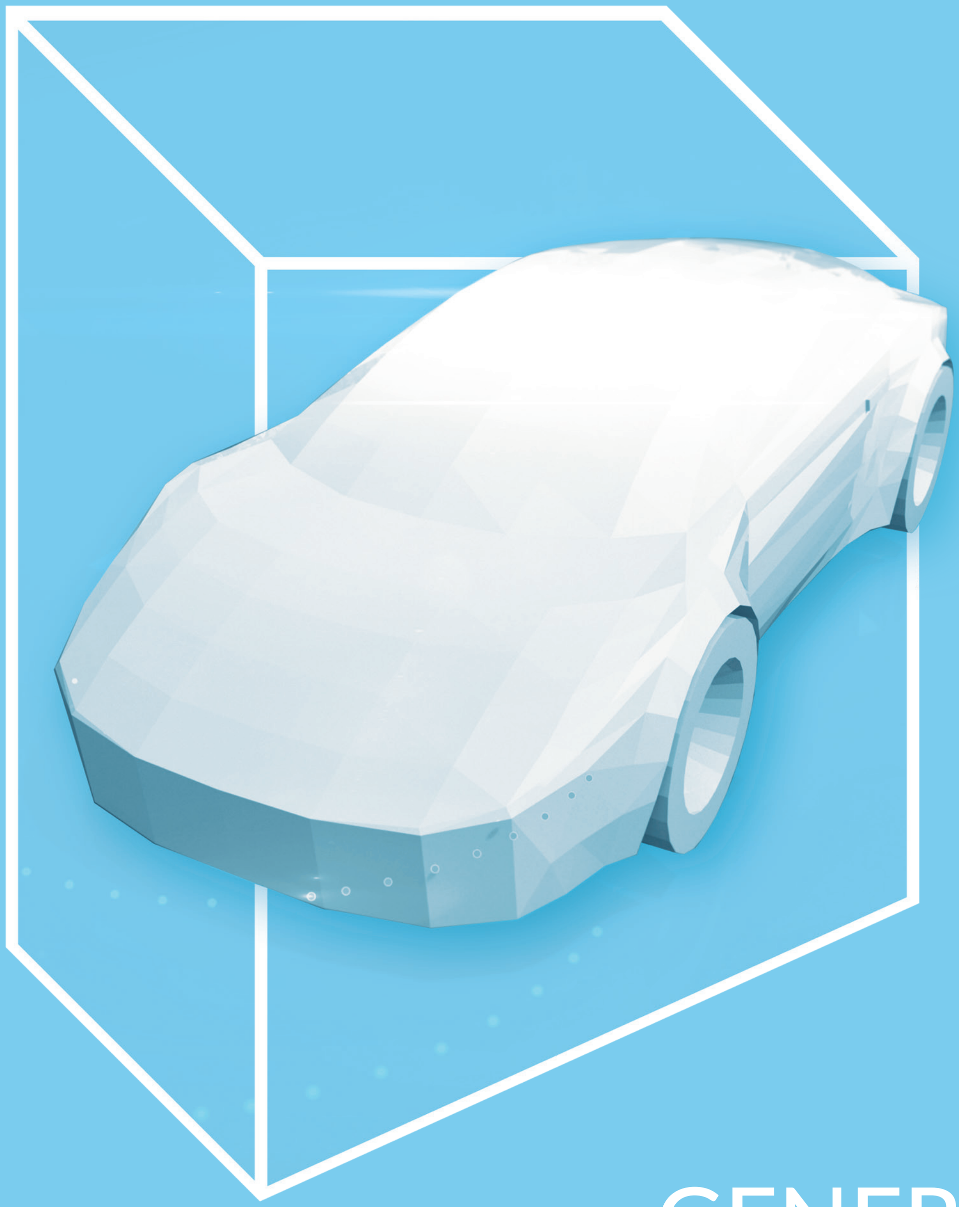
iBASIS
POWERED BY TOFANE | BE THERE FIRST



THE NEXT GENERATION SIM AND HOW IT WORKS

An iBASIS Whitepaper By Richard Pellegrini

This paper will look at the characteristics of the traditional, Standard SIM and of the next generation of SIM and explain how they are different and the resulting benefits of the next generation of SIM technology

THE NEXT GENERATION SIM AND HOW IT WORKS

Internet of Things providers who offer a thing and a thing service will often deploy their globally delivered or traveling smart devices with a standard or "roaming-only" global SIM capability. With a roaming-only global SIM, data must originate and terminate from the network of the "home" mobile network operator (the mobile network operator whose network credentials are currently being used to connect to the foreign mobile network). As a result, data that is generated by a connected device can be routed across very long distances before it is consumed for use. This can result in poor user experience. With the next generation SIM capability, the credentials of a mobile network operator in the country or region can be dynamically downloaded to the smart device, allowing for data access in the local area and resulting in lower latency and, therefore, improved user experience.

This paper will look at the characteristics of the Traditional, Standard SIM and of the Next Generation SIM and explain both how they are different as well as the resulting benefits of the next generation of SIM technology.

CONNECTING TO A MOBILE NETWORK

ATTRIBUTES OF A TRADITIONAL SIM

Mobile devices can only connect to mobile networks to which they are authorized to connect. As a result, an authentication procedure is performed every time a mobile device initiates a connection to a mobile network. Once authenticated, mobile devices can only use the mobile services to which they are subscribed. On Global System for Mobile Communications (GSM) networks, a small removable computing module installed in the mobile device called a Subscriber Identity Module (SIM) controls the authentication and service access establishment process.

IDENTIFYING INFORMATION

The SIM consists of a smart card container called a Universal Integrated Circuit Card (UICC) and Mobile Network Operator (MNO) credentials (network connection data) called the Operator Profile. A UICC is referenced by an identification number called the Integrated Circuit Card Identifier (ICCID). The ICCID is a 20 digit number that identifies the MNO that issued the SIM including the operator's mobile country code (MCC) and mobile network code (MNC).

Within the Operator Profile data is additional information that identifies the mobile device. The International Mobile Subscriber Identity (IMSI) is a unique number that identifies the device within the carrier's network. The IMSI is a 15 digit number that includes the MNO's MCC, MNC, and a Mobile Subscriber Identification Number (MSIN). Depending on mobile services allowed on a particular IMSI (data only, voice, or SMS), for voice or SMS, a Mobile Station International Subscriber Directory Number (MSISDN) is required to route phone calls and messages (SMS) to the mobile device.

A representation of a traditional, standard SIM is shown in **Figure 1.** As shown, the standard SIM contains a single Operator Profile, or set of network credentials, and must connect to local mobile network or foreign mobile networks in a roaming arrangement. As a single operator SIM, the issuing MNO has full over-the-air (OTA) control of updating profile configuration files.

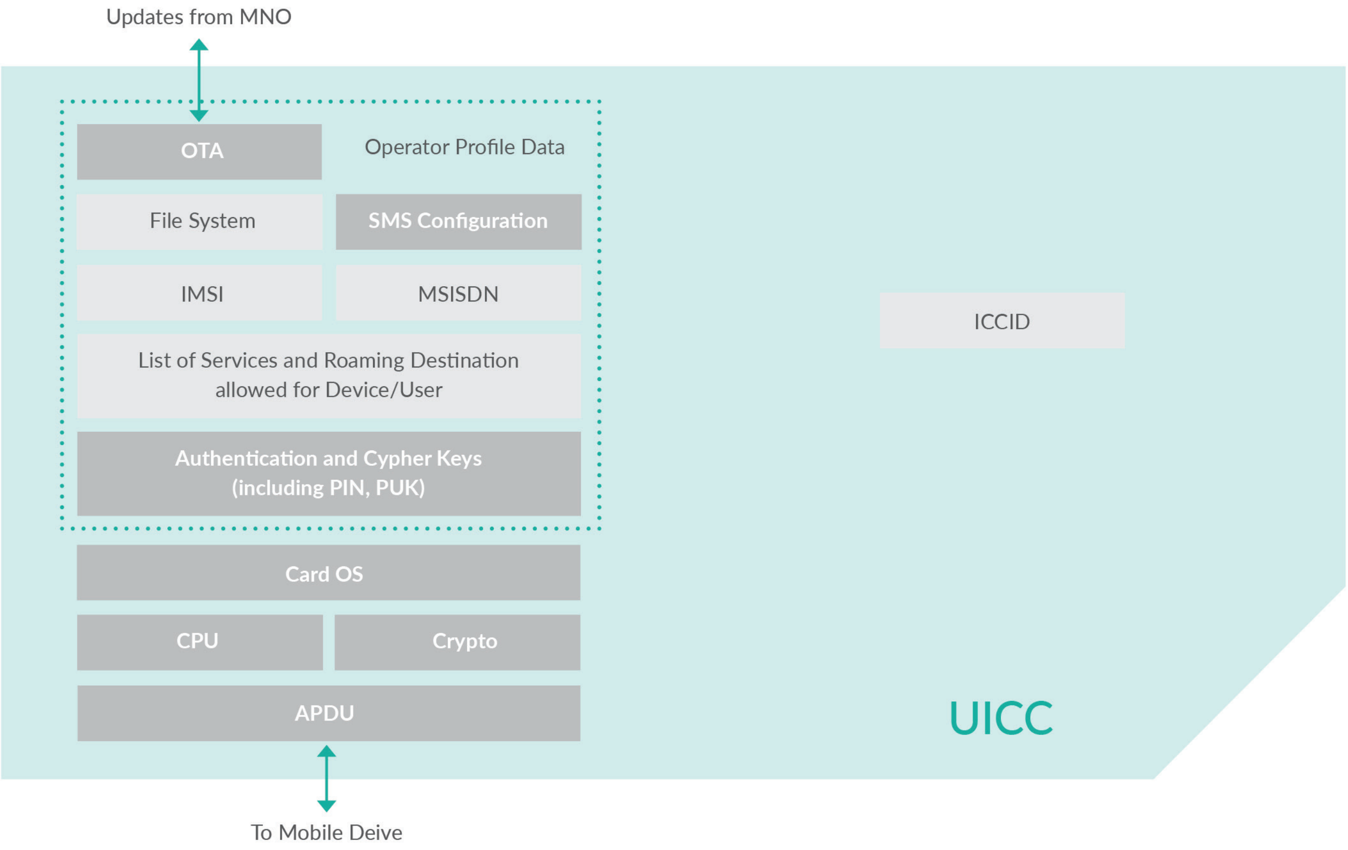


Figure 1 Representation of a Standard SIM

SECURITY INFORMATION

The Subscriber Identity Module provides many security features for Internet of Things devices communicating on mobile networks including:

- Secure identification of devices (identity management) via EIR
- Authentication and authorization
- End-to-end encryption of device data and signaling using Public Key Infrastructure (PKI)

Within its single security domain, the SIM can be protected with a Personal Identification Number (PIN). If the PIN is incorrectly entered multiple times (usually three), the SIM card blocks itself. If this occurs, the MNO can provide an eight digit Personal Unblocking Key (PUK) to unblock the device.

CONNECTING TO A MOBILE NETWORK

ATTRIBUTES OF THE NEXT GENERATION eSIM

Similar to the traditional SIM, a computing module called an Embedded SIM (eSIM) controls the authentication and service access establishment processes for next generation mobile devices (e.g. smart watches, wearables, connected cars). However, unlike a traditional SIM, an eSIM is a remotely programmable, embedded or “electronic” SIM. The eSIM is most often in the form of an integrated circuit chip soldered into the device circuit board, but is also offered in traditional SIM packages like the micro and nano formats you would find in your smartphone.

The eSIM consists of a smart card container called an embedded Universal Integrated Circuit Card (eUICC) and MNO credentials. An eUICC is referenced by an identification number called the eUICC ID (EID). The EID is a 32 digit number that identifies the mobile services issuer of the eSIM including the issuer’s mobile country code (MCC) and issuer ID. The eUICC can be thought of as a “larger container” than the UICC of a standard SIM.

Compared with the standard SIM, the Operator Profile data on an eSIM holds additional information that identifies the mobile device

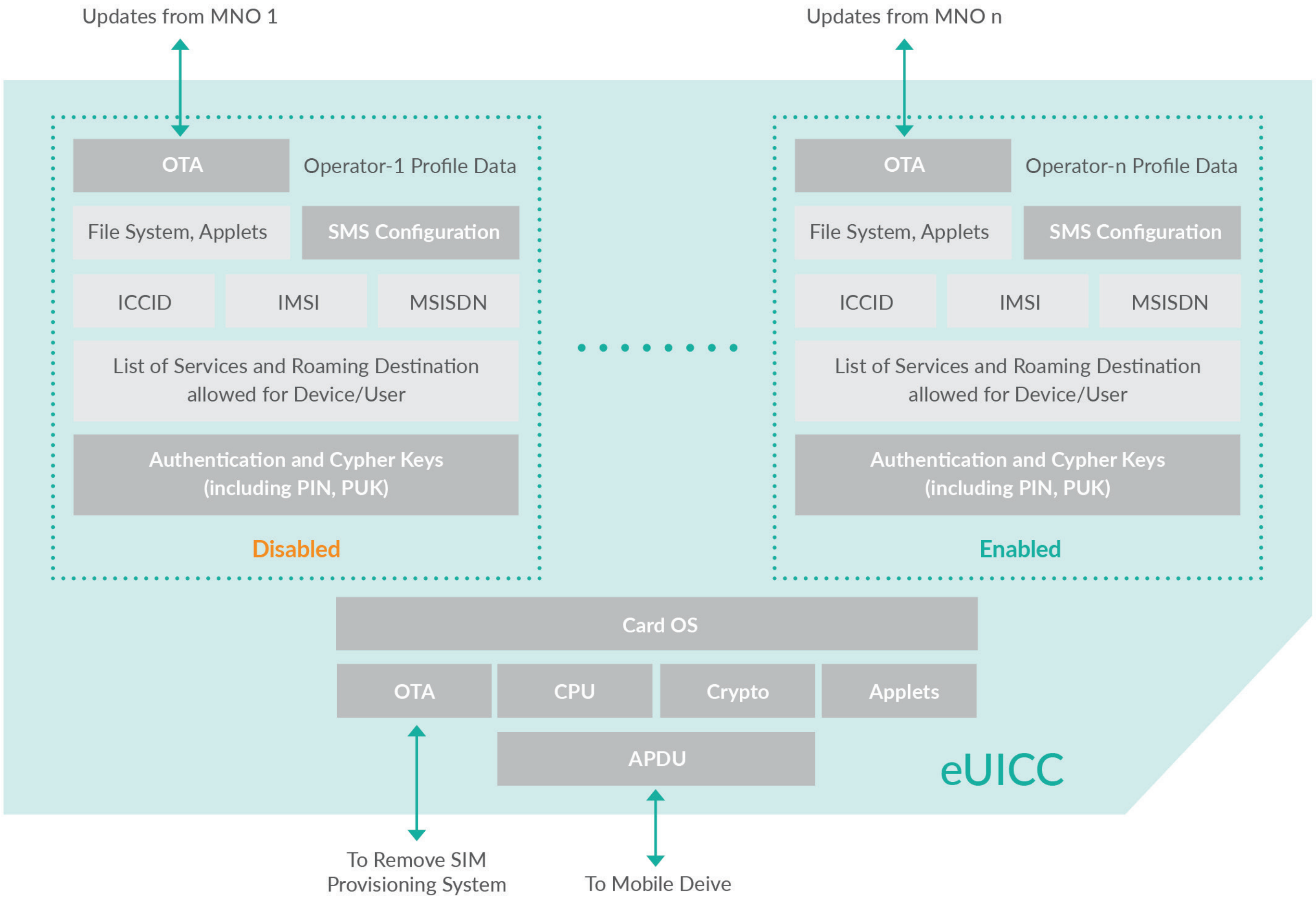

Updates from MNO 1
Updates from MNO n
OTA
Operator-1 Profile Data
File System, Applets
SMS Configuration
ICCID
IMSI
MSISDN
List of Services and Roaming Destination allowed for Device/User
Authentication and Cypher Keys (including PIN, PUK)
Disabled
OTA
Operator-n Profile Data
File System, Applets
SMS Configuration
ICCID
IMSI
MSISDN
List of Services and Roaming Destination allowed for Device/User
Authentication and Cypher Keys (including PIN, PUK)
Enabled
Card OS
OTA
CPU
Crypto
Applets
APDU
eUICC
To Remove SIM Provisioning System
To Mobile Deive

Figure 2 Representation of an eSIM

on a particular MNO's network. Unlike the standard SIM, however, the eSIM can hold multiple sets of Operator credentials or "virtual profiles". Each MNO's virtual profile includes the IMSI that identifies the device within that MNO's network, and depending on the mobile services allowed on a particular IMSI, an MSISDN is still required to route phone calls and messages to the device. Also, each of the virtual profiles can be thought of as a virtual SIM in their own MNO specific container with their own ICCID.

A representation of a next generation eSIM is shown in **Figure 2**. As shown, the eSIM contains multiple Operator virtual profiles where each MNO profile owner has full over-the-air (OTA) control of updating the configuration files of their own virtual profile when it is active.

A PROGRAMMABLE SIM

HOW DOES IT WORK?

The eSIM is a remotely programmable SIM. Within the eSIM there exists multiple security domains, one for the controlling authority (usually the eUICC Manufacturer) and one each for the MNO profiles or Issuers of the virtual profiles. In simple terms, there is a shared portion of the eSIM and there can be multiple MNO profile locations depending on the overall memory size of the eUICC chip. The controlling authority domain, also known as eSIM Root System, controls the transmission, storage, activation, deactivation, and deletion of MNO profiles from the eUICC by communicating over-the-air with an off-chip Remote SIM Provisioning (RSP) system operated by the controlling authority. Only one virtual profile or MNO security domain can be active at given time on the eUICC. This represents one virtual SIM with its corresponding ICCID, IMSI and MSISDN. **Table 1** summarizes the differences between the Standard SIM and the eSIM.

Table 1

ATTRIBUTE	STANDARD SIM	eSIM
Operator Credential Programming	In SIM Manufacturing only	Over-the-Air (OTA)
Operator Credentials	One Operator Profile	Multiple Operator *Virtual Profiles*
Security	Less Secure (removable)	More Secure (most often embedded, non-removable)
Update Logistics (for new permanent location or new MNO)	Card must be removed and replaced	Card is remotely programmed OTA with new MNO credentials

GOVERNED BY STANDARDS

The GSM Association's (GSMA) Embedded SIM Specification provides a single, de-facto standard mechanism for the remote provisioning and management of Machine to Machine (M2M) connections, allowing the "over the air" provisioning of an initial operator subscription as well as future changes of subscription from one operator to another. GSMA Embedded SIM is a vital enabler for M2M connections including the simple and seamless mobile connection of all types of connected machines.

WHAT PROBLEMS DOES THE eSIM SOLVE?

The logistics associated with shipping, testing, and activating millions of IoT devices around the world requires significant orchestration and resources. With standard SIM technology, an IoT Service Provider (IoTSP) needs to order and stock SIMs from multiple MNO partners around the globe. When shipping their connected devices to customers, the IoTSP must be cognizant of the delivery destination and insert into the device the correct SIM card for the desired regional mobile operator. With eSIM technology, the SIM is a single programmable SIM that can be incorporated as an integrated circuit chip on a device circuit board or can be a commercial pluggable (e.g. 3FF or 4FF) or ruggedized (e.g. MFF1 or MFF2) format. With the eSIM, the IoTSP can insert the same eSIM card in every device delivered and program the card, or embedded chip in the device, to the correct regional mobile operator when the device is turned on in the delivered country

ABOUT iBASIS

iBASIS is the leading communications solutions provider enabling operators and digital players worldwide to perform and transform. Powered by Tofane Global, iBASIS represents an estimated USD 1+ billion in annual revenue, is the third largest wholesale voice operator, ranks as the Top 3 LTE IPX vendor with 660+ LTE destinations and serves 1,000+ customers across 18 offices worldwide. iBASIS optimizes access, connectivity, and value-added solutions, so customers achieve high return on voice, mobile data, and IoT requirements to be first in their respective markets and in the digital era.

iBASIS provides the end-to-end Global Access for Things™ connectivity solution, delivering single source access for local LTE-M and NB-IoT worldwide provisioned through GSMA-standard eSIM/eUICC technology. The solution simplifies IoT devices connection through one unified platform for seamless, remote, programmable, and secure provisioning management and data analytics. For more information, visit www.iBASIS.com.