Overview

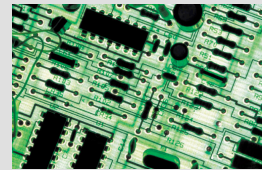## A. Hardware overview

CPUs, memory types, I/O, cryptographic co-processors, random number generators
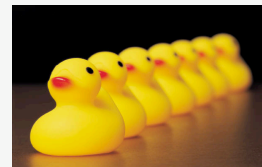
B. Communication modes and protocols
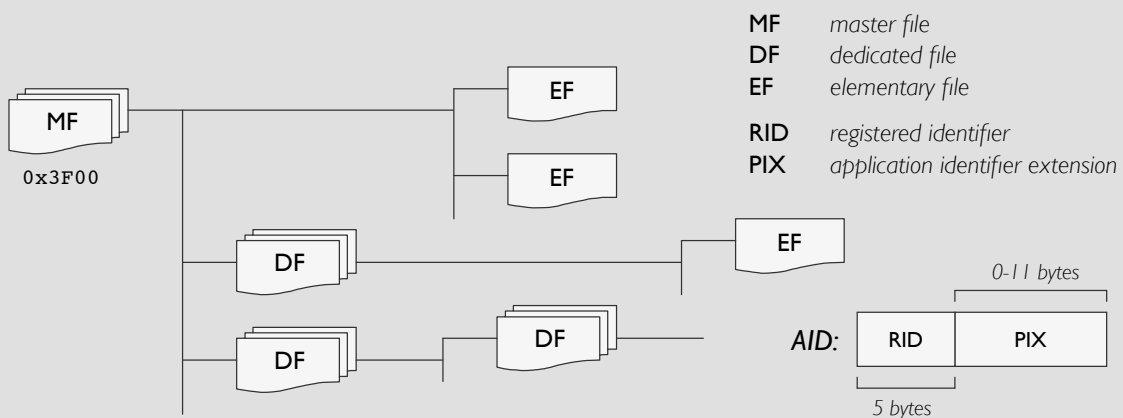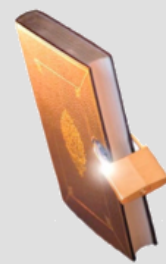
interaction model, contact-based vs. contact-less

C. Classification of smart-card operating systems

static vs. dynamic, file-system-based vs. object-oriented

C. Classification: Traditional

- **static, file-system-based, proprietary**
  - *proprietary operating system w/ static set of applications*
  - *standard application: ISO 7816-4 hierarchical file system*
    - file names
      - *2 bytes file identifiers (FID) − relative addressing*
      - *5-16 bytes application identifier (AID) − absolut addressing*

MF	*master file*
DF	*dedicated file*
EF	*elementary file*
RID	*registered identifier*
PIX	*application identifier extension*

MF
0x3F00

EF

EF

DF

EF

DF

DF

AID: | RID | PIX |
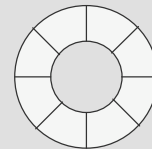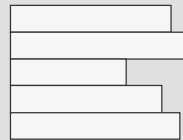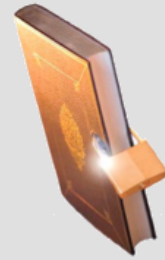
0-11 bytes

5 bytes

C. Classification: Traditional

- static, file-system-based, proprietary
  - *proprietary operating system w/ static set of applications*
  - *standard application: ISO 7816-4 hierarchical file system*
    - file names
      - *2 bytes file identifiers (FID) – relative addressing*
      - *5-16 bytes application identifier (AID) – absolut addressing*
    - file types
      - *transparent: unstructured binary, byte and block access*
      - *linear fixed: up to 254 records of identical size (1-254 bytes), random access*
      - *linear variable: up to 254 records of different sizes (1-254 bytes), random access*
      - *cyclic: identical to linear fixed but with changing record numbering*
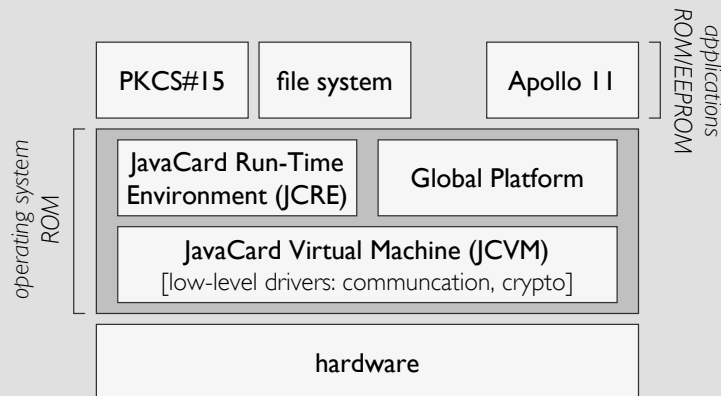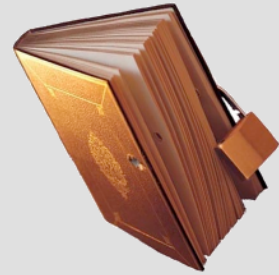

C. Classification: Traditional

- static, file-system-based, proprietary
  - *proprietary operating system w/ static set of applications*
  - *standard application: ISO 7816-4 hierarchical file system*
    - file names
      - *2 bytes file identifiers (FID) – relative addressing*
      - *5-16 bytes application identifier (AID) – absolut addressing*
    - file types
      - *transparent: unstructured binary, byte and block access*
      - *linear fixed: up to 254 records of identical size (1-254 bytes), random access*
      - *linear variable: up to 254 records of different sizes (1-254 bytes), random access*
      - *cyclic: identical to linear fixed but with changing record numbering*
    - file operations
      - *append, create/delete, invalidate/rehabilitate, lock, read/seek, write/update*

C. Classification: Modern

- dynamic, object-oriented, open standards
  - *standard-compliant operating system with open API*
  - *virtual machine abstracts from the underlying hardware*
  - *high-level object-oriented programming language*
  - *post-issuance application installation/deletion*

PKCS#15	file system		Apollo 11
JavaCard Run-Time Environment (JCRE)		Global Platform	
JavaCard Virtual Machine (JCVM) [low-level drivers: communcation, crypto]			
hardware			

applications ROM/EEPROM

operating system ROM

C. Classification: Modern

- dynamic, object-oriented, open standards
  - *standard-compliant operating system with open API*
  - *virtual machine abstracts from the underlying hardware*
  - *high-level object-oriented programming language*
  - *post-issuance application installation/deletion*

applet

JC/GP