Tutorial Title	AKiS, Smart Card Operating System
Instructor information	Mustafa BAŞAK, TÜBİTAK-UEKAE PK. 74 Gebze/KOCAELİ – TURKEY Tel : +902626481335
Email contact	mbasak@uekae.tubitak.gov.tr

Instructor bio-sketch

BORN : 02/01/1966, Istanbul,

UNIVERSITY :
Electronics Engineering Department of Engineering Faculty, University of Hacettepe (B.S. 1987).

EXPERIANCE IN : Smart Cards Operating system, Crypto systems, Communication systems.

PERSONAL EXPERIENCE

TÜBİTAK-UEKAE : 2001 - ?

Duty : Project Manager
Duty related activities : Project Manager of the National Smart Card Operating System project (AKiS).

INFORM A.Ş. : 1999 - 2001

Duty : Software / Firmware Engineer
Duty related activities : Designed the control and communication control units of the UPS Systems. developed all SW programs of the UPS and Remote Control Units.

SIEMENS - SIMKO : 1995 - 1999

Duty : Software / Firmware Engineer
Duty related activities : Designed the control and communication control units of the Moduler Power Supply Systems RC-16 and developed all SW programs.

Alcatel BELL : 1993 - 1995

Duty : HdS engineer and B-ISDN test engineer.
Duty related activities : Worked in Broadband enginerring department (ATM dept.).
Designed the Basic Handler unit SW and self test SWs of the ATM modules.

Alcatel TELETAS : 1991 - 1993

Duty : Software Engineer
Duty related activities : Designed the control and communication control units of the Moduler Power Supply Systems MERT-2 and developed all SW programs.

ORTAS A.S. : 1991 (April - October, 7 months)

Duty : Project Advisor
Duty related activities : Worked in ISPBX project.

TELETAS : 1987 - 1990

Duty : Software Engineer
Duty related activities : Developed Network Layer and Consol unit (MMI) SWs of Teletas N-ISDN Telephone set.

Abstract

AKiS is a native smart card operating system which can be used in personal identification, digital sign and information security applications. AKiS capabilities are data storage, system authentication, encryption/decryption by using symetric (DES-ECB, 3DES-ECB) and asymetric (RSA1024, RSA2048) techniques and hash by using SHA-1 algorithm. It is not permitted to load the program into the EEPROM memory of the chip for the security reasons.

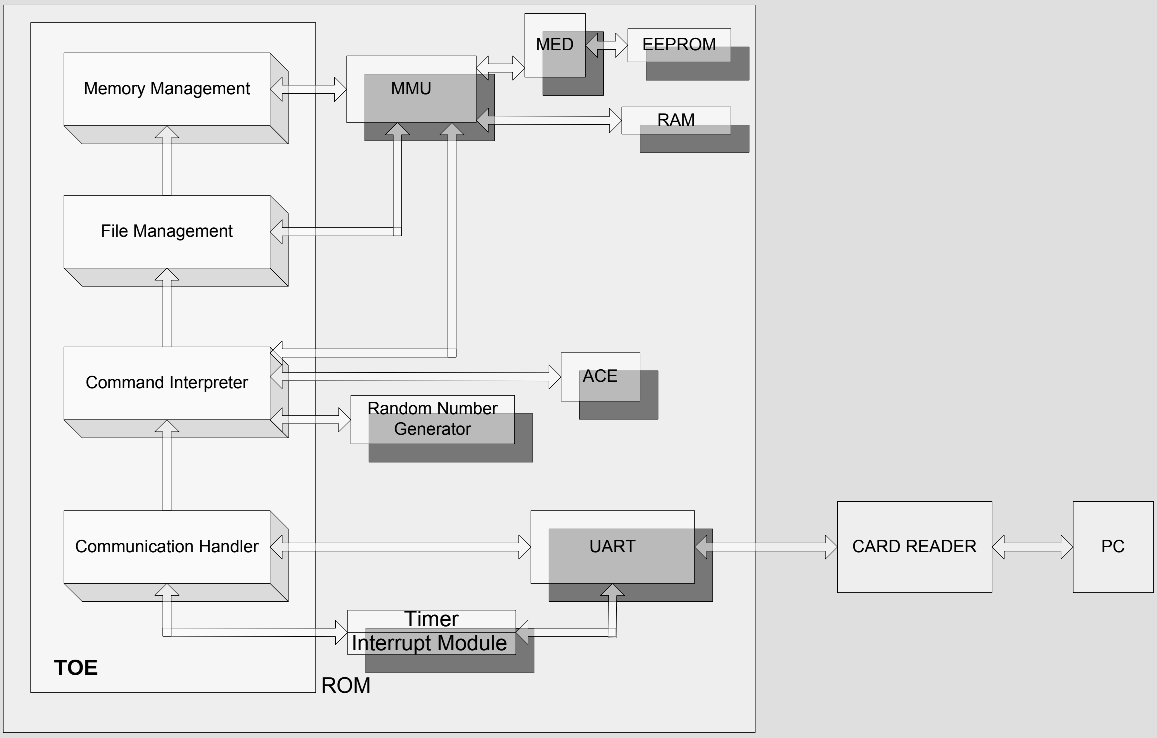
Outline

AKiS is a native smart card operating system. It is loaded into ROM part of the chip during the manufacturing phase. AKiS:

- Is loaded into ROM of the infineon's secure Smart Card chip which is SLE66CX680PE,
- Communicates with the PC via card reader according to ISO/IEC 7816-4 T = 1 protocol,
- Implements user and interface authentication,
- Is capable of binary file operations (open, write, read),
- Supports fixed length linear, variable length linear, fixed length cyclic file structures and file operations (open, write record, read record)
- Follows the life cycles (manufacturing, initialization, personalization, administration and operation) and operates functions according to the present life cycle
- Does not allow loading of executable files
- Encrypts, decrypts, digitally signs and verifies with RSA/DES/3DES cryptographic algorithms by using HW modules of the SLE66CX680PE
- Calculates SHA-1 hash.

AKİS components and Software structure is shown in the following figure.

- Memory Manager
- File Manager
- Command Interpreter
- Communication Handler



Tutorial Goals

- Smart Cards are the simpliest tools for Personal Information Security
- AKiS supplies Information security for applications via using symmetric and asymmetric cryptographic methodes.
- Public and Secret data is stored seperately via structured OS of AKIS
- AKIS has different security criterias for different application and user types in the life cycle;
    - AKİS Specific Initialization and Personalization Commands supply fast, secure and high capacity production
    - On request Personalization can be made independently
    - AKIS has a special phase (Administration Phase) that can be used to develop unique applicaitons (Format, Open Folder and Open File commads are used to create the file tree)
- Electronic tool for digital sign/verify applications.
- Electronic identification by using stored personal biometric data.