Written evidence submitted by Ericsson

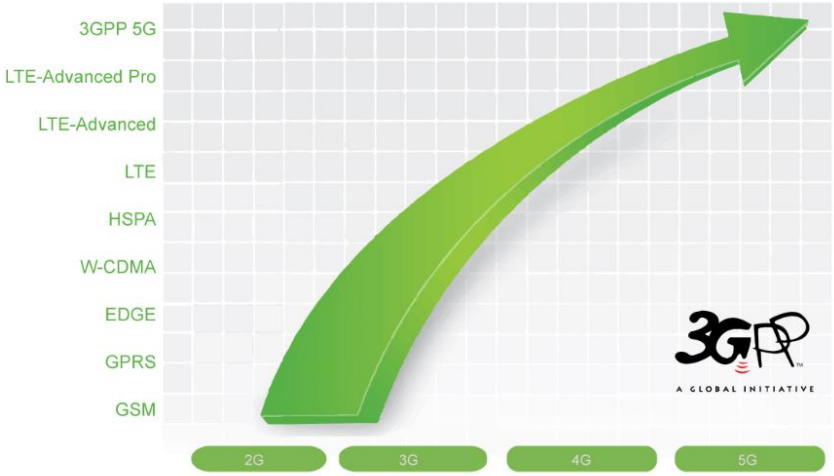
The Security of 5G Inquiry

Contents

1. What is 5G and why is 5G critical?

Global standards are fundamental to today's ubiquitous connectivity and have evolved beyond pure interoperability solutions enabling global and dynamic ecosystems. It is as a result of global standards that mobile technology connects the world's population. At the current trajectory, mobile broadband will provide network coverage to around 92% of the world's population by 2024. This scale brings an unprecedented opportunity to address global challenges of sustainable development.
3GPP, 3rd Generation Partnership Project unites seven telecommunications standard development organizations (ARIB, ATIS, CCSA, ETSI, TSDSI, TTA, TTC), known as "Organizational Partners" providing their members with a stable environment to produce specifications that define 3GPP technologies. 3GPP was created in December 1998 by the signing of "The 3rd Generation Partnership **Project Agreement**". The latest **3GPP Scope and Objectives document** has evolved from this original Agreement.[1] 3GPP Standards are developed in a multi-stakeholder[2], collaborative approach and focuses on providing an end-to-end architecture from network level to devices while collectively driving Radio Access Networks (RAN), Core and Communication systems and service architectures. The 3GPP frameworks are the basis for regulatory requirements and approvals world-wide, bringing a strong and equal quality base line across the world. The 3GPP systems specification consist of many thousand engineers making 100,000+ plus contributions to the standards. As an example of the level of collaboration 19,000 contributions were made just in Q4 2019 alone. 3GPP standards are updated every 15-18 months and are available to everyone.
3GPP specifies several interfaces that enable interoperability between different vendors and domains including hardware and software. Today, +95% of all mobile networks have 3GPP compliant equipment and Software from multiple vendors.

The major focus for all 3GPP releases is to make the system backwards and forwards compatible, to ensure that the operation of user equipment is uninterrupted. Each progressive 3GPP radio access technology aims to reduce complexity and avoid fragmentation of technologies.

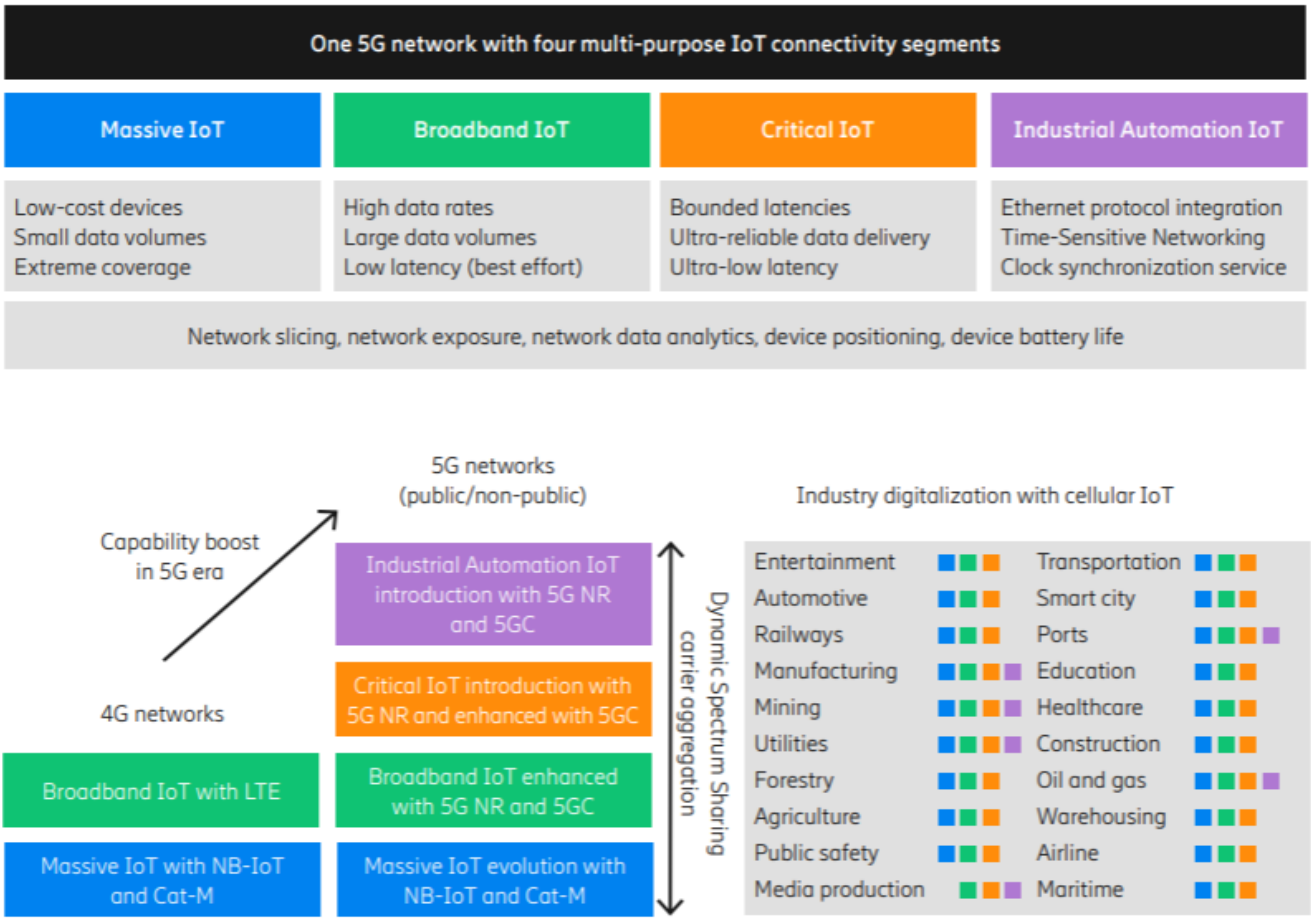


The 3GPP-based global mobile networks are connecting things-to-things and things-to-persons across borders. Many industries are experiencing the benefits of mobile internet of Things (IoT), for example in the consumer electronics, automotive, railway, mining, utilities, healthcare, agriculture, manufacturing and transportation sectors. There are over 1 billion cellular IoT connections today in 2020, and Ericsson forecasts around 5 billion connections by 2025. With 5G in the market, almost every industry is exploring the potential of Mobile connectivity for fundamentally transforming businesses. In some regions, governments are encouraging adoption of IoT via direct and indirect incentives to promote sustainability, innovation and growth.

[1] https://www.3gpp.org/about-3gpp

[2] https://www.3gpp.org/about-3gpp/membership

The wireless connectivity across various industries can be grouped into four distinct sets of requirements. Ericsson has defined four IoT connectivity segments: Massive IoT, Broadband IoT, Critical IoT and Industrial Automation IoT, as illustrated in the figure below. Each IoT connectivity segment addresses multiple use cases in multiple industries.



IoT capabilities are being further enhanced with the introduction of 5G radio and core networks. With powerful, ultra-reliable and ultra-low latency capabilities, 5G networks are going to enable Critical IoT for time-critical communications. To seamlessly integrate 5G networks with Ethernet-based industrial wired communications networks, 3GPP has standardised additional capabilities that would be offered by Industrial Automation IoT connectivity. The four IoT connectivity segments can co-exist in one 5G network, whether deployed for public or non-public access. Some devices may need multiple IoT connectivity segments for executing one or more use cases, for example, an autonomous vehicle with rich requirements.

Massive IoT

Massive IoT connectivity targets many low-cost, narrow-bandwidth devices that infrequently send or receive small volumes of data. These devices can be situated in challenging radio conditions requiring extreme coverage and may rely solely on battery power supply. Most industry stakeholders foresee a huge amount of relatively simple devices that will need connectivity and create valuable data sets. Some devices only send a few messages per day – such as status indicators for temperature, monitoring climate for Agriculture development. – while others may require voice capabilities to guide a remote repair technician.

Broadband IoT
Broadband IoT connectivity provides much higher data rates and lower latency and enables additional capabilities such as extended device battery life, extended coverage, enhanced uplink data rates and enhanced device positioning precision. Broadband IoT is relevant for all industries. There are more than 500 million Broadband IoT users in 2020, primarily with LTE access. Commercial usage today is dominated by personal cars, commercial vehicles, trains, wearables, gadgets, cameras, sensors, actuators and trackers.

Critical IoT
Critical IoT connectivity is for time-critical communication. It enables ultra-high reliability and ultra-low latency communication at a variety of data rates. The reliability is defined as the probability of successful data delivery within a specified time duration. In contrast to Broadband IoT, which achieves low latency on best effort, Critical IoT can deliver data within strict latency bounds with required guarantee levels, even in heavily loaded networks. Typical use cases with demanding combinations of reliability, latency and data rates include AR/VR, autonomous vehicles, mobile robots, real-time human machine collaboration, cloud robotics, haptic feedback, real-time fault prevention, and coordination and control of machines and processes. Such use cases are relevant in almost every industry. Some industries are piloting these applications with 5G, for example, in the entertainment, automotive, manufacturing, mining, harbour, airport, construction and utilities sectors.

Industrial Automation IoT
Industrial Automation IoT aims at enabling seamless integration of 5G connectivity into the wired industrial infrastructure used for real-time advanced automation. It includes capabilities for integrating 5G systems with Ethernet and Time-Sensitive Networking (TSN) used in industrial automation networks.
Even if an industrial system is within 5G coverage, certain components of the system might stay connected with cables due to various factors; for example, not having a major need for a wireless solution, having long life cycles, or having extreme performance needs that are beyond 5G's current capabilities (for example, micro-second level deterministic latency). It is important that 5G supports seamless integration into the current and evolving wired infrastructure.

Cellular IoT Evolution for Industry Digitalization, Ericsson White Paper: https://www.ericsson.com/en/reports-and-papers/white-papers/cellular-iot-evolution-forindustry-digitalization
https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/boosting-smart-manufacturing-with-5g-wireless-connectivity

Driving transformation in the automotive and road transport ecosystem with 5G, Ericsson Technology Review, 2019: https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/transforming-transportation-with-5g

The 5G Eco System is continuously developing.

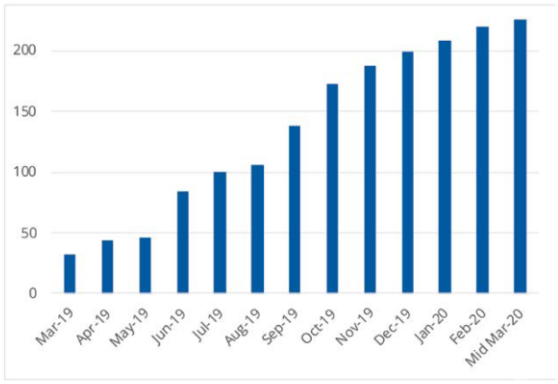


Figure 1: Growth of announced 5G devices (not all commercially available)

- five industrial grade CPE/routers/ gateways
- three robots
- three televisions
- three tablets
- three USB terminals/dongles/modems
- two snap-on dongles/adapters
- two drones
- two head-mounted displays
- one switch
- one vending machine.

Not all devices are available immediately and specification details remain limited for some devices.

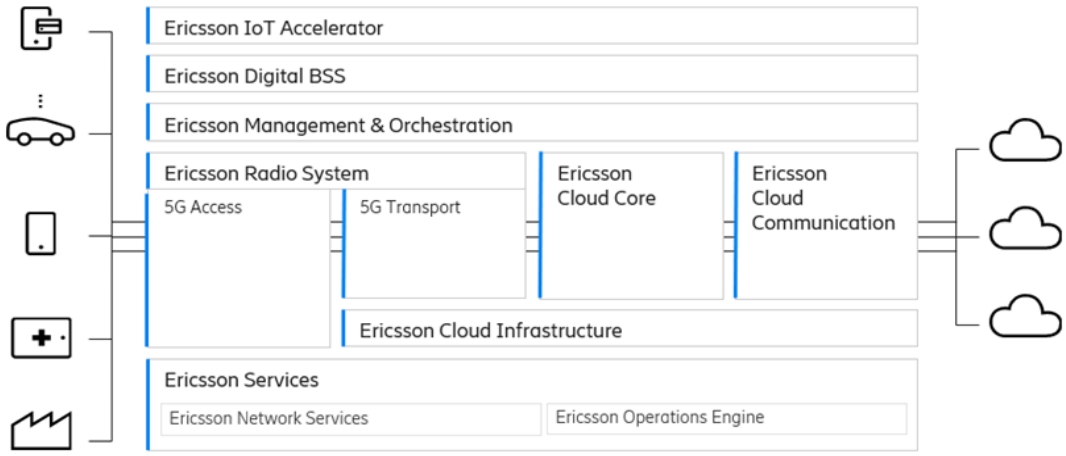
GSA has identified **208** announced 5G devices from **78** vendors; at least **60** are commercially available.

16 form factors are available, including:

- 62 phones (at least 35 commercially available)
- 14 hotspots (at least 9 commercially available
- 69 CPE devices (indoor and outdoor, at least 12 commercially available)
- 35 modules
- 25 others (robots, snap - on dongles/adapters, routers, drones, head-mounted displays, laptops (notebooks), switch, USB terminals/dongles, televisions, vending machine).

Source: https://gsacom.com/, 5G device ecosystem, January 2020 the key component in 5G architecture

Overview of key portfolio required for 5G network deployments.



IoT Accelerator Global connectivity and device management

Digital BSS/Telecom BSS Real-time charging and billing, digital customer

Management and Orchestration A modular solution that enables unparalleled automation in OSS to provision and assure the hybrid network

Ericsson Radio System Hardware, software, and related services to build modular and scalable radio access networks.
5G Access - RAN Compute and baseband, radio, and site
5G Transport - Fronthaul, backhaul, edge and core transport

Cloud Core A cloud native dual-mode 5G Core with common operations and maintenance for EPC and 5GC

Cloud Communication Providing communication services such as voice, video and messaging for

Cloud Infrastructure NFV Infrastructure for distributed cloud environments

Network automation Network management, automation and orchestration of nodes,

networks and capabilities

Ericsson Operations Engine - Data-driven, predictive Managed Services leveraging AI and Automation

2.Network Security Considerations in the era of 5G

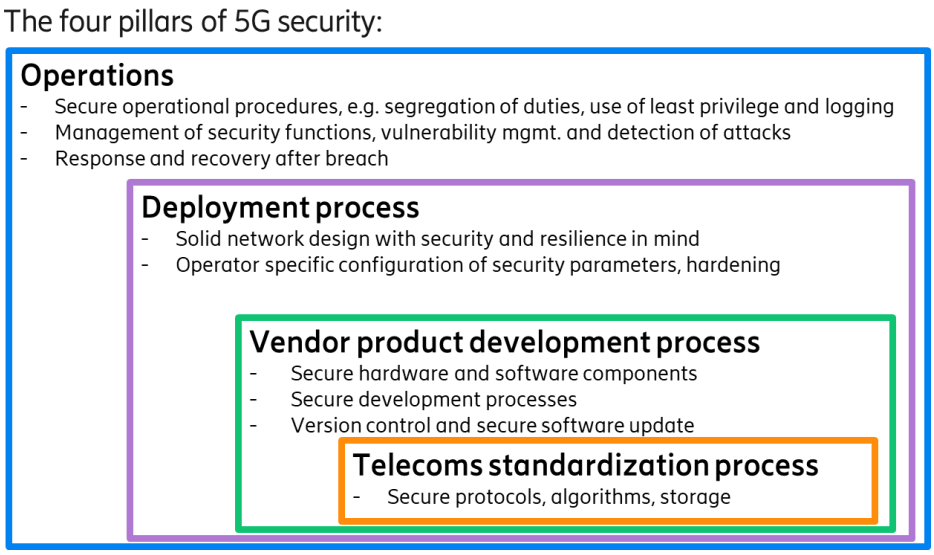
Telecommunication networks are evolving rapidly across a broad technological environment which includes virtualisation, IoT and Industry 4.0. This is met by an equally broad yet deteriorating cybersecurity environment.

Advances in technology, together with the broader development of networks are expected to have a significant impact on security, such as 5G New Radio (NR), software-defined networking (SDN), network function virtualisation (NFV), mobile edge computing (MEC) and Network Slicing. The 5G 3GPP standard is agnostic, in that it is flexible enough to allow for different types of physical and virtual overlap between the radio access network (RAN) and core network components, NFV and MEC.

In the era of 5G, it's important to conceptualise security on a system wide level where telecom networks are an important component, while adopting a strong understanding of the following:

- Increased value at stake and decreased risk tolerance
- Cyber-physical dependencies
- Security of standards, products, deployments and operations
- Proactive cybersecurity measures
- Vulnerability management
- Securing the supply chain

Building a secure 5G network requires a holistic approach rather than a focus on individual technical parts in isolation. For example, interactions between user authentication, traffic encryption, mobility, overload situations, and network resilience aspects need to be considered together. It is also important to understand relevant risks and how to address them appropriately.



A comprehensive approach to security requires a strategy and mitigation in four key layers, standards, products, and development processes, network deployments, and network operations. Collectively, these four areas define the security status of live networks and hence the de-facto end-user security experience. A comprehensive approach ensures that mitigating measures are implemented in such a way that interdependencies between the layers as well as specifics for a layer in question are addressed effectively.

Building the inherently secure 5G system in standards requires a holistic effort, rather than focusing on individual parts in isolation. Several organisations such as the 3GPP, ETSI, and IETF have worked together to jointly develop the 5G system, each focusing on specific parts.

The 3GPP working group SA WG3 is responsible for security and privacy requirements, specifying the security architectures and protocols in 3GPP standards. The working group ensures the availability of cryptographic algorithms which need to be part of the portfolio specifications.

Ericsson welcomes the contributions and active participation from UK government authorities in 3GPP, ETSI NFV/SEC and IETF. Ericsson also actively contributes to these standards bodies.
An overview of 3GPP 5G security standards can be found at this link. https://www.ericsson.com/en/blog/2019/7/3gpp-5g-security-overview

While the fundamental security features are specified in 3GPP standardisation, vendors enjoy a lot of room to manoeuvre throughout the development process, and so too operators throughout the deployment and operation processes.

Vendors implement common technologies differently. Main features like interoperability and roaming are necessary, while non-common features (e.g. value adding features) differ from vendor to vendor. Product security assurance is vital for success in security. Security assurance is critical for software development and contains a set of sub-processes on different levels to ensure that a product functions and performs as it is intended. Vulnerability assessment, penetration testing, risk assessment and privacy impact assessments are examples of such sub-processes. In addition, code is reviewed and scanned for flaws and vulnerabilities. Security assurance is not limited to internal activities only. Supply chain security controls form a crucial part of security activities. Similar standards of internal security are required to be extended to suppliers of components and third-party software used in products and solutions. Many of the vulnerabilities exploited in live networks are publicly known vulnerabilities, often present in commonly used software components. Therefore, extra attention is needed to monitor and respond to any vulnerabilities in any third-party components which are used.

Ericsson applies the Ericsson Security and reliability model and PSIRT processes, an overview can be found here:-
https://www.ericsson.com/en/security/ericssons-security-reliability-model
https://www.ericsson.com/en/about-us/enterprise-security/psirt

Operators need to ensure a network design that considers security and reliability requirements. 3GPP standards allow for flexibility in deployments such as the deployment of RAN and Core functions and therefore does not ensure a fully secure network design or network deployment.
Operational security is dependent upon among others on strict access controls implementation. There is a need for an operational security solution that constantly monitors security compliance, detects and responds to new threats, supporting cost-efficient security operations, ideally in an automated way.

Risks to 5G infrastructure are not unique to a specific country. The UK has been contributing to the EU 5G related risks assessments and risk mitigating measures. Ericsson welcomes the UK's continued leadership and collaboration with the EU and globally on 5G security measures and requirements.
The EU-wide Risk assessment is documented here https://ec.europa.eu/digital-single-market/en/news/eu-wide-coordinated-risk-assessment-5g-networks-security
The ENISA 5G threat landscape is documented here https://www.enisa.europa.eu/publications/enisa-threat-landscape-for-5g-networks

Ericsson recommends continued global collaboration and coordination on security standardisation and broader Telecoms Security Requirements for network operations, network design network deployments and vendor assessments.
Ericsson would advise caution when considering developing additional national baseline requirements to mandate technical baseline security requirements and suggests instead to rely on coordinated approach interacting with relevant industry security best-practices and standardisation such as 3GPP.

Ericsson supports the approach defined by the GSMA NESAS and 3GPP SECAM/SCAS security assessment frameworks. Standardised approach is important for achieving global interoperability and avoiding additional cost and conflicting requirements.

It should be noted that operators and suppliers' investment on new technical security features are impacted by the market's ability to pay for security. Increased transparency in the market is an essential prerequisite to develop a market where investments in security are rewarded by the market.

Further considerations for 5G security –
https://www.ericsson.com/en/reports-and-papers/white-papers/5g-security---enabling-a-trustworthy-5g-system
https://www.ericsson.com/en/internet-of-things/iot-security
https://www.ericsson.com/495922/assets/local/policy-makers-and-regulators/5-key-facts-about-5g-radio-access-networks.pdf
https://www.ericsson.com/en/reports-and-papers/white-papers/security-in-5g-ran-and-core-deployments

3.Evidence based, Ericsson's position as a world leader in 5G.

Ericsson is the first company to launch live commercial 5G networks on four continents. Today, 70% of the top service providers evaluated in global public 4G network tests use Ericsson's radios and basebands, which are the key to 5G performance. Ericsson Core solutions are supporting 2.5 billion subscribers from 2G to 5G, representing one-third of the global population. And thanks to our ongoing interoperability engagements with six out of six chipset vendors, Ericsson 5G technology is evolving continuously to support a variety of 5G devices. This ensures Ericsson we can cater to the wide-ranging 5G use cases of today and tomorrow.

As of April 2020 Ericsson, has 88 commercial 5G agreements or contracts with unique operators, with 42 of these being publicly announced. more importantly, we have already supplied 30 live commercial networks.

We're proud to say that communication service providers all around the world have chosen to deploy 5G using our leading network technology. Our list of commercial agreements and contracts with unique operators is growing rapidly.

88	42	30
Commercial 5G agreements	Publicly announced 5G contracts	Live 5G networks

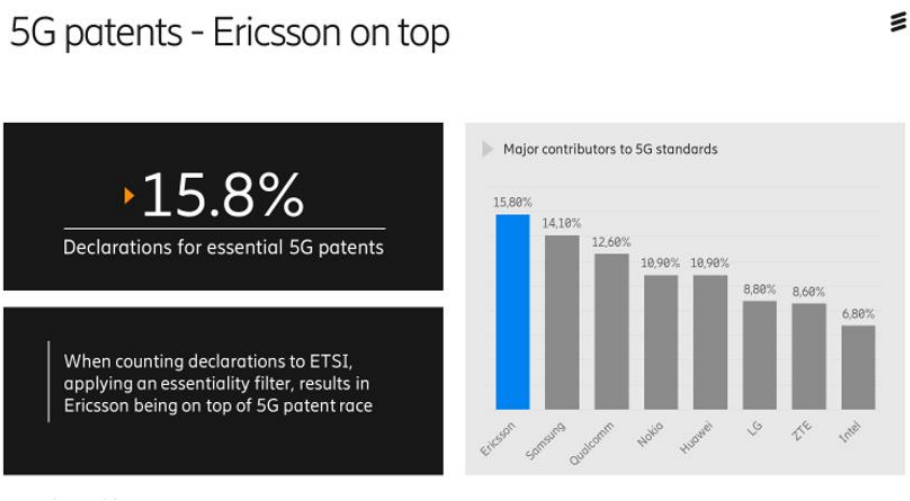
https://www.ericsson.com/en/5g/5g-networks/5g-contracts

Ericsson's technology delivered the first commercial 5G live network in Europe with Swisscom, on April 17, 2019, Swisscom switched on the first European commercial 5G network, powered 100% by Ericsson. Having initially taken its 5G network live in 102 locations in 54 different towns, Swisscom expanded quickly in the major cities, tourist areas and across the countryside, achieving 90% nationwide population coverage by the end of 2019 with the help of Ericsson Spectrum Sharing.

https://www.ericsson.com/en/news/2019/11/5g-spectrum-sharing-call-ericsson-swisscom-qualcomm

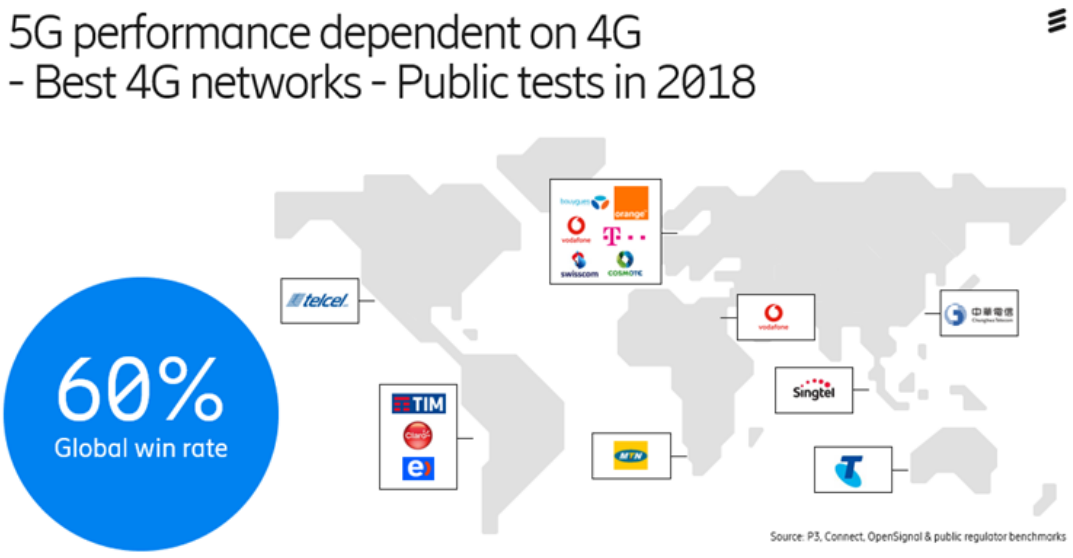
On April 3, 2019 KT, South Korea's largest telecommunications company, officially switched on its nationwide commercial 5G network, ushering in a new era of super-fast and ultra-reliable connectivity for consumers and businesses. Ericsson is providing 3GPP standards-based 5G New Radio (NR) hardware and software from Ericsson's complete 5G platform to cover KT's 3.5 GHz Non-Standalone (NSA) network. The deployment coverage quickly expanded to cover more than 80% of the population coverage by the end of 2019. In early 2019 SK Telecom switched on its commercial Ericsson 5G network, announcing the "Beginning of the Age of Hyper-Innovation with 5G On April 3rd, With 5G downlink speeds that are 10 times faster than 4G, and that exceed 1 Gbit/s in stationary mode and 500 Mbit/s in mobile mode, SK Telecom has positioned 5G as a premium service as they take their customer experience to the next level. In addition to ultra-high speeds, 5G delivers rich content in diverse areas spanning gaming, ultra-high definition (UHD) video, and augmented and virtual reality (AR & VR) based applications. Today, South Korea is the world's largest 5G market with more than 5 million 5G subscribers. 5G is also driving higher data usage with an average data consumption that has grown from 9 GByte/month on 4G to more than 25 GByte/month on 5G. To be the industry best in terms of 5G coverage, speed and latency, SK Telecom has been rolling out 5G in the main population areas of eighty-five cities, and other highly populated areas that have high concentrations of data traffic like university districts, high-speed trains, sports stadiums, metropolitan subway lines, and expressways. SK Telecom is also expanding coverage to include nationwide subways, national parks and festival sites. 5G coverage expected to expand.

Ericsson leading with 15.8 % share when it comes to declarations for 5G essential patents when an essentiality weighting is applied (study by Bird&Bird, May 2019) https://www.twobirds.com/~/media/pdfs/news/articles/2019/determining-which-companies-are-leading-the-5g-race.pdf?la=en&hash=8ABA5A7173EEE8FFA612E070C0EA4B4F53CC50DE



5G performance and user experience depends on having a well performing 4G network. In 2018 Ericsson 4G outperformed the competition supporting our customers to win 60% of the Public tests globally. That is the result of unique capabilities in Ericsson Radio System like lean carrier and elastic RAN, flexibility on the deployment with our multistrand baseband, our advice on how to build the network with precision, and the optimization tools and services. Total number of existing public benchmarks, considered in 2018, with published and official results, with or without Ericsson footprint, was 61 61 representing all the public benchmarks, with published results: -

- P3 Connect in 2018 (9): Australia; Germany; Austria; Singapore; Spain; Switzerland; The Netherlands; UK; USA
- P3 Certificates in 2018 (20): Albania; Brazil; Croatia; Czech Republic; Egypt; Greece; Hungary; Ireland; Italy; Kazakhstan; Kenya; Macedonia; New Zealand; Portugal; Qatar; Romania; Slovakia; South Africa; Thailand; Vietnam;
- Opensignal in 2018 (28): Colombia; Spain; Taiwan; Portugal; Brazil; Peru; Canada; Chile; South Africa; Cambodia; Belgium; Netherlands; Philippines; Mexico; Malaysia; UK; Thailand; Australia; India; Italy; Myanmar; Germany; Argentina; Singapore; Switzerland; Indonesia; Costa Rica; Ecuador;
- Netcheck / Chip Magazine (3): Germany; Switzerland; Austria
- Regulator benchmarks (1): France



About Ericsson

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 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

17 April 2020