What is a SIM card?

A SIM card, also known as a **subscriber identity module**, is a subscriber identity module application on a smartcard that stores data for GSM/CDMA Cellular telephone subscribers. Such data includes user identity, network authorization data, personal security keys, contact lists and stored text messages.

Security features include Authentication and encryption to protect data and prevent eavesdropping.

The smartcard with Subscriber identity module application is generally known as **SIMCARD.** But, In reality, the SIM is effectively a mass-market smartcard.

When the SIM is viewed as a smartcard, it opens up security possibilities that resonate far beyond the mobile world.

By combining stored evidence of identity (such as a key) with personal information only the user will know (a password, for example), it offers the same two-tier authorisation provided by smartcards.

It is becoming clear that the SIM --- a feature unique to the mobile world --- has applications far beyond those for which it was originally designed. The clue is in the name --- Subscriber Identity Module. It was created to remotely authenticate users to the network and to the billing systems that allow operators to generate revenues from voice traffic.

The GSM standards as specified by ETSI requires authentication of a mobile subscriber through a secure device (the SIM card).

Functionality of the SIM card?

The SIM card performs the following valuable functions:

1) **Identification** of a subscriber: The IMSI programmed on the SIM card, is the identity of a subscriber. Each IMSI is mapped to a mobile number and provisioned on the HLR to allow a subscriber to be identified.
2) **Authentication** of a subscriber: This is a process, where, using the authentication algorithm (COMP128V3 for 2/2.5 G GSM, CAVE for CDMA and Milenage for 3G) on the SIM card, a unique response is provided by each subscriber based on IMSI, Ki (stored on SIM) and RAND (provided by network). By matching this response with values computed on the network a legal subscriber is logged on to the network and he or she can now make use the services of the mobile service provider.
3) **Storage**: To store phone numbers and SMS.
4) **Applications**: The SIM Tool Kit or GSM 11.14 standard allows creating applications on the SIM to provide basic information on demand and other applications for m-commerce, chatting, cell broadcast, phonebook backup, location based services etc.

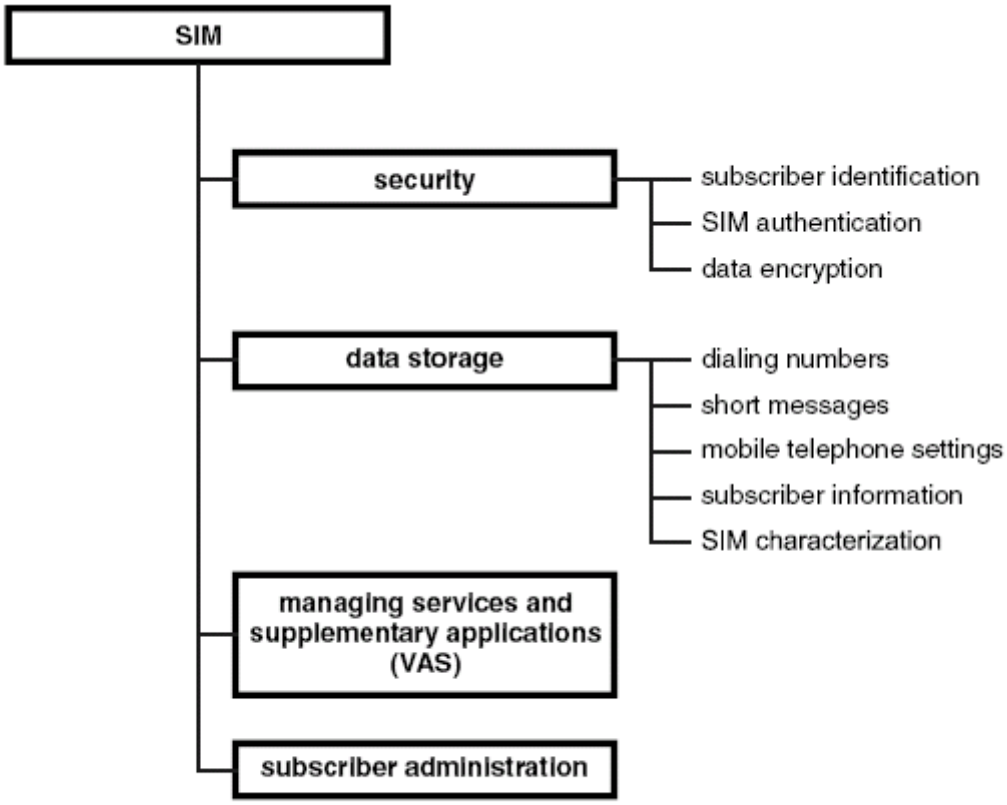

Figure 13.10 Classification of the basic functions of the SIM in the GSM system

Subscriber information, such as the IMSI (International Mobile Subscriber Identity), is stored in the Subscriber Identity Module (SIM).

The Subscriber Identity Module (SIM) can be used to store user-defined information such as phonebook entries.

One of the advantages of the GSM architecture is that the SIM may be moved from one Mobile Station to another. This makes upgrades very simple for the GSM telephone user.

Why is the SIM card secure?

SIM card in reality is a mass market smartcard with a subscriber identity module application. SIM Cloning can not be confused with smartcard cloning. It is not possible to clone the smartcard and only data can be read when application allows the reading of the data.(SIM Cloning is covered below)

Smartcard is very secure and provides

i) the secure loading of the applications
ii) Secure data storage for the application data and application cryptographic keys
iii) Secure Crypto operation support.

However, Application security depends on the application design and smartcard only provides a secure platform for developing secure applications. The security of smart card is similar to the security offered by HSM(Hardware security module).

Security of Subscriber Identity Module(SIM application)

The Presence of **Cryptographic algorithm and secret key in SIM card makes the SIM card secure.**
The most sensitive information of SIM card is the cryptographic algorithm A3, A8, secret Ki, PIN, PUK and Kc. A3, A8 algorithm were written into the SIM card in the producing process, and most people could not read A3, A8 algorithm. HN code could be settled by the phone owners. PUK code is held by the operator. Kc was derived in the process of encryption from Ki.

The other factors which make the SIM secure are….

PIN and PUK:
PIN –Personal Identification Number
2 PINs exist (PIN 1 and PIN2)
Limited attempts on PIN access
PUK –PIN Unblocking Code
Resetting PUK, resets PIN and the attempt counter
Too many attempts on PUK blocks use permanently

Two ways of Storing Data in SIM

1. As GSM Files
   The data used for Telco and GSM operation are all stored over the files.
   Telco/operator can change the Data this file through RFM in a secure channel.
   Only upon successful verification of file access condition a file can be read.
   All files are protected by access conditions.
2. As application data within an STK application as instance data.
   mChek stores all its secured encrypted information within application data. All the information stored is in persistent objects. Only mChek Server can access these data through mChek OTA platform.

Further, data on the SIM is protected by Administrative keys which are in hexadecimal and it is proven, that to compromise the security of a SIM one requires physical access to the SIM, enormous supercomputing ability and lots of time to crack one single card.

Till date there are no instances of COMP128V3 (GSM), CAVE (CDMA) or Milenage (3G) being compromised.

The few reported cases in the media are of COMP128V1, which is phased out and it is acknowledged that this version has been hacked and with physical access it is possible to clone these cards.

The applications on the SIM(for GSMA)/RUIM(for CDMA) cards are protected by the same set of administrative keys and are hence subject the same levels of security.

In addition, the messages transmitted from the SIM can be encrypted with DES/TDES which are well accepted in banking industry as a secure encryption standard.

Additional security can be enforced by implementing more complex algorithms and digital certificates (issued by CA).

M-banking applications have been implemented across the world from Latin America to Europe to Asia.

What are the current SIM card capabilities in the Market Place ?

From the Year 2003, the SIM cards which were provided in the Market Place were Java 2.0, however, because there was no need of porting the application and due to commercial implications this was discontinued for about 2 years and has again started to be issued.

However, the market would have about 50% of the cards OTAC enabled
(Source: GemAlto).

Though this is the position in the market place, getting all the SIM cards which are OTAC enabled application portable compliant there is a lot of work that needs to be done with the customer's SIM card and each individual SIM vendor.
Operationally this is absolutely not feasible.

However, in the past we have seen with the 8K to 32K migration keeping in mind the kind of churn rate that we see in the Industry it will take about 3 years for all old SIM cards to move to a new Portable SIM card which can house secure banking applications.

Also Telecom Operators (Bharti Airtel has already started the exercise) can provide new secure applications in all new activations and also ensure that they are application portable compliant.

What needs to be done to ensure that the SIM cards in the Market Place can house safe banking based applications?

SIM(smartcard) provides the secure platform for developing a highly secure applications. The banking application should be designed with out any security loop holes by utilizing the secure storage and secure cryptographic operation provided by smartcard.

The Cryptographic keys used by the banking application can be loaded in to banking application data storage on the smartcard.

The Global Platform standards can be adopted for the design and development of Banking applications.

The SIM/RUIM is a device which is easy to distribute and cuts across the entire subscriber base of a mobile service provider. Secure applications on a SIM/RUIM address the entire base of a mobile service provider.

Conclusion

1. The current market scenario does not allow the SIM cards available in the market place to be ported with applications over the air.

2. New SIM card seeding would be required for this activity which some Telco's have already started working on.

3. SIM card is extremely secure as a mode and is ideal for Banking Applications to be ported on.