Smart Cards As Building Blocks for Dependable Distributed Systems

Saurabh Bagchi

IEEE Presentation
April 24, 2003

What is the Smart Card?

- A "credit card" sized form factor with a small-embedded computer chip
- Provides memory and computational capacity
- Self-contained and therefore considered resistant to attacks

How Does It Work?

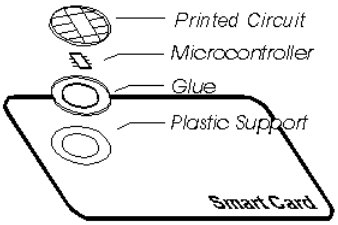
- Smart Card inserted into Card Acceptor Device (CAD), aka card reader
- Communicated with CAD through half duplex serial lines with a data rate of up to 9600 bits per second
- Commands follow standard ISO 7816 specifications
- Smart Card can get information from host computer, provide identification, do encryption/decryption, etc. etc.

Where Are They Used?

- All over the place, more so outside the US
- Medical applications: In Germany 80 million people can use smart cards when they go to the doctor
- Voting: In Sweden you can vote with your smart card
- Entertainment: Most DSS dishes in the U.S. have smart cards
- Telecommunications: Many cellular phones come with smart cards

Physical Structure & Life Cycle

- Physical structure specified by ISO Standard 7810, 7816



- Printed circuit provides five connection points for power and data
- Capability of Smart Card defined by IC chip
  - Microprocessor
  - ROM
  - RAM
  - EEPROM

Life Cycle

- OS and security keys inside each smart card which have different visibility rules
- Hence life cycle as card passes from manufacturer to application provider to user

Fabrication Phase
- Chip manufacturer
- Fabrication key (KF) added

Pre-personalization Phase
- Card supplier
- KF replaced by Personalization key (KP)
- Physical memory instructions disabled
Personalization lock (V_{PER}) written to prevent KP change

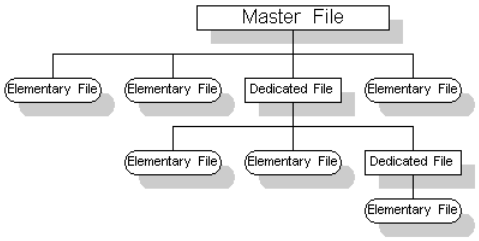
Personalization Phase
- Card issuer
- Information about Card holder stored
- Utilization lock V_{UTIL} written

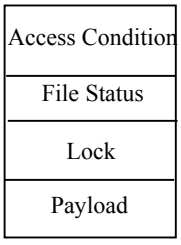
Utilization Phase
- Use by card holder
- Access controls & logical file access enabled

Invalidation Phase

Logical Structure

- Once card is in use, access of data through logical file structure





- Master File: Body contains header of all files in hierarchy.
- Dedicated File: Contains all immediate children. May also contain data.

Access Control

- OS allows horizontal or vertical movement in hierarchy
- Once file is selected, its header retrieved
- Access to data depends on access conditions being met