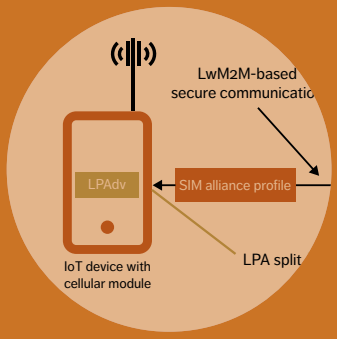
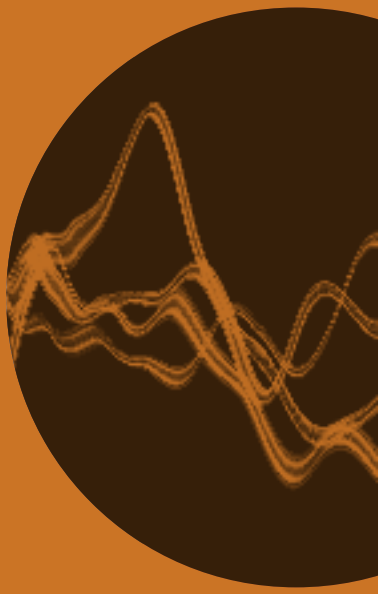
CHARTING THE FUTURE OF INNOVATION | #04·2020

ERICSSON TECHNOLOGY Review





UICC MODULES AND THE IoT

ERICSSON

OPTIMIZING

UICC modules for IoT applications

The UICCs used in all cellular devices today are complex and powerful minicomputers capable of much more than most Internet of Things (IoT) applications require. Until a simpler and less costly alternative becomes available, it makes sense to find ways to reduce the complexity of using them and use their excess capacity for additional value generation.

BENEDEK KOVÁCS,
ZSOLT VAJTA,
ZSIGMOND PAP

UICCs are used today to facilitate network connection in all 3GPP user equipment – mobile phones, IoT devices and so on.

The most important tasks of UICC modules – commonly referred to as SIM cards – in today's mobile networks are to store network credentials and to run network security and access applications in a secure and trusted environment. In addition, they are also capable of storing a large amount of extra information and running multiple toolkit applications. A UICC's own operating system provides a full Java environment. It can run dozens of Java-based applications in parallel and support powerful remote management operations.

Backward-compatibility is provided by running a network service application on UICC modules, which can emulate the file system for storing necessary credentials and old-school smartcard protocols, extended with features such as enhanced security, extended telephone register and operator logo image. The interface between the UICC module and the user equipment (devices) is standardized, which enables operators to run value-added applications, such as mobile wallet or mobile lottery, on the UICC module.

While the advanced features of UICC modules continue to provide considerable value in mobile phone applications, most of them are superfluous in IoT applications. In light of this, the industry is working to find a less sophisticated solution that is more appropriate for applications that require massive numbers of devices in price-sensitive environments. Industry alignment on such a solution is expected to be a challenging and time-consuming process, however, due to the fact that the IoT area is fragmented into many different verticals, application areas and use cases.

Ericsson is fully committed to supporting the long-term, industry-aligned solution. In the meantime, however, it is vital to find workarounds to ensure that the cost of UICCs does not stifle IoT growth. While the definitive solution to the question of what should replace the UICC is hard to predict, two mid-term workarounds are clear: the complexity of using UICCs and leveraging their excess capacity to generate additional value.

Reducing the complexity of using UICCs

There are three main approaches to reducing the complexity of using UICCs in IoT applications: optimization, usage of 3GPP standardized certificate-based authentication, and virtualization.

Optimization

A typical operator profile on a 3GPP consumer mobile phone is up to tens of kilobytes; the average IoT sensor only requires 200-300 bytes. And of all the functionality that a UICC can provide, an IoT device only really needs the Universal Subscriber Identity Module application and the remote SIM provisioning (RSP) application, which allows remote provisioning of subscriber credentials (also known as operator profiles).

One good way to significantly reduce the footprint of the UICC is to optimize the operator profile and the necessary software environment within the UICC module. Doing so not only saves storage in the device but also reduces energy consumption during over-the-air download. Further size reduction of the device may be achieved when the UICC is completely integrated into the baseband modem or application processor (integrated UICC or iUICC [2]). This simplified and integrated solution could work effectively for use cases that require low-cost, simple, secure and low-power IoT devices in high volumes.

The use of an iUICC requires an effective RSP protocol [3, 4] that makes it possible to change subscription credentials. Current RSP standards are too complex for iUICCs for many reasons, including their use of HTTPS

Definition of key terms

Identity describes the link between the identifier of an entity and the credentials that it uses to prove that it is the rightful owner of the identity.

First used in Finland in 1991, the original **subscriber identity module** (SIM) was a smart card with a protected file system that stored cellular network parameters. It was designed to connect expensive user equipment – mobile phones – with expensive subscriptions to the cellular network.

When it became clear that smart cards did not have the capacity to provide an adequate level of security in next-generation cellular networks, they were replaced with **universal integrated circuit cards** (UICCs) – minicomputers equipped with general microprocessors, memory and strong cryptographic co-processors [1].

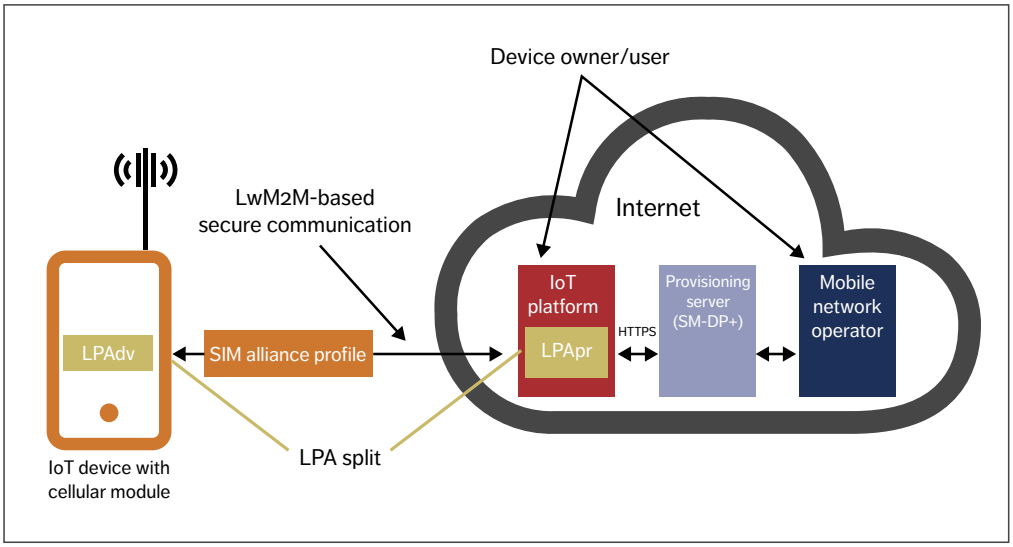


Figure 1 Remote provisioning using IoT-optimized technology

(Hypertext Transfer Protocol Secure) and reliance on SMS support. HTTPS is typically not part of the protocol stack of constrained low-power IoT devices. Instead, these devices use a stack with Constrained Application Protocol (CoAP), Datagram Transport Layer Security (DTLS) and User Datagram Protocol. In some cases, the Lightweight Machine-to-Machine (LwM2M) protocol is used on top of CoAP for device and application data management. The use of only one stack keeps the cost of the device down.

Ericsson proposes utilizing the same protocol stack for profile download and profile management as is used for device and application data management. *Figure 1* illustrates how to achieve this by adapting the GSMA embedded-SIM solution for consumer devices for use with IoT devices. In this solution, the local profile assistant (LPA) is split into two parts. To reduce device footprint, the main part of the LPA (including the use of HTTPS) is moved from the device to a device or connectivity management server. The device management protocol stack (Open Mobile Alliance (OMA) LwM2M [1], for example) handles the communication between the two LPA parts. Profile protection is still end-to-end between the iUICC/embedded-UICC (eUICC) and the provisioning server (Subscription Manager-Data Preparation – SM-DP+).

Usage of 3GPP standardized certificate-based authentication

Another way to reduce the need for a UICC is to use a network authentication mechanism different to the classical 3GPP Authentication and Key Agreement (AKA). The use of certificates is a classic solution used in the internet that may easily fit into the existing network architecture of an enterprise/service provider. In public 5G networks, authenticating with certificates is possible as a secondary authentication for a service using AKA, but only after primary network

authentication has been performed. According to the 3GPP, authentication in private networks such as Industry 4.0 solutions may rely entirely on certificate-based solutions such as Extensible Authentication Protocol over Transport Layer Security. Without a UICC for securely storing and operating on secret long-term credentials for network access authentication, another secure environment with secure storage solution is needed.

For certain applications a lower level of security might be accepted. The value of the data that the IoT device provides or handles, in relation to the cost of the IoT device, determines the required security level of the secure environment for protecting network access authentication credentials. In the case of a UICC being used, it determines the realization of the UICC functionality. For some low-cost constrained IoT devices, a realization using a hardware-isolation-based trusted execution environment may be acceptable. As there is no universal and perfect solution, operators must decide which solution is most suitable for any given application. It is likely that the UICCs and eUICC-based solutions will remain the technology of choice in public networks for the next few years.

Virtualization

Virtualizing the UICC is yet another alternative that addresses the cost issue associated with UICC technology. One way to do this is to run a UICC environment in a virtual machine (or at least on a separated processor core) inside the application processor or the baseband modem. Another approach is to store the operator profiles in the security zone of the application processor, then download them to empty physical UICC hardware on demand.

The biggest advantages of these virtualization solutions is flexibility and better utilization of existing hardware resources, while at the same time maintaining many of the advantages of current technology. These methods are particularly effective when an IoT device needs to manage multiple operator profiles – a circumstance that will become increasingly common, according to an analysis carried out by the GSMA [5].

The disadvantages of virtualization are similar to those of certification-based solutions. Most notably, certification is harder when a trusted environment is integrated with the rest of the device compared with using an isolated UICC or eUICC.

> “OPERATORS MUST DECIDE WHICH SOLUTION IS MOST SUITABLE FOR ANY GIVEN APPLICATION”

Generating additional value from the UICC

Experience shows that it is significantly less expensive to limit a protected and certified manufacturing environment to a dedicated hardware module such as a UICC than to ensure that all the software running in the mobile equipment can be trusted. In light of this, we believe that communication service providers will continue using UICC modules for at least the next 5-10 years. During this period, it makes sense to exploit the potential of the UICCs to better support IoT applications by creating value-added services for operators and enterprises. Three examples of this are using the UICC as cryptographic storage, using it to run higher-layer protocol stacks, and using it as a supervisory entity.

Using the UICC as cryptographic storage

UICC modules were designed to serve as cryptographic storage and are used today mainly for the storage of security credentials for 3GPP connectivity. We propose, in accordance with GSMA IoT SAFE [1], that the UICC itself should also be used as a crypto-safe for the IoT platform, providing support to establish encrypted connection of the applications.

A generic IoT device has multiple identities for use in multiple security domains. Every identity has at least one identifier and credential, all of which must be stored somewhere. Although there are multiple options, a hardware element that is powerful enough to play the role of the root of trust is definitely needed. The UICC is perfect for this role, as it is already used as an identity for 3GPP networks, storing International Mobile Subscriber Identity, intensified charge-coupled device, Wi-Fi and OMA LwM2M [6] credentials along with dozens of other identifiers. The necessary trusted and certified environment and infrastructure are already available to manufacture the module, download and update its content and carry out remote management as well.

To cover every aspect, UICC-based solutions require cooperation between the UICC ecosystem and the IoT device security subsystem (ARM Trust Zone [7], for example). ID and credential management itself is device-independent, which saves development cost and increases the security level. Additional advantages of using UICC as a root of trust are:

- it has its own local processor
- it is usually equipped with powerful cryptographic co-processors
- it comes with a powerful, standardized remote management subsystem (RMS)
- it is handled through a separate logistics chain.

The UICC can generate key-pairs and store private keys for multiple security domains effectively and securely. Effectiveness comes from its powerful cryptographic co-processors, while security is provided by the combination of the standardized RMS and the UICC's ability to run cryptography processes inside the module. This means that the keys never leave the hardware and therefore they cannot be exposed to the application. Not only does this architecture provide security, it can also securely tie the 3GPP connectivity credentials and other IoT certificates to each other.

The recently released GSMA IoT SAFE [8] offers a solution where the UICC is utilized as a root of trust for IoT security. Here, an applet on the UICC/eUICC provides cryptographic support and storage of credentials for establishing secure communication (for example, using DTLS) to an IoT service. The existing UICC management system (UICC OTA mechanism) is used by the operator to establish trusted credentials between the device and the IoT service. The GSMA IoT SAFE defines an application programming interface for interoperability between SIM applets from different operators.

> “EFFECTIVENESS COMES FROM ITS POWERFUL CRYPTOGRAPHIC CO-PROCESSORS”

Using the UICC to run higher-layer protocol stacks

In addition to providing security and encryption functions, UICC modules could also serve as main application processors. Today, a low-cost, sensor-like IoT device usually has at least three processors on board: one is on the UICC module, another runs inside the baseband modem, and a third – the application processor itself (sometimes combined) – collects data and hosts higher level communication stacks such as LwM2M, CoAP or MQ Telemetry Transport.

Shifting the higher-level communication stack from the application processor to the UICC module can lead to cheaper hardware and lower development costs, as well as providing a unique approach to interoperability. As a result, some modem manufacturers have implemented these protocols inside the modem, running a complete OMA LwM2M protocol stack in the baseband chip, for example. While this may free up an external application processor and speed up device development, this solution is rather inflexible.

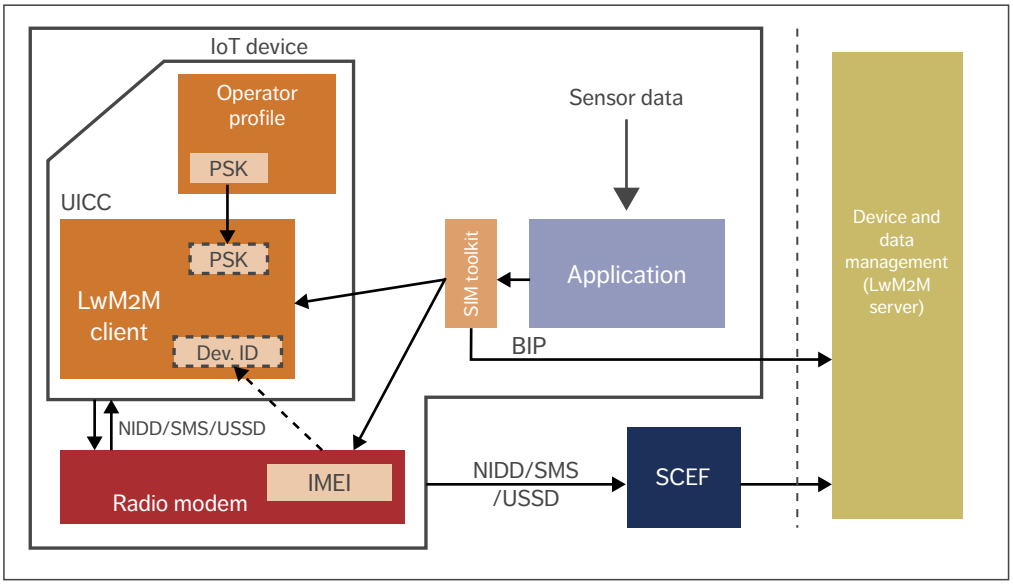


Figure 2 IoT device with LwM2M client running on the UICC module, using NIDD

Since modem firmware is a closed environment, it is difficult to upgrade and to customize its protocol stacks (extending them with proprietary added values). In addition, a small security hole in the protocol stack can be enough for a hacker to take control of the whole modem.

Alternatively, these higher-layer protocol stacks can be moved to the UICC. *Figure 2* depicts a block diagram of a device, where the OMA LwM2M client runs on the UICC module and uses a non-IP data delivery (NIDD) protocol connection to send information to the device management system.

Running higher-level protocols in the UICC module can improve security in several ways. For example, it is possible to run the LwM2M stack over a NIDD connection [9] and even to allow this code to execute on the UICC module instead of on the device processor. In this scenario, command/control is never exposed on the IP layer because it is running in the signaling network of the operator. An additional advantage of this approach is that it increases interoperability.

There is a standardized way of upgrading the communication stack in the UICC – it is even possible to insert the communication stack into the operator profile. This does not completely solve compatibility and interfacing problems, but a certified operator can handle these issues on a higher security level to provide wider solution matching.

In the simplest IoT devices, it might even be possible to run the actual IoT application on the UICC module. This would open for edge-computing solutions in which simple tasks are executed on the device – data filtering to reduce the amount of data being sent over the air, for example. Security can also be improved if the binary is stored on the UICC instead of on the device application processor.

Using the UICC as a supervisory entity

Zero-touch provisioning (ZTP) is yet another possibility for better utilization of the UICC module. ZTP refers to the possibility of adding an identity to a device when required, with automatic setup of the working environment (requiring manual intervention).

An effective automatic provisioning system requires remote provisioning management, key and credential storage, identity mapping of UICC modules and applications as well as strong flexibility in case of operator profiles, but all of this is far from enough. Provisioning of IoT devices is a complex, slow and costly procedure. Although there is a joint effort to extend mobile networks to support standardized, automatic device and subscription provisioning, it is at a very early stage.

> A UICC MODULE CAN STORE SENSITIVE INFORMATION

During the provisioning procedure, two or more identities are given to the device, which entails that these identifiers are downloaded, and different subsystems are configured (mobile network, device management system, data management system, and so on). Several standardized technologies exist to support this process but, unfortunately, they are not connected into a working, efficient, fully automated and cooperative system.

The most straightforward way to connect different subsystems in a flexible and programmable way is to run a centralized service above or at the same level as these subsystems. This ZTP service is connected to the 3GPP network (for instance to subscriber data management), to the SM-DP+ system (usually operated by the UICC module vendor or an independent bootstrap operator), to the device management system and to the data management system. The connection to the IoT device itself, to the manufacturer or even to the installer of the device can also be established. The main purpose of this service is to drive the IoT device through the steps of automatic device provisioning from the very beginning (ordering the device) to the final decommissioning.

Although this over-the-top service (OTT) can speed up the provisioning process significantly, it has some disadvantages. It should not store sensitive data, but only manage it indirectly. Furthermore, if the device has no connection at all, it cannot do anything. Scaling could also be a problem.

Terms and abbreviations

AKA – Authentication and Key Agreement | **BIP** – Bearer Independent Protocol | **CoAp** – Constrained Application Protocol | **DTLS** – Datagram Transport Layer Security | **eUICC** – Embedded UICC (soldered to the device board) | **HTTPS** – Hypertext Transfer Protocol Secure | **IMEI** – International Mobile Equipment Identity | **IoT** – Internet of Things | **IUICC** – Integrated UICC (integrated to a microchip) | **LPA** – Local Profile Assistant | **LPAdv** – LPA (device), interfacing to the UICC | **LPApr** – LPA (proxy), interacting with the device owner and SM-DP+ | **LwM2M** – Lightweight Machine-to-Machine | **NIDD** – Non-IP Data Delivery | **OMA** – Open Mobile Alliance | **OTT** – Over-the-Top | **PSK** – Pre-shared Keys | **RMS** – Remote Management Subsystem | **RSP** – Remote SIM Provisioning (protocol) | **SCEF** – Service Capability Exposure Functions | **SM-DP** – Subscription Manager–Data Preparation | **UICC** – Universal Integrated Circuit Card | **USSD** – Unstructured Supplementary Service Data | **ZTP** – Zero-Touch Provisioning

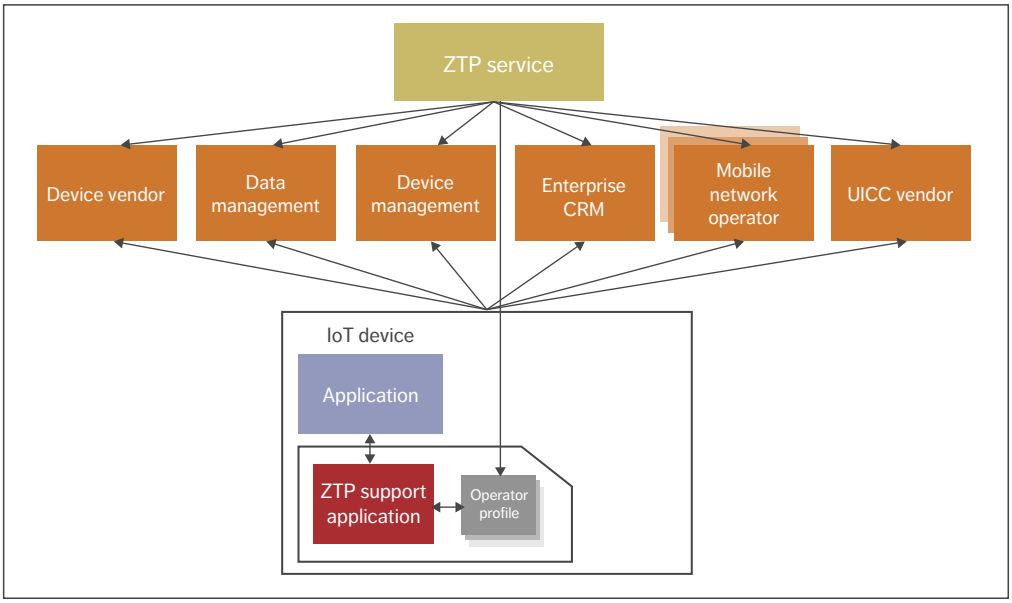


Figure 3 ZTP system with central ZTP service and UICC support

This is where a UICC application can help and support an OTT ZTP service. A UICC module can store sensitive information from different security domains. As it works close to the IoT device, it can do corrective actions locally if there is a problem with the connectivity (attempt to activate another profile and connect to another operator). In addition, it is scaling together with the IoT devices. Since this solution is completely under the control of the operator, it can be independent of the application, thereby also saving development costs.

Figure 3 shows an example of this system: a central ZTP service, in connection with multiple subsystems and a support application on the UICC module.

The central ZTP service working together with the ZTP support application on the UICC module can be very effective. The ZTP service and the ZTP support application together can cover almost every use case and solve the problems the IoT area is struggling with today.

The UICC application can be used to monitor connectivity and fix issues locally. This can be highly effective if credentials are stored on the UICC module and if the IoT protocol stack is also running on the UICC module.

For narrowband IoT, the traditional profile download solution and the machine-to-machine SM-DP is ineffective. Significantly better results can be achieved by using the SM-DP+ in a new way. For example, running the LPA proxy on the UICC module makes it possible to use completely new options for device provisioning.

Conclusion

The universal integrated circuit card (UICC) modules present in all 3GPP IoT devices today are costly and underutilized.

The industry is looking for ways to replace them with a next-generation solution, but for the foreseeable future UICC modules are here to stay. While there are a few ways to reduce the complexity of using UICC modules and thereby reducing the cost of IoT devices, it is also possible to extend the application of UICC modules well beyond the cellular domain. For example, members of the existing UICC ecosystem can start exploiting UICC capabilities for storing IoT identities, executing IoT protocols, increasing security, providing end-to-end connectivity as a service, and/or supporting zero-touch provisioning.

References

1. **Ericsson blog, Evolving SIM solutions for IoT, May 27, 2019, Smeets, B; Ståhl, P; Fornehed, J, available at:** *https://www.ericsson.com/en/blog/2019/5/evolving-sim-solutions-for-iot*
2. **UICC card HW specification for P5Cxxxx cards, available at:** *http://www.e-scan.com/smart-card/nxp.pdf*
3. **GSMA, RSP Technical Specification Version 2.1, February 27, 2017, available at:** *https://www.gsma.com/newsroom/wp-content/uploads/SGP.22_v2.1.pdf*
4. **GSMA, Remote Provisioning Architecture for Embedded UICC Technical Specification Version 4.0, February 25, 2019, available at:** *https://www.gsma.com/newsroom/wp-content/uploads/SGP.02-v4.0.pdf*
5. **GSMA Intelligence: The future of the SIM: potential market and technology implications for the mobile ecosystem, February 2017, Iacopino, P; Rogers, M, available at:** *https://www.gsmaintelligence.com/research/?file=3f8f4057fdd7832b0b923cb051cb6e2c&download*
6. **OMA, Lightweight Machine to Machine Technical Specification: Core, July 10, 2018, available at:** *http://www.openmobilealliance.org/release/LightweightM2M/V1_1-20180710-A/OMA-TS-LightweightM2M_Core-V1_1-20180710-A.pdf*
7. **ARM, ARM Security Technology, available at:** *http://infocenter.arm.com/help/topic/com.arm.doc.prd29-genc-009492c/PRD29-GENC-009492C_trustzone_security_whitepaper.pdf*
8. **GSMA, IoT SAFE, available at:** *https://www.gsma.com/iot/iot-safe/*
9. **OMA, white paper, Lightweight M2M 1.1: Managing Non-IP Devices in Cellular IoT Networks, October 2018, Slovetskiy, S; Magadevan, P; Zhang, Y; Akhouri, S, available at:** *https://www.omaspecworks.org/wp-content/uploads/2018/10/Whitepaper-11.1.18.pdf*

Further reading

- **Ericsson Technology Review, Key technology choices for optimal massive IoT devices, January 2019, available at:** *https://www.ericsson.com/en/reports-and-papers/ericsson-technology-review/articles/key-technology-choices-for-optimal-massive-iot-devices*
- **Ericsson, eSIM – Let's talk business, available at:** *https://www.ericsson.com/en/digital-services/trending/esim*
- **Ericsson blog, Secure IoT identities, available at:** *https://www.ericsson.com/en/blog/2017/3/secure-iot-identities*
- **Ericsson blog, Secure brokering of digital identities, available at:** *https://www.ericsson.com/en/blog/2017/7/secure-brokering-of-digital-identities*

The authors would like to thank the following people for their contributions to this article: Gergely Seres, John Fornehed, Per Ståhl, Peter Mattsson, Bogdan Dragus, Robert Khello and Tony Uotila.

THE AUTHORS

Benedek Kovács

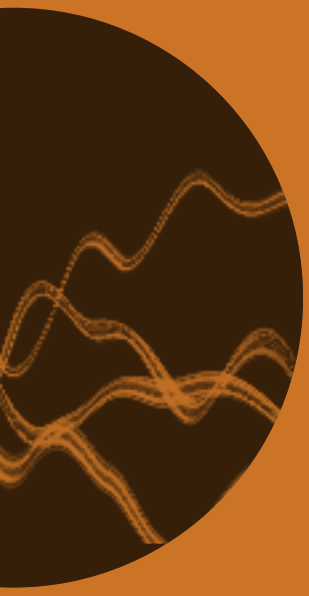
◆ joined Ericsson in 2005. Over the years since he has served as a system engineer, R&D site innovation manager (Budapest) and characteristics, performance management and reliability specialist in the development of the 4G VoLTE solution. Today he works on 5G networks and distributed cloud, as well as coordinating global engineering projects. Kovács holds an M.Sc. in information engineering and a Ph.D. in mathematics from the Budapest University of Technology and Economics in Hungary.

Zsigmond Pap

◆ joined Ericsson in 2012. After working in the cloud native and 5G packet core areas as technical manager and system architect respectively, he moved into the IoT area. He specializes in low-level software development and he has participated in multiple hardware and firmware developments related to custom hardware solutions. He holds an M.Sc. in the area of hardware and embedded computers and a Ph.D. in information engineering from the Budapest University of Technology and Economics in Hungary.

Zsolt Vajta

◆ joined Ericsson in 2015 as a software developer focused on developing and maintaining modules to implement the link aggregation control protocol in the IP operating system. In 2018, he became involved in research on IoT device activation and zero-touch provisioning. As of early 2020, he has joined the packet core area as a product owner. He holds an M.Sc. in informatics and physics as well as a Ph.D. in nuclear physics from the University of Debrecen in Hungary.



ISSN 0014-0171
284 23-3343 | Uen

Ericsson
SE-164 83 Stockholm, Sweden
Phone: +46 10 719 0000