Capgemini engineering

HOW ZERO TOUCH WILL TRANSFORM IOT DEVICE DEPLOYMENT

e-SIM and i-SIM technology accelerates zero-touch IoT installation, lowering cost and labor

Table of contents

03... Executive summary

06... The need for zero touch in IoT ecosystems

08... Making the shift to zero touch

14... Transitioning to zero touch

22... Three zero-touch use cases

29... Manual versus automated cost based on zero touch

32... Challenges and drawbacks

33... Solid growth ahead for IoT devices, e-SIMs, and i-SIMs

34... Conclusion

36... References

Executive summary

The slow deployment of Internet of Things (IoT) devices has resulted in a loss of revenue for mobile network operators (MNOs), communications service providers (CSPs), cloud platform providers, OEMs, and ODMs. One reason is unpredictable sales. In addition, the installation and configuration of each IoT device and actuator is a painfully long experience that requires significant effort and technical knowledge by field specialists. (See Figure 1.)

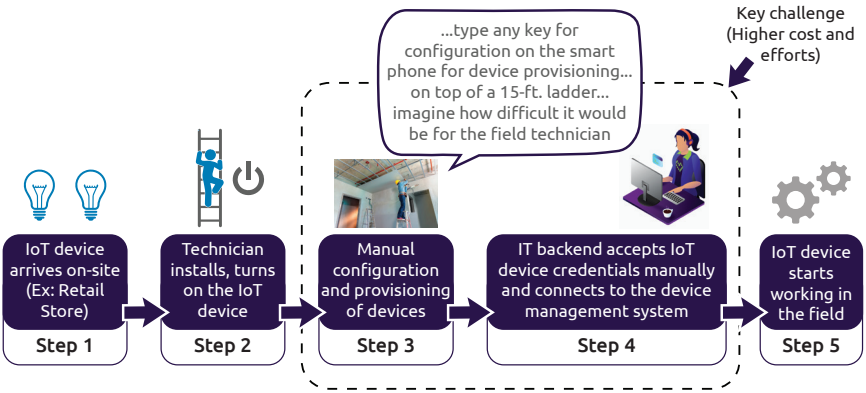


Figure 1: The IoT device manual provisioning process

Source: Capgemini Engineering

The expectation for deploying IoT devices on a large scale in a smart airport, smart retail store, smart factory, or smart city requires simplifying the onboarding processes by reducing the number of manual steps necessary to make the devices operational. The goal for managing the overall IoT device life cycle is to set up each IoT device (short-range and long-range) to communicate with its intended destination.

There are approximately 20 billion connected IoT devices in the global market today. By 2025, the IoT market is expected to expand to $1 trillion, with more than 25 billion IoT connections, according to the GSMA.[1] As OEMs manufacture more IoT devices, they need to be installed manually and configured to connect seamlessly with the IoT network. However, the manual provisioning of IoT devices today requires scheduling an appointment at the

1 "New GSMA Study: Operators Must Look Beyond Connectivity to Increase Share of $1.1 Trillion IoT Revenue Opportunity," May 30, 2018, GSMA https://www.gsma.com/newsroom/press-release/new-gsma-study-operators-must-look-beyond-connectivity-to-increase-share/

customer location for a field technician to manually set up the IoT devices. In addition, the field technician must test the functionality of each IoT device, which leads to higher labor costs and the potential for human error.

To address and overcome device installation and commissioning challenges, major players – including system-on-chip (SoC) and subscriber identity module (SIM) manufacturers, device manufacturers, MNOs, cloud platform providers, and machine-to-machine (M2M) and IoT service providers – have proposed a methodology called "Zero Touch" for deploying IoT devices in various market segments. (See Figure 2.) Zero Touch helps reduce human errors and delays during the deployment of IoT devices. It also reduces travel costs, manpower requirements and allows field technicians to focus on other operational tasks like preventive and reactive maintenance work.

The Zero-Touch feature is attractive because the IoT devices are automatically installed without needing a specialized IoT technician to be available in the field. Therefore, Zero Touch can streamline the installation and commissioning process of IoT devices. For example, when a new IoT device is installed, such as a thermostat, the user switches it on and connects to the cloud platform. The device network automatically verifies the service that has been pre-loaded in the IoT device during the manufacturing stage. After verification of the service and required authorization, the cloud platform starts measuring the data flow based on the usage of the IoT device, and the service enabled in the IoT device gets integrated into the billing system of the service provider's network. The user pays a monthly or annual cost based on the service and usage.

Zero Touch saves time, effort, and cost, making it a highly desirable solution that brings enormous benefits to industries that depend on IoT, including the oil and gas sector, smart buildings, smart factories, smart airports, and smart cities.

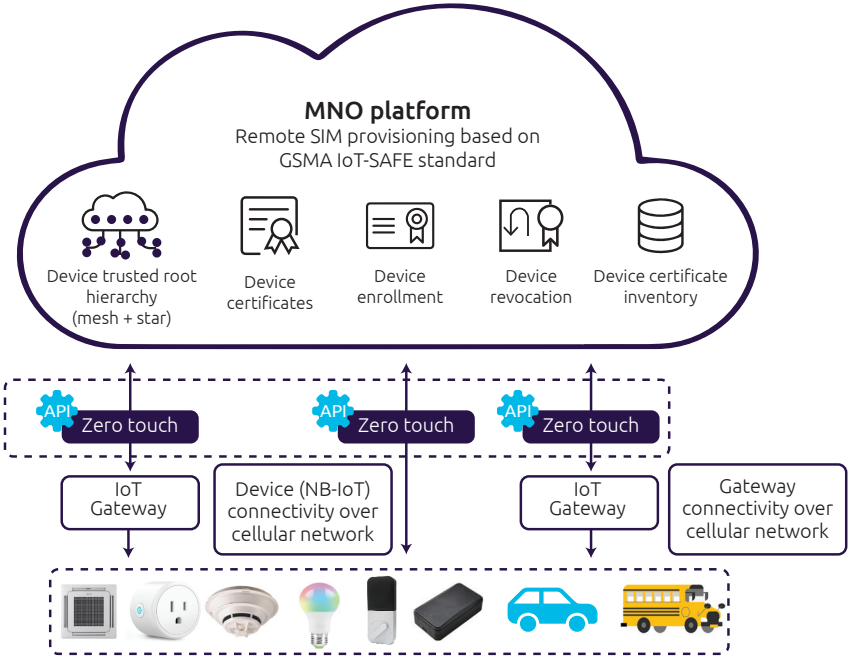


Figure 2: The Zero-Touch concept

Source: Capgemini Engineering

Zero Touch helps automate and enhance certain aspects of the IoT network. This, in turn, helps major industries begin the slow and steady transition to automated systems, which will be required, given the rapid growth forecasted for the IoT market over the next few years.

This white paper provides insight into Zero-Touch provisioning and an overview of the challenges many industries face for device provisioning in IoT networks, focusing on SIM-based IoT devices. The trends around embedded-SIM (e-SIM) IoT device provisioning are based on the evolving GSMA IoT-SAFE standard that addresses the provisioning and deployment challenges and the cost benefits and savings from enabling the Zero-Touch feature in the IoT network system.[2]

2 White paper, "IoT SAFE: Robust IoT security at scale," Jun 2021,GSMA https://www.gsma.com/iot/iot-safe/

The need for zero touch in IoT ecosystems

Manual onboarding of a large number of IoT devices is a significant challenge for IoT service providers and device manufacturers across various industries. Five primary device onboarding challenges are captured in Figure 3 and are detailed below.

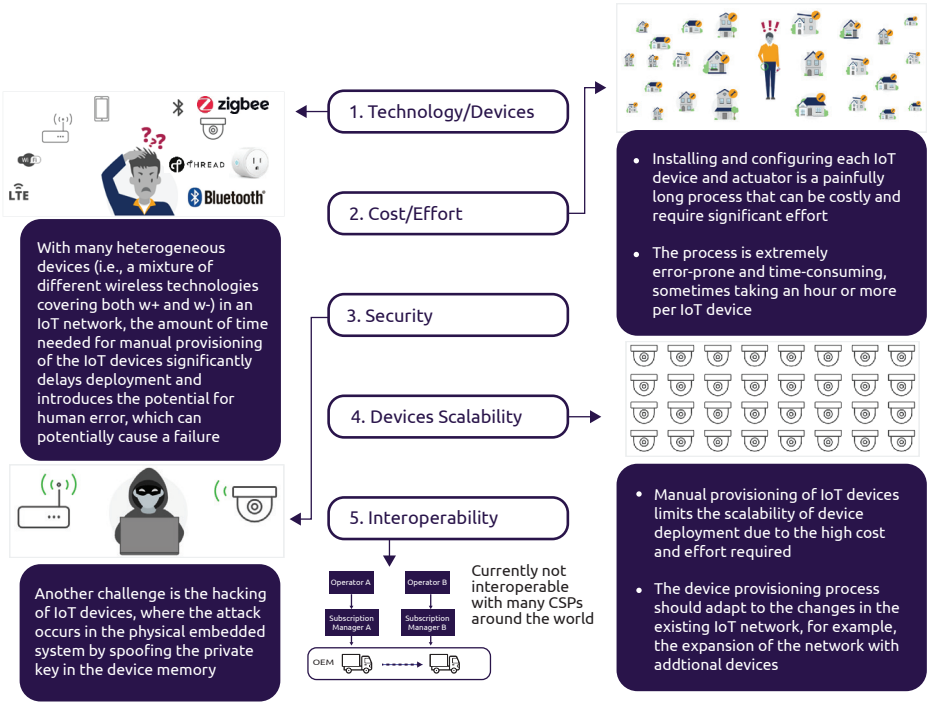


Figure 3: The five critical challenges of device provisioning

Source: AnyConnect

The **first challenge** is the broad technology landscape in the IoT ecosystem for device positioning, which covers short- and long-range technologies like NB-IoT, LTE-M, LoRa, Zigbee, Z-wave, Thread, Bluetooth Low Energy, and Wi-Fi. As a result, deploying IoT devices in a large-scale environment that includes these different technologies is becoming a significant challenge. (See Figure 4.)

The **second challenge** is the cost of people and travel and the effort required to configure each IoT device based on the functionalities of the sensors and actuators. For example, it can take an hour per IoT device to provision the devices in the field. In addition, manual installation is extremely error-prone, where 80 to 90 percent of the downtime is attributed to human error.

The **third challenge** is security and the hacking of IoT devices during the device provisioning process. The attack typically happens in the embedded system of IoT devices by hackers spoofing the private key located in the device memory. Consequently, many industries have moved to hardware-based security to protect from unauthorized firmware updates, strengthen device identity protection, and prevent identity spoofing. However, at the same time, hackers are probing weaknesses in the IoT embedded system design to exploit many connected devices in the larger IoT network.

The **fourth challenge** is scalability, where manual provisioning of IoT devices limits the scalability of IoT-device deployment due to the high cost and effort, which, in turn, affects business opportunities. Nevertheless, as market forecasts suggest, there will be an increase in demand for IoT devices in the coming years.

The **fifth challenge** is interoperability, where many cellular-based IoT devices (SIM-based) are not interoperable with the existing networks deployed by MNOs across the globe.

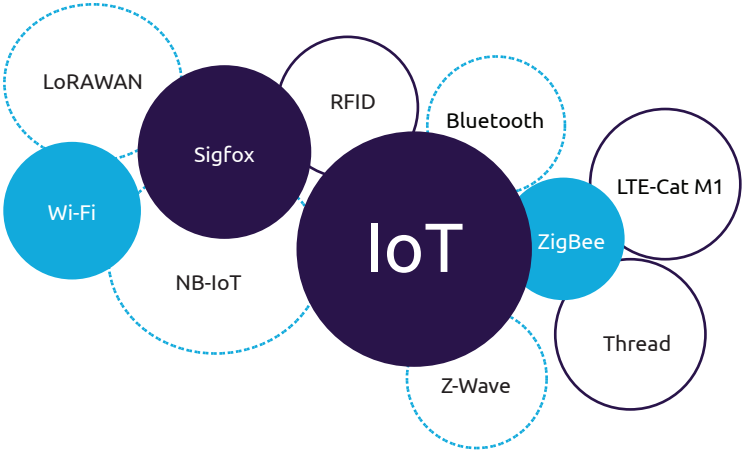


Figure 4: The complex technology landscape of device provisioning
Source: IEEE

Making the shift to zero touch

The Zero-Touch methodology is currently used in the IoT industry to address many device provisioning challenges. The process is typically applied in the second level (provision) and third level (configure) of IoT device life-cycle management. (See Figure 5.) The main goal is to eliminate the manual provisioning process in a more extensive IoT network deployment by configuring the IoT devices automatically.

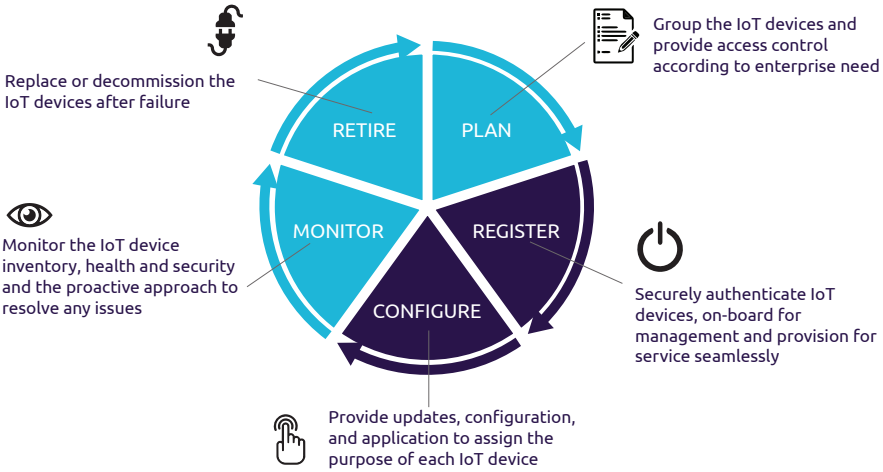


Figure 5: IoT device life-cycle management

Source: Capgemini Engineering

Many companies expect Zero Touch will generate new business opportunities and revenue. They consider Zero Touch an IoT end-to-end automation system, where the device installer in the field does not need to be highly technical but can connect the IoT device or gateway to the network. This shift will substantially reduce manual errors and installation time. It also avoids the manual provisioning process and enables remote device provisioning. In addition, Zero-Touch technology will allow network administrators to connect and control millions of IoT devices with little effort and human intervention.

The industry landscape

Today, SIM technology in many IoT devices deployed in the field ties each SIM card to a single cellular network operator. The only way for end-users to change cellular network operators (e.g., from AT&T to Verizon) is to swap out their plastic SIM cards. (See Figure 6.) So, the current challenge is that each IoT device is tied to a SIM card connected to a single cellular network operator. Changing the subscription requires swapping the SIM card for each IoT device.

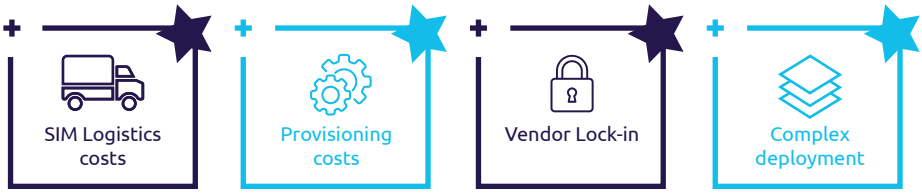


Figure 6: Traditional challenges identified in device deployment

Source: Capgemini Engineering

For nearly 30 years, plastic SIM cards have played a significant role in mobile communications, where it is easy for end-users to change the SIM card in a mobile phone or for any 3G/4G-based USB dongle. However, it is more challenging for small-form-factor IoT devices widely deployed in applications like asset tracking and fleet management. These IoT devices are used in thousands of fleets in different geographical locations. Also, the growing number of SIM-enabled IoT devices is a severe problem for both maintenance and management, as it is not feasible to change the SIM cards in millions of existing IoT devices if the cellular network connectivity needs to be changed. Also, plastic-based SIM cards cannot function in harsh environments like industrial automation plants with extremely high and low temperatures and vibration. Also, generating the relevant certificates and distributing them to IoT devices in the field is a time-consuming, expensive, and inefficient exercise.

Therefore, the new IoT devices manufactured today need to accept the credentials issued by cellular network operators to scale and secure IoT devices successfully. This is an entirely different operational and business model that needs to be worked out for IoT devices to have flexibility connecting with different cellular network operators, such as AT&T, Verizon, Sprint, Airtel, Vodafone, and others, more seamlessly. Also, network operators need to establish trust with cloud platform providers to develop easier, more scalable ways to manage the provisioning of larger IoT devices.

Trend 1: e-SIM

Standard SIM cards are now transforming into e-SIM cards in the IoT device market to address SIM-based IoT device provisioning challenges. The reason is that the traditional SIM card is not suitable for measuring IoT data parameters in complex environments, such as vibration, temperature, and humidity, typically in large industrial plants. Therefore, the GSMA IoT-SAFE standard defines embed SIM technology to address the challenges, where e-SIM creates opportunities for the IoT device manufacturers to create various IoT applications to work in harsh environments where the life cycle of an e-SIM is ten to fifteen years.

e-SIM cards are a reliable and scalable solution compared to plastic SIM cards, especially for the IoT market. The e-SIM evolution is based on the open, vendor-neutral standard developed by the GSMA IoT-SAFE standard. This new standard allows each IoT device to have a fixed e-SIM hardware-secure element inside the IoT device when manufactured instead of inserting the CSP's discrete plastic SIM cards for connectivity to the cellular network.

The GSMA IoT-SAFE standard proposes that the e-SIM be used as a crypto-safe platform, i.e., a trusted execution environment (TEE), to establish an end-to-end encrypted connection. (See Figure 7.) Most IoT devices will become cellular-enabled in the coming years, which covers emerging 5G technology. e-SIM will remove the barrier for cellular-based IoT device deployment, especially for fleet management, asset tracking, conditional-based monitoring, smart metering, smart parking, smart lighting, video surveillance, and many other applications.

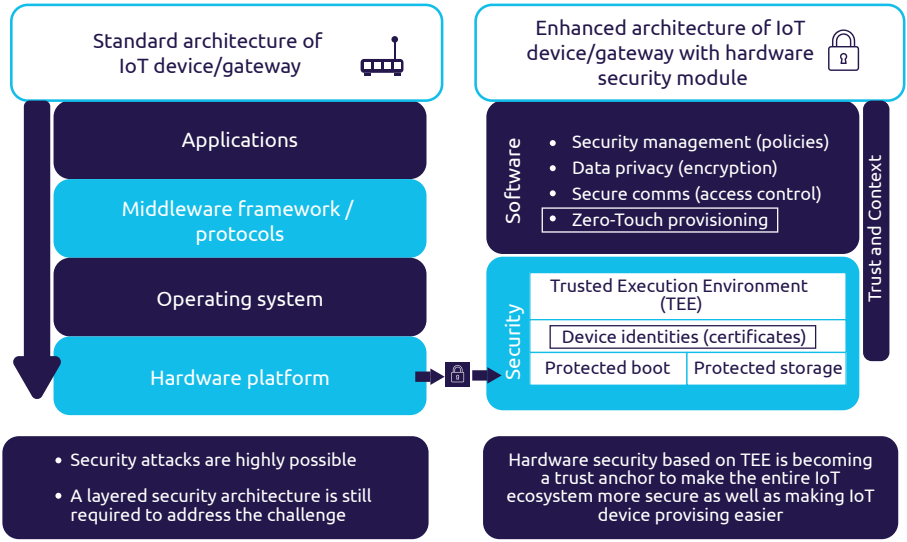


Figure 7: Approach towards e-SIM with Trusted Execution Environment (TEE)

Source: Capgemini Engineering

Trend 2: i-SIM

Over the last few years, integrated SIM (i-SIM) has been gaining ground based on the similar functionality of the e-SIM. While the e-SIM is a dedicated chip soldered to an embedded platform and connected to an IoT device's processor, the i-SIM is integrated into the processor core, and the data is encrypted within the SoC. This is important for many critical IoT use cases, as it is low-cost, low-power, and secure in a small form factor. Furthermore, the i-SIM functionality is built directly into the base processor, eliminating the need for SIM slots, SIM cards, and the external e-SIM hardware interface. The growth of e-SIM and i-SIM is driving seamless connectivity over cellular-based IoT networks as

large numbers of IoT devices will be deployed in the coming years, including 5G-based IoT devices.

The e-SIM-based approach has numerous compelling IoT use cases, such as smart manufacturing, where IoT device manufacturers can buy large batches of e-SIMs with predefined bootstrap profiles and embed them in their IoT devices. In addition, MNOs, such as AT&T, Verizon, and Sprint, will be chosen based on where the IoT devices are being deployed, allowing the IoT device manufacturer to avoid selecting specific operators that need to ship to multiple regions. (See Figure 8.)

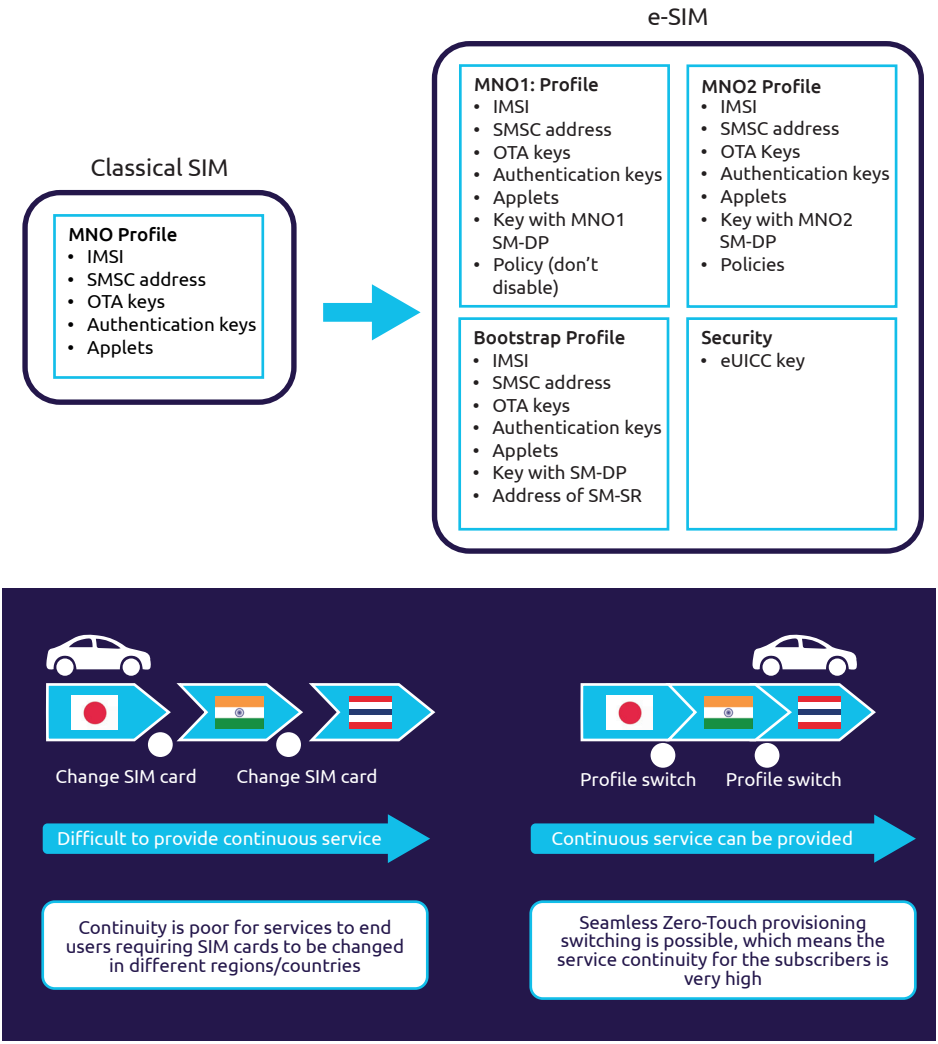


Figure 8: Seamless provisioning of IoT devices

Source: IEEE and Capgemini Engineering

For example, when the end-user buys a service bundle from an MNO for a specific IoT device, such as a smart bulb, the MNO profile is loaded in the e-SIM of the IoT device and stored in the secure storage memory on the e-SIM chip. At some point, if the end-user buys a service package from another MNO, the new service package also gets stored in the e-SIM module of the IoT device. Now, both profiles are stored, and the end-user can swap or switch between the two MNOs based on the need and service bundle offered. As a result, the selection mechanism of the MNO effectively eliminates using a physical plastic SIM card with the e-SIM chip, where multiple MNO profiles can be stored, remotely updated, added, and deleted based on the standard defined by GSMA IoT SAFE.

With e-SIM and i-SIM-based provisioning adhering to the GSMA IoT-SAFE standard enablement in the IoT ecosystem, greater value-add can be delivered to end customers globally utilizing Zero-Touch connectivity. This advancement is a game-changer for accelerating the growth of the IoT market by unlocking the critical business benefits for the industrial market segments. It means that Zero-Touch connectivity reduces the need for end-users to contact the IoT device provider or MNO, which is a critical factor of Zero Touch that will spur widespread adoption of IoT.

Zero Touch delivers a pre-installed firmware in the e-SIM, which intelligently manages security, connectivity, and certificate credentials between the IoT device and the cloud via the MNO, ensuring a consistent global out-of-the-box experience. Based on the GSMA IoT-SAFE standard, Zero Touch can take advantage of better utilization of the e-SIM module. It creates the possibility of adding an identity to an IoT device when required, with automatic setup provisioned by the MNO, and enables global, secure connectivity via IoT cloud platform providers.

The GSMA IoT-SAFE standard enables cellular service providers and IoT device manufacturers to allow e-SIM and i-SIM to remotely install and manage the IoT devices' connectivity profiles and subscriber identities in the field. It also makes the SIM a robust, scalable, and standardized hardware root of trust to protect IoT data communications over cellular networks. The developers can implement IoT SAFE in i-SIM, which takes the existing remote programming and bootstrapping features of i-SIM to an entirely new level on the IoT device. Zero Touch can better utilize the e-SIM module by creating the possibility of adding an identity to an IoT device when required, with automatic setup of the working environment.

The Zero-Touch service in e-SIM includes the following features:

- When the e-SIM is active, the Zero-Touch service is enabled in the IoT device and communicates to the IoT cloud platform without any limitation
- If the IoT data traffic needs to be blocked temporarily to and from the IoT device, Zero Touch can make the e-SIM switch to a suspended state
- If the e-SIM must be retired, Zero Touch can be switched to the cancel state
- Zero Touch can provide the status of the IoT devices that are currently active or inactive to the IoT cloud platform
- Zero Touch can share the health status of the IoT device with the service provider

In summary, the SIM applet that runs on e-SIM based on the GSMA IoT-SAFE standard enables secure end-to-end communications that allow IoT device manufacturers and service providers to leverage e-SIM and i-SIM as reliable, scalable, and normalized hardware that protects data communications of IoT devices over cellular networks.

The applet that runs on e-SIM and i-SIM offers many advantages:

- Helps to solve challenges for provisioning millions of IoT devices
- Manufacturers of IoT devices can access SIM-based security services as a hardware root of trust based on standardized APIs
- Offers a simpler way for developers and cloud providers to create applications that further removes device fragmentation issues
- Provides significant savings due to Zero-Touch provisioning
- Reduces the risks of an attack on the device
- Makes the management of IoT devices simple and secure at every stage of the life cycle
- Uses e-SIM /i-SIM as a mini "crypto-safe" within the IoT device to securely establish a Datagram Transport Layer Security (DTLS) session with the corresponding IoT cloud platform over a 3G or 4G network
- Securely performs mutual DTLS authentication on a cloud platform using either asymmetric or symmetric security schemes
- Computes shared secrets and stores long-term key secrets

Transitioning to zero touch

Today each network operator and service provider has a unique technical approach, based on their proprietary deployment methodology, to handle the personalization of their SIMs in the IoT cloud platform. Therefore, significant difficulties arise when the end-user wants to connect the IoT device with two different cellular networks, where the software needs to be provisioned remotely in the SIM to connect with these two cellular networks. To address these challenges, a standardized subscription management (SM) architecture, defined by GSMA IoT SAFE, is recommended to reduce the cost and complexity of the SIM-based IoT devices deployment.

The GSMA IoT-SAFE standard is based on a single common and global specification defined by GSMA that adheres to technical specifications SGP.01, SGP.02, and SGP.11. This adherence ensures the cellular-based IoT device market will grow. The GSMA IoT-SAFE standard specifies the remote SIM provisioning (RSP) concept to address the secure management of storing network operator profiles in the secure element embedded in the IoT device using over-the-air (OTA) commands. The GSMA-based subscription management platform consists of two components:

- Subscription Management - Data Preparation (SM-DP)
- Subscription Management - Secure Routing (SM-SR)

The main goal of these two components (SM-DP and SM-SR) is to create a Zero-Touch provisioning feature for the SIM-supported IoT devices and other aspects by enabling user-end data security, where attackers cannot access endpoint authentication information.

The SM-DP is connected securely to the SM-SR and is responsible for preparing and saving MNO profiles in an e-SIM compatible format. Based on the command received from the MNO backend, the SM-DP encrypts and pushes the MNO profile to the e-SIM on the IoT device. (See Figure 9.) The SM-DP is primarily responsible for the secure storage of e-SIM profiles on the IoT devices, the subscriptions and personalization along with required subscription data, and the preparation for secure over-the-air (OTA) download and software installation onto the e-SIM in the IoT device.

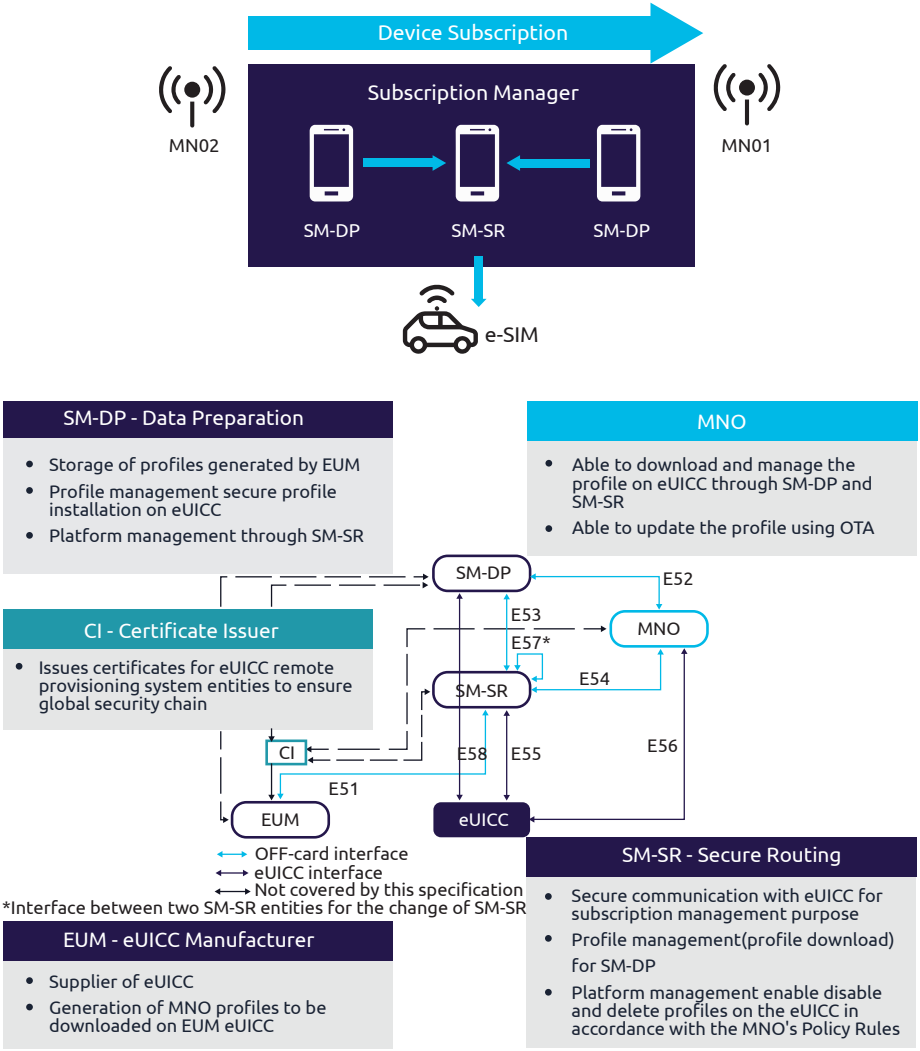


Figure 9: Remote provisioning components

Source: GSMA IoT SAFE

The SM-SR is often deployed by the owner of the e-SIM, such as an MNO or IoT device manufacturer. The e-SIM owner will often deploy the SM-DP, and the MNO that wants to manage the e-SIM profiles may also deploy an SM-DP connected to an SM-SR.

The SM-SR is responsible for establishing a secure channel for each individual e-SIM registered to the SM-SR. It performs remote management operations (e.g., download/install, enable, disable, delete, and other functions) directly to the e-SIM profiles. The SM-SR entity securely

delivers the encrypted MNO credentials to the e-SIM and installs the same within the e-SIM OTA. When the credentials are installed, it remotely manages the e-SIM, thereby enabling, disabling, and deleting the credentials as and when necessary during the IoT product life cycle. The e-SIM vendor registers with the SM-SR (e.g., the certificate and identity). The SM-SR is the only unit capable of contacting the e-SIM to manage subscriptions directly and maintain a secure connection to the e-SIM. The SM-SR can apply the profile policies (e.g., profile disablement) and route commands from the MNO and SM-DP to the e-SIM. If the customer decides to use a different MNO or profile, the e-SIM will reconnect to the SM-SR platform and download a new profile. The sequence of operation for loading the profiles is described in Figure 10.

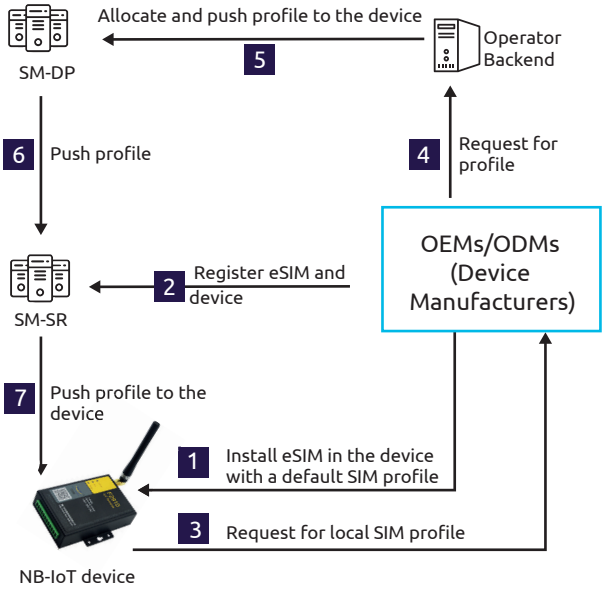


Figure 10: Profile loading sequence of operation into e-SIM-based IoT device

Source: IEEE

Also, various interfaces are defined by the GSMA IoT-SAFE standard for different interconnecting parties that include OEMs, MNOs, and SIM manufacturers.

- ES1 - the interface between the two entities fulfilling the role of the embedded universal integrated circuit card (eUICC) manufacturer and SM-SR
- ES2 - the interface between the two entities fulfilling the roles of MNO and SM-DP
- ES3 - the interface between the two entities fulfilling the roles of SM-DP and SM-SR
- ES4 - the interface between the two entities fulfilling the roles of MNO and SM-SR

- ES5 - the interface between the SM-SR and e-SIM
- ES6 - the interface between the MNO and e-SIM vendor
- ES7 - the interface between the two entities fulfilling the roles of SM-SR and SM-SR
- ES8 - the interface between SM-DP and e-SIM

There are two variants proposed by the GSMA IoT-SAFE standard: the M2M variant and the consumer variant.

- The M2M variant targets Industrial IoT (IIOT) devices that include asset tracking and electric meters, which are typically used in an industrial, non-end-user interactive environment
- The consumer variant targets consumer devices, such as mobile phones, tablets, laptops, and other flavors of consumer IoT devices such as wearables

The M2M variant that covers asset tracking and electric meters operates on the push model, which depends on the backend infrastructure of the SM-DP/SM-SR server components deployed in the MNO infrastructure to execute e-SIM profiles related to management operations.

How Remote SIM Provisioning Works

During the manufacturing and deployment process, the e-SIM manufacturer, MNO, or IoT device manufacturer registers the SIMs with the SM-SR and maintains a secure connection with the e-SIM to manage subscriptions. The SM-DP will encrypt and download the new MNO profile to the e-SIM after receiving commands from the MNO. Furthermore, the SM-DP will provide interfaces that let the MNO enable or disable a profile on the e-SIM. The advantage of using e-SIM instead of plastic SIM cards is that the e-SIM offers flexibility for building relationships between end-users, MNOs, and the e-SIM provider by offering over-the-air updates to load MNO profiles on e-SIMs instead of replacing the plastic SIM cards. In addition, since the e-SIM is manufactured with a bootstrap profile, it makes the IoT device connection with RSP much easier.

The GSMA IoT-SAFE standard addresses other areas, including chip-to-cloud security that makes IoT device communications more secure. With IoT SAFE, the IoT devices can securely establish TLS or DTLS authentication sessions with a corresponding IoT-based cloud platform provider through the MNO. IoT SAFE creates a reliable and normalized mutual authentication mechanism between IoT devices and cloud platforms and handles data encryption and integrity. This makes large-scale device deployments secure and straightforward at a global level with Zero-Touch provisioning. The Zero-Touch model handles the security logic for e-SIM and i-SIM, focusing on secure management, troubleshooting, provisioning, and de-provisioning of the IoT devices more simply. Based on the Zero-Touch Java API running on the e-SIM, the IoT-SAFE software can be connected either to the MNO or the cloud platform for validating the authentication mechanism at the application level that creates a secure channel of communication between the IoT device and network. (See Figure 11.)

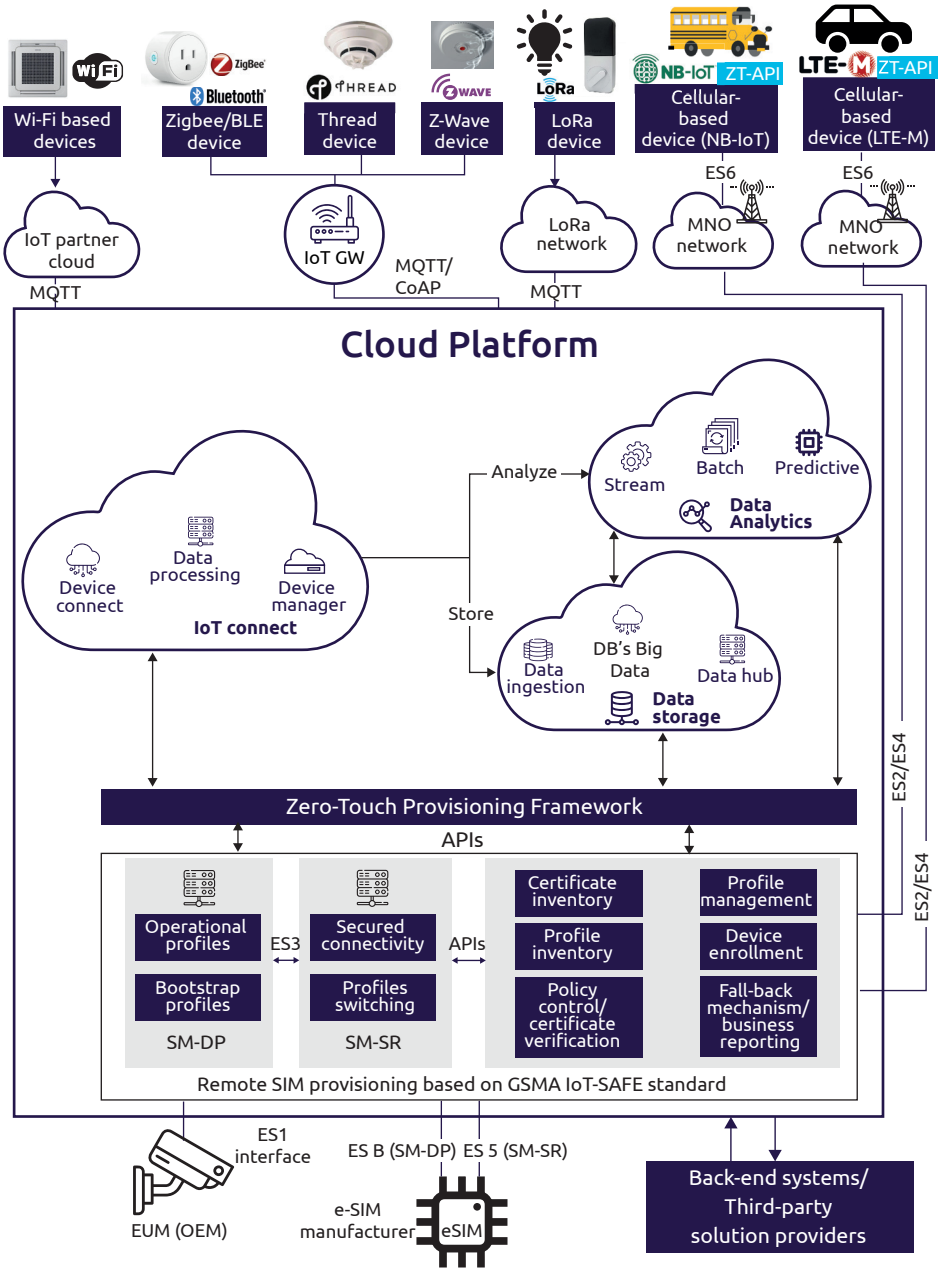


Figure 11: Remote SIM provisioning and its interface with the cloud platform provider

Source: Capgemini Engineering

GSMA IoT SAFE utilizes e-SIM as a root of trust for IoT security. The Zero-Touch API (ZT API) running on the e-SIM provides cryptographic support and storage of credentials for establishing secure communication examples by using DTLS for data transmission and reception. By chipset vendors enabling root-of-trust support on the hardware platform, GSMA IoT SAFE promotes interoperability across IoT device manufacturers and service providers, which is a more reliable way from a deployment standpoint for the IoT devices to work with any MNO network. In addition, the devices based on Zero Touch can instantly access connectivity, which simplifies the initial provisioning, and protects ongoing daily operations with a robust security mechanism.

Device security based on the IoT cloud platform

The direct connectivity between the IoT device and the cloud platform is one approach for verifying and validating end-to-end security. Authentication and authorization happen between the IoT device and the IoT cloud platform without depending on the MNO's security network components. The IoT security service resides in the IoT cloud platform. (See Figure 12.)

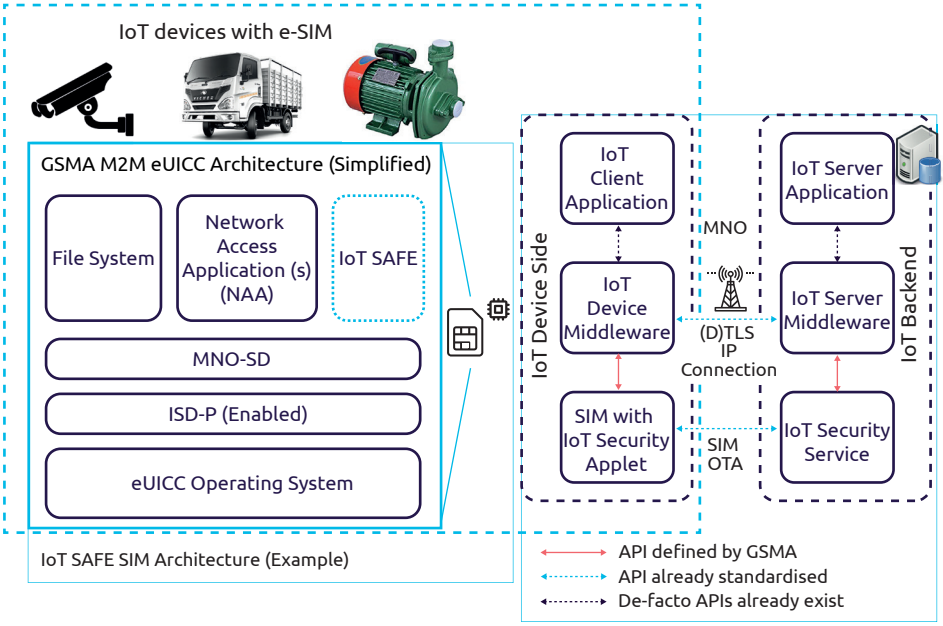


Figure 12: Security mechanism based on the IoT cloud platform

Source: GSMA IoT SAFE

This approach enables higher levels of security, including identity verification and encryption. It provides a way to talk to the e-SIM card and provide support to add more features independently from the standard MNO offerings.

The e-SIM profile loading can be done either at the time of manufacturing or via the OTA server, where the remote update of Java applets on the e-SIM can be done quickly on the IoT device. The drawback of the cloud-platform-based

approach for handling the security feature is that the IoT cloud platform provider should offer a dedicated security service to manage all the keys, credentials, and device certificates, which would be overhead for the cloud platform provider. In addition, this approach may not be able to leverage existing security functionality from the MNO platform already available in the cellular network infrastructure.

Device security based on the MNO platform

The bootstrapping server function (BSF), a core network element defined in 3GPP TS 33.220, is under the control of the MNO. The BSF connects with the middleware of an IoT device to authenticate each device using the 3GPP AKA protocol. The BSF generates a session key that is deployed between the network application function (NAF) and the IoT client application. The NAF uses a generic bootstrapping architecture (GBA) to create a secure communication tunnel between the NAF and IoT client provided by the MNO. Once the bootstrapping has been completed between the NAF and IoT device client application, the IoT device runs the application-specific protocol, using the session keys generated during the GBA process. The home subscriber service (HSS) is a network element of the MNO, where the HSS stores all the user security settings used in GBA. (See Figures 13a and 13b.)

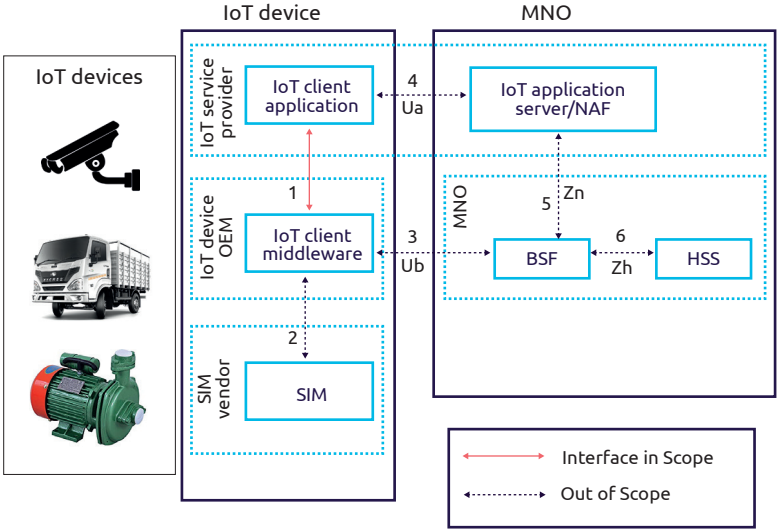


Figure 13a: End-to-end system

Source: GSMA IoT SAFE

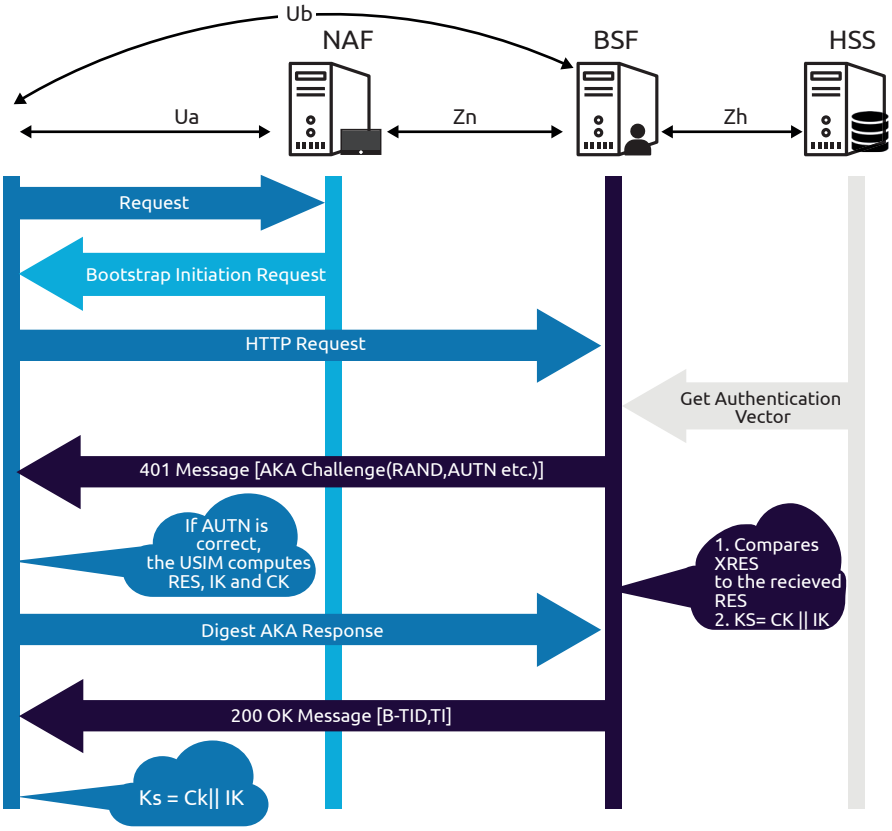


Figure 13b: Call-flow diagram

Source: 3GPP

Since the GBA leverages the existing identity and authentication infrastructure deployed by MNOs based on the 3GPP standard TS 33.220, there are no additional costs involved in obtaining data protection for 3GPP-enabled IoT devices. The GBA approach is low-cost compared to the public key infrastructure since there is no need to securely deploy the keys. The GBA security framework does not require maintenance, as it reuses the credentials in the e-SIM. Authentication is possible if the user has a valid identity on the HSS or the home location register. The authentication method is integrated into both the IoT device and MNO platform, as it is based on HTTP digest access authentication.

The drawback based on the GBA approach is that the implementation depends on MNO components to realize the security procedure for authentication and key exchange. Also, MNOs will require more partnerships for the IoT device to work in different regions to realize remote SIM provisioning.

The three use cases detailed below show how Zero-Touch provisioning works for SIM-based IoT devices such as video surveillance, asset management (e.g., smart metering), and fleet management.

Three zero touch use cases

Use case 1: video surveillance

Video surveillance is the positioning of networked cameras for real-time remote monitoring of activity in many applications, including smart factories, processing plants, smart grids, and other environments. The challenge is to install the network of cameras quickly to minimize the time technicians spend in the field. (See Figure 14a and 14b)

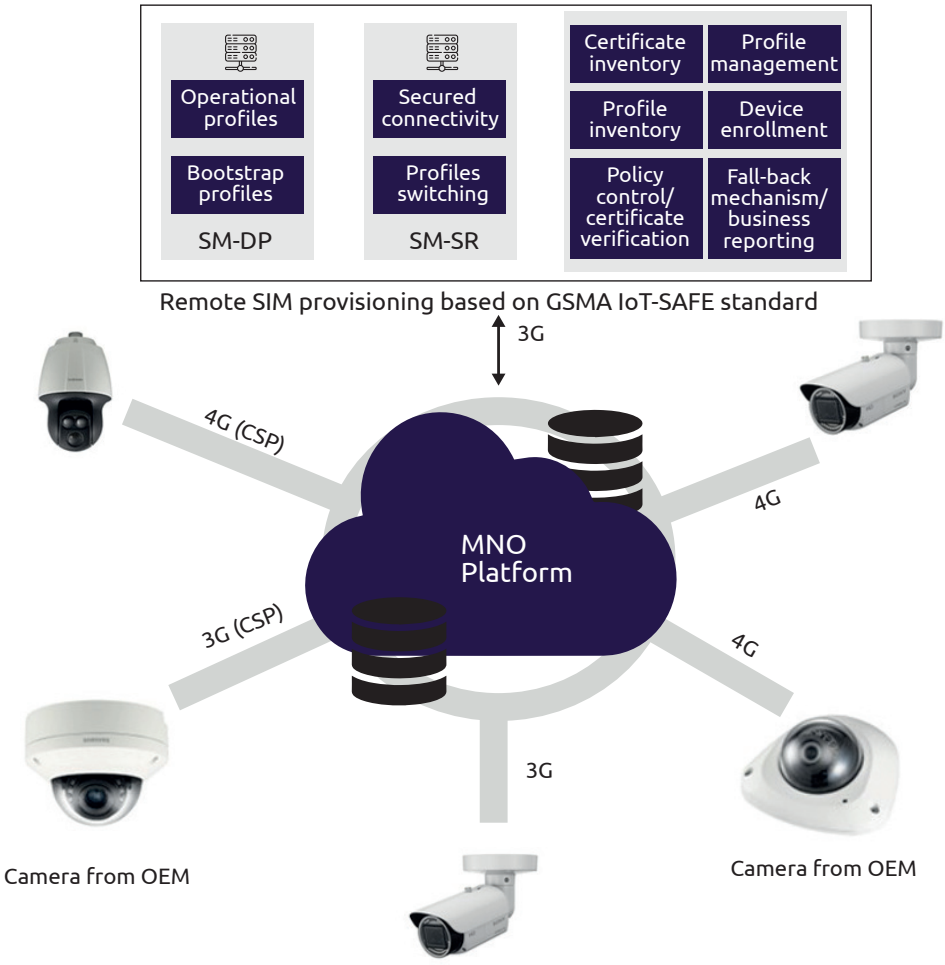


Figure 14a: Surveillance camera connectivity with e-SIM

Source: Capgemini Engineering

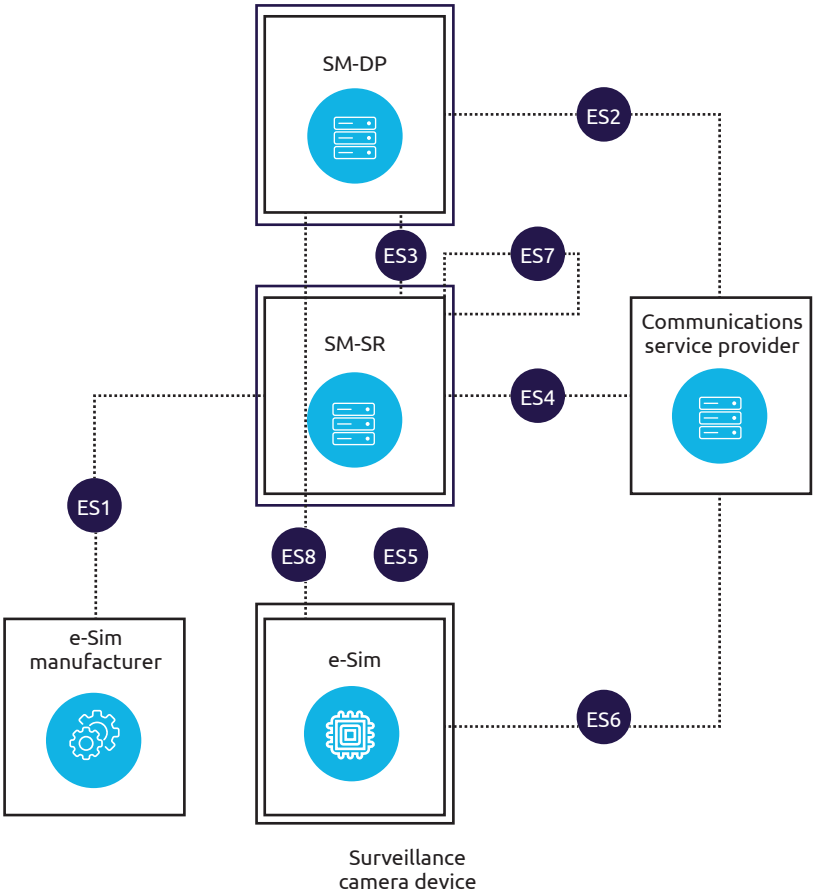


Figure 14b: Camera interface with RSP

Source: GSMA IoT SAFE

Step 1: The MNO procures a batch of customized e-SIMs from a SIM vendor for the MNO at a SIM factory, along with the software installation of the IoT security ZT API on each e-SIM. Also, one or more randomized private keys are installed in the e-SIM as part of the personalization process and never leave the area inside the factory. The certificate corresponds to the private keys that the SIM vendor shares with the MNO. (See Figure 15.)

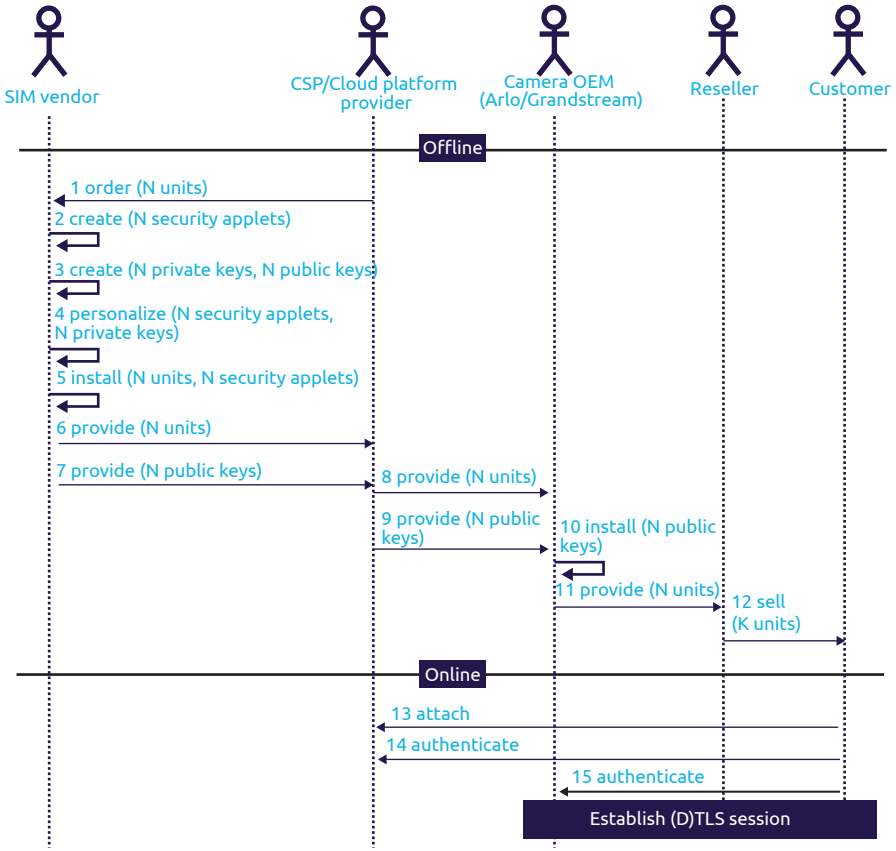


Figure 15: Call flow for enabling surveillance cameras from the OEM, MNO, and SIM vendor

Source: GSMA IoT SAFE

Step 2: The MNO builds a commercial relationship or partnership with an OEM that manufactures cellular-connected video cameras, such as Grandstream or Arlo. The MNO supplies e-SIMs to the camera OEM and creates a copy of the public key for the OEM that is stored in the IoT security ZT API on every e-SIM. The OEM installs the MNO's e-SIMs into its security cameras at the manufacturing center, creates a public key for every camera combination, and ships the cameras to the reseller.

Step 3: A customer buys a camera from the reseller, takes it home and switches it on. The camera connects to the MNO and authenticates the e-SIM within the camera. The camera then connects to the IoT cloud platform and initiates an authentication procedure to establish a secure DTLS connection with the IoT cloud platform via the MNO. Finally, the camera is authorized using the private key created based on the ZT API within the e-SIM. After being authorized, the camera and the IoT cloud platform communicate securely. The end user streams the video fetched

over a 3G or 4G network from the surveillance camera with the secured data pipeline created.

Use case 2: asset management

A smart meter OEM (SM-OEM) purchases e-SIMs from a SIM manufacturing company and solders them into every cellular (NB-IoT) connected smart meter. (See Figure 16.) The SM-OEM sells these smart meters to their customers, who are responsible for deploying them in their respective markets. For example, a third-party energy service provider could connect their smart meters to the MNO's network and host their IoT cloud platform for seamlessly provisioning the smart meters and the services required to fetch data from the smart meter.

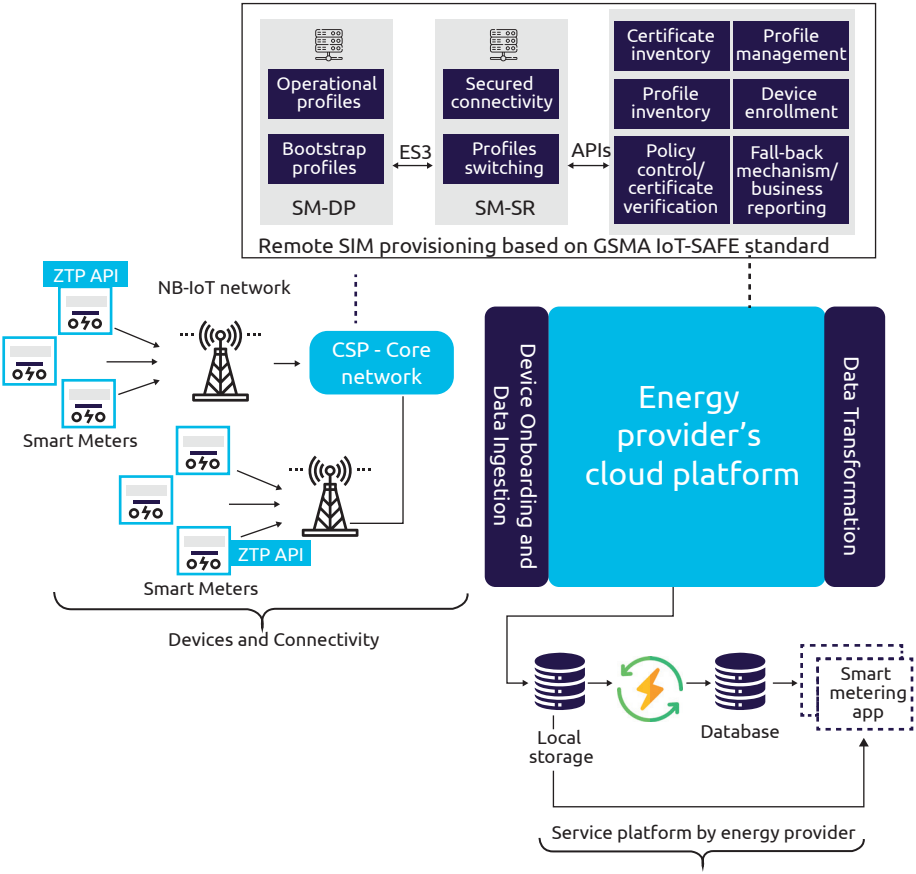


Figure 16: Asset management for a third-party energy provider

Source: Capgemini Engineering

Figure 17 shows the supply chain management of an intelligent metering system. The first time a smart meter is used it is activated and the MNO profile that was pre-loaded during manufacturing is initiated. The smart meter is further authenticated with the MNO based on the Zero-Touch onboarding feature. Zero-Touch enablement of the IoT device mitigates the risk

of security attacks by taking care of privacy with the technician's automatic plug-in of meters in the field. This process dramatically reduces the installation and onboarding time from hours to seconds.

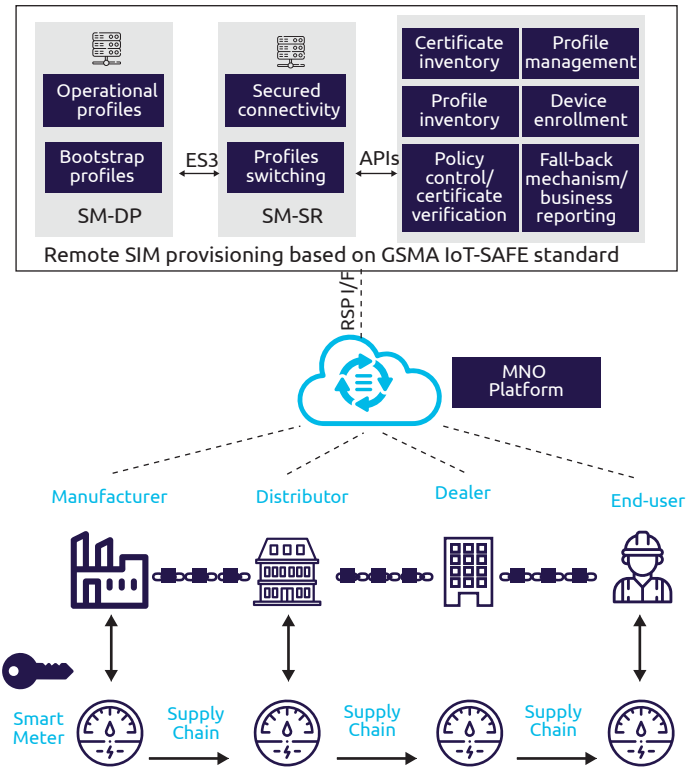


Figure 17: A smart metering system for supply chain management

Source: Capgemini Engineering

For example, when the RSP platform is registered, the MNO requests the IoT security applet in the e-SIM to produce a public/private key pair and then sends the public key to the MNO. Next, the energy provider's cloud platform generates a certificate signing request (CSR) to a certificate authority (CA) server. The MNO presents the CA and signed certificates to the IoT security applet that runs on the smart meter IoT device. Next, the smart meter establishes a secure DLTS connection to the company's cloud platform and sends the meter readings. The MNO or the company can renew or revoke the credentials stored if the smart meter is moved from its location or reaches end-of-life.

Use case 3: fleet management

An MNO provides cellular connectivity to a truck manufacturer's onboard units (OBUs) and creates a secure connection between the OBUs and OEM cloud platforms. (See Figure 18.) The OEM operates a CA server in its cloud platform

to provide certificates to trucks, allowing all the IoT devices to connect the OBUs to the OEM's cloud platform securely.

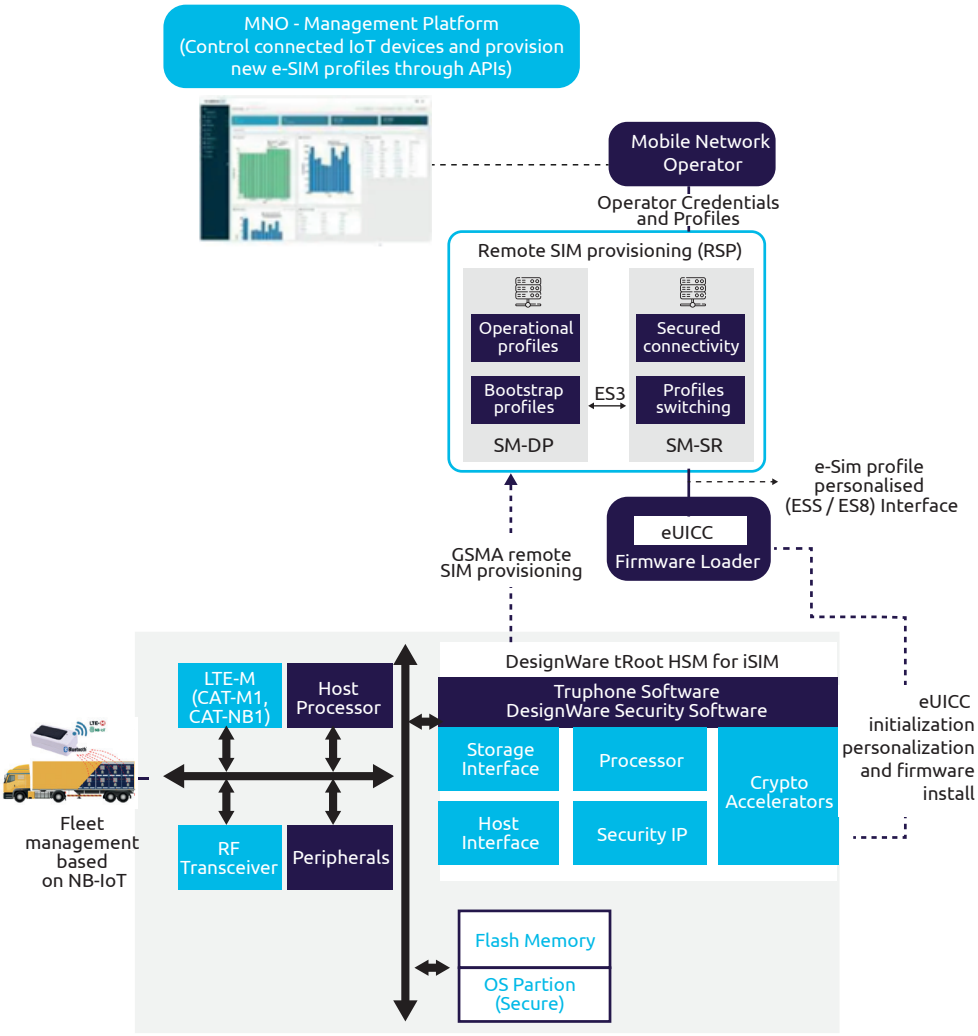
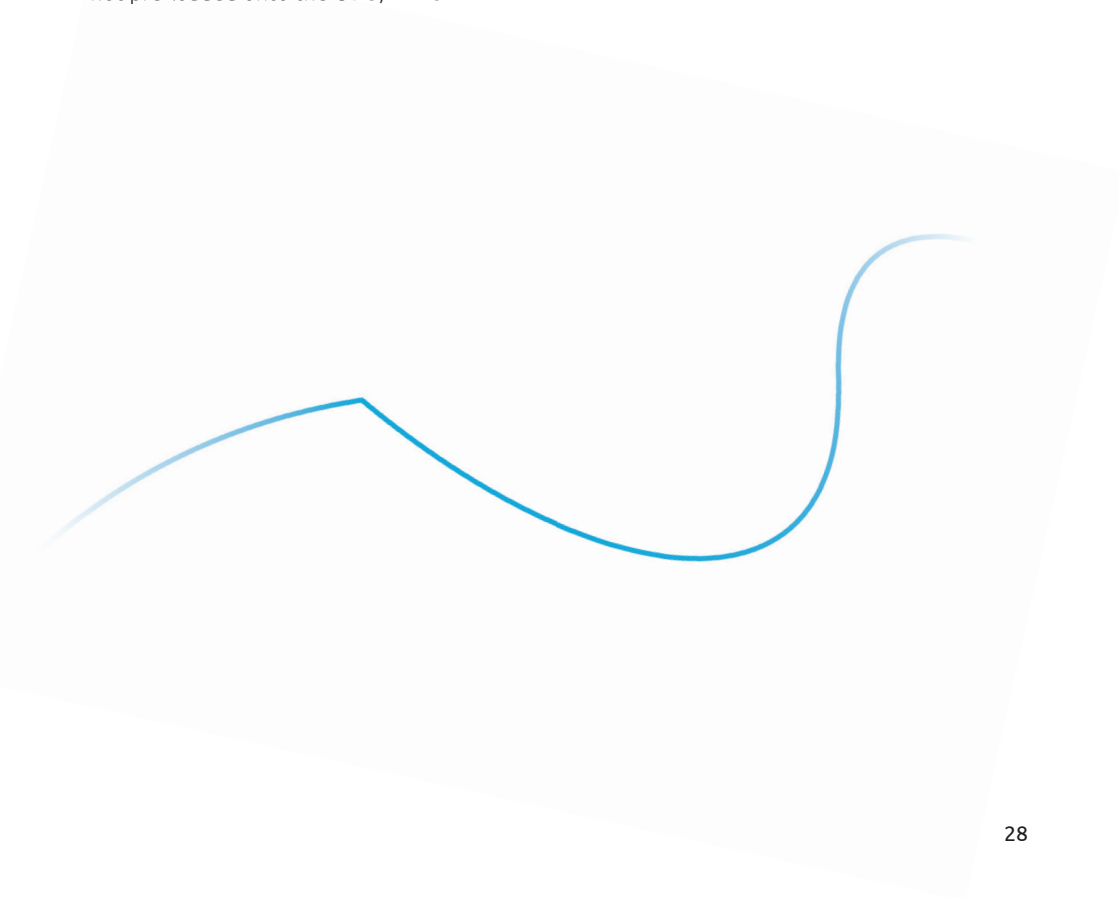


Figure 18: Fleet management
Source: Capgemini Engineering

The Tier-1 OBU supplier provides the OEM with the number of units required, and each OBU is installed on the truck by the OEM. After installation and activation, the OBUs start communicating with the OEM's IoT cloud platform through the cellular networks that monitor the services, such as tracking and monitoring. The MNO delivers configured e-SIMs to the OEM and embeds e-SIM onto the OBU hardware platform in each truck. Before delivering the OBUs to end-users, the OEM binds the truck ID to an OBU device ID and its mobile subscriber identity and configures the OBU with the IP address of the OEM's cloud platform.

When the OBU connects with the MNO, it initiates the certification process with the OEM cloud platform. Since the security credentials are not pre-loaded onto the OBU, the OEM cloud platform requires the OBU to do authentication by triggering a bootstrapping procedure. This process can be initiated based on the lightweight M2M (LWM2M) standard. After authentication, the OEM cloud platform generates a session key and sets up an end-to-end secure tunnel.

The OBU can send the device ID and the certificate public key to the OEM cloud platform when the secured tunnel is created. The OEM cloud platform receives the certificate and signs it accordingly. With the secure tunnel created, the OBU downloads the signed certificate and stores it in a secure location on the e-SIM. Similarly, the OBUs can obtain certificates and credentials from the OEM cloud platform, so there is no need for OBUs to provide or share certificates or keys on the production line.



Manual versus automated cost based on zero touch

Zero Touch for the IoT market is critical for large-scale deployments in terms of cost and time for managing and provisioning IoT devices for killer applications such as fleet management, asset tracking, conditional-based monitoring, and video surveillance, and creating more business opportunities focused on generating additional ROI. (See Figure 19.) Zero Touch saves time and helps onboard hundreds or even millions of IoT devices in the IoT ecosystem with minimal, near-zero effort. As a result, prominent IoT players such as AWS, Infineon, Intel, Microsoft, and NXP have initiated Zero-Touch implementation to help improve device provisioning, security, and adoption for the broader IoT market.

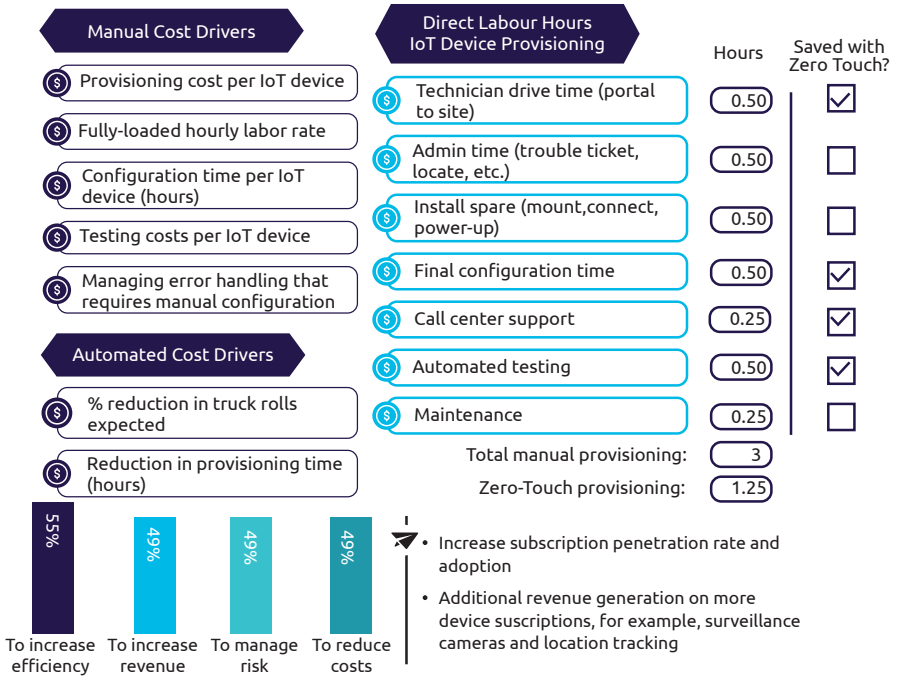


Figure 19: Cost drivers for device provisioning

Source: Capgemini Engineering

The return on investment from adopting Zero-Touch solutions enables device manufactures, service providers, and mobile network operators to achieve a competitive advantage, including: Zero-Touch provisioning support will drive future growth for IoT devices in three ways:

- Increased revenues
- Lower costs
- Reduction of repair time
- One-time configuration
- Enhanced data and device security
- Improved customer experiences
- Increased customer satisfaction
- Support for advanced IoT services deployment
- Easy system integration and migration in the IoT ecosystem
- Reallocate valuable resources to other tasks
- Accelerate time-to-market

Zero-Touch provisioning support will drive future growth for IoT devices in three ways:

- **Direct savings**
  - Per IoT device activation
  - Network activation
  - Fewer errors to repair
- **Indirect savings**
  - Managing stock-keeping unit (SKU) inventory of IoT devices
  - Training for technical staff
- **Better business opportunities**
  - Enables the implementation of better business cases through deployment savings and faster introduction of new services
  - Creates a self-onboarding process that takes only a few seconds, with no need to schedule a technician visit to the field
- **More advantages**
  - Much faster revenue generation
  - Introduction of new IoT services in less time

Figure 20 captures the cost savings and market growth potential by adopting a Zero-Touch approach to provisioning IoT devices in the wireless communication network.

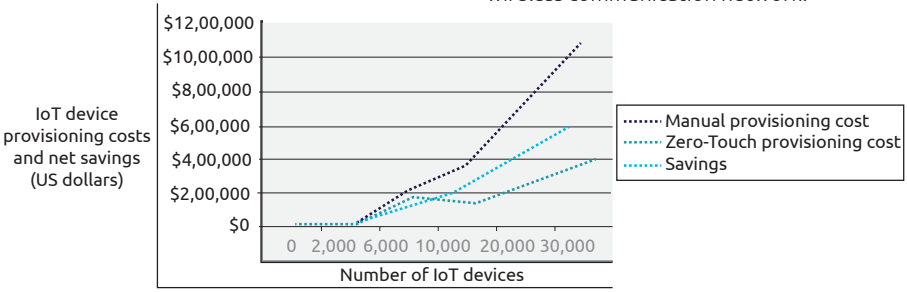


Figure 20: Cost comparison of manual versus Zero-Touch device provisioning

Source: Capgemini Engineering

Challenges and drawbacks

Combining the Zero-Touch experience with Industry 4.0, Edge, and 5G will make the entire IoT ecosystem more automated, which will create substantially greater value-add in large-scale IoT deployments for many sectors, including oil and gas, smart grid, and smart factory. However, while e-SIMs are generally regarded as the future of IoT connectivity, some challenges and drawbacks need to be addressed:

Difficulties in network switching between MNOs

- Although e-SIMs are designed to support multiple cellular network profiles, MNO profiles have to be used separately. Changing from one MNO profile to another requires a fair amount of heavy lifting and additional cost. Also, when the changeover is agreed upon, the MNO has to allocate a new IP address and access point name to the IoT device to become the new home network. Some of these steps can be complex so take time to complete them. If any of the steps fail, the IoT device will be left unconnected in the cellular network. So the end-user needs to have confidence that the new MNO can define, implement, test, and validate the updates according to their needs

Technical challenges in managing several MNOs

- In today's mobile communications industry, the mobile operator that provides specific services like 3G and 4G to particular countries owns their SIM management platform which is taken care of by the respective MNOs in their region
- Suppose the user has to switch to a different service provider. In that case, the ecosystem can deny moving the IoT device from one wireless network to another that the e-SIMs promise. It can also make the management of large IoT deployments chaotic, complex, and potentially costly. Therefore, logically speaking, there is a need for every e-SIM supplier to have a common management platform, where the platform can support multiple MNOs to keep the connectivity process as simple as possible. However, today very few e-SIM management platforms are set up to support multiple MNO subscriptions available worldwide. This means that there is still a high probability of dealing with more than one e-SIM management platform

Loss in revenue for MNOs

- Traditional SIMs are owned and controlled by the MNO. The whole point of the e-SIM concept is to identify the way to take complete control from the MNO and provide the benefit to the IoT device user to have connectivity with different MNOs based on the need. However, operators risk losing revenue by providing easy support for end-users to switch between different cellular networks. Also, many MNOs are reluctant to make their subscription profiles widely available. MNOs continue to place restrictions on how, when, and where their profiles can be used for IoT device deployments on their network. This mindset is expected to change when the growth rate of IoT device deployments starts to accelerate

Solid growth ahead for IoT devices, e-SIMs, and i-SIMs

According to market research firm Strategy Analytics, the number of connected devices in the IoT market is projected to nearly double between 2020 and 2025.[3] The firm projects unit sales of e-SIMs for IoT applications to grow to 326 million units by 2025, up from 150 million in 2020. (See Figure 21.) e-SIM developments are ramping-up as the industry is now aligned with clear standards from the GSMA, and a broad ecosystem of partners, with over 200 carriers supporting e-SIM, according to Strategy Analytics.

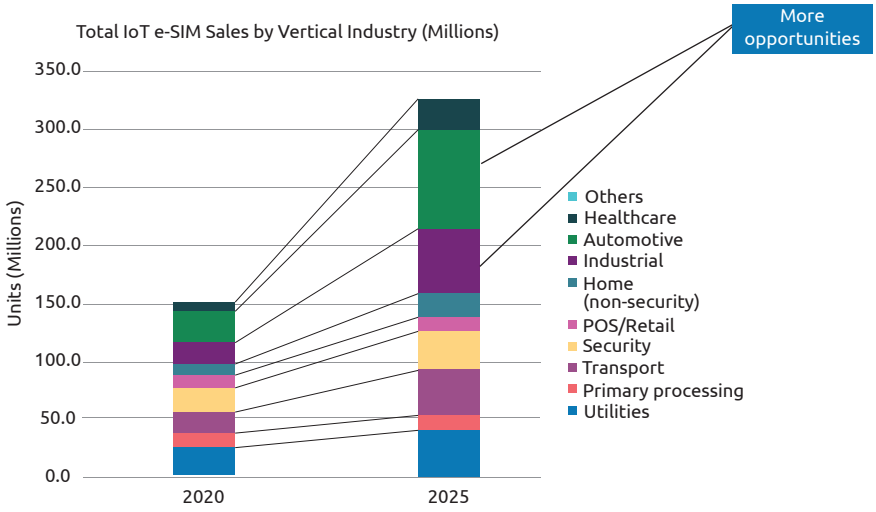


Figure 21: Broad industry growth forecast for the e-SIM market

Source: Strategy Analytics

3 "Strategy Analytics: Annual eSIM Sales in the IoT Will More Than Double by 2025," Sep 16, 2020, Business Wire

Conclusion

Today, the manual onboarding process of IoT devices and data/device security is a critical challenge for network operators and platform providers. To address the challenge, mobile network operators have launched a trusted new onboarding Zero-Touch service based on the GSMA IoT-SAFE standard. The Zero-Touch service is deployed in existing networks through partnerships with device manufacturers, cloud platform providers, and SoC vendors. (See Figure 22.) The goal is to provide IoT devices for condition monitoring, asset tracking, fleet management, and other applications that save time and money and produce a positive return on investment.

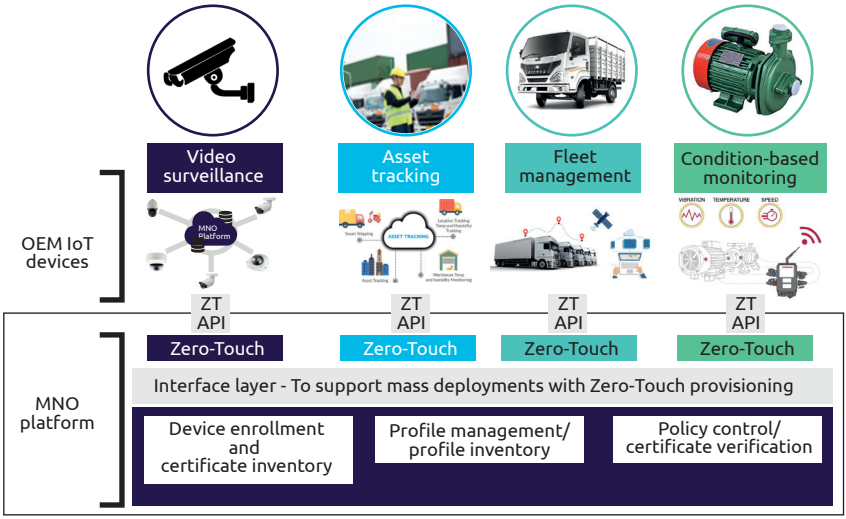


Figure 22: Zero-Touch provisioning framework

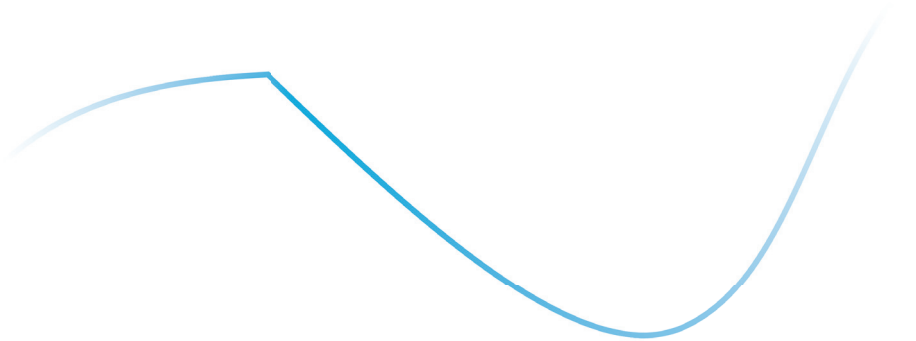
Source: Capgemini Engineering

The Zero-Touch framework on IoT cloud platforms helps service providers monitor and troubleshoot large-scale IoT device deployments by automating the provisioning of devices in the field. The Zero-Touch software package can track ownership credentials of multiple IoT devices through various distributors and retailers and inform the IoT cloud platform when the IoT devices are delivered and activated. As Zero-Touch provisioning and other cutting-edge technologies like 5G and edge computing mature, the IoT networks could soon become entirely automated and create greater benefits for industrial and IoT market segments.

For service providers and cloud platform providers, Zero Touch could create significant ROI benefits such as an increase in the average revenue per device, increase in device adoption, revenue generation from growth in device subscriptions, and scalable device management for a fleet of IoT devices based on GMSA IoT SAFE, and e-SIM and i-SIM growth trends.

As the GSMA IoT-SAFE standard evolves, network operators, service providers, and cloud platform providers will create new Zero-Touch business models that could increase the average revenue per IoT device in various market segments and generate market-share growth. Furthermore, with Zero-Touch provisioning based on GSMA IoT SAFE and other cutting-edge technologies, such as 5G and Edge computing network architectures, one day soon, IoT networks will become entirely automated.

The promise of faster service activation, lower operational cost, scalability, and fewer human errors with Zero-Touch provisioning has created significant interest within the IoT industry and triggered SoCs, OEMs, ODMs, MNOs, cloud platform providers and other service providers to invest in the Zero-Touch solution for emerging IoT market segments.



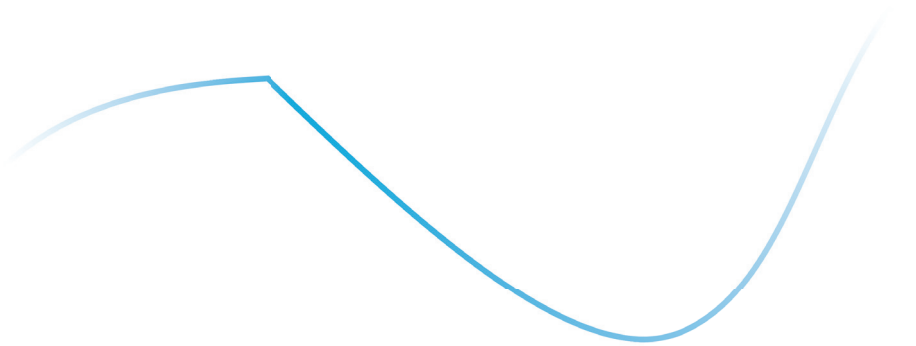
References

1. "Using the SIM as a 'Root of Trust' to Secure IoT Applications," Mar 12, 2019, GSMA https://www.gsma.com/iot/wp-content/uploads/2019/12/IoT.04-v1-Common-Implementation-Guide.pdf
2. Nick Lethaby, "Run-time provisioning of security credentials for IoT devices," Mar 23, 2020, EE News Europe https://www.eenewseurope.com/news/run-time-provisioning-security-credentials-iot-devices
3. Rich Nass, "Zero-Touch Provisioning for 5G Networks," Nov 14, 2019, insight.tech https://www.insight.tech/content/zero-touch-provisioning-for-5g-networks
4. "Telit OneEdge Overview, " Telit https://www.telit.com/oneedge/
5. "What is Zero Touch Provisioning and How Does it Enhance Network Automation? " Apr 25, 2018, Lanner Electronics Canada Ltd https://www.lanner-america.com/blog/zero-touch-provisioning-enhance-network-automation/
6. Juhi Fadia, "The State of Zero Touch in Industrial IoT," Mar 18, 2020, IoT Evolution World https://www.iotevolutionworld.com/iot/articles/444835-state-zero-touch-industrial-iot.htm
7. Azure IoT Edge documentation, "Create and provision an IoT Edge device using X.509 certificates," Jun 18, 2021, Microsoft https://docs.microsoft.com/en-us/azure/iot-edge/how-to-auto-provision-x509-certs
8. Anthony Mashford, "Announcing support for X.509 CA on Azure IoT," Oct 10, 2017, Mashford's Musings Hub https://blog.mashfords.com/2017/10/10/announcing-support-for-x-509-ca-on-azure-iot-hub/
9. "What is Azure IoT Hub Device Provisioning Service?" Apr 4, 2019, Microsoft https://docs.microsoft.com/en-us/azure/iot-dps/about-iot-dps
10. John Blyler, "Zero Touch" IoT Security Is Key to Continued Growth," Jan 4, 2018 insight.tech https://www.insight.tech/content/8220-zero-touch-8221-iot-security-is-key-to-continued-growth
11. webpage, "Zero-Touch Provisioning, Faster Deployment, Fewer Mistakes; The role of StableNet® in zero-touch provisioning," StableNet https://www.infosim.net/stablenet/zero-touch-provisioning/
12. Stephen Evanczuk, "Take the Zero-Touch Approach to Securely Lock Down an IoT Device," Apr 26, 2017, Digi-Key Electronics https://www.digikey.com/en/articles/take-zero-touch-approach-securely-lock-down-iot-device
13. "Breaking Down What an IoT SIM Card is and How it Works," Jul 21, 2020, Telnyx https://telnyx.com/resources/iot-sim-card-explained
14. "The Difference Between a Regular Smartphone SIM and an IoT SIM for Enterprises," Dec 10, 2020, EMnify https://www.emnify.com/blog/the-difference-between-a-regular-smartphone-sim-and-an-iot-sim-for-enterprises
15. Ian Marsden, "Zero Touch Global Connectivity – Unlocking the Benefits of IoT," Feb 3, 2020, CK Hutchison Holdings https://insights.ckhiod.com/insights/zero-touch-global-connectivity-unlocking-the-benefits-of-iot
16. Lucy Holden, "How to Supercharge eUICC for IoT? – IoT Uncovered," Jul 21, 2020, Eseye, https://www.eseye.com/how-to-supercharge-euicc-for-iot-iot-uncovered/
17. [17] Brian Jackson, "Bell launches LTE-M network targeting IoT devices," Jun 2, 2017, IT World Canada https://www.itworldcanada.com/article/bell-launches-lte-m-network-targeting-iot-devices/393705
18. "What is Trust Onboard?" Twilio Docs, https://www.twilio.com/docs/iot/wireless/trust-onboard
19. "Curiosity OS: Simplify management of diverse IoT requirements," Sprint https://wholesale.sprint.com/iot/curiosity-os
20. Mayank G., "What is eSIM? how it's different than SIM Card? Everything about eSIM," Sep 20, 2018, TRENDINFOCUS https://trendinfocus.com/esim-card/
21. Christine Jorgensen, "The rise of eSIMs and iSIMs and their impact on IoT," Nov 20, 2019, Qualcomm Developer Network https://developer.qualcomm.com/blog/rise-esims-and-isims-and-their-impact-iot
22. Andrew Brown, "What is eUICC and why is it important?" Jul 7, 2016, IoT Now https://www.iot-now.com/2016/07/07/49682-what-is-euicc-and-why-is-it-important/
23. E Ben Smeets, Per Ståhl, John Fornehed "Evolving SIM solutions for IoT," May 27, 2019, Ericsson, https://www.ericsson.com/en/blog/2019/5/evolving-sim-solutions-for-iot
24. "Everything You Need To Know About eSIM Cards," Nov 26, 2018, Redbytes https://www.redbytes.in/everything-know-about-esim-cards/
25. "Secure Device Onboard," 2020, Github https://secure-device-onboard.github.io/docs/latest/
26. "Device Onboarding," 2020, AnyConnect Private Limited https://anyconnect.com/device-onboarding/
27. Charlie Ashton, "Zero-Touch Automation Moves

Telecom Networks from Automatic to Autonomous," Jun 24, 2018, Wind River Systems https://blogs.windriver.com/wind_river_blog/2018/06/zero-touch-automation-moves-telecom-networks-from-automatic-to-autonomous/

28. Filippo Galimberti, "Zero Touch Provisioning: Value Added to Service Providers' Business," 2005, Cisco Systems Inc. https://www.cisco.com/c/dam/global/en_uk/training-events/isp/NG-ISPZeroTouchDeployment-FilippoGalimberti.pdf

29. Press release, "Strategy Analytics: Annual eSIM Sales in the IoT Will More Than Double by 2025," Sep 16, 2020, Strategy Analytics https://www.businesswire.com/news/home/20200916005097/en/Strategy-Analytics-Annual-eSIM-Sales-in-the-IoT-Will-More-Than-Double-by-2025



Author

Vijay Anand
Assistant Vice President,
Technology, and Chief IoT Architect,
Capgemini Engineering

Vijay plays a strategic leadership role building connected IoT solutions in a number of market segments including consumer and industrial IoT. He has over 25 years of experience and has published 19 research papers, including IEEE award-winning articles. He is currently pursuing a Ph.D. at the Crescent Institute of Science and Technology, India.

Capgemini engineering

About Capgemini Engineering

Capgemini Engineering combines, under one brand, a unique set of strengths from across the Capgemini Group: the world leading engineering and R&D services of Altran – acquired by Capgemini in 2020 – and Capgemini's digital manufacturing expertise. With broad industry knowledge and cutting-edge technologies in digital and software, Capgemini Engineering supports the convergence of the physical and digital worlds. Combined with the capabilities of the rest of the Group, it helps clients to accelerate their journey towards Intelligent Industry. Capgemini Engineering has more than 52,000 engineer and scientist team members in over 30 countries across sectors including aeronautics, automotive, railways, communications, energy, life sciences, semiconductors, software & internet, space & defence, and consumer products.

For more details, contact us:
www.capgemini-engineering.com

Write to us at:
engineering@capgemini.com