SIM card

A **subscriber identity module** or **subscriber identification module** (**SIM**), widely known as a **SIM card**, is an integrated circuit running a card operating system (COS) that is intended to securely store the international mobile subscriber identity (IMSI) number and its related key, which are used to identify and authenticate subscribers on mobile telephony devices (such as mobile phones and computers). It is also possible to store contact information on many SIM cards. SIM cards are always used on GSM phones; for CDMA phones, they are needed only for LTE-capable handsets. SIM cards can also be used in satellite phones, smart watches, computers, or cameras.

A typical SIM card (mini-SIM with micro-SIM cutout)

The SIM circuit is part of the function of a universal integrated circuit card (UICC) physical smart card, which is usually made of PVC with embedded contacts and semiconductors. SIM cards are transferable between different mobile devices. The first UICC smart cards were the size of credit and bank cards; sizes were reduced several times over the years, usually keeping electrical contacts the same, so that a larger card could be cut down to a smaller size.

T-Mobile nano-SIM card with NFC capabilities in the SIM tray of an iPhone 6s

A SIM card contains a unique serial number (ICCID), international mobile subscriber identity (IMSI) number, security authentication and ciphering information, temporary information related to the local network, a list of the services the user has access to, and two passwords: a personal identification number (PIN) for ordinary use, and a personal unblocking key (PUK) for PIN unlocking. In Europe, the serial SIM number (SSN) is also sometimes accompanied by an international article number (IAN) or a European article number (EAN) required when registering on line for the subscription of a prepaid card.

A TracFone Wireless SIM card has no distinctive carrier markings and is only marked as a "SIM CARD".

Contents

History and procurement

The SIM card is a type of smart card,[1] the basis for which is the silicon integrated circuit (IC) chip.[2] The idea of incorporating a silicon IC chip onto a plastic card originates from the late 1960s.[2] Smart cards have since used MOS integrated circuit chips, along with MOS memory technologies such as flash memory and EEPROM (electrically erasable programmable read-only memory).[3]

The SIM was initially specified by the European Telecommunications Standards Institute in the specification with the number TS 11.11. This specification describes the physical and logical behaviour of the SIM. With the development of UMTS, the specification work was partially transferred to 3GPP. 3GPP is now responsible for the further development of applications like SIM (TS 51.011[4]) and USIM (TS 31.102[5]) and ETSI for the further development of the physical card UICC.

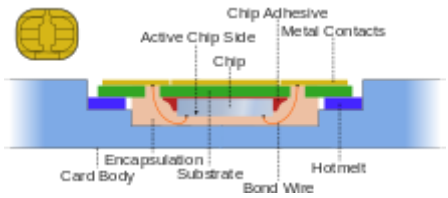
The first SIM card was developed in 1991 by Munich smart-card maker Giesecke & Devrient, who sold the first 300 SIM cards to the Finnish wireless network operator Radiolinja.[6][7]

Today, SIM cards are ubiquitous, allowing over 7 billion devices to connect to cellular networks around the world. According to the International Card Manufacturers Association (ICMA), there were 5.4 billion SIM cards manufactured globally in 2016 creating over $6.5 billion in revenue for traditional SIM card vendors.[8] The rise of cellular IoT and 5G networks is predicted to drive the growth of the addressable market for SIM card manufacturers to over 20 billion cellular devices by 2020.[9] The introduction of embedded-SIM (eSIM) and remote SIM provisioning (RSP) from the GSMA[10] may disrupt the traditional SIM card ecosystem with the entrance of new players specializing in "digital" SIM card provisioning and other value-added services for mobile network operators.

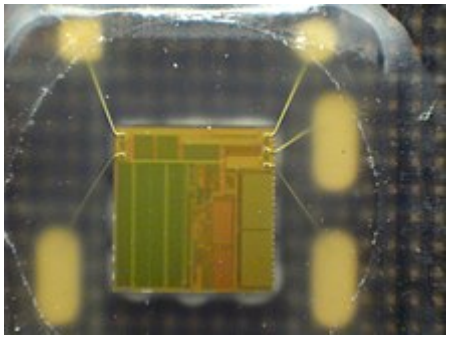
Design

There are three operating voltages for SIM cards: 5 V, 3 V and 1.8 V (ISO/IEC 7816-3 classes A, B and C, respectively). The operating voltage of the majority of SIM cards launched before 1998 was 5 V. SIM cards produced subsequently are compatible with 3 V and 5 V. Modern cards support 5 V, 3 V and 1.8 V.

Modern SIM cards allow applications to load when the SIM is in use by the subscriber. These applications communicate with the handset or a server using SIM Application Toolkit, which was initially specified by 3GPP in TS 11.14. (There is an identical ETSI specification with different numbering.) ETSI and 3GPP maintain the SIM specifications. The main specifications are: ETSI TS 102 223 (the toolkit for smartcards), ETSI TS 102 241 (API), ETSI TS 102 588 (application invocation), and ETSI TS 131 111 (toolkit for more SIM-likes). SIM toolkit applications were initially written in native code using proprietary APIs. To provide interoperability of the applications, ETSI chose Java Card.[11] A multi-company collaboration called GlobalPlatform defines some extensions on the cards, with additional APIs and features like more cryptographic security and RFID contactless use added.[12]



SIM chip structure and packaging


4 by 4 millimetres (0.16 in × 0.16 in) silicon chip in a SIM card which has been peeled open. Note the thin gold bonding wires, and the regular, rectangular digital memory areas.

Data

SIM cards store network-specific information used to authenticate and identify subscribers on the network. The most important of these are the ICCID, IMSI, authentication key (K_i), local area identity (LAI) and operator-specific emergency number. The SIM also stores other carrier-specific data such as the SMSC (Short Message service center) number, service provider name (SPN), service dialing numbers (SDN), advice-of-charge parameters and value-added service (VAS) applications. (Refer to GSM 11.11.[13])

SIM cards can come in various data capacities, from 8 KB to at least 256 KB. All can store a maximum of 250 contacts on the SIM, but while the 32 KB has room for 33 mobile network codes (MNCs) or *network identifiers*, the 64 KB version has room for 80 MNCs. This is used by network operators to store data on preferred networks, mostly used when the SIM is not in its home network but is roaming. The network operator that issued the SIM card can use this to have a phone connect to a preferred network that is more economic for the provider instead of having to pay the network operator that the phone discovered first. This does not mean that a phone containing this SIM card can connect to a maximum of only 33 or 80 networks, but it means that the SIM card issuer can specify only up to that number of preferred networks. If a SIM is outside these preferred networks it uses the first or best available network.

ICCID

Each SIM is internationally identified by its integrated circuit card identifier (ICCID). ICCID is the identifier of the actual SIM card itself – i.e. an identifier for the SIM chip. Nowadays ICCID numbers are also used to identify eSIM profiles, and not only physical SIM cards. ICCIDs are stored in the SIM cards and are also engraved or printed on the SIM card body during a process called personalisation. The ICCID is defined by the ITU-T recommendation E.118 as the *primary account number*.[14] Its layout is based on ISO/IEC 7812. According to E.118, the number can be up to 22 digits long, including a single check digit calculated using the Luhn algorithm. However, the GSM Phase 1[15] defined the ICCID length as an opaque data field, 10 octets (20 digits) in length, whose structure is specific to a mobile network operator.

The number is composed of the following subparts:

Issuer identification number (IIN)

Maximum of seven digits:

- Major industry identifier (MII), 2 fixed digits, **89** for telecommunication purposes.
- Country code, 2 or 3 digits, as defined by ITU-T recommendation E.164.
  - NANP countries, apart from Canada, use **01**, i.e. prepending a zero to their common calling code +1
  - Canada uses **302**
  - Russia uses **701**, i.e. appending 01 to its calling code +7
  - Kazakhstan uses **997**, even though it shares the calling code +7 with Russia
- Issuer identifier, 1–4 digits.
  - Often identical to the mobile network code (MNC).

Individual account identification

- Individual account identification number. Its length is variable, but every number under one IIN has the same length.
  - Often identical to the mobile subscription identification number (MSIN).

Check digit

- Single digit calculated from the other digits using the Luhn algorithm.

With the GSM Phase 1 specification using 10 octets into which ICCID is stored as packed BCD, the data field has room for 20 digits with hexadecimal digit "F" being used as filler when necessary.

In practice, this means that on GSM SIM cards there are 20-digit (19+1) and 19-digit (18+1) ICCIDs in use, depending upon the issuer. However, a single issuer always uses the same size for its ICCIDs.

To confuse matters more, SIM factories seem to have varying ways of delivering electronic copies of SIM personalization datasets. Some datasets are without the ICCID checksum digit, others are with the digit.

As required by E.118, the ITU-T updates a list of all current internationally assigned IIN codes in its Operational Bulletins which are published twice a month (the last as of January 2019 was No. 1163 from 1 January 2019).[16] ITU-T also publishes complete lists: as of January 2019, the list issued on 1 December 2018 was current, having all issuer identifier numbers before 1 December 2018.[17]

International mobile subscriber identity (IMSI)

SIM cards are identified on their individual operator networks by a unique international mobile subscriber identity (IMSI). Mobile network operators connect mobile phone calls and communicate with their market SIM cards using their IMSIs. The format is:

- The first three digits represent the mobile country code (MCC).
- The next two or three digits represent the mobile network code (MNC). Three-digit MNC codes are allowed by E.212 but are mainly used in the United States and Canada.
- The next digits represent the mobile subscriber identification number (MSIN). Normally there are 10 digits, but can be fewer in the case of a 3-digit MNC or if national regulations indicate that the total length of the IMSI should be less than 15 digits.
- Digits are different from country to country.

Authentication key (K_i)

The K_i is a 128-bit value used in authenticating the SIMs on a GSM mobile network (for USIM network, you still need K_i but other parameters are also needed). Each SIM holds a unique K_i assigned to it by the operator during the personalization process. The K_i is also stored in a database (termed authentication center or AuC) on the carrier's network.

The SIM card is designed to prevent someone from getting the K_i by using the smart-card interface. Instead, the SIM card provides a function, *Run GSM Algorithm*, that the phone uses to pass data to the SIM card to be signed with the K_i. This, by design, makes using the SIM card mandatory unless the K_i can be extracted from the SIM card, or the carrier is willing to reveal the K_i. In practice, the GSM cryptographic algorithm for computing a signed response (SRES_1/SRES_2: see steps 3 and 4, below) from the K_i has certain vulnerabilities[18] that can allow the extraction of the K_i from a SIM card and the making of a duplicate SIM card.

Authentication process:

1. When the mobile equipment starts up, it obtains the international mobile subscriber identity (IMSI) from the SIM card, and passes this to the mobile operator, requesting access and authentication. The mobile equipment may have to pass a PIN to the SIM card before the SIM card reveals this information.
2. The operator network searches its database for the incoming IMSI and its associated K_i.
3. The operator network then generates a random number (RAND, which is a nonce) and signs it with the K_i associated with the IMSI (and stored on the SIM card), computing another number, that is split into the Signed Response 1 (SRES_1, 32 bits) and the encryption key K_c (64 bits).
4. The operator network then sends the RAND to the mobile equipment, which passes it to the SIM card. The SIM card signs it with its K_i, producing Signed Response 2 (SRES_2) and K_c, which it gives to the mobile equipment. The mobile equipment passes SRES_2 on to the operator network.
5. The operator network then compares its computed SRES_1 with the computed SRES_2 that the mobile equipment returned. If the two numbers match, the SIM is authenticated and the mobile equipment is granted access to the operator's network. K_c is used to encrypt all further communications between the mobile equipment and the operator.

Location area identity

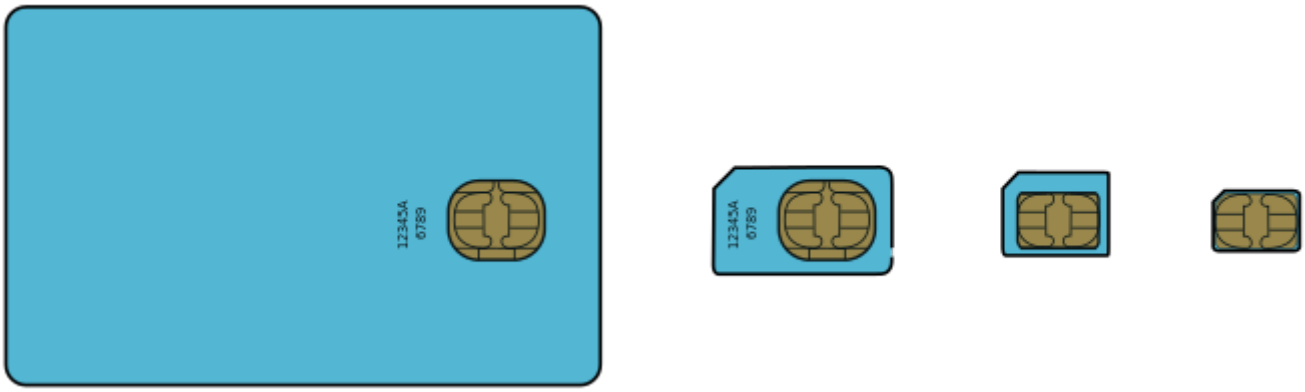
The SIM stores network state information, which is received from the location area identity (LAI). Operator networks are divided into location areas, each having a unique LAI number. When the device changes locations, it stores the new LAI to the SIM and sends it back to the operator network with its new location. If the device is power cycled, it takes data off the SIM, and searches for the prior LAI.

SMS messages and contacts

Most SIM cards store a number of SMS messages and phone book contacts. It stores the contacts in simple "name and number" pairs. Entries that contain multiple phone numbers and additional phone numbers are usually not stored on the SIM card. When a user tries to copy such entries to a SIM, the handset's software breaks them into multiple entries, discarding information that is not a phone number. The number of contacts and messages stored depends on the SIM; early models stored as few as five messages and 20 contacts, while modern SIM cards can usually store over 250 contacts.

Formats

SIM cards have been made smaller over the years; functionality is independent of format. Full-size SIM were followed by mini-SIM, micro-SIM, and nano-SIM. SIM cards are also made to embed in devices.



From left, full-size SIM (1FF), mini-SIM (2FF), micro-SIM (3FF), and nano-SIM (4FF)

SIM card formats and dimensions

SIM card format	Introduced	Standard reference	Length	Width	Thickness
Full-size (1FF)	1991	ISO/IEC 7810:2003, ID-1	85.6 mm (3.37 in)	53.98 mm (2.125 in)	0.76 mm (0.030 in)
Mini-SIM (2FF)	1996	ISO/IEC 7810:2003, ID-000	25 mm (0.98 in)	15 mm (0.59 in)	0.76 mm (0.030 in)
Micro-SIM (3FF)	2003	ETSI TS 102 221 V9.0.0, Mini-UICC	15 mm (0.59 in)	12 mm (0.47 in)	0.76 mm (0.030 in)
Nano-SIM (4FF)	early 2012	ETSI TS 102 221 V11.0.0	12.3 mm (0.48 in)	8.8 mm (0.35 in)	0.67 mm (0.026 in)
Embedded-SIM (eSIM)	2016	ETSI TS 102.671 V9.0.0 JEDEC Design Guide 4.8, SON-8 GSMA SGP.22 V1.0	—	—	—

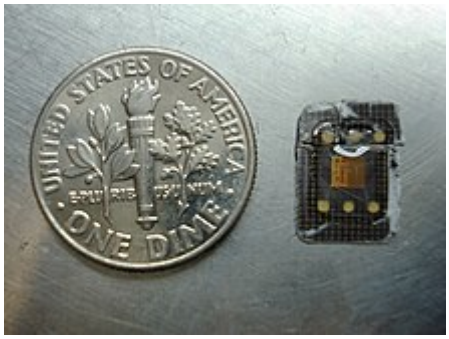
All versions of the non-embedded SIM cards share the same ISO/IEC 7816 pin arrangement.

Full-size SIM

The *full-size SIM* (or 1FF, 1st form factor) was the first form factor to appear. It was the size of a credit card (85.60 mm × 53.98 mm × 0.76 mm). Later smaller SIMs are often supplied embedded in a full-size card from which they can be removed.

Mini-SIM

The *mini-SIM* (or 2FF) card has the same contact arrangement as the full-size SIM card and is normally supplied within a full-size card carrier, attached by a number of linking pieces. This arrangement (defined in ISO/IEC 7810 as ID-1/000) lets such a card be used in a device that requires a full-size card – or in a device that requires a mini-SIM card, after breaking the linking pieces. As the full-size SIM is no longer used, some suppliers refer to the mini-SIM as a "standard SIM" or "regular SIM".

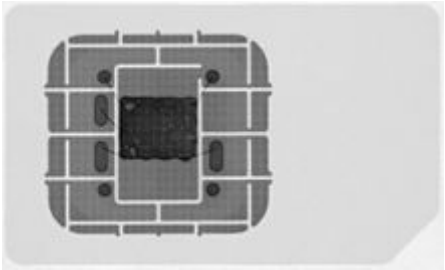


The memory chip from a micro-SIM card without the plastic backing plate, next to a US dime, which is approx. 18 mm in diameter

Micro-SIM

The *micro-SIM* (or 3FF) card has the same thickness and contact arrangements, but reduced length and width as shown in the table above.[19]

The micro-SIM was introduced by the European Telecommunications Standards Institute (ETSI) along with SCP, 3GPP (UTRAN/GERAN), 3GPP2 (CDMA2000), ARIB, GSM Association (GSMA SCaG and GSMNA), GlobalPlatform, Liberty Alliance, and the Open Mobile Alliance (OMA) for the purpose of fitting into devices too small for a mini-SIM card.[20][21]


X-ray image of a mini-SIM, showing the chip and connections

The form factor was mentioned in the December 1998 3GPP SMG9 UMTS Working Party, which is the standards-setting body for GSM SIM cards,[22] and the form factor was agreed upon in late 2003.[23]

The micro-SIM was designed for backward compatibility. The major issue for backward compatibility was the contact area of the chip. Retaining the same contact area makes the micro-SIM compatible with the prior, larger SIM readers through the use of plastic cutout surrounds. The SIM was also designed to run at the same speed (5 MHz) as the prior version. The same size and positions of pins resulted in numerous "How-to" tutorials and YouTube videos with detailed instructions how to cut a mini-SIM card to micro-SIM size.[24]

The chairman of EP SCP, Dr. Klaus Vedder, said[23]

> ETSI has responded to a market need from ETSI customers, but additionally there is a strong desire not to invalidate, overnight, the existing interface, nor reduce the performance of the cards.

Micro-SIM cards were introduced by various mobile service providers for the launch of the original iPad, and later for smartphones, from April 2010. The iPhone 4 was the first smartphone to use a micro-SIM card in June 2010, followed by many others.

Nano-SIM

The *nano-SIM* (or 4FF) card was introduced on 11 October 2012, when mobile service providers in various countries started to supply it for phones that supported the format. The nano-SIM measures 12.3 mm × 8.8 mm × 0.67 mm (0.484 in × 0.346 in × 0.026 in) and reduces the previous format to the contact area while maintaining the existing contact arrangements. A small rim of isolating material is left around the contact area to avoid short circuits with the socket. The nano-SIM is 0.67 mm (0.026 in) thick, compared to the 0.76 mm (0.030 in) of its predecessors. 4FF can be put into adapters for use with devices designed for 2FF or 3FF SIMs, and is made thinner for that purpose,[25] and telephone companies give due warning about this.[26]

The iPhone 5, released in September 2012, was the first device to use a nano-SIM card, followed by other handsets.

Security

In July 2013, Karsten Nohl, a security researcher from SRLabs, described[27][28] vulnerabilities in some SIM cards that supported DES, which, despite its age, is still used by some operators.[28] The attack could lead to the phone being remotely cloned or let someone steal payment credentials from the SIM.[28] Further details of the research were provided at BlackHat on 31 July 2013.[28][29]

In response, the International Telecommunication Union said that the development was "hugely significant" and that it would be contacting its members.[30]

In February 2015, it was reported by The Intercept that the NSA and GCHQ had stolen the encryption keys (Ki's) used by Gemalto (the manufacturer of 2 billion SIM cards annually), enabling these intelligence agencies to monitor voice and data communications without the knowledge or approval of cellular network providers or judicial oversight.[31] Having finished its investigation, Gemalto claimed that it has “reasonable grounds” to believe that the NSA and GCHQ carried out an operation to hack its network in 2010 and 2011, but says the number of possibly stolen keys would not have been massive.[32]

Developments

When GSM was already in use, the specifications were further developed and enhanced with functionality such as SMS and GPRS. These development steps are referred as releases by ETSI. Within these development cycles, the SIM specification was enhanced as well: new voltage classes, formats and files were introduced.

USIM

In GSM-only times, the SIM consisted of the hardware and the software. With the advent of UMTS this naming was split: the SIM was now an application and hence only software. The hardware part was called UICC. This split was necessary because UMTS introduced a new application, the universal subscriber identity module (USIM). The USIM brought, among other things, security improvements like the mutual authentication and longer encryption keys and an improved address book.

UICC

"SIM cards" in developed countries today are usually UICCs containing at least a SIM application and a USIM application. This configuration is necessary because older GSM only handsets are solely compatible with the SIM application and some UMTS security enhancements rely on the USIM application.

Other variants

On cdmaOne networks, the equivalent of the SIM card is the R-UIM and the equivalent of the SIM application is the CSIM.

A *virtual SIM* is a mobile phone number provided by a mobile network operator that does not require a SIM card to connect phone calls to a user's mobile phone.

Embedded-SIM (eSIM)

An embedded-SIM (eSIM) is a form of programmable SIM that is embedded directly into a device. The surface mount format provides the same electrical interface as the full size, 2FF and 3FF SIM cards, but is soldered to a circuit board as part of the manufacturing process. In M2M applications where there is no requirement[10] to change the SIM card, this avoids the requirement for a connector, improving reliability and security. An eSIM can be provisioned remotely; end-users can add or remove operators without the need to physically swap a SIM from the device.[33]

Embedded SIM from M2M supplier Eseye with an adapter board for evaluation in a mini-SIM socket

Usage in mobile phone standards

The use of SIM cards is mandatory in GSM devices.

The satellite phone networks Iridium, Thuraya and Inmarsat's BGAN also use SIM cards. Sometimes, these SIM cards work in regular GSM phones and also allow GSM customers to roam in satellite networks by using their own SIM card in a satellite phone.

SIM cards of various German mobile operators

Japan's 2G PDC system (which was shut down in 2012; SoftBank Mobile has already shut down PDC from 31 March 2010) also specifies a SIM, but this has never been implemented commercially. The specification of the interface between the Mobile Equipment and the SIM is given in the RCR STD-27 annex 4. The Subscriber Identity Module Expert Group was a committee of specialists assembled by the European Telecommunications Standards Institute (ETSI) to draw up the specifications (GSM 11.11) for interfacing between smart cards and mobile telephones. In 1994, the name SIMEG was changed to SMG9.

Japan's current and next generation cellular systems are based on W-CDMA (UMTS) and CDMA2000 and all use SIM cards. However, Japanese CDMA2000-based phones are locked to the R-UIM they are associated with and thus, the cards are not interchangeable with other Japanese CDMA2000 handsets (though they may be inserted into GSM/WCDMA handsets for roaming purposes outside Japan).

CDMA-based devices originally did not use a removable card, and the service for these phones bound to a unique identifier contained in the handset itself. This is most prevalent in operators in the Americas. The first publication of the TIA-820 standard (also known as 3GPP2 C.S0023) in 2000 defined the Removable User Identity Module (R-UIM). Card-based CDMA devices are most prevalent in Asia.

The equivalent of a SIM in UMTS is called the universal integrated circuit card (UICC), which runs a USIM application. The UICC is still colloquially called a *SIM card*.

SIM card for Thuraya satellite phone

KDDI's au IC-Card

NTT DoCoMo's FOMA card

UMTS modem with Beeline's SIM card

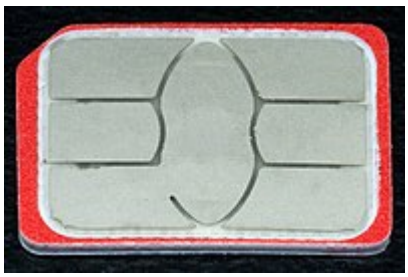
SIM card and the mobile phone

Three UK SIM card with packaging

H2O Wireless prepaid SIM card

Deutsche Telekom mini-SIM with pre-cut micro- and nano-SIM

A mini-SIM card next to its electrical contacts in a Nokia 6233



Nano-SIM card

SIM and carriers

The SIM card introduced a new and significant business opportunity for MVNOs – mobile virtual network operators – who lease capacity from one of the network operators rather than owning or operating a cellular telecoms network, and only provide a SIM card to their customers. MVNOs first appeared in Denmark, Hong Kong, Finland and the UK. Today they exist in over 50 countries, including most of Europe, United States, Canada, Mexico, Australia and parts of Asia, and account for approximately 10% of all mobile phone subscribers around the world.

On some networks, the mobile phone is locked to its carrier SIM card, meaning that the phone only works with SIM cards from the specific carrier. This is more common in markets where mobile phones are heavily subsidised by the carriers, and the business model depends on the customer staying with the service provider for a minimum term (typically 12, 18 or 24 months). SIM cards that are issued by providers with an associated contract are called *SIM-only* deals. Common examples are the GSM networks in the United States, Canada,

Australia, the UK and Poland. Many businesses offer the ability to remove the SIM lock from a phone, effectively making it possible to then use the phone on any network by inserting a different SIM card. Mostly, GSM and 3G mobile handsets can easily be unlocked and used on any suitable network with any SIM card.

In countries where the phones are not subsidised, e.g., India, Israel and Belgium, all phones are unlocked. Where the phone is not locked to its SIM card, the users can easily switch networks by simply replacing the SIM card of one network with that of another while using only one phone. This is typical, for example, among users who may want to optimise their carrier's traffic by different tariffs to different friends on different networks, or when traveling internationally.

In 2016, carriers started using the concept of automatic SIM reactivation[34] whereby they let users reuse expired SIM cards instead of purchasing new ones when they wish to re-subscribe to that operator. This is particularly useful in countries where prepaid calls dominate and where competition drives high churn rates, as users had to return to a carrier shop to purchase a new SIM each time they wanted to churn back to an operator.

SIM-only

Commonly sold as a product by mobile telecommunications companies, "SIM-only" refers to a type of legally binding contract between a mobile network provider and a customer. The contract itself takes the form of a credit agreement and is subject to a credit check.

Within a SIM-only contract the mobile network provider supplies their customer with just one piece of hardware, a SIM card, which includes an agreed amount of network usage in exchange for a monthly payment. Network usage within a SIM-only contract can be measured in minutes, text, data or any combination of these. The duration of a SIM-only contract varies depending on the deal selected by the customer, but in the UK they are available over 1, 3, 6, and 12-month periods.

SIM-only contracts differ from mobile phone contracts in that they do not include any hardware other than a SIM card. In terms of network usage, SIM-only is typically more cost effective than other contracts because the provider does not charge more to offset the cost of a mobile device over the contract period. Short contract length is one of the key features of SIM-only – made possible by the absence of a mobile device.

SIM-only is increasing in popularity very quickly.[35] In 2010 pay monthly based mobile phone subscriptions grew from 41 percent to 49 percent of all UK mobile phone subscriptions.[36] According to German research company GfK, 250,000 SIM-only mobile contracts were taken up in the UK during July 2012 alone, the highest figure since GfK began keeping records.

Increasing smartphone penetration combined with financial concerns are leading customers to save money by moving onto a SIM-only when their initial contract term is over.

Multiple-SIM devices

Dual SIM devices have two SIM card slots for the use of two SIM cards, from one or multiple carriers. Multiple SIM devices are commonplace in developing markets such as in Africa, East Asia, South Asia and Southeast Asia, where variable billing rates, network coverage and speed make it desirable for consumers to use multiple SIMs from competing networks. Dual SIM phones are also useful to separate one's personal phone number from a business phone number, without having to carry multiple devices. Some popular devices, such as the BlackBerry KeyOne have dual SIM variants, however dual SIM devices were not common in the US or Europe due to lack of demand. This has changed with mainline products from Apple and Google featuring either two SIM slots or a combination of a physical SIM slot and an eSIM.

Thin SIM

Dual SIM slots as shown on a Chinese phone

A **thin SIM** (or **overlay SIM** or **SIM overlay**) is a very thin device shaped like a SIM card, approximately 120 microns thick. It has contacts on its front and back. It is used by sticking it on top of a regular SIM card. It provides its own functionality while passing through the functionality of the SIM card underneath. It can be used to bypass the mobile operating network and run custom applications, particularly on non-programmable cell phones.[37]

Its top surface is a connector which connects to the phone in place of the normal SIM. Its bottom surface is a connector which connects to the SIM in place of the phone. With electronics, it can modify signals in either direction, thus presenting a modified SIM to the phone, and/or presenting a modified phone to the SIM. It is a similar concept to the Game Genie, which connects between a game console and a game cartridge, creating a modified game.

In 2014, Equitel, an MVNO operated by Kenya's Equity Bank, announced its intention to begin issuing thin SIMs to customers, raising security concerns by competition, particularly concerning the safety of mobile money accounts. However, after months of security testing and legal hearings before the country's Parliamentary Committee on Energy, Information and Communications, the Communications Authority of Kenya (CAK) gave the bank the green light to roll out its thin SIM cards.[38]

See also

- Apple SIM
- GSM 03.48
- International Mobile Equipment Identity (IMEI)
- IP Multimedia Services Identity Module (ISIM)
- Mobile broadband
- Mobile equipment identifier (MEID)
- Mobile signature
- Regional lockout
- SIM cloning
- SIM connector
- Single Wire Protocol (SWP)
- Tethering
- Transponder
- GSM USSD codes – Unstructured Supplementary Service Data: list of standard GSM codes for network and SIM related functions
- VMAC
- W-SIM (Willcom-SIM)

References

1. Tait, Don (25 August 2016). "Smart card IC shipments to reach 12.8 billion units in 2021" (https://technology.ihs.com/582859/smart-card-ic-shipments-to-reach-128-billion-units-in-2020). *IHS Technology*. IHS Markit. Retrieved 24 October 2019.

2. Chen, Zhiqun (2000). *Java Card Technology for Smart Cards: Architecture and Programmer's Guide* (https://books.google.com/books?id=qaG0bwxJ-DEC&pg=PA3). Addison-Wesley Professional. pp. 3–4. ISBN 9780201703290.
3. Veendrick, Harry J. M. (2017). *Nanometer CMOS ICs: From Basics to ASICs* (https://books.google.com/books?id=Lv_EDgAAQBAJ&pg=PA315). Springer. pp. 315, 481–2. ISBN 9783319475974.
4. "3GPP specification: 51.011" (http://www.3gpp.org/dynareport/51011.htm). Retrieved 29 April 2016.
5. "3GPP specification: 31.102" (http://www.3gpp.org/dynareport/31102.htm). Retrieved 29 April 2016.
6. Asif, Saad Z. (2011). *Next Generation Mobile Communications Ecosystem*. John Wiley & Sons. p. 306. ISBN 978-1119995814.
7. "G&D – History of Giesecke & Devrient" (http://www.gi-de.com/usa/en/about_g_d/company/history/history.jsp). Retrieved 29 April 2016.
8. "Official Publication of the International Card Manufacturers Association February 2017 Volume 27 No1" (https://s3-us-west-2.amazonaws.com/pageturnpro.com/Publications/201703/1354/77336/PDF/131328561544014816_ICMAFebCM12017Final.pdf) (PDF). Retrieved 28 May 2017.
9. "Ericsson Mobility Report November 2015" (https://www.ericsson.com/res/docs/2015/mobility-report/ericsson-mobility-report-nov-2015.pdf) (PDF). Retrieved 28 May 2017.
10. "GSMA Embedded SIM and RSP" (http://www.gsma.com/rsp/). Retrieved 28 May 2017.
11. "ETSI TS 102 241: UICC API for Java Card™ Release 13" (https://www.etsi.org/deliver/etsi_ts/102200_102299/102241/13.00.00_60/ts_102241v130000p.pdf) (PDF). Retrieved 8 August 2019.
12. "Specifications Archive: Secure Element (Card)" (https://globalplatform.org/specs-library/?filter-committee=se). *GlobalPlatform*.
13. "3GPP specification: 11.11" (http://www.3gpp.org/dynareport/1111.htm). Retrieved 29 April 2016.
14. ITU-T, ITU-T Recommendation E.118, The international telecommunication charge card, Revision history (http://www.itu.int/rec/T-REC-E.118), Revision "05/2006" (http://www.itu.int/rec/dologin_pub.asp?lang=e&id=T-REC-E.118-200605-I!!PDF-E&type=items)
15. ETSI, ETSI Recommendation GSM 11.11, Specifications of the SIM-ME Interface, Version 3.16.0 (http://www.3gpp.org/ftp/Specs/archive/11_series/11.11/1111-3G0.ZIP)
16. "Operational Bulletin No. 1163 (1.I.2019)" (https://www.itu.int/pub/T-SP-OB.1163-2019). *www.itu.int*. Retrieved 5 January 2019.
17. "List of issuer identifier numbers for the international telecommunication charge card (in accordance with Recommendation ITU-T E.118 (05/2006))" (https://www.itu.int/pub/T-SP-E.118-2018). *International Telecommunication Union*. 5 January 2015.
18. "Hackers crack open mobile network" (https://www.bbc.co.uk/news/technology-13013577). bbc.co.uk. 20 April 2011. Retrieved 13 August 2011.
19. "What is a microsim card?" (https://archive.today/20130222172411/http://simonlypro.nl/what-is-a-microsim-card-en/). SimOnlyPro.nl. Archived from the original (http://simonlypro.nl/what-is-a-microsim-card-en/) on 22 February 2013. Retrieved 14 October 2012.
20. Gaby Lenhart (1 April 2006). "The Smart Card Platform" (http://docbox.etsi.org//Workshop/2006/Salud%20Mexico/Gaby%20Lenhart%20-%20CENETEC_2006_04.ppt). ETSI Technical Committee Smart Card Platform (TB SCP). Retrieved 30 January 2010. "SCP is co-operating on both technical and service aspects with a number of other committees both within and outside the telecommunications sector."
21. Segan, Sascha (27 January 2010). "Inside the iPad Lurks the 'Micro SIM' " (https://www.pcmag.com/article2/0,2817,2358489,00.asp). *PC Magazine*. Retrieved 30 January 2010.

22. "DRAFT Report of the SMG9 UMTS Working Party, meeting #7 hosted by Nokia in Copenhagen, 15–16 December 1998" (http://www.3gpp.org/ftp/TSG_T/WG3_USIM/TSGT3_01/docs/t3-99003.pdf) (PDF). 3GPP. 25 January 1999. Retrieved 27 January 2010. "One manufacturer stated that it may be difficult to meeting ISO mechanical standards for a combined ID-1/micro-SIM card."
23. Antipolis, Sophia (8 December 2003). "New form factor for smart cards introduced" (https://web.archive.org/web/20100426104206/http://www.smartcardstrends.com/det_atc.php?idu=287). SmartCard Trends. Archived from the original (http://www.smartcardstrends.com/det_atc.php?idu=287) on 26 April 2010. Retrieved 30 January 2010. "The work item for the so-called Third Form Factor, "3FF", was agreed, after intensive discussions, at the SCP meeting held last week in London."
24. How to make MicroSIM (https://www.youtube.com/watch?v=6B0G_qjebJY) on YouTube
25. Dr. Klaus Vedder (18 January 2012). "The UICC – Recent Work of ETSI TC Smart Card Platform" (https://web.archive.org/web/20170830041146/https://docbox.etsi.org/Workshop/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION/UICC_ETSISCP_Vedder.pdf) (PDF). ETSI. p. 12. Archived from the original (http://docbox.etsi.org/workshop/2012/201201_SECURITYWORKSHOP/3_INTERNATIONAL_STANDARDIZATION/UICC_ETSISCP_Vedder.pdf) (PDF) on 30 August 2017. Retrieved 22 July 2012. "Thinner to allow adapters so that the 4FF can be "clicked" into adapters for use as a Plug-in SIM or 3FF SIM giving a kind of backward usability"
26. Virgin Mobile. "An important guide to inserting your SIM into your mobile" (https://web.archive.org/web/20180125015505/http://www.virginmobile.com/vm/media/images/howdoi/007017_Leaflet_113x127mm_des_v2_LR.pdf) (PDF). Archived from the original (http://www.virginmobile.com/vm/media/images/howdoi/007017_Leaflet_113x127mm_des_v2_LR.pdf) (PDF) on 25 January 2018. Retrieved 21 January 2017. "You may also have to use one of the enclosed adaptors. If you don't follow these guidelines your phone warranty could be invalidated. We're afraid we can't accept responsibility for any damage to your phone if you choose to ignore this advice."
27. Encryption Bug in SIM Card Can be Used to Hack Millions of Phones (http://securitywatch.pcmag.com/mobile-security/313914-encryption-bug-in-sim-card-can-be-used-to-hack-millions-of-phones), published 2013-07-21, accessed 2013-07-22
28. Rooting SIM cards (https://srlabs.de/rooting-sim-cards/), SR Labs, accessed 2013-07-22
29. "Black Hat USA 2013" (https://www.blackhat.com/us-13/briefings.html#Nohl). Retrieved 29 April 2016.
30. UPDATE 1-UN warns on mobile cybersecurity bugs in bid to prevent attacks (https://www.reuters.com/article/2013/07/21/mobile-hacking-idUSL6N0FR0JD20130721), Reuters, 2013-07-21, accessed 2013-07-21
31. "The Great SIM Heist – How Spies Stole the Keys to the Encryption Castle" (https://firstlook.org/theintercept/2015/02/19/great-sim-heist/). *The Intercept*. The Intercept (First Look Media). 19 February 2015. Retrieved 19 February 2015.
32. "Gemalto: NSA/GCHQ Hack 'Probably Happened' But Didn't Include Mass SIM Key Theft" (https://techcrunch.com/2015/02/25/gemalto-2/). *techcrunch.com*. 25 February 2015. Retrieved 2 April 2015.
33. "eUICC – The Future for SIM Technology" (https://podm2m.com/euicc-future-sim-technology/). *PodM2M*. 5 July 2019.
34. "Gemalto pioneers SIM reactivation" (http://globenewswire.com/news-release/2016/11/03/886048/0/en/Gemalto-pioneers-SIM-Reactivation-solution-to-help-operators-seamlessly-reconnect-with-lapsed-prepaid-subscribers.html). Retrieved 3 November 2016.
35. "A nation addicted to smartphones" (http://media.ofcom.org.uk/2011/08/04/a-nation-addicted-to-smartphones/). Ofcom.

36. "UK sales of SIM-only mobile contracts set a new record" (http://thefonecast.com/Home/TabId/61/ArtMID/538/ArticleID/6219/UK-sales-of-SIM-only-mobile-contracts-set-a-new-record.aspx). The Fone Cast. Retrieved 29 October 2012.
37. CCS 2016 (7 November 2016). "Keynote by Ross Anderson at CCS 2016" (https://www.youtube.com/watch?v=IbfG_KSlTD4) – via YouTube.
38. Heuler, Hilary. "Africa's new thin SIM cards: The line between banks and telcos just got thinner – ZDNet" (https://www.zdnet.com/article/africas-new-thin-sim-cards-the-line-between-banks-and-telcos-just-got-thinner/).

External links

- GSM 11.11 (http://www.3gpp.org/ftp/specs/html-info/1111.htm) – Specification of the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface.
- GSM 11.14 (http://www.3gpp.org/ftp/specs/html-info/1114.htm) – Specification of the SIM Application Toolkit for the Subscriber Identity Module-Mobile Equipment (SIM-ME) interface
- GSM 03.48 (http://www.3gpp.org/ftp/specs/html-info/0348.htm) – Specification of the security mechanisms for SIM application toolkit
- GSM 03.48 Java API (https://github.com/opentelecoms-org/gsm0348) – API and realization of GSM 03.48 in Java
- ITU-T E.118 (http://www.itu.int/rec/T-REC-E.118-200605-I/en) – The International Telecommunication Charge Card 2006 ITU-T