



SIM Card Report

4th General Body Meeting - MPFI

think
fresh.
deliver
more.

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.
- **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 authorization provided by smartcards.

Functionality of a SIM card

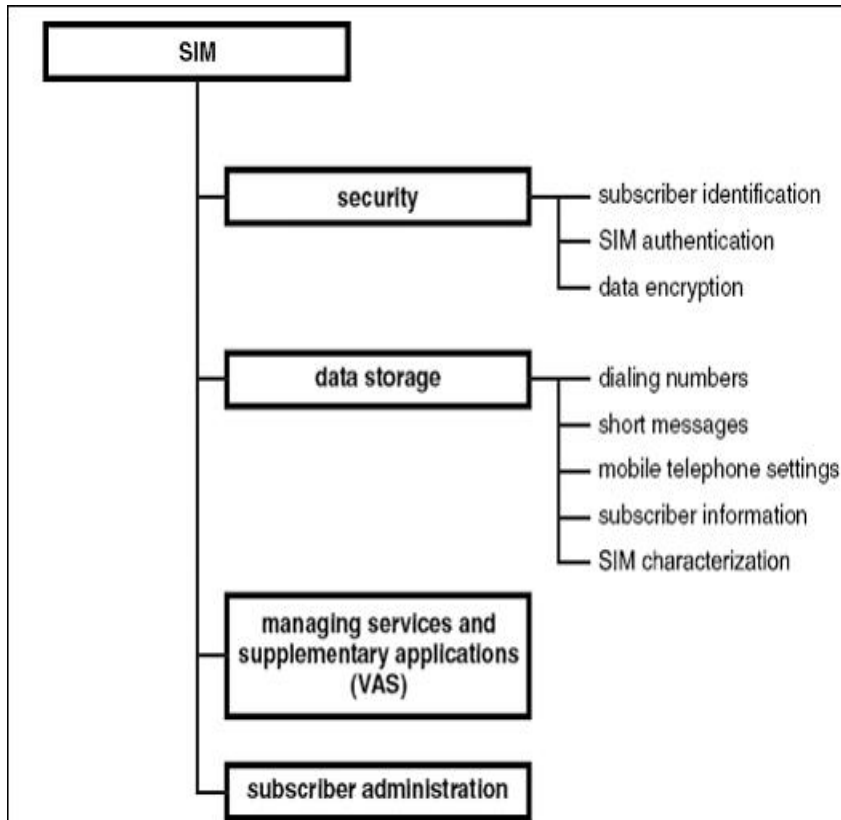


Figure 13.10 Classification of the basic functions of the SIM in the GSM system

• Functionalities

- Identification of the customer
 - 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.
- Authentication of the customer
 - 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).
- Storage
- 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

Current SIM 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.

Going Forward

- 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.

Conclusions

- SIM card is extremely secure as a mode and is ideal for Banking Applications to be ported on.
- The current market scenario does not allow the SIM cards available in the market place to be ported with applications over the air.
- New SIM card seeding would be required for this activity which some Telco's have already started working on.

The background is a solid dark red color. It features several faint, overlapping circles of varying sizes and colors (light red, orange, and yellow) scattered across the page. In the center, the words "Thank You" are written in a large, bold, white sans-serif font.

Thank You

think
fresh.
deliver
more.