Smartjac Industries Inc. - Kanalvägen 1A
2nd floor
SE-194 61 Upplands Väsby
Sweden
www.smartjac.com / www.smartjac.biz

Phone: +46(8)41071230 - Email: order@smartjac.com

Smartjac Test (U) SIM card - Configure Your SIM card !

Brand: Smartjac Industries Inc
Product Code: SMATEST101

Short Description
You can quickly choose the options you need for your test SIM cards; mini 2FF, micro 3FF or nano 4FF form factor, network, algorithm, applications on the card, etc. You can also order and purchase some samples (10-20 pcs) if you only need a monir qty of sim cards prior larger batches of cards.

Description
General Card Physical Characteristics

Follows ISO 7816 containing standards (produced by International Standard Organization) for Integrated Circuit Cards with contacts (smart card). Supports class A (5V), B (3V), and C (1.8V) mobile equipment.
Communication protocol: ISO T=0.

Authentication Algorithm Milenage/Dummy XOR/Cave/Toak.

Minimum Compliance with

- Java Card™
- Java Card™ 2.1.1 API Specification.

- Java Card™ 2.1.1 Runtime Environment Specification.
- Java Card™ 2.1.1 Virtual Machine Architecture Specification.

Note: Java Card™ 2.2.1 available also.

GP2.1.1 (multi-SD support)

What is a SIM card ?

A subscriber identity module or subscriber identification module (SIM), widely known as a SIM card, is an integrated circuit 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 only needed for newer LTE-capable handsets. SIM cards can also be used in satellite phones, smart watches, computers, or cameras.

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.

A SIM card contains its **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 code (PUC) for PIN unlocking.

Specifications

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[1]) and USIM (TS 31.102) and **ETSI** for the further development of the physical card UICC.

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. 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. The introduction of Embedded SIM (**eSIM**) and Remote SIM Provisioning (**RSP**)from the GSMA 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

SIM chip structure and packaging
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.

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.
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, ETSI TS 102 241, ETSI TS 102 588, and ETSI TS 131 111. SIM toolkit applications were initially written in native code using proprietary APIs. To provide interoperability of the applications, ETSI chose Java Card. Additional standard size and specifications of interest are maintained by GlobalPlatform.

Data and Techical Info
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 (Ki), 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)

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 'saw' 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

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. Each SIM is internationally identified by its integrated circuit card identifier (ICCID). 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. Its layout is based on ISO/IEC 7812. According to E.118, the number is up to 22 digits long, including a single check digit calculated using the Luhn algorithm. However, the GSM Phase 1 defined the ICCID length as 10 octets (20 digits) with operator-specific structure.

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, 1–3 digits, as defined by ITU-T recommendation E.164.
Issuer identifier, 1–4 digits.
Individual account identification

Individual account identification number. Its length is variable, but every number under one IIN has the same length.

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 is No. 1163 from 1 January 2019).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.

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 (Ki)

The Ki is a 128-bit value used in authenticating the SIMs on a GSM mobile network (for USIM network, you still need Ki but other parameters are also needed). Each SIM holds a unique Ki assigned to it by the operator during the personalization process. The Ki 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 Ki 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 Ki. This, by design, makes using the SIM card mandatory unless the Ki can be extracted from the SIM card, or the carrier

is willing to reveal the Ki. In practice, the GSM cryptographic algorithm for computing SRES_2 from the Ki has certain vulnerabilities that can allow the extraction of the Ki from a SIM card and the making of a duplicate SIM card.

Authentication process

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.
The operator network searches its database for the incoming IMSI and its associated Ki.
The operator network then generates a random number (RAND, which is a nonce) and signs it with the Ki 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 Kc (64 bits).
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 Ki, producing SRES_2 and Kc, which it gives to the mobile equipment. The mobile equipment passes SRES_2 on to the operator network.
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. Kc is used to encrypt all further communications between the mobile equipment and the network.

Location area identity

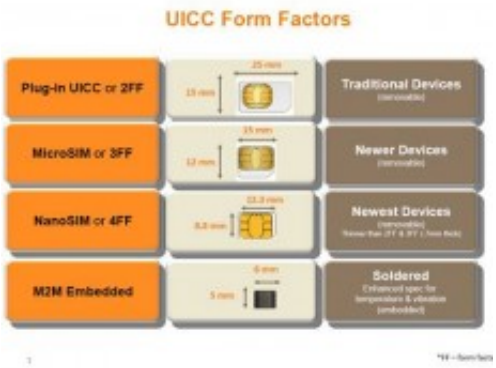
The SIM stores network state information, which is received from the Location Area Identity (LAI). Operator networks are divided into Location Areas, each having a unique LAI number. When the device changes locations, it stores the new LAI to the SIM and sends it back to the operator network with its 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.



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

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 (0.03
	Mini-SIM (2FF)	1996	ISO/IEC 7810:2003, ID-000	25 mm (0.98 in)	15 mm (0.59 in)	0.76 mm (0.03
	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 (0.03
	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 (0.02
	Embedded-SIM (eSIM)		JEDEC Design Guide 4.8, SON-8 ETSI TS 103 383 V12.0.0 GSMA SGP.22 V1.0	6 mm (0.24 in)	5 mm (0.20 in)	

Embedded-SIM (eSIM)

An embedded-SIM (**eSIM**) or embedded universal integrated circuit card (**eUICC**) 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 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.

eSIM is a global specification by the **GSMA** which enables remote SIM provisioning of any mobile device, and GSMA defines eSIM as the SIM for the next generation of connected consumer device, and networking solution using eSIM technology can be

widely applicable to various IoT scenarios, including connected cars (smart rearview mirror, OBD, vehicle hotspot), AI translator, Mi-Fi device, smart earphone, smart metering, tracker, DTU, bike-sharing, advertising player, and video surveillance devices, etc.

The GSMA had been discussing the possibilities of a software-based SIM card since 2010. While Motorola noted that eUICC is geared at industrial devices, Apple "disagreed that there is any statement forbidding the use of an embedded UICC in a consumer product." In 2012, The European Commission has selected the Embedded UICC format for its in-vehicle emergency call service known as eCall. All new car models in the EU must have one by 2018 to instantly connect the car to the emergency services in case of an accident. Russia has a similar plan with the GLONASS (national satellite positioning system) called ERA-GLONASS. Singapore is seeking public opinions on introducing eSIM as a new standard as more compatible devices enter the market.

Apple implemented eSIM support in its Apple Watch series 3 and second generation iPad Pro devices. In October 2017, Google unveiled the Pixel 2, which added eSIM support for use with its Project Fi service.The following year, Apple released the iPhone XS and iPhone XR with eSIM support. eSIM support on iPhone requires iOS 12.1 or later.

Plintron implemented eSIM4Things product based on eSIM support for the devices and available in 28 countries