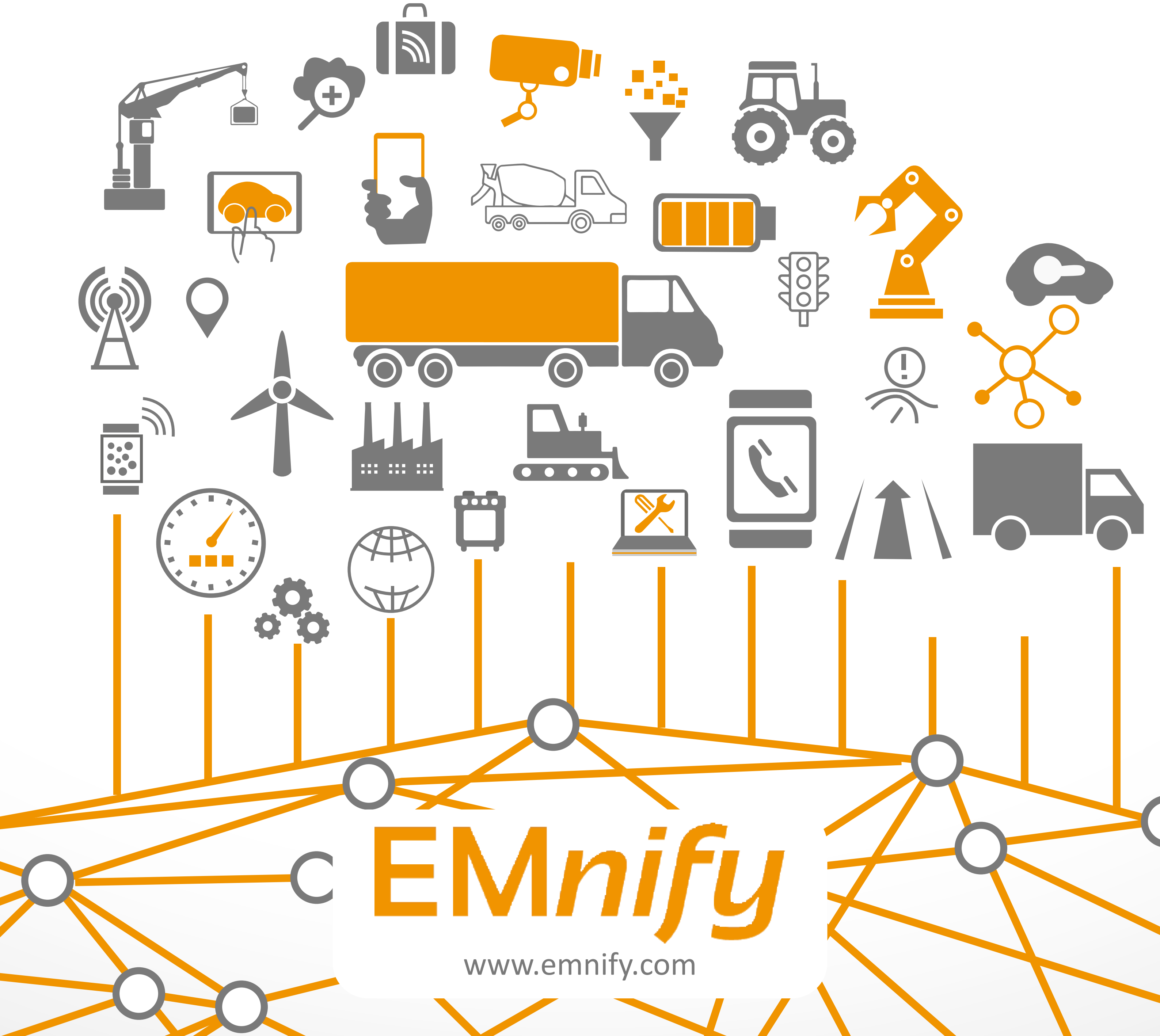
Globalized M2M & IoT Connectivity



EMnify

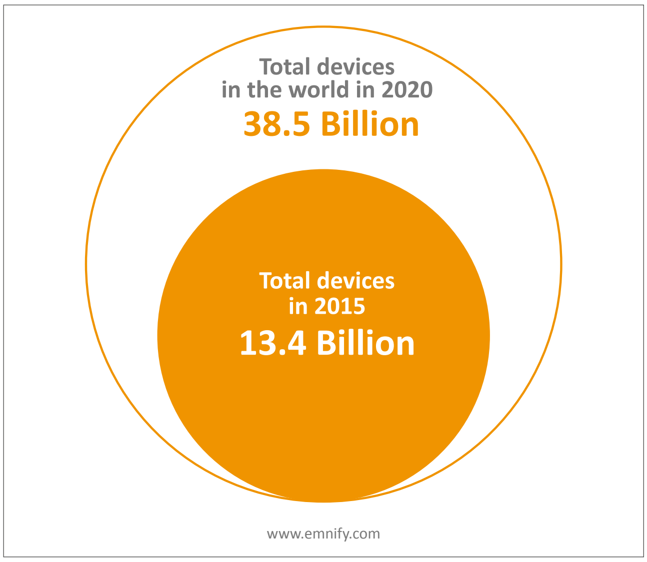
www.emnify.com

Content

Introduction

The Internet of Things is taking the world by storm with millions of devices coming online every day.

Over 13 billion connected devices are predicted to be in existence according to the analysis firm Juniper Research.[1] Over 5.5 million new devices are coming online every day, representing a 30 percent increase in the number of connected devices from 2015.[2]



The challenge many enterprises face with an ever-growing network of connected 'things' is how to effectively capture and channel the data being exchanged. 'Things' in the **Internet of Things (IoT)** refers to any wire- or wirelessly connected physical object, including transportation vehicles, sensors, mobile phones or even people. This is where Machine to Machine (M2M) technology comes into play - M2M enables the connection of 'things'.

This white paper explores M2M connectivity, including a definition of the concept and various connection options. It dives into how IoT applications are enabled by M2M, and describes the existing options for IoT connectivity. Next, a business case for global connectivity solutions through a relatively new hardware, **Universal Integrated Circuit Cards (UICC)**, is presented. The case demonstrates how UICC technology could influence and shape both connectivity and business in the future. Furthermore, this paper will address questions of data management and security for manufacturers who are preparing for a global deployment of internet-enabled devices.

Challenges of M2M/IoT connectivity include:

- **Cost control**
  As more devices become connected, how can businesses monitor, manage and adapt to connectivity costs?
- **Management of many devices**
  How can businesses best keep track of, maintain and regulate the connectivity of each device without excessive time and resources?
- **Security**
  How do businesses deal with an increased amount of data communicated via public channels like the internet? How can businesses protect against hackers gaining access to private networks and misusing data?
- **Increased complexity**
  How should businesses best interpret and use their data to effectively monetize the IoT using advanced tools and APIs?

While the advantages and benefits provided through global connectivity are vast, planning and executing a global deployment of devices can be a demanding process.

This paper addresses these questions and offers insight into the key components that are needed for an efficient and effective M2M connectivity platform.

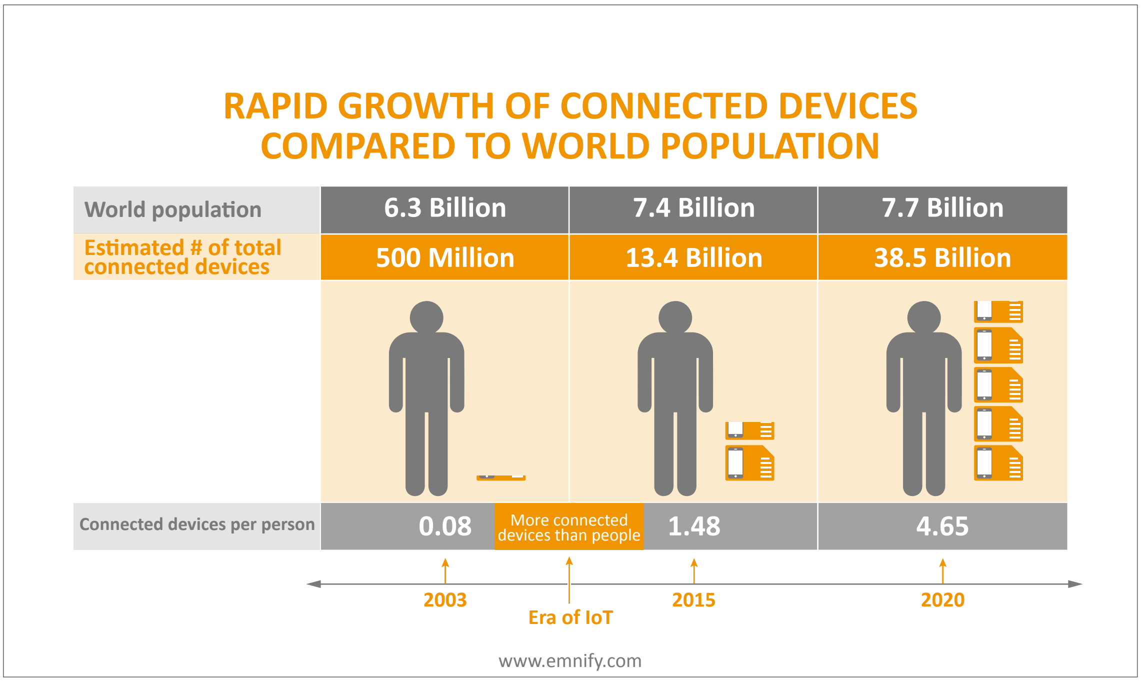
Overview - What is M2M?

Machine-to-Machine (M2M) refers to the technologies that enable products or “things” (within the IoT) to communicate with each other - and with other Internet-enabled devices and systems. There are a range of technologies and protocols that enable M2M connectivity; the best technology choice greatly depends on the specific use case. For example, smart home connectivity is mostly provided via Bluetooth variants, while the logistics and transportation industry typically utilizes cellular M2M connectivity to cover larger regions.

The concept of enabling devices with the ability to communicate with each other, without human interaction, has been a subject of experimentation many times throughout the decades. From the 1930s to the 1980s, the technical history of early M2M closely evolved with the needs of military surveillance and industrial productivity.[3] However, as early as 1968, Theodore G. Paraskevakos began working on a concept to enable telephones to exchange caller information with each other; his concept forms the basis of modern day caller ID systems.

In recent years, the global number of Internet-enabled devices has skyrocketed. According to Cisco it was between 2008 and 2010 that the number of connected devices first exceeded the number of people in the world.[4] It is this point that the era of IoT was born.

It is widely estimated that in the next four years (in 2020), more than 38 billion connected devices will come online.[5]



IoT Applications Enabled by M2M

In a world with billions of connected devices and endless information being communicated between them, the opportunities for businesses to harness and channel incoming data are great. Developers and enterprises can now connect and communicate with many assets, in real-time, anywhere in the world. This means the ability to track cost, usage, device lifecycle and many other factors relating to products and customer cases.

Products enabled with communicative capabilities – and the M2M systems used to aid these communications – have become incredibly advanced and varied. They range from remote surveillance to smart metering and smart grids; from monitoring stock in vending machines to fleet management; from pet tracking to monitoring smoke detector functionality. Product deployments on small and large scales can now be automated to gather information and perform commands. Automations can help businesses to manage resources, perform operational tasks according to predefined rules, tailor customer experiences by monitoring behavioral/purchase patterns and much more.

Connectivity Options of IoT

There are a range of technologies that enable M2M connectivity, each with benefits and restrictions that are explored below. The most common connectivity options include **Wireless Local Area Networks (WLAN), Bluetooth, Lower-Power Wide Area Networks (LPWAN) and Cellular**.

WLAN

Wireless Local Area Network technology operates in the license-free, global 2.4 GHz and 5 GHz industrial, scientific and medical (ISM) radio frequency band. This means it has high bandwidth capabilities, and is typically the go-to solution for home or office internet connectivity. It allows users to transfer large amounts of data, such as file exchange, video or audio streaming.

However, Wi-Fi connectivity from WLAN has a limited possible range - typically no more than 32 meters from the access point/router, provided there is a clear line of sight.[6] In light of this, it is not suitable for long-range connectivity.

EXAMPLES
of IoT applications through WLAN connectivity:

- Smart home thermostats/power meters
- Smart city technology such as parking meters

Bluetooth

Bluetooth is also a short-range connectivity solution. It operates on the license-free, global 2.4 GHz to 2.485 GHz ISM frequency band. It is also able to ‘hop’ between frequencies to reduce interruptions in connection from other wireless technologies sharing the same ISM spectrum. Due to it being a low bandwidth connection, it is not suitable for transferring large amounts of data; it is best suited to linking sensors and small electronic devices.

EXAMPLES
of IoT applications through Bluetooth connectivity:

- Audio and mobile applications
- Sports and fitness accessories (‘wearables’)

Lower-Power Wide Area Networks (LPWAN)

Lower-power wide area networks are a type of telecommunication network designed to allow long range communications at a low-bit rate for devices such as battery operated sensors. LPWAN work in the license-free ISM frequency bands.

Two of the main players in the LPWAN space are **LoRA (long range radio)** and **SigFox**. Each have a niche in the market, and warrant a detailed discussion:

Long Range Radio (LoRA)

LoRa wide-area network (LoRa WAN) is a LPWAN specification intended for wireless, low-cost, battery operated devices in regional, national or global networks.[7]

LoRa WAN is a product of the LoRa Alliance, an open, non-profit association of industry leaders that believe the IoT era is now, and built the network specifically for IoT/M2M connectivity. The goal of the alliance is to standardize LPWANs being deployed around the world to enable IoT, M2M, smart city and industrial applications.

The solution is designed to connect over long distances (up to 16 kilometers away), in harsh environments, and in isolated areas (e.g., underground). LoRa provides bi-directional communication between end-devices and enterprises via a gateway. This means it is not possible to connect devices as a standalone service, and businessess still require a Wi-Fi or cellular connection to enable communication from the gateway to the server network.

EXAMPLES
of IoT applications through LoRa connectivity:

- Smart agriculture
- Sensor networks

SigFox

SigFox, a French company founded in 2009, deploys LPWAN using ISM band frequencies for low-energy objects. The company uses a cellular style system for connecting remote devices, and 'ultra-narrow' band technology that enables signals to pass through solid objects, making it ideal for devices deployed under-ground or in rough terrain. In open space the connection range is over 40 kilometers.[8]

It also has an extremely reduced power usage rate, making the system practical for remote deployments that cannot be easily accessed for battery maintenance. The standby time for two AA batteries in SigFox connected devices is 10 years or more.[9]

However, the network is limited to transmitting only small amounts of data with a wireless throughput of up to 100 bits per second and a payload size of 12 bytes per message.[10] The SigFox network is best suited to M2M use cases that do not require large amounts of data being communicated and/or do not require frequent communication.

EXAMPLES
of IoT applications through SigFox connectivity:

- Remote monitoring systems
- Remote alarm systems

Cellular

Cellular is a **WAN (wide area network)** with the long-range ability to connect globally using radio waves that are sent and received via cell towers. Strong connections can be made between a device and a cell tower within 16 kilometers. It is also possible to connect to cellular networks via satellite, further eliminating barriers to connectivity in remote areas.

Roaming capabilities ensures that a cellular connected device maintains network connectivity while traveling. Through a cellular roaming network, a device can benefit from continuous coverage for data, voice and SMS when traveling outside of its home network. This occurs because devices are allowed to hop between mobile network operators. Depending on the roaming agreement between two networks, large fees can be levied per minute of voice service, per SMS message and per megabyte of data used.

However, it is important to note that connectivity depends on the strength of coverage, as well as the number of cell towers in the area. Reliable cellular coverage is available in 250+ territories and countries through the networks of over 990 **Mobile Network Operators (MNOs)**.[11] Cellular bandwidth is not as high as Wi-Fi, however the majority of IoT applications use little bandwidth (on average 3-5 MB per device each month). Cellular is easily able to accommodate the connectivity demands of these applications.

Cellular connectivity has a higher power consumption, especially for continuous service, and is more suited to easily accessible devices, or devices that can be fitted with mobile battery packs. The benefits of cellular to enable mobile, global connectivity far outweigh drawbacks of power consumption. It is in many ways an optimal choice for M2M and IoT devices.

EXAMPLES

of IoT applications through cellular connectivity:

- Logistics - asset tracking for fleet management
- Transport - smart car technology and keyless locking systems

CONNECTIVITY OPTIONS

Characteristics of Options	WLAN	Bluetooth	LPWAN		Cellular
			LoRa	SigFox	
Frequency Band	Unlicensed, global 2.4 GHz ISM	Unlicensed, global 2.4GHz-2.48GHz ISM	WLAN or Cellular	LPWAN or ISM	Radio frequencies
Range	Very limited: Maximum 32 meters	Limited: Maximum 100 meters	Good: Max. 16 kilometers	Good: Max 40 kilometers	Very good: WAN (Wide area network) – tower dependent; reliably strong signal up to 16 kilometers from tower
Unique feature	Ability to transfer large amounts of data quickly	Ability to 'hop' between frequencies	Proven in harsh environments & underground	Very reduced power usage	Long range potential, global connectivity through cell-towers
Drawbacks	Extremely limited range	Limited range Not suitable to transfer large amounts of data	Can't connect to devices as standalone service	Not suitable to transfer large amounts of data	High power consumption
Examples	Smart streetlights Parking meters Smart home power meters	Audio & mobile apps Wearables Smart home security sensors	Smart agriculture Sensor networks	Remote monitoring systems Alarms	Logistics – asset tracking Transport – keyless locking Smart metering applications

M2M Cellular Connectivity Explored

As cellular connectivity is both a common and advantageous choice for many M2M use cases, it's important to understand the variety of cellular network solutions & **SIM (subscriber identity module) options for global deployment**.

Networks

When using cellular connectivity there is a choice of which Generation of mobile network the device uses (i.e., 2G, 3G, 4G). The higher the number, the faster the ability to send and receive data through the network.

2G

2G was launched in 1991 and was the first network generation to introduce narrow band digital network connectivity. This meant better call quality as well as the ability to connect globally for the first time through a Semi-Global Roaming System. The network only enabled users to connect via voice and SMS, but the low cost of hardware affiliated with this network and its general reliability continue to make it appealing to businesses.

The viability of the 2G network as a solution is uncertain as many major cellular network operators are discontinuing connectivity. AT&T in the United States has announced it will discontinue 2G service by 2017,[12] and Telstra in Australia at the end of 2016.[13]

3G

3G was launched in 1998, heralding a new era for cellular connectivity by enabling users to connect mobile devices to the internet for the first time. The network range of 3G is faster than 2G, enabling more data transmission including voice, SMS, files and streaming. This is the most common network for cellular M2M connectivity with most products and SIMs possessing the ability to connect to it.

4G

4G, launched in 2012, enables users the same functionality as 3G at a much faster rate and with greater capacity for transferring large amounts of data. This is the fastest network available to date, transmitting data at a rate up to 300 megabytes per second compared to the rate of 3G, which around 7 megabytes per second.[14]

4G-enabled devices are newer and have a higher processing power, and tend to be more expensive. 4G also demands higher power consumption, therefore requiring frequent device charging. As improvements to battery life are developed and devices become cheaper, 4G will likely become the new standard for M2M connectivity.

Developments in 5G

Research is already underway in the development of a **5G** network. It is widely expected that 5G will be available in time to meet the business and connectivity needs of 2020. The Next Generation Mobile Network Alliance (NGMA) - made up of mobile operators, vendors, manufacturers and research institutes - published a white paper stating that the next generation network will ensure:[15]

- Much greater throughput
- Much lower latency
- Ultra-high reliability
- Much higher connectivity density
- Higher mobility range
- Capability to control a highly heterogeneous environment
- Capability to ensure security and trust, identity and privacy

SIM Specifications

SIM cards come in a variety of sizes and have features optimal for different business cases.

Form Factors

SIM cards come in four standard sizes. These include 1FF, the first and largest SIM to be developed which is no longer used in modern applications; 2FF, the 'mini-SIM'; 3FF, the 'micro-SIM'; and 4FF or the 'nano-SIM', the latest and smallest in SIM design technology. There is also an embedded SIM option, the MFF2.

Which size of SIM used is dependent on the size of the device and the amount of space available to accommodate a SIM. Household pet tracking devices, for example, utilize nano-SIM technology in order to fit on the collar of an animal.

It is also possible to select industrial-grade SIMs in the form factors 2FF-4FF. These come with a thicker pin plate to safeguard the device from corrosion, vibrations and other environmental factors such as extreme temperature (between -40°C and +105°C).

MFF2 (embedded M2M SIM)

Embedded SIMs are typically the most common choice for M2M applications due to a few key benefits:

- **Aesthetics** - enhanced design of a device by negating the need to adapt the size or style of the product to accommodate a SIM portal.
- **Durability** - embedded SIMs enable a stronger device design. Due to it being vacuum sealed and embedded within a device, the SIM is shielded from the weather elements and reduces the chance of malfunction due to shock. It also better protects the SIM from physical tampering and theft.
- **Lifespan** - an embedded SIM has a typical lifespan up to 10-17 years at the industrial grade, which allows it to operate throughout the entirety of the devices' lifecycle.

Globalized Connectivity: A Business Case for UICC

The greatest disadvantages of embedded SIM cards arise when there is a need or desire to switch operators after a device has been deployed into the market. Until recently, the only way to change operators would be to physically change the SIM card, which for an embedded SIM would mean replacing the entire device. A relatively new feature concept is now available on the market. The Universal Integrated Circuit Card, or UICC, is a multi-operator SIM card that simultaneously supports several different operator pro-files. It is common for UICC to be mistakenly referenced as a form factor (MFF2). UICC is a feature of the SIM, not a hardware concept, and is available in all form factors on the market (2FF-4FF and MFF2). Therefore, it can either be a function of an embedded SIM, or as a normal SIM card that is removable. Embedded UICC cards, or eUICC, comes with form factor durability and the flexibility of multiple operators over the lifetime of the SIM.

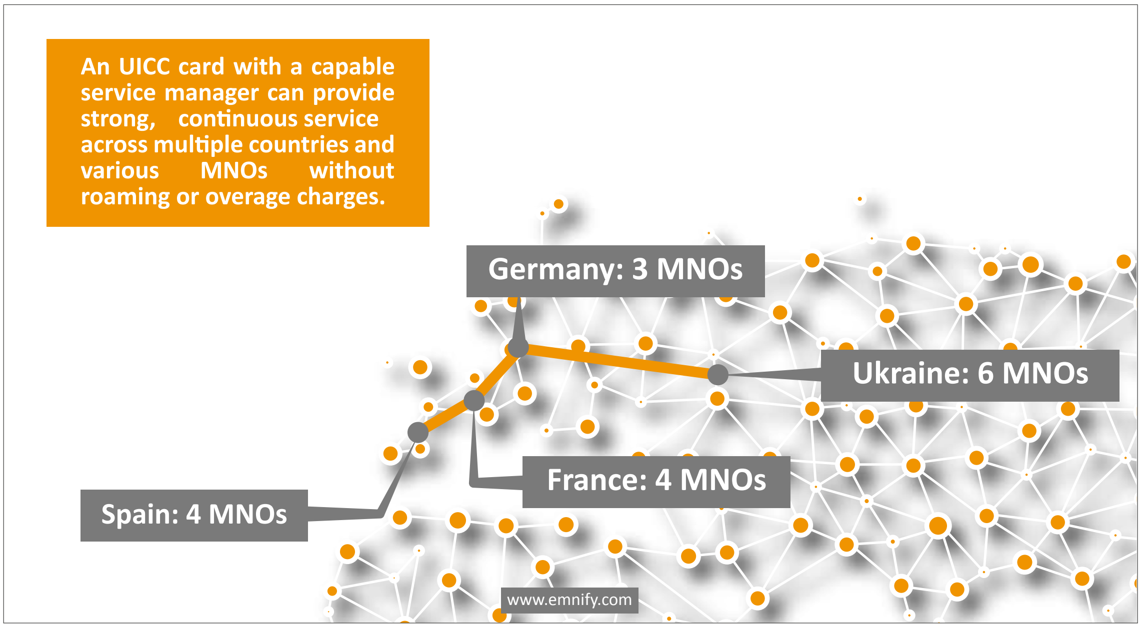
Network agnostic SIM cards

The breakthrough capability of UICC is the ability to host multiple profiles. A traditional SIM is provisioned with a single profile which usually has 64KB or 128KB of memory. An UICC can host multiple profiles and requires a minimum memory of 512KB.

The key benefits of enabling a cellular M2M deployment with eUICC connectivity include[16]:

- **Logistics** - each device has a SIM embedded as soon as it leaves the factory; this negates the need for local logistics and makes it ready for use instantly, no matter where in the world it's de-ployed. Devices and SIM become one component built anywhere that work globally. Installing the SIM during the manufacturing stage also saves costs on production and distribution as well as inventory as only a single stock-keeping unit (SKU) is required.
- **Provisioning** - management of the SIM and switching MNOs are all Over-The-Air (OTA) with an UICC. Traditional SIMs are provisioned with the provider profile of a single MNO. This profile contains information the MNO requires to enable the SIM connectivity (and therefore allow the SIM to function). Traditionally, these profiles are locked to the SIM; meaning if the MNO is changed the SIM will need to be physically replaced. UICCs are able to host multiple provider profiles and can be programmed to use a specific profile or change profiles at any time without the need for physical replacement.

- **Connectivity** - wireless capability is available out-of-the box. This considerably reduces deployment time and provides ease of access/use for end users.



Choosing UICC for Global Connectivity

The globalization of business processes is accelerating at a very fast pace. Often when a global business is developed, the local services of a communication provider are employed in each country or region. However, and especially for SIM cards which are device-specific, it becomes cost and time restrictive to switch SIMs based on the geographical destination of each device[17].

An UICC-enabled device is becoming the best solution for businesses with global deployment.

Use cases specific to global companies, such as the need for continuous device connectivity regardless of international borders, is easily solved with UICC SIM capabilities.

Use Case: Continuous Service

When M2M devices are used globally, they must have the ability to connect to different mobile network operators (MNOs) for uninterrupted service. A device that crosses an international border, or travels through remote areas of one country, is subjected to weaker service and service cessation. For example, a global delivery enterprise using traditional SIM cards would need a different card for each country in which they operate (either built into the device or swapped at each border). The delivery enterprise would additionally need to establish and manage contracts and data usage with different MNOs, adding to logistical and monetary costs. With the introduction of UICC, it is possible to switch profiles using the process that is most convenient for the user.

An UICC enabled device will provide network-agnostic connectivity, but it is equally important to utilize a platform that manages cellular connectivity. A service management platform allows for remote provisioning of a device during its lifetime and the ability to adapt to changing networks and service requirements. In turn, devices that can be well managed yield fewer maintenance costs.

UICC Service Management

An UICC card allows storage of multiple communication profiles, but only one can be enabled at a time. It is when switching profiles that the limitations of an UICC can arise. While the SIM does not have to be physically replaced, there are multiple dependencies to be resolved for a successful profile change. These include reintegration of a service profile, abiding by rules and controls to new MNOs and dealing with the nuances of infrastructure changes.

Connectivity management, billing and provisioning systems all depend on a service profile and an MNO's established rules and controls. The complexity of these dependencies and the potential interruption to service in the event of an MNO change means that forward-planning when initiating an UICC deployment is important.

When selecting a SIM and connectivity platform and/or provider it is important to ask:

- How does the platform/provider aid in MNO changes to lower the chance of service interruptions?
- Does the platform/provider enable global connection, or are multiple service contracts required?
- How scalable is the platform/provider to ensure future deployments can be handled efficiently and effectively?

Managing Data Usage and Cost Control

To ensure the ability to view and manage SIMs and devices in real time, it's essential to work with a provider that has a trusted connectivity management platform. Without the ability to remotely access usage and cost data via an online platform or application program interface (API), there is no practical way to monitor usage or check the balance on a SIM.

When seeking or designing an online application or API for asset management, the following functionalities should be top of mind: service plan management, control over SIM functionality and connectivity protocols.
Through service plans it is possible to personalize and control the price level devices can reach when accessing mobile networks. It is also possible to control which regions, countries and networks the devices are allowed to connect online. Furthermore, it is possible to tailor rules and profiles for each SIM card, enabling it with the ability to achieve the best possible connection or the least expensive connection.

In addition to cost optimization, it is important to have the ability to manage and define usage rules. A good service management platform will enable businesses to view the data, SMS, USSD or voice usage of a SIM in real-time online. It will also enable businesses to define and isolate the level at which a SIM can access these services. Businesses must be empowered to define their own service profiles, for example specifying which network (2G, 3G, 4G, satellite) devices can access. Capabilities such as these make a business more agile, scalable, transparent and cost controlled in regards to the functionality of SIMs and devices.

Security & Enforcement Policies

For any business, security is imperative. With the introduction of new devices and technology - and the increase in global deployments - there are a whole myriad of new security issues that need to be considered and factored in when deploying M2M devices globally.

Initially, it's important to consider a physical security plan that prevents unauthorised access to devices in remote locations. Moreover, a robust remote-access security protocol is needed that allows:

- SIM functionality to be locked to specific devices
- Connectivity to be remotely disable in the event that the physical security is breached

Sending and receiving messages through remotely deployed devices is in itself a security risk. Connecting devices and enabling communication using public-access networks, such as cellular and Wi-Fi, opens up messages and data for interception. Encrypting messages is a step in the right direction, but using public-networks to send sensitive data demands more. EMnify recommends building private networks and **access point names (APNs)** into security protocols to ensure the protection of important, private data.

Additionally, the sheer number of connected devices proves to be its own barrier to implementing a secure, efficient M2M program. This year there will be approximately 13.4 billion connected devices in the world, and that is set to increase nearly threefold by 2020.[2] The complexity of managing devices and the mass of data communicated between them can be daunting; hence the need for a secure management system. Furthermore, the security/authentication protocols for such a system need to be multi-level. If a management platform is hacked, it could mean the entire deployment is compromised and all the sensitive data stored within.

The amount of devices also makes monitoring each device for security issues difficult; therefore it is recommended to have a set of policies and protocols within firewalls, that can automatically detect intrusions or hacking attempts.

The following is an overview of the security features recommended before any SIM-enabled device is deployed.

IMEI lock

An International Mobile Station Equipment Identity (IMEI) is the unique ID number found on most mobile devices. An IMEI lock protocol will enable the configuration of SIM functionality to a specific IMEI in real time to prevent the SIM being removed and used in any other device.

Secure data transfer

By using an APN, accessed through a virtual private network (VPN), it ensures the data communicated between devices is transported with the highest security. An APN is a gateway between a SIM mobile network (e.g., 3G, 4G, etc) and the internet. Creating a private gateway isolates a device from other mobile users. A

VPN is a private network that runs across the internet, and utilizing both an VPN and an APN protects data transferred to, from or between devices and the wider public-network internet.

Network based firewall

A firewall is a network security system that operates at the application layer of a protocol stack. It allows for personalised configuration regarding how data is communicated and transported via networks, enabling businesses to monitor and block certain content or functionalities. It can also detect intrusions or hacking attempts by flagging activities that do not align with pre-configured policies.

When selecting a service manager, best practices include the ability to have fully customizable communication rules on both protocol and device levels. Enterprises should be able to control the type of data transmitted, and which specific devices can send and receive it.

Conclusion

The IoT and M2M industries are continually growing and enabling businesses to reach new levels of achievement and profitability on a global scale. However, an enterprise's ability to monetize the IoT depends greatly on the quality of the connectivity platform and M2M technology they use.

We have assessed the various connectivity methods available for M2M devices, looking at the typical use cases and benefits for each. We have determined that for large-scale, global deployments, cellular M2M connectivity is the most effective solution. However, simply enabling devices with a SIM and cellular connection doesn't make an effective cellular M2M program.

To truly make the most of the next-generation connectivity abilities of M2M technologies and monetize the IoT, businesses need a program that ensures: sustained global coverage; usage and cost control tools - including an online portal or API; a robust security system, including all the features specified above.

At EMnify we specialize in M2M connectivity, providing network agnostic M2M SIM cards and an IoT cloud services platform to securely manage deployments through. We have built our software and infrastructure from the ground up, with the goal of giving customers the most flexibility, scalability and device control in the market. For more information or to talk to us about a solution for your business, please visit our website www.emnify.com.

Additional useful resources

EMnify: IoT and M2M - taking the world by storm (definition of IoT and M2M)
EMnify: SIM form factors explained (analysis of which form factor is best for your IoT application)
EMnify: eUICC - what it is and why it matters (analysis of eUICC benefits and use cases)
EMnify: IoT for transport and logistics (analysis of fleet management and asset tracking enabled by IoT)

Endnotes

1. Juniper Research. (2015, July 28). 'Internet of Things' connected devices to almost triple to over 38 billion units by 2020 [Press release]. Retrieved 7 May 2016, from http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.
2. Gartner. (2015, November 10). Gartner says 6.4 billion connected 'things' will be in use in 2016, up 30 percent from 2015 [Press release]. Retrieved 7 May 2015, from http://www.gartner.com/newsroom/id/3165317.
3. Inglesby, T. (2009, July/August). The History of M2M. Connected World Magazine.
4. Evans, Dave. (2011, April). Cisco: The Internet of Things How the Next Evolution of the Internet Is Changing Everything. Retrieved 8 May 2016, from http://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoT_IBSG_0411FINAL.pdf.
5. Juniper Research. (2015, July 28). 'Internet of Things' connected devices to almost triple to over 38 billion units by 2020 [Press release]. Retrieved 7 May 2016, from http://www.juniperresearch.com/press/press-releases/iot-connected-devices-to-triple-to-38-bn-by-2020.
6. Wikipedia. (2016). Long Range Wi Fi. Retrieved June 1, from https://en.wikipedia.org/wiki/Long-range_Wi-Fi
7. LoRa Alliance. (2016). LoRa Technology. Retrieved 7 May 2016, from https://www.lora-alliance.org/What-Is-LoRa/Technology.
8. SIGFOX (2016). About SIGFOX. Retrieved 8 May 2016, from http://makers.sigfox.com/.
9. Wireless Mag. (2015, December 2). In search of the low-power wide area network standard for IoT. Retrieved 1 June 2016, from http://www.wireless-mag.com/Features/38228/in-search-of-the-low-power-wide-area-network-standard-for-iot.aspx.
10. Radio-Electronics (2016). SigFox for M2M & IoT. Retrieved 1 June 2016, from http://www.radio-electronics.com/info/wireless/sigfox/basics-tutorial.php.
11. GSMA (2015, February 20). The global MVNO footprint: a changing environment. Retrieved 9 May 2016, from https://www.gsmaintelligence.com/research/2015/02/the-global-mvno-footprint-a-changing-environment/490/.
12. AT&T. (2016). Frequently Asked Questions Regarding 2G Sunset.Retrieved 7 May 2016, from https://www.business.att.com/content/other/2G-Sunset-FAQ_2016.pdf.
13. Wright, M. (2014, May). It's time to say goodbye old friend [Blog Post]. Retrieved 7 May 2016, from http://exchange.telstra.com.au/2014/07/23/its-time-to-say-goodbye-old-friend/.
14. 4G.co,uk (2016, March 30). How fast is 4G? 4G speeds and UK network performance. Retrieved 1 June 2016, from http://www.4g.co.uk/how-fast-is-4g/.
15. El Hattachi, R.; Eranian, J. (2015). Next Generation Mobile Networks Alliance: NGMA 5G white paper. Retrieved 7 May 2016 from, https://www.ngmn.org/uploads/media/NGMN_5G_White_Paper_V1_0.pdf.
16. EMnify (2016, January 29). eUICC: What it is and why it matters [Blog Post]. Retrieved 7 May 2016, from https://www.emnify.com/2016/01/29/euicc-what-it-is-and-why-it-matters/.
17. Suzuki, L., & Azuma, T. (2014). Standardization of Embedded UICC Remote Provisioning. NTT DOCOMO Technical Journal, 16(2), 36-41. Retrieved May 17, 2016, from https://www.nttdocomo.co.jp/english/binary/pdf/corporate/technology/rd/technical_journal/bn/vol16_2/vol16_2_005en.pdf#page=1.

For any inquiries, please contact us:

EMnify enables connectivity for the IoT
Ernst-Reuter-Platz 8
10587 Berlin
Germany
+49-931-4973-9270
info@emnify.com
www.emnify.com