migration toward 5G, the product can store 2G, 3G, 4G and 5G subscription profiles, thanks to its ability to interwork with legacy databases (CUDB) and Front Ends (HSS-FE), and new 5G Front Ends (UDM).

Automated operations for speed and efficiency

Beyond functional compliance to 3GPP specifications and advanced functionalities, Ericsson's dual-mode 5G Core solution includes several enhancements.

Examples include cloud native software architecture, Continuous Integration/ Continuous Delivery (CI/CD), unified O&M and MANO/ONAP support, as well as network slice optimizations. All these enable service differentiation and efficient network operation with lower TCO.

Cloud native and microservice architecture
Ericsson's software architecture is based on cloud native design principles. Applications are delivered and executed as a set of containers and designed to run on a Vanilla Kubernetes Container as a Service (CaaS). It is designed to get the right balance between requirements from two different domains – IT and the telecom environment.

The modularity of Ericsson software, known as microservices (see Figure 7), has been selected to facilitate a short TTM for future functionalities with limited inter-module dependencies. LCM is moved from NF to microservice level, including support for In-Service Software Update (ISSU) and automated upgrades. ISSU greatly improves TCO, going from maintenance windows and traffic migration to smaller daytime updates as a subscription offering service (CI/CD).

The adopted cloud native design principles:[3]

Agnosticity
The ability to run applications in any cloud infrastructure, regardless of the CaaS and Infrastructure as a Service (IaaS) combination. The cloud native applications (CNA) must be able to run in any modern kernel without requiring any proprietary additions.

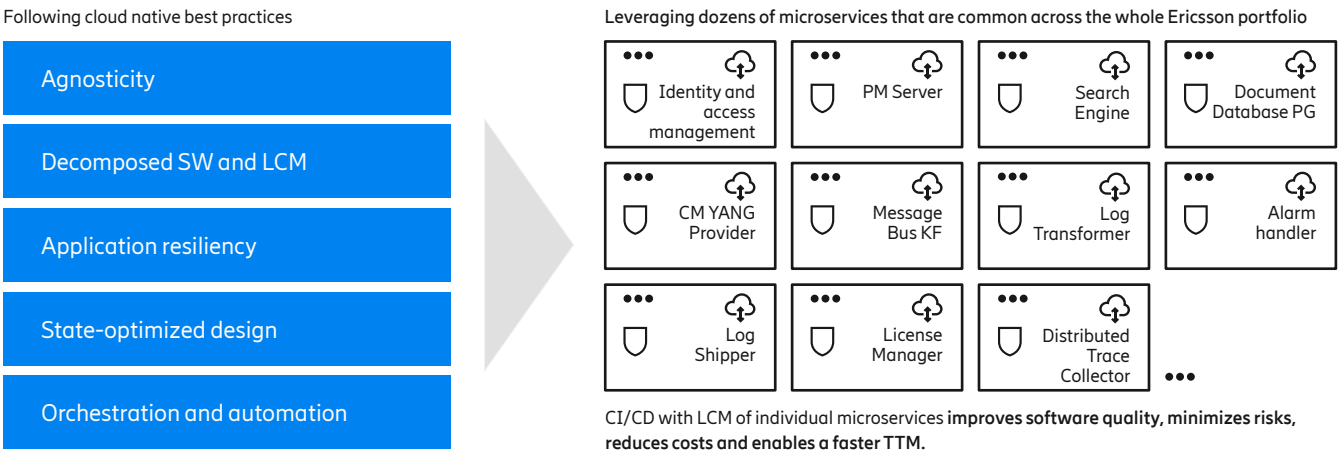
Decomposed software
Leveraging containers and microservice architecture, common across the entire Ericsson portfolio.

Application resiliency
Fault tolerance in applications and services, supporting the combination of failures at any time, without full restart and loss of service. If one instance of each required microservice is alive, the service will be provided.

State-optimized design
This is decided based on the type of state/data and application context. A state-optimized design considers the impact severity of a state/data loss to CNA function, impact on the user, and also the cost/benefit considerations pending frequency of changing states.

Orchestration and automation
Fully automated Lifecycle Management (LCM) of internal microservices. Some examples of automation are auto-scaling, auto-healing and update/ upgrade containers orchestrated by Kubernetes. MANO/ONAP support is provided in alignment with cloud native orchestration and automation; for example, software image registry during software updates.

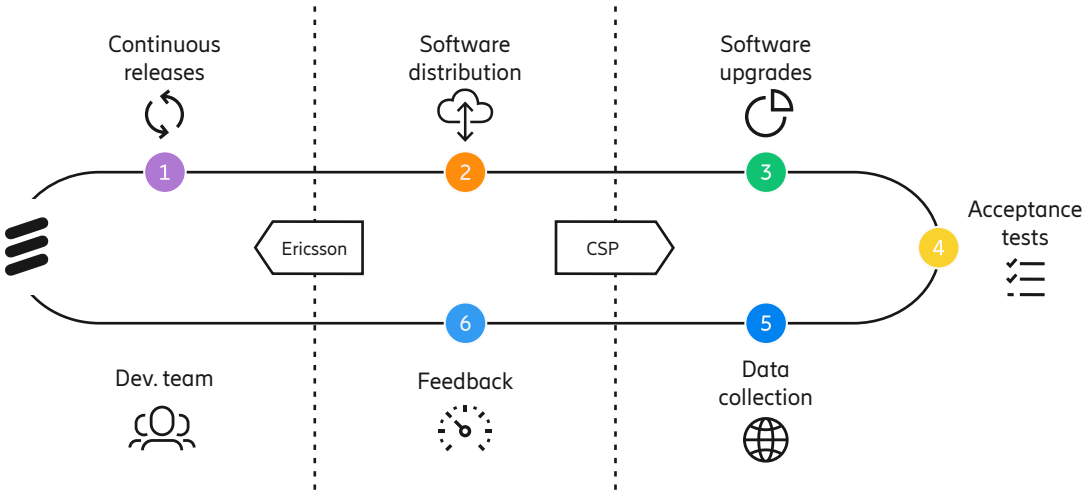
Figure 7: Best practices and leveraging microservices



CI/CD with LCM of individual microservices **improves software quality, minimizes risks, reduces costs and enables a faster TTM.**

[3] Ericsson, Cloud native is happening now

Figure 8: Our approach – automating the entire flow – CI/CD



CI/CD

Ericsson's continuous software integration, delivery and deployment are based on decades of experience in telco app characteristics and have been explored with several CSP leaders in Virtual Network Function (VNF) introduction.

CI/CD is fundamental in leveraging cloud native benefits, and Ericsson is now introducing "zero touch" to automate software LCM to the next level. This includes an automated pipeline that developers commit to testing, and also involves deployment in production and continuous feedback from live deployments within minutes of delivery. All this is to secure continuously improved software quality, reduced opex and faster TTM.

A key enabler to cut time and cost of software deployment is Ericsson's Automated Acceptance Tests (AAT) tool for CSP acceptance test procedure. It simulates RAN, including 5G NR and end-user traffic, and can perform automatic verification of the whole dual-mode solution.

LCM, high automation and unified O&M

Ericsson's dual-mode 5G Core solution's NFs offer a common management interface, covering both EPC and 5GC capabilities, designed to fit with a next-generation Operations Support System (OSS).

This simplifies automation of the solution's O&M, but does not prevent more granular LCM of individual software modules.

It can be used for dynamic and flexible scaling of individual software modules based on capacity needs, such as rebalance EPC versus 5GC resource usage as terminal fleet evolves over time.

With dual-mode, the cloud infrastructure can be dimensioned on an aggregated level and our calculations show savings in the order of 20 percent.

Network slicing and distributed cloud support

The dual-mode 5G Core solution comes with built-in network slicing capabilities to enable new business models across a wide range of industries.

It allows CSPs to segment the network to support particular services, and deploy multiple logical networks for different service types over one common infrastructure.

Ericsson and BT's study on network slicing shows up to 35 percent increased revenue, based on a network with 40 slices.[4]

Network slicing capabilities are supported in 4G, such as enhancements for Dedicated Core Networks (eDECOR) in EPC, and are further enhanced with new functionality in the dual-mode 5G Core. With 5GC, a device can simultaneously be connected to multiple slices, opening up some new use cases. Slice selection can be made based on user-subscription data and any dynamic policies, supported by the slice database.

Furthermore, new functions and procedures are supported which allow for better control of how devices can connect to slices and for end-to-end monitoring.

Network slicing, in combination with the possibility to distribute applications across centralized and distributed edge data centers, depending on use case requirements, is a key enabler to simplifying operations and increasing deployment flexibility.

Ericsson's dual-mode 5G Core and its products are built on these design principles and tools through:

- common design rules
- common architecture principles
- a common reference orchestration platform
- a common set of platform services
- common and powerful CI/CD and deployment pipelines

This enables true DevOps with all its benefits. If applications are not ready for cloud native data center infrastructure, Ericsson can deliver a CaaS layer. Ericsson CaaS can operate on top of an IaaS VM or bare metal for x86-compliant hardware infrastructure.

[4] Ericsson and BT, "Network Slicing is key for the IoT Business Case"

Securing service availability in 5G Core

5G Core service availability has become a top concern as a result of the increased attack surface of 5G networks over multiple dimensions.

As well as enabling new use cases, 5G dramatically increases the role of security for core network assets. Aside from its massive increase in bandwidth speeds, ultra-low latency and geographical coverage, 5G is creating myriad new use cases, including IoT. The number of DDoS attacks rose by 542 percent between Q4 2019 and Q1 2020.[5] The majority of attack sources were IoT devices, powered by Linux (access threats).

Increases in international interconnection roaming agreements, due to 5G deployment and the 28 percent year-on-year growth in roaming subscribers,[6] have led to growing threats from external roaming networks (roaming threats).

In the 5G era, 3GPP networks can meet non-3GPP networks (such as Wi-Fi) and malicious internet applications (internet threats).

The mobile network security market is highly fragmented, with enterprises using up to 70 different security vendors in each company.[7] This is likely due to the challenge of identifying each solution's functionality and interoperability.

Some of these security solutions are "dedicated", since they typically require a separate NF to operate. This triggers TCO penalties in the form of increased capex (hardware dependencies) and opex (more NF to orchestrate and maintain).

Another of dedicated security solutions' shortcomings is the degradation of 5G latency. To maintain this, time-to-mitigation should be kept to milliseconds – which dedicated security solutions can't deliver.

Considering hardware capacity limitations on the edge, scaling of dedicated edge security solutions to accommodate new 5G use cases becomes cost-prohibitive.

Fusion of UP security and advanced security functions

Packet Core Firewall is a cloud native product, providing a fusion of UP security and advanced security functions. It addresses security use cases for core network deployments in MBB and IoT segments, and leverages the following functionality:

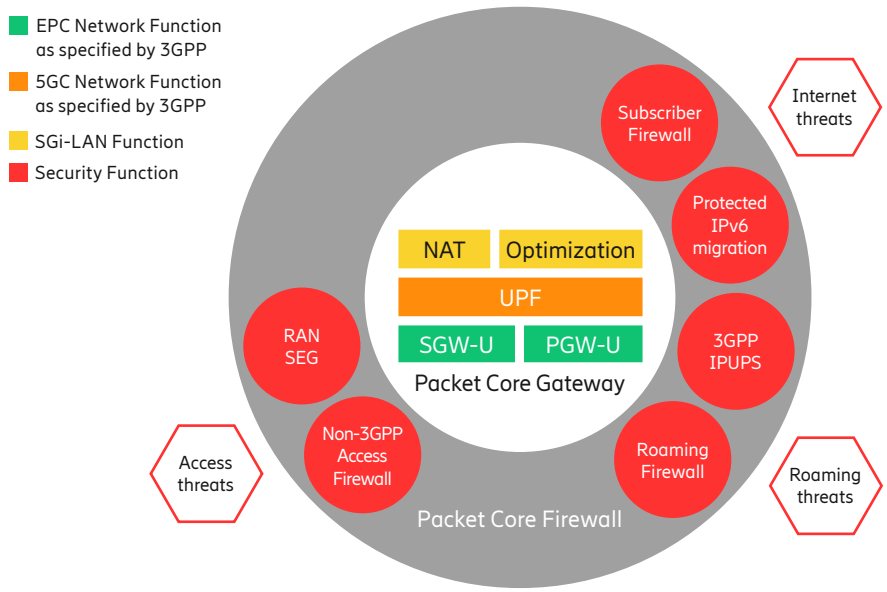
- stateful zone-based firewall policy enforcement and exposure to end-to-end security components (Ericsson Security Manager)
- roaming with integrated inter-PLMN UPF security
- DMZ and non-3GPP access asset protection with cloud native deployment
- advanced threat recognition and behavior change detection based on machine learning
- time-to-mitigation closer to 5G bandwidth demands with inline mitigation capabilities, and closed loop automated recognition with most rapid, business logic-aware decision to mitigate
- effective delegation of mitigation toward transport equipment with coverage of 80 percent of DDoS/DoS attacks toward UP from internet and access directions

Packet Core Firewall ensures better TCO than any other Packet Core security solution with optimized 5G latency and throughput. At its core is a single CNF solution with efficient user session traffic management and no NFVI traffic steering, giving 50 percent TCO savings in NFVI SDN compared to dedicated security solutions.

This means that Packet Core Firewall is tightly integrated with the UP function, triggering no hardware dependencies or orchestration complexities. Latency and throughput performance are optimized since there is no extra hop in the NFVI.

Packet Core Firewall is powered by A10 Networks and ready for edge deployments and 5G use cases. A single CNF solution means it scales in and out simultaneously with the UP, meeting specific 5G use case requirements, including edge/deep edge and small-scale deployments.

Figure 9: The integrated Packet Core Firewall



[5] Nexusguard, "DDoS Threat Report" (Q1 2020)
[6] Juniper Research, "Wholesale roaming – the impact of 5G and RCS" (January 2020)
[7] ZDNet

TCO benefits

Ericsson's dual-mode 5G Core has been conceived to handle the programmability, automated operation and digital exposure required to meet future challenges and business needs.

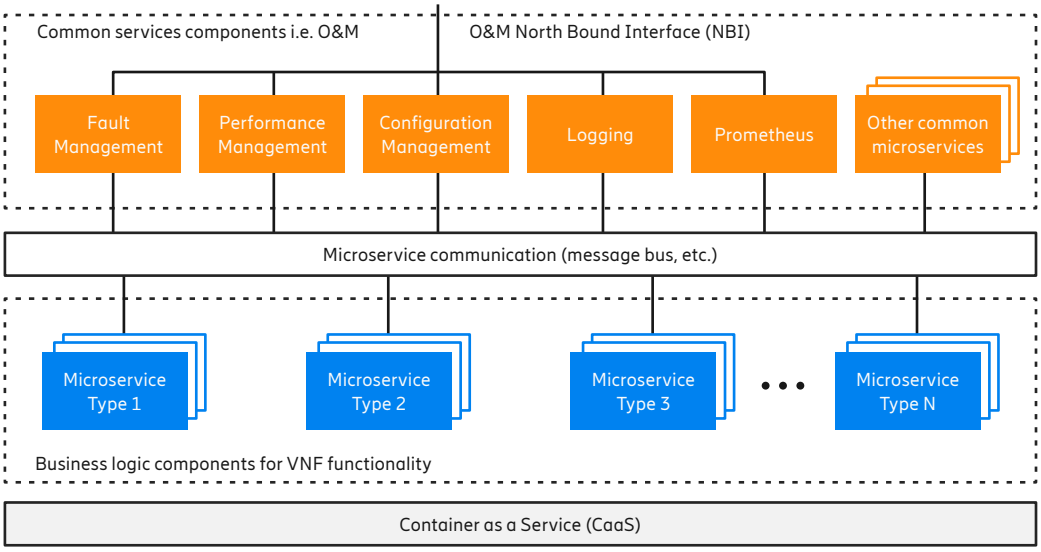
As outlined in this paper, TCO is addressed in numerous ways. Benefits from new technology and architecture are introduced while protecting current investments for smooth migration to a 5G Core.

The introduction of 3GPP SBA and microservice-based cloud native NFs, delivered as one software platform, enables substantial benefits.

Leveraging the SBA together with one unified O&M reduces network and O&M integration costs by up to 80 percent when adding new NFs, compared to today. The dual-mode software platform also creates a foundation for new capabilities and ways of working. Together with the application of CI/CD, it provides more than 60 percent savings in a fully cloud native environment for software upgrades.

In-service software upgrades and individual life cycle management per microservice permit upgrades during daytime, leaving the costly nightly maintenance windows behind and taking these savings even further.

Figure 10: One unified O&M



A cornerstone in Ericsson's dual-mode 5G Core is the unified O&M for EPC and 5GC, as described in Figure 10. A unified NBI with information models, naming of counters, alarms etc. helps to reduce complexity and learning. The platform also includes MANO/ONAP support, enabling automation with artificial intelligence and machine learning, and flexibility in the orchestration solution for easy migration from EPC.

The dual-mode 5G Core solution also contributes to efficient use of resources. During the uptake period of 5G, terminals will move between LTE and NR during the day. With dynamic allocation of resources, dimensioning can be done on aggregated traffic, saving up to 20 percent of infrastructure, though this will be specific from case to case. Ericsson also sees significant footprint and integration cost savings with an open and flexible UP with internal service chaining. Peak rates of 20/10Gbps (downlink/uplink) per UE and up to 193Gbps per dual-socket server also contribute to an efficient TCO.

One example of an additional function in the platform that can significantly improve ease of use and reduce TCO is the built-in software probe solution which enables efficient interface mirroring and event reporting with KPIs.[8]

Data is streamed to external consumers which reduces the need for external tapping and probes, resulting in up to 60 percent footprint savings and 90 percent opex savings with built-in software probes compared to external hardware probes.

Another example is the Network License Server, which handles licenses from one network area instead of local certificates per CNF.

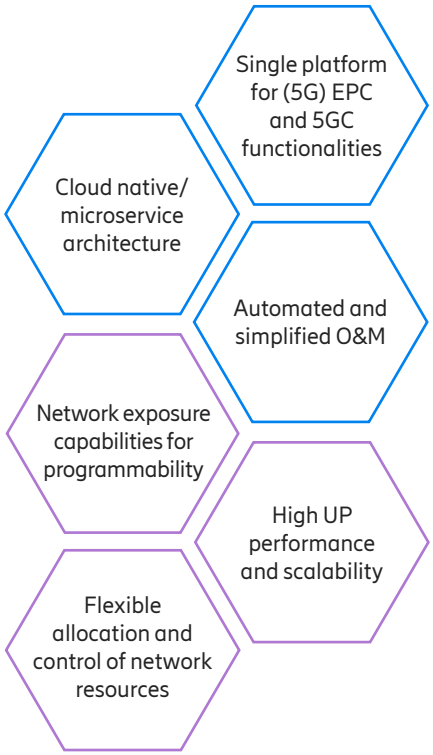
[8] Ericsson, "Securing the 5G experience with software probes"

Summary

Ericsson's dual-mode 5G Core solution delivers a programmable core network for a secure and cost-efficient evolution of your existing networks.

It is based on cloud native design principles, a flexible combination of NFs and a multi-access core solution that includes support for 5G NR (NSA and SA).

Figure 11: Solution highlights



Ericsson's dual-mode 5G Core includes:

- 20 percent savings in infrastructure
- 30 percent less UP footprint
- 50 percent less capex compared to dedicated UP security solutions
- over 60 percent reduction in opex for software upgrades
- 80 percent cost savings in network integration
- 60 percent footprint savings and 90 percent opex savings with built-in software probes
- over 4 percent ARPU for network exposure

5G will greatly change how consumers use their devices and experience the world

For more insight into how TCO can be managed, please see Ericsson's "Dual-mode 5G Core: TCO benefits" report.

Ericsson enables communications service providers to capture the full value of connectivity. The company's portfolio spans Networks, Digital Services, Managed Services, and Emerging Business and is designed to help our customers go digital, increase efficiency and find new revenue streams. Ericsson's investments in innovation have delivered the benefits of telephony and mobile broadband to billions of people around the world. The Ericsson stock is listed on Nasdaq Stockholm and on Nasdaq New York.

www.ericsson.com

Ericsson
SE-164 80 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com

12/28701-FGB1010909