



www.PhoneVolts.ie
28 North Lotts, Dublin 1, Ireland
Tel: 01 8728722
Email: info [AT] phonevolts.com

PhoneVolts is owned and operated by GSMsolutions.ie



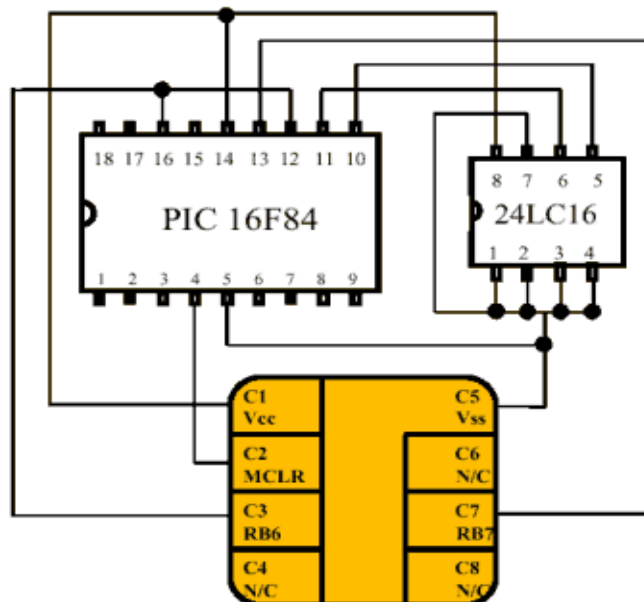
SIM Card's

A Subscriber Identity Module (SIM) is a removable smart card, available in two standard sizes. The first the size of a credit card (85.60 mm × 53.98 mm x 0.76 mm), while its more popular mini version has a width of 25 mm, a height of 15 mm, and a thickness of 0.76 mm. SIM cards store securely the key identifying a mobile phone service subscriber.

The SIM card allows users to change phones easily by removing the SIM card and inserting it into another mobile phone, thereby eliminating the need for activation of the new mobile phone on the network. The use of SIM card is mandatory in the GSM world. The equivalent of a SIM in UMTS is called the Universal Integrated Circuit Card (UICC), whereas the Removable User Identity Module (RUIM) is more popular in the CDMA world.

CONTACT DESCRIPTION

Pin#	Name	Function
C1	Vcc	Power Supply
C2	MCLR	Master Clear
C3	RB6/Osc1	Clock Input
C4	N/C	No Connect
C5	Vss	Ground
C6	N/C	No Connect
C7	RB7	Data I/O
C8	N/C	No Connect



Memory storage size

Typical low cost SIM card (GSM 11.11 only) has little memory, 2-3 KB (telephone directory and so on). Such data used by phone directly. The market segment of low cost SIM shrunk constantly.

SIMs with additional applications (GSM11.14) are available in many storage sizes, the largest being the 512 KB SIM. Smaller sized SIMs such as the 32 KB and 16 KB are most prevalent in areas with less-developed GSM networks. There are also Large Memory SIMs, in the order of 128 - 512 megabytes.

Operating systems

SIM operating systems come in two main flavors: Native and Java. Native SIMs are based on proprietary, vendor specific software whereas (There is typically a low cost SIM card market segment), the Java SIMs are based on the Java programming language. Java cards have the advantage of being hardware independent and interoperable.

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). The SIM also stores other carrier specific data such as the SMSC (Short Message Service Centre) number, Service Provider Name (SPN), Service Dialing Numbers (SDN), and Value Added Service (VAS) applications.

ICCID

Each SIM is internationally identified by its ICCID (International Circuit Card ID). ICCIDs are stored in the SIM cards and are also engraved or printed on the SIM card body during a process called personalization.

IMSI

SIM cards are identified on their individual operator networks by holding a unique International Mobile Subscriber Identity. Mobile operators connect mobile phone calls and communicate with their market SIM cards using their IMSI.

Authentication key

The Ki is a 16 byte value used in authenticating the SIMs on the mobile network. Each SIM holds a unique Ki assigned to it by the operator during the personalization process. The Ki is also stored on a database (known as Home Location Register or HLR) on the carrier's network.

Authentication process

On mobile startup the SIM sends its IMSI to the Mobile Operator requesting access and authentication.

The operator network searches its database for the incoming IMSI and its associated Ki.

The operator network then generates a Random Number (Rand) and signs it with the SIM's Ki computing another number known as Signed Response (SRES_1)

The operator network then sends the RAND to the SIM card that also signs it with its Ki and sends the result (SRES_2) back to the operator network.

The operator network then compares its computed SRES_1 with the SIMs computed SRES_2. If the two numbers match the SIM is authenticated and granted access to the operator's network. The GSM "crypto" algorithm of computation SRES_2 has a weak point. It enable extract Ki from SIM card and make duplicate of SIM card SIM_cloning.

Location area identity

The SIM stores network state information which is broadcast to it from the network, such as the Location Area Identity (LAI). Operators networks are divided into Location Areas, each having a unique LAI number. When the Mobile changes its location from one Location Area to another it stores its new LAI in SIM and sends it to the operator network to inform network with its new location. If the handset is turned off and back on again it will take data off the SIM and search for the LAI it was in. This saves time by avoiding having to search the whole list of frequencies that the telephone normally would.