Getting closer to the vision of more than 50 billion connected devices means knowing how to address the diverse connectivity needs of a massive number and variety of devices, while simultaneously facilitating smooth and efficient network provisioning.

Drivers for the Ericsson Device Connection Platform

Estimates from different market analysts vary in terms of predicted figures—but they all agree that data usage will at least double every year until 2015, when data will outweigh voice 30 times over. These predictions are based on the concept that anything that benefits from being connected will be connected.

Consumers are increasingly getting used to constantly connected devices, behavior patterns are changing and the value of connectivity for people, business and society is becoming more evident. More than 50 billion connected devices is a vision where the convenience brought to people’s lives through the use of mobile networks will be considered normal and expected; a vast number of M2M interactions will constantly take place; and a myriad of new services will raise dependency on mobile networks and secure a massive number of connections.

Devices will access mobile networks directly or through gateways. They will communicate with each other, be part of an end-to-end M2M system, as well as communicating with individuals and central control systems. People will make use of numerous everyday devices that benefit from M2M connectivity at home, at work, on the move, in remote locations and elsewhere. The most obvious examples include: washing machines, coffee makers, car keys, ticket machines, fridges, window sensors, and utility meters. In addition, mobile devices will be adapted to serve as many other things: such as a connected wallet, a connection to medical services, and an interactive location guide. In the world of connected devices, we all benefit from these applications.

In the world of more than 50 billion connected devices there are fewer accidents due to improved safety, our way of life is more sustainable due to more efficient use of resources, we are energy smart, and healthcare and education are available for everyone.

Operators have started to realize that their networks can provide value beyond existing flat-rate plans. This will come about by applying differentiated connectivity packages tailored to meet the needs of different devices and different types of users.

Today’s networks are designed to

More than 50 billion connected devices
deliver and enforce different connectivity packages and types. However, to fully cater for the demands created by new types of devices and applications, innovative support systems will be required.

The fundamental features of such systems include:

- support for IP connectivity over private networks, as well as over the internet;
- efficient provisioning for a large number of subscriptions;
- capabilities to create and enforce tailored subscriptions with respect to QoS and charging models; and
- mobile network operator and enterprise-management portals.

To meet the market need for M2M support systems, Ericsson provides a SaaS solution – Ericsson Device Connection Platform (EDCP) – offering operators and M2M enterprises an initial low-cost solution for connecting devices and supporting applications, with the potential to expand and adapt to the growing needs of the market.

Ericsson Device Connection Platform Architecture

Functional architecture

Figure 3 shows how the EDCP solution interfaces with enterprises as well as mobile operators, providing functionality in three main areas:

- device connectivity;
- policy control and charging; and
- management and provisioning of subscriptions and devices.

Devices are connected to enterprise applications through the EDCP and via the operator’s mobile network. For transparent IP connectivity, the GGSN supports private IP networks, while the device access enabler (DAE) grants access to devices on the internet. The platform includes a service execution environment, which provides support functionality to enterprise applications such as a subscribe/notify communication scheme and location services.

The policy and charging control block handles the various settings for tailored subscriptions, such as data capping and charging levels. Enforcement of the parameters takes place in the GGSN and online charging systems (OCSs). The latter components also pre-rate and sort charging information – Call Detail Records (CDRs) – for each enterprise and operator. CDRs are then transferred to the operator’s billing system according to a desired control cycle.

For operator and enterprise users, dedicated portals provide access to the platform for SLA, order and account management components. The operator can, for example, create enterprise-specific subscriptions, set up portals and monitor SLA reports. Through the self-service portal the enterprise can purchase services, order SIM cards, and monitor real-time/statistical data on devices. The self-service portal also includes provisioning of subscriptions into the EDCP components as well.
as auto configuration of connectivity parameters into the devices. All devices supported by the EDCP are provisioned in the subscription database.

The OSS/diagnostics component provides operational and maintenance functions, such as alarm handling, as well as statistics for SLA reporting. A subset of status information and alarms is provided to the operator’s network operation center.

Not all of the more than 50 billion connected devices will be equipped with SIM cards. Figure 4 shows a probable scenario in which EDCP interacts with M2M devices via a gateway. The gateway, which can be connected to several different M2M devices, handles communication over the mobile network. Communication protocols used may be of any type. This example shows HTTP being used between EDCP and the gateway and the IETF-specified CoAP between the gateway and devices.

Ericsson Device Connection Platform deployment architecture

SaaS offered in a cloud style is a convenient and cost-effective way to connect devices and applications. The cloud model features pay-as-you-grow characteristics, rapid elasticity of system resources and ease of use. In the M2M arena there will be many different devices. Some will send and receive small amounts of data infrequently, some will send small amounts often and others will send and receive large amounts of data often or rarely. What M2M devices have in common, however, is that they could all benefit from the convenience of re-using infrastructure nodes for M2M services, such as provisioning, connectivity, charging and policy. The EDCP will be deployed as a SaaS to support this convenience and will interface to several nodes, as shown in Figure 5.

Below are short examples of how EDCP will support multi-tenant services in areas such as provisioning; OSS; charging; and accessing devices from the internet.

To handle the use of the subscription database (HLR), which is shared among customers, for its own or MNO-owned IMSI series, the EDCP will typically have its own HLR/AUC and interface to
SGSN via the Gn/Gp/Gr interface. The different MNOs share the EDCP but use their own radio and core networks for sending messages to the platform.

When the M2M device is equipped with an EDCP SIM card, 3GPP messages such as Attach and Authentication messages, which will be routed via the IMSI number to the EDCP HLR and processed according to standard 3GPP methods. When the M2M device issues a PDP context activation message, that message will be routed to the EDCP GGSN via the MNO-controlled SGSN by a DNS lookup of the Access Point Name (APN) derived from the M2M device plus the EDCP IMSI number.

For MNO-owned IMSI series, the routing to EDCP HLR will additionally be based on Mobile Station Identification Number MSIN (plus the ordinary usage of MCC and MNC). Operators will need to configure their networks to route messages to EDCP HLR for specific ranges of IMSI.

**Tailored subscriptions**

The envisaged more than 50 billion connected devices will differ greatly in functionality, ranging from smart meters to real-time video-surveillance cameras. A smart meter, for example, might report a kilobyte or two of data every other week or so, in which case accuracy is vital—as it determines costs reflected on the subscriber’s bill— but bandwidth and latency are unimportant. On the other hand, a video-surveillance camera constantly requires a lot of bandwidth (uploads of between 120kbps and 2MBps depending on the video quality, and even up to 10MBps for very high quality, such as is required for telepresence). Both smart meters and video-surveillance cameras are, for the most part, stationary, whereas other applications are mobile and require constant connectivity. Vehicle-tracking devices, would for the most part be on the move and as such, a fleet management application would require constant connectivity. These examples show that both devices and applications involved in M2M have very different connectivity requirements.

One size no longer fits all

The conclusion is that one size does not fit all, which is illustrated in Figure 2. For an MNO to be competitive in the world of more than 50 billion devices, such as EDCP, is needed. EDCP provides the means to create tailored subscriptions and offers the possibility to fine-tune and tailor subscriptions for specific devices and applications. Differentiated tariffs go hand in hand with tailored subscriptions, adding the requirement on such a platform to provide the functionality to rate a tailored subscription with a differentiated tariff.

Tables 1-2 show some examples of tailored subscriptions and corresponding differentiated tariffs.

These examples show the multitude of parameters that can be tuned when designing tailored subscriptions. The different subscription parameters are controlled and enforced by the different parts of the EDCP architecture.

The policy and charging control block uses the 3GPP-standardized interfaces Gx and Gy, based on the Diameter protocol, towards the GGSN that enforces these policies. The Gy interface is used to control usage (such as number of bytes, number SMSs, and voice minutes), ensuring that a device stays within the caps specified by the MNO and allows or denies access depending on time and location. The Gx interface and HLR profiles are responsible for policy control parameters such as mobility and bandwidth. The DAE controls SMS wake-up and finally the SLA, order and account manager controls the configuration of the device.

The realization of the tailored subscription is truly distributed on many nodes.

**Ericsson Device Connection Platform web portals**

EDCP provides one web portal to the MNO and one to the enterprise, where Ericsson manages the MNO accounts and the MNO manages the enterprise accounts. The EDCP web portal provides one single point of access to create tailored subscriptions, realized by different nodes, and ensures data consistency.

The MNO web portal is multi-tenant and offers the tools to design tailored subscriptions and manage their enterprise accounts. The enterprise web portal supports the enterprise to manage the M2M SIM cards and monitor device usage of the EDCP communication services.

The objective of the EDCP web portal is to be the M2M one-stop shop for management of M2M communication aspects provided by EDCP, tailored by

---

**Figure 2** Ericsson Device Connection Platform general deployment
MNOs, and used by enterprises. The portal, which is built on the concept of self-service, is automated as far as possible, minimizes the need for help desks, support and sales personnel thus lowering opex costs for MNOs and enterprises.

EDCP supports the operator in creating tailored subscriptions and differentiated tariffs, managing enterprise customers and controlling SIM cards, as well as facilitating follow-up on agreed SLAs. With EDCP operators can allocate resources such as APN and SIM cards to its enterprise customers in a straightforward manner. The portal provides the operator with the functionality to ensure that credit limits and other thresholds, such as data caps, are enforced. If a given threshold is exceeded, the operator has the option to increase charges or limit bandwidth.

Figure 6 shows the demo version of the EDCP portal. Listed on the left are tailored subscriptions created by the operator. The panel on the right illustrates how a tailored subscription can be defined.

The enterprise part of the portal will include all the necessary tools to administrate, manage and monitor devices that use EDCP services. Enterprise functions such as ordering SIM cards, connecting SIM cards to a tailored subscription, device management and viewing data or SMS consumption will be supported.

EDCP also offers APIs that can be used by the MNO or the enterprise. The APIs provide portal functionality that the MNO and enterprise may use to integrate that functionality into their platforms, systems or portals – instead of or in combination with the EDCP web portal.

Device Access Enablement

Mobile devices – in other words, any device connected to a mobile network – reside on a logical IP radio network or APN, several of which can coexist in the same radio network. An APN can be connected to the public internet or a private network. In both cases the connection point is the GGSN. When connected via the public internet, devices can connect to any available server on the internet, whereas devices on a private network can only connect to servers on that network.

There are a number of limitations associated with connecting devices to a private network. In most cases, companies or enterprises implement security measures on their private networks to limit access to authorized users and devices. Consequently, establishing a connection between an operator and an enterprise requires the exchange of network topology knowledge and involves tedious manual work for both parties. The enterprise would require a VPN-capable router, a RADIUS-server and the competence to configure and manage them both. As a result, lead times are often measured in weeks and the number of APNs that can be provided is restricted. Connecting devices via the internet overcomes these challenges and is a less expensive option – unless security is a priority. Additionally, connecting devices via the internet implies that they can be accessed from any other connected device – phones, computers, notebooks, tablets, cameras and so on – via the DAE.

EDCP will connect and share devices via the internet and shared intranets in a secure way. It will ensure that it is possible to identify, address and communicate with devices as if they were attached to the internet via a fully-fledged server position in a manner that is transparent to the device and the enterprise server. Consequently, EDCP will add value to the existing M2M domain without requiring any change or update on the device side or the enterprise server.

Because the number of connected devices will be enormous, it will not be possible to assign a unique public IPv4 address to each. While this issue will eventually be solved when IPv6 is fully deployed across networks, servers and devices, an interim solution is needed to uniquely identify connected devices. An APN is usually connected to the internet via an operator NAT. Each device will
have a private IP address that is unique on its APN, but not globally. Such an address has no meaning on the internet. When a device on the APN connects to a server on the internet, the NAT translates the source IP address to that of the NAT itself and temporarily assigns a source port on the internet to which the contacted server can reply. NAT deployment works for device-initiated connections. However, it does not work for connections initiated on an internet server. If devices do not have unique IP addresses, there is no way for the servers to initiate a connection to them.

EDCP’s access-enablement functionality solves the addressing issue using standard internet mechanisms – by using the internet host name. Devices connected to the EDCP will automatically be assigned a hostname that contains the device IMSI. The host name will be published together with the IP address of the NAT on the DNS. By using a standard domain name lookup, a server application can retrieve the IP address of the NAT and use it to initiate a connection to the device. Identifying the specific device to which a connection should be forwarded will be resolved using novel mechanisms for which patents are currently pending.

DNS and hostname publishing, together with novel forwarding mechanisms, will remove the demand for tedious device and application programming to support network-initiated access to devices. By supporting different authentication mechanisms, the EDCP access enabler can provide device and server authentication. For devices, single sign-on mobile access network authentication procedures are used, which means that all existing devices using a mobile access network can transparently benefit from EDCP. For server-side application authentication Access control lists (ACLs) or SSL-based authentication is used.

Additionally, EDCP access enablement offloads the installation and execution of security packages on the device. When server-side applications require a secure connection, the DAE implements the security requirements on the server side.

The DAE will provide several connectivity models appropriate for different business scenarios:

- single enterprise to multiple device;
- multiple enterprise to single service; and
- multiple enterprise to multiple device.

The DAE will support IPv4 and IPv6 on both the device and enterprise side, as well as supporting any transition method between the two.

### Ericsson Device Connection Platform application support

M2M devices will, in many cases, produce data that an M2M application needs to interpret and take action upon. For example, an M2M device sends to indicate that the current temperature is 47°C. An M2M application receives the information, interprets it and takes some action. Depending on the nature of the data and of the corresponding action, the data exchange between device and application can occur synchronously, which requires a real-time connection, or asynchronously. In many cases, M2M devices will produce data that can be consumed by the application at a later point in time. For example, the data supplied by an electricity meter to a billing application can be communicated at any time, the only requirement being that the information is accurate. Communication during off-peak hours is cost-effective in such cases. On the other hand, it is vital that – in the event of an accident – data be sent from a vehicle to an emergency-services application immediately. Asynchronous communication requires a mechanism for interim data storage. A later release of EDCP will have a solution for secure asynchronous device-application communication.

Today, M2M applications are typically hosted and executed on the premises of an enterprise. Alternatively, M2M applications can be deployed and executed in the cloud. Cloud providers, including some mobile operators as well as public providers, offer execution platforms suitable for many M2M application types. In a later release, EDCP will have an M2M execution platform that can be deployed in private, hybrid or public clouds. This will provide the mobile operator with the ability to support EDCP initial offerings such as tailored subscriptions and enhanced provisioning, as well as an execution environment for M2M applications. Enterprise M2M applications can benefit from well-known cloud characteristics, such as:

### Table 1: Smart meter subscription

<table>
<thead>
<tr>
<th>APN type:</th>
<th>Private</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility:</td>
<td>No</td>
</tr>
<tr>
<td>Roaming:</td>
<td>No</td>
</tr>
<tr>
<td>Bandwidth:</td>
<td>10kbps</td>
</tr>
<tr>
<td>Usage:</td>
<td>5kb/month</td>
</tr>
<tr>
<td>Tariff 1:</td>
<td>00.00-05.00, Monday-Friday, X1 cent/kb</td>
</tr>
<tr>
<td>Tariff 2:</td>
<td>00.00-05.00, Saturday and Sunday, Y1 cent/kb</td>
</tr>
<tr>
<td>Tariff 3:</td>
<td>05.01-23.59, everyday, Z1 cent/kb</td>
</tr>
<tr>
<td>Automatic device configuration:</td>
<td>No</td>
</tr>
<tr>
<td>SMS wake-up:</td>
<td>No</td>
</tr>
</tbody>
</table>

### Table 2: Video surveillance

<table>
<thead>
<tr>
<th>APN type:</th>
<th>DAE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Mobility:</td>
<td>No</td>
</tr>
<tr>
<td>Roaming:</td>
<td>No</td>
</tr>
<tr>
<td>Bandwidth:</td>
<td>5MB/s</td>
</tr>
<tr>
<td>Usage:</td>
<td>350 GB/week</td>
</tr>
<tr>
<td>Tariff 1:</td>
<td>UL&lt;500kbps, X2 cent/MB</td>
</tr>
<tr>
<td>Tariff 2:</td>
<td>500-&lt;UL, &lt;5MB/s, Y2 cent/MB</td>
</tr>
<tr>
<td>Automatic device configuration:</td>
<td>Yes</td>
</tr>
<tr>
<td>SMS wake-up:</td>
<td>No</td>
</tr>
</tbody>
</table>
Ericsson Device Connection Platform is an important step towards realizing the vision of more than 50 billion connected devices. It provides tools for actors, such as operators and enterprises, to handle provisioning in a self-service way. It also delivers methods to tailor subscriptions to meet the varied connectivity requirements of the massive number and variety of connected M2M devices. The device access enabler function in EDCP solves the issue with find and connect in a world of NATs and firewalls, and at the same time shields M2M devices from unsolicited usage. EDCP, offered as SaaS, is a way to re-use nodes and functions between several business domains and different mobile operators.

Solving connectivity challenges is the natural first step towards achieving the vision. The next step will be to offer solutions for application support — in other words, to develop, install and execute M2M applications in a more cost-effective and convenient way.

Robert Skog

- is an expert in the service layer at Ericsson’s Business Unit Multimedia.
- After completing an M.Sc. in electrical engineering from the Royal Institute of Technology (KTH), in Sweden, he joined Ericsson’s two-year trainee program for system engineers. Since then, he has worked mainly in the service layer area with everything from the first WAP solutions to today’s M2M solutions. In 2005, he was awarded the prestigious Ericsson Inventor of the Year Award.

Miguel Blockstrand

- is a senior product manager for connected devices and industries. He has 20 years’ experience in telecoms and is currently responsible for the connected devices portfolio offering within Business Unit Networks. Most recently, he has been responsible for the Mobile TV and IPTV network infrastructure portfolios within Ericsson. Prior to his current engagements in the TV area, he held several senior management positions within R&D, Marketing and Business Development. He was involved in the first deployments of GSM, the Japanese PDC mobile system and WCDMA. He holds an M.Sc. in mechanical engineering from Chalmers University of Technology, Sweden.

Berndt Wallin

- joined Ericsson in 1986 and is an expert in media-handling architectures.
- Apart from a two-year period of mobile-phone development at Research Triangle Park, North Carolina, US, he has worked for the last 15 years with speech- and media-processing products such as transcoders, echo cancellers, media gateways, messaging and TV systems. For the past year he has led the Ericsson Device Connection Platform development program. He holds an M.Sc. in electrical engineering from KTH, Sweden.

Tomas Holm

- is a system manager and has worked with IMS since he joined Ericsson in 2005. During the past year he has been responsible for cross-area system issues in Ericsson Device Connection Platform. He has vast experience in IT software development, having held various roles at several companies and holds an M.Sc. in computer science and engineering from KTH, Sweden.

Lars-Örjan Kling

- is an appointed expert in IP technology at Ericsson’s Business Unit Networks, currently engaged in the 50 Billion Connected Devices R&D program with a focus on technology strategies. He joined Ericsson in 1980 to work as a computer architect. Following this, he was active in many areas including multi-processing, high availability, mathematical specification methods and neural computing. In 1997, he entered the datacom area where he had the role of chief architect for router data plane design. Later engagements included areas such as deep inspection, media streaming and internet-caching techniques. He holds an M.Sc. in electrical engineering from KTH, Sweden.

Conclusion

Ericsson Device Connection Platform is an important step towards realizing the vision of more than 50 billion connected devices. It provides tools for actors, such as operators and enterprises, to handle provisioning in a self-service way. It also delivers methods to tailor subscriptions to meet the varied connectivity requirements of the massive number and variety of connected M2M devices. The device access enabler function in EDCP solves the issue with find and connect in a world of NATs and firewalls, and at the same time shields M2M devices from unsolicited usage. EDCP, offered as SaaS, is a way to re-use nodes and functions between several business domains and different mobile operators.

Solving connectivity challenges is the natural first step towards achieving the vision. The next step will be to offer solutions for application support — in other words, to develop, install and execute M2M applications in a more cost-effective and convenient way.

More than 50 billion connected devices

Reference