ERICSSON

BUILDING NETWORK OF THINGS

The roles of Policy and Subscriber Data Management in IoT

INGRESS

The Internet of Things (IoT) is transforming the world we live in, shaping the Networked Society and opening new business opportunities for network carriers and industries. However, big things don't come easy. Compared to traditional voice and data services, IoT creates new requirements for telecom networks to deliver massive and critical IoT services.

To support network carriers in meeting these requirements, the Ericsson Unified Data Management (UDM) solutions provide a full set of functionalities that address connectivity and security concerns, help in tailoring the network according to user needs and facilitate the monetization of IoT data.

A BRIEF INTRODUCTION TO IOT MARKET DIVERSITY

The Internet of Things (IoT) enables radical innovations and creates completely new services that either change businesses or transform entire industries.

Devices that did not exist a few years ago are now used on a daily basis as they make our life easier and more enjoyable – from smart bands that monitor our health and fitness to connected cars that are part of an intelligent transport solution.

There are an estimated 5.6 billion connected devices in the world today and the number is forecast to grow to 18 billion by 2022 (Source: Ericsson Mobility Report, November 2016).

When all these smart products are connected, it makes it much easier for us to get more relevant information and make decisions, whether it applies to our daily life or to business.

IoT devices are divided into two segments: short-range and wide-range.

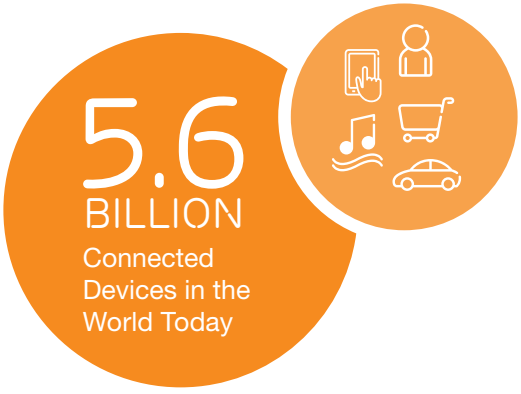
The short-range segment consists of devices connected by unlicensed radio with a typical radio range of up to 100 meters, such as Wi-Fi, Bluetooth and ZigBee. This category also includes devices connected over fixed line local area connections.

The wide-area IoT category consists of 3GPP-based cellular connections and operates in two distinctive sub-categories: massive and critical applications.

Massive IoT connections are characterized by high connection volumes and small data traffic volumes, low cost devices and low energy consumption.

At the other end of the scale, critical IoT connections place different demands on the network: ultra-reliability, availability, low latency and high data throughput.

However, there are many use cases between these two extremes, which today rely on 2G, 3G or 4G connectivity.



IOT-READY MOBILE NETWORKS

While Telecom Core Network requirements change for each segment and device type, adding new levels of complexity to be managed by network carriers, the revenue per IoT subscription is expected to be lower than normal voice and data subscription.

In order to maintain profit, carriers need to tailor their networks to meet the IoT demand while ensuring a low Total Cost of Ownership (TCO). Traditional Core Network technologies offer limited possibilities to differentiate voice and data users from IoT devices and optimize the use of network resources accordingly. However, new technologies such as Network Function Virtualization (NFV), Network Slicing and Cloud offer new tools that allow tailoring of the network in a more flexible and dynamic way to meet IoT demand.

Massive and critical IoT devices have different requirements in terms of latency, bandwidth consumption and Quality of Service (QoS). They have also challenged the concepts of Busy Hour Call Attempts (BHCA) and peak hour traffic that for decades were the baseline of the dimension of the networks.

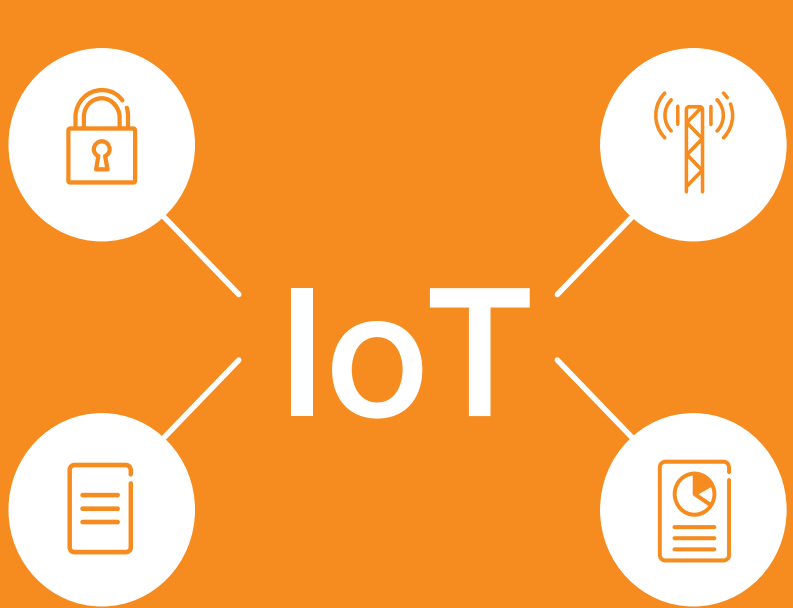
Moreover, for some types of critical devices and services such as surveillance cameras and Professional Mobile Radio (PMR), networks need to quickly adjust to different traffic patterns and events in a more automated and dynamic way.

From a security perspective, there are challenges to manage all IoT devices connected to the networks, which increases the risk of malicious or malfunctioning devices generating signaling storms and affecting network services. Therefore, deploying trusted security solutions ensure proper authentication and authorization of IoT devices in the network and prevent traffic peaks in the IoT domain affecting other network domains.

For the successful implementation of profitable IoT strategies, there are four main areas where the Ericsson UDM solutions for Subscriber Data Management (SDM) and Policy Management can play a main role. These areas are:

> Connectivity
> Security
> Adaptability
> Analytics

This paper explores each of these areas explaining the most common challenges and what Ericsson UDM solutions have to offer to overcome them.



Security

> Authentication
> Fraud detection
> Non-SIM
> eSIM
> DDoS mitigation

Connectivity

> 2G/3G/4G
> WiFi
> Massive IoT (NB-IoT, CAT-M1, EC-GSM)
> Robustness
> Network Slicing

Adaptability

> Dynamic QoS
> Assurance
> Priority Handling
> Time/Location-based Policies
> Quota Control

Analytics

> Event exposure
> Operational Efficiency
> Slice closed loops
> Exposure to vertical ecosystem

CONNECTIVITY

The assurance of efficient connectivity is the foundation for IoT enablement; however, while carriers have been providing fixed and mobile connectivity for decades and Machine-to-Machine (M2M) services in more recent years, connecting IoT devices is not as simple as it may look like.

To realize massive IoT, networks will have to cope with new diverse requirements compared to what they have been handling at the moment. On top of the profit/cost paradigm and network resource optimization, carriers will also have to address new requirements of devices.

Massive IoT use cases require devices with low battery consumption such as telemetry sensors in remote areas and low chipset complexity to drive down the device cost. On the other hand, critical IoT devices require a differentiated treatment with focus on maximizing performance and availability, such as autonomous cars.

Different IoT devices will connect to the network using different access technologies. While GPRS/EDGE is widely used to connect M2M devices at present, IoT will use most, if not all, of the cellular access technologies such as 2G, 3G, 4G and 5G and non-cellular, such as Wi-Fi, or non-3GPP technologies.

In addition, the emerging low power wide area access technology for licensed spectrum such as Nb-IoT, CAT-M1 and EC-GSM will help meet the demand of massive IoT in terms of reducing the device cost, extending battery life and providing wider coverage.

Addressing the diverse characteristics of IoT connectivity, while being extremely efficient, is not the only challenge facing carriers. IoT traffic patterns are different from human traffic patterns, which networks have been accustomed to handle until now. For example, a simultaneous restart of thousands of devices sharing the same application could trigger a massive network attach procedure, creating a signaling storm that would need to be properly handled by the network in order to secure service continuity and prevent congestion initiated in the IoT domain from propagating to voice and mobile broadband domains.

Some of the main challenges carriers may face to connect IoT devices are:

> Managing IoT device diversity in network
> Offering different IoT access technologies and using them efficiently
> Optimizing the network for resource and cost efficiencies
> Protecting network from signaling storms and congestion caused by IoT devices
> Allowing partitioning of the network to better address specific segments requirements

SECURITY

The exponential growth of connected IoT devices, and most of them being manufactured for mass market, is making it extremely difficult, but not impossible, for carriers to manage devices' compliance with specific security standards.

To protect their network, carriers need to ensure that connected devices function properly and that effective mechanisms are in place to defend against malicious attacks. Hence, device authentication, service assurance and fraud protection are key measures that should be enforced.

The first step in security is the authentication and authorization of IoT users to allow access to network and services. Authentication is the cornerstone of any security solution, as it ensures that the devices that are attempting to connect to the network are who they claim to be and that they are trusted parties. Massive IoT devices will be connected via cellular technologies using SIM cards or eSIM (embedded SIM) and via non-cellular technologies using SIM-less devices.

SIM and its evolved version, eSIM, provide a robust security framework which IoT devices can leverage on to ensure safe network access, data confidentiality and data integrity. However, SIM-less devices will require other authentication methods such as the use of digital certificates, which is widely used in the IT domain – for example, public key infrastructure (PKI).

Security can also be compromised by devices that have not gone through the required approval and certification processes by carriers and therefore have invalid or even cloned IMEI (International Mobile Equipment Identity). For such cases, the authentication of devices itself is crucial, and a typical mobile network function called Equipment Identity Register (EIR) provides the necessary functionality to blacklist devices that should not have access to the network or grey list suspicious devices wherein the devices are kept under temporary observation and are eventually blocked when the operator conducts the investigation.

However, authentication alone is not enough to secure the network. IoT devices typically transmit low amount of data, but with malicious software they can generate massive fake traffic that can derive into a Denial-of-Service Attack (DoS). Additionally devices can be hijacked and used for purposes far beyond what its owner was aiming for.

Some of the main challenges carriers may face in the security area are:

> Authenticating and authorizing users irrespective of the connection type, through SIM, eSIM or non-SIM, or access network
> Controlling physical devices from connecting to the network, that is device authentication
> Detecting DoS attacks as soon as possible and implement actions to avoid disturbances in the network
> Identifying fraudulent usage of devices

ADAPTABILITY

Diverse IoT devices and use cases are driving networks to stretch their limits, and hence networks will now have to be more adaptable than before. A quick adaptability to different IoT needs will not only help improve efficiency and profitability but also lead to innovation in the highly competitive market where new IT entrants will compete directly with network carriers.

However, only adaptability is not enough. The players who will succeed and reap profits from IoT will be the ones who can adapt to different business environments and needs with a faster Time-to-Market (TTM).

Some devices will always be connected while others will send small amount of data over short-time windows. Also, some devices will handle critical data and some will work on a best-effort connection. Devices that handle critical data would need to be sent in optimal conditions and minimum time. This will only happen under certain conditions and at a certain time. This traffic would need to be prioritized and the last one to be preempted under a scarce resource situation.

Some devices will also be included in family data plans. For these users, it is important to have control over the whole pie for the total data packet as well as each piece of the pie used by different family members. Rules to define consumption limits per user are important.

There will also be similar types of devices that will function based on their location. For such cases, the network behavior has to be adapted according to the device location.

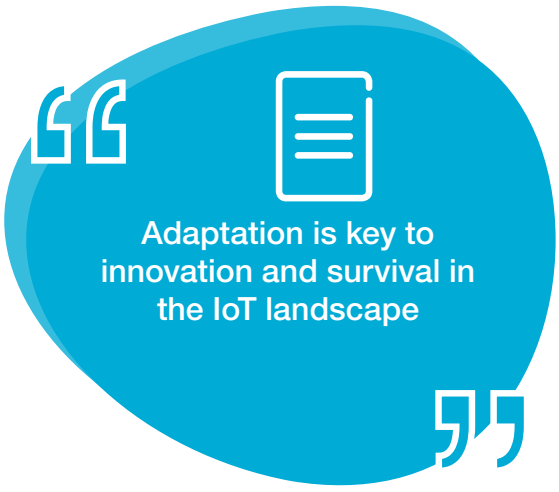
In more complex cases, the network will need to quickly adapt to serve many different devices in a given location only for a period of time, providing the required individual characteristics for each device type and user. For example, a stadium holding a musical or a sports event will see huge demand for connectivity for a couple of hours. This demand will be generated from thousands of people who would be using devices and mobile phones to upload and download data, surveillance cameras, television broadcasters, automatic vending machines and telemetry sensors, among others. All these require different network resources and have different traffic patterns but are handled by the same network. This network needs to dynamically adapt to the scenario for the specific time period of the event and later free up resources without significant human intervention.

An IoT-capable network handles dynamic QoS assurance, priority handling, time- and location-based policies and quota management dynamically, with Policy Management solution providing additional network efficiency and operational control.

Some of the main challenges carriers may face to quickly adapt their networks to IoT devices are:

> Identifying and addressing different demands from different IoT devices
> Having flexible tools to create an appealing IoT data offering that gives higher value than competition
> Setting up the network in a way that the service is rendered in the expected conditions
> Adapting network in a dynamic and automated way

To be able to implement automated processes for network adaptability, knowledge from network users is key. How to gain this knowledge? The answer is… This knowledge can be gained through analytics.



ANALYTICS

At this point it is clear what needs to be considered in order to connect IoT devices safely and to adapt the network aiming on low cost and high network efficiency. It is also clear that the needs and behaviors of human users and IoT devices differ and hence the network needs to be prepared to cope with them efficiently.

Another aspect that needs to be remembered is that the millions of connected IoT devices will create challenges in network operations that need to be managed effectively. Importantly, carriers need to diagnose issues with IoT devices actively and quickly in a process different to that used for human users who contact a call center when they face problems with the network or services.

Thus a question arises: how is it possible to use own network information to overcome this challenge and add more efficiency in the daily handling of IoT devices?

The knowledge gained by managing IoT device subscription data can be valuable to help overcome these challenges. This knowledge will not only help manage IoT connections more efficiently but also help leverage on subscription data to create additional revenue for carriers and empower them to add more value to the IoT industry. However, the challenge is to unlock the full business value of the IoT subscriber data asset to extract useful and timely insights, and this can be done through data analytics.

Subscriber Data Management (SDM) solutions host useful subscription data from IoT devices that can be used to improve operational efficiency, for example, enabling massive provisioning changes for IoT devices fulfilling certain conditions such as roaming location, APN usage or type of device. This is particularly important when changes affect thousands of devices efficiently. Another example of how subscription data can help improve operational efficiency is the real-time cross-checking of network database with databases in the Business Support System (BSS) systems. As eventual mismatch between the two databases can cause revenue leakage or service problem, the immediate detection of issues is particularly important in the IoT environment.

The data found in the network's subscriber database is crucial for the dynamic adaptability of the network. In more advanced use cases, carriers can also expose the IoT subscription data to industry verticals and partners, providing them insights into the usage of their devices, functional status and roaming situation, among others, to help them improve their operational efficiency and services offered to their customers. Importantly, this data exposure should be done in a secure and controlled way.

Some of the main challenges carriers may face while analyzing and exposing IoT data are:

> Extracting useful and timely insights from subscription data in a simple, fast and cost efficient way
> Exploring and exposing data safely and protecting network performance and data privacy and integrity
> Taking advantage of the insights to infer actionable changes in the network

EXPAND NETWORK TO SUPPORT IOT OR BUILD A NEW NETWORK FOR IOT?

With so many challenges and unique requirements, the most frequently asked question is: what is more efficient to support massive IoT? To use the same network resources as used for human subscribers by leveraging on an already implemented infrastructure and aiming higher resources usage optimization or to build a new network silo dedicated exclusively to IoT to avoid mixing the two diverse network users and business models.

There is no simple answer. There are many pros and cons for each approach. Carriers will no doubt choose the best strategy on a case-by-case basis, but what is clear is that present and future network technologies will allow efficient management of IoT no matter what choice they make.

For carriers who opt for a shared network for both human users and IoT devices, new technologies such as Network Slicing and Network Function Virtualization will allow the creation of dedicated network instances for IoT on a user or application level, providing traffic separation between IoT, MBB and voice.

With efficient solutions for data analytics and adaptability, these networks will be able to quickly adjust themselves to assist different IoT devices, either by changing the different slice configurations or by moving users and IoT devices between slices on-demand.

From an end-to-end perspective, different core network selection techniques such as Multi-operator Core Network (MOCN), DECOR (Dedicated Core Networks), eDECOR and Radio Access Network (RAN) based selection will serve different needs and strategies.

Importantly, irrespective of the approach chosen, the subscriber data management solution in the network will need to efficiently support the different needs when it comes to Connectivity, Security, Adaptability and Analytics.

REALIZING IOT WITH ERICSSON UDM SOLUTIONS

To address these challenges and provide flexibility to network carriers in choosing the best solution for their IoT business plans, the Ericsson UDM solutions provides a full set of functionalities that address connectivity and security concerns, help in tailoring the network according to user needs and facilitate the monetization of IoT data.

CONNECTIVITY:

With a centralized and consolidated database approach, Ericsson SDM can serve any type of cellular access technology, including new 3GPP massive IoT technologies such as Nb-IoT, CAT-M1 and EC-GSM, and host all subscription data in one place, both for human users and machines. Moreover, the solution supports the authentication of SIM, eSIM and non-SIM devices.

The database can also be partitioned to keep a logical or physical data separation between human users and machine devices and even between different types of machine devices.

Subscriber profiles are tailored to include the relevant data for the given type of IoT device. This allows for efficiency in the usage of database resources and lowers capex.

Under a potential signaling storm, Ericsson SDM offers a best-in-class and unique overload protection and load regulation mechanism. It allows to maximize traffic during an overload, reduce time to recover from overload and avoid node outages (read more on add reference to the respective brochure).

Looking toward a 5G-ready network, network slicing will provide mechanisms to separate Core IoT Networks among different IoT use cases or enterprises. Ericsson UDM solutions are a key enabler for network slicing. On one hand Ericsson SDM supports 3GPP specified DECOR mechanism for Slice Selection. On the other hand Ericsson Policy Management can dynamically select a network slice based on input conditions.

SECURITY:

Ericsson SDM offers a strong authentication mechanism for SIM-based devices and also supports its evolution to eSIM.

For non-SIM-based devises, Ericsson SDM provides an authentication mechanism based on Public Key Infrastructure.

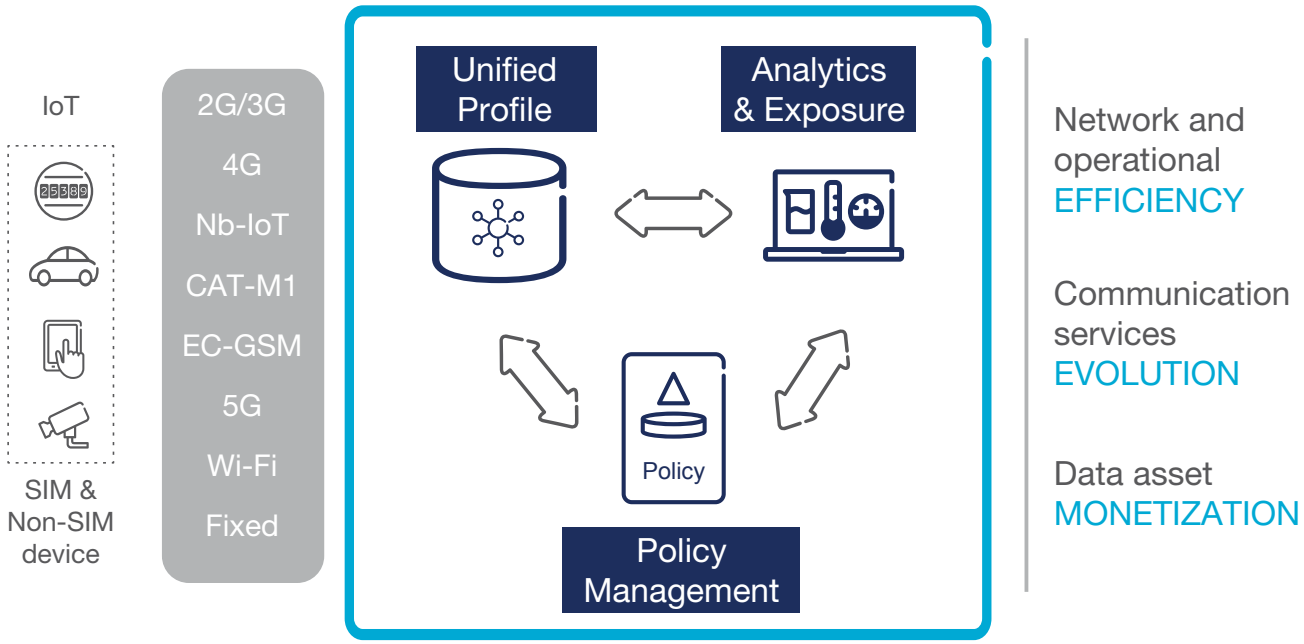
Ericsson SDM's EIR component takes care of IMEI authentication that decides which device will be granted access to the network.

Ericsson's Policy Management helps safeguard the operator network and connecting things. Policy Management is capable of handling preventive quota for things connected to the operator network and also track its location. If quota is consumed at a higher rate than expected or location is changed unexpectedly, Policy Management will detect a possible misuse of the device, even a Denial-of-Service (DoS) attack in extreme cases, and block the device or group of devices from gaining access to the network.

ADAPTABILITY:

Adaptability is important in both massive and critical IoT. Ericsson's Policy Management solution can handle different tiers where devices can be classified in. Devices transmitting a small amount of data such as electricity meters will be suited to low data allowance tiers while services close to real-time communications with heavy exchanges of data will better suit different tiers with an increased data allowance. Different monthly flat rate can be linked to the different tiers according to the type of devices they are targeting. With a set of dynamic policies based on time and location it is possible to take dynamic decisions that will regulate the conditions to access to the network (authorization, quality of service). Quota control and dynamic policies are suitable for both massive and critical IoT.

More specifically to critical IoT, the right handling of QoS and priorities is key to secure a timely delivery of the information and the accurate Policy Management will secure that the services related with mission critical communications or government institutions will have the reliability and speed they need.



ANALYTICS:
Ericsson UDM's embedded data analytics capabilities ensures a quick access to all the data in the database and provides timely insights that can translate into opex savings or new revenue streams.

The embedded analytics module provides operators with real-time insights from the connected devices and services usage. This can be used to improve operational efficiency by enabling massive provisioning changes for IoT devices to fulfill conditions such as roaming location, APN usage or device type. This is particularly important when a change affects thousands of devices efficiently. Another example is the possibility for real-time cross-checking of network database with databases in the BSS system.

Carriers can also expose IoT subscription data to verticals safely, allowing for added value rather than just providing connectivity.

One key characteristic of the solution is that massive analytics are performed without affecting the network database in-service performance (ISP), a concept that is called fresh database. As subscriber databases are critical nodes in the network to secure access to services, all analytics actions are performed in a real-time copy of the database, ensuring that network performance and safety is guaranteed all the time.

The combination of Ericsson's embedded Analytics and Policy Management creates powerful loops that are key for automation. As an example analytics can learn from the network usage to understand future behaviors of devices or group of devices and then apply those learnings as new policies on the network . Closed loops could be implemented in both individual slices or in the whole network to optimize the resources utilization. Automation is key to lower OPEX, CAPEX and create self-adaptive networks.

CONCLUSION

Telecommunication networks need to provide flexible and innovative solutions to address the diverse demands of connected devices to realize the full potential of IoT.

Managing IoT devices is different from managing human users, and while the big projections for the number of connected devices could be seductive to carriers, the resulting revenue may at times be modest. In order to maximize the revenue, the network needs to be efficient and adaptable to the changing needs and future requirements of connected devices.

While there is a threat of new entrants in this emerging market, network carriers are in the best position to succeed, thanks to their market presence, standardized access networks, strong authentication solutions and recognized know-how to meet user needs.

Connectivity, Security, Adaptability and Analytics are the four main areas network carriers need to focus on when defining their IoT business strategies. SDM and Policy Management are key to address the needs in these areas and Ericsson UDM solutions provide a full set of functionalities to allow carriers to excel in all of them.

Further reading:

1. Cross-domain identity of things
2. Ericsson mobility report
3. Internet of Things – get the while picture (video)
4. Handling of signaling storms in mobile networks
5. User and IoT Data Analytics
6. User and IoT Data Analytics presentation

GLOSSARY

3GPP	3rd Generation Partnership Project
APN	Access Point Name
BHCA	Busy Hour Call Attempts
BSS	Business Support System
CAPEX	Capital Expenditure
CAT-M1	Category M1
DDoS	Distributed Denial-of-Service
DECOR	Dedicated Core Networks
DoS	Denial-of-Service
EC-GSM	Extended Coverage GSM
EDGE	Enhanced Data for Global Evolution
EIR	Equipment Identity Register
eSIM	Embedded SIM
GPRS	General Packet Radio Service
IMEI	International Mobile Equipment Identity
IoT	Internet of Things
ISP	In-service Performance
M2M	Machine-to-Machine
MBB	Mobile Broadband
MOCN	Multi-operator Core Network
NB-IoT	Narrowband Internet of Things
NFV	Network Function Virtualization
OPEX	Operating Expenditure
PKI	Public Key Infrastructure
PMR	Professional Mobile Radio
QoS	Quality of Service
RAN	Radio Access Network
SDM	Subscriber Data Management
TCO	Total Cost of Ownership
TTM	Time-to-Market
UDM	Unified Data Management

Leading transformation through mobility

We are a world leader in the rapidly changing environment of communications technology – providing equipment, software and services to enable transformation through mobility.

Some 40 percent of global mobile traffic runs through networks we have supplied. More than 1 billion subscribers around the world rely every day on networks that we manage. With more than 37,000 granted patents, we have one of the industry's strongest intellectual property rights portfolios.

Our leadership in technology and services has been a driving force behind the expansion and improvement of connectivity worldwide. We believe that through mobility, our society can be transformed for the better. New innovations and forms of expression are finding a greater audience, industries and hierarchies are being revolutionized, and we are seeing a fundamental change in the way we communicate, socialize and make decisions together.

These exciting changes represent the realization of our vision: a Networked Society, where every person and every industry is empowered to reach their full potential.

Ericsson
SE-126 25 Stockholm, Sweden
Telephone +46 10 719 0000
www.ericsson.com