

# Operační systémy čipových karet

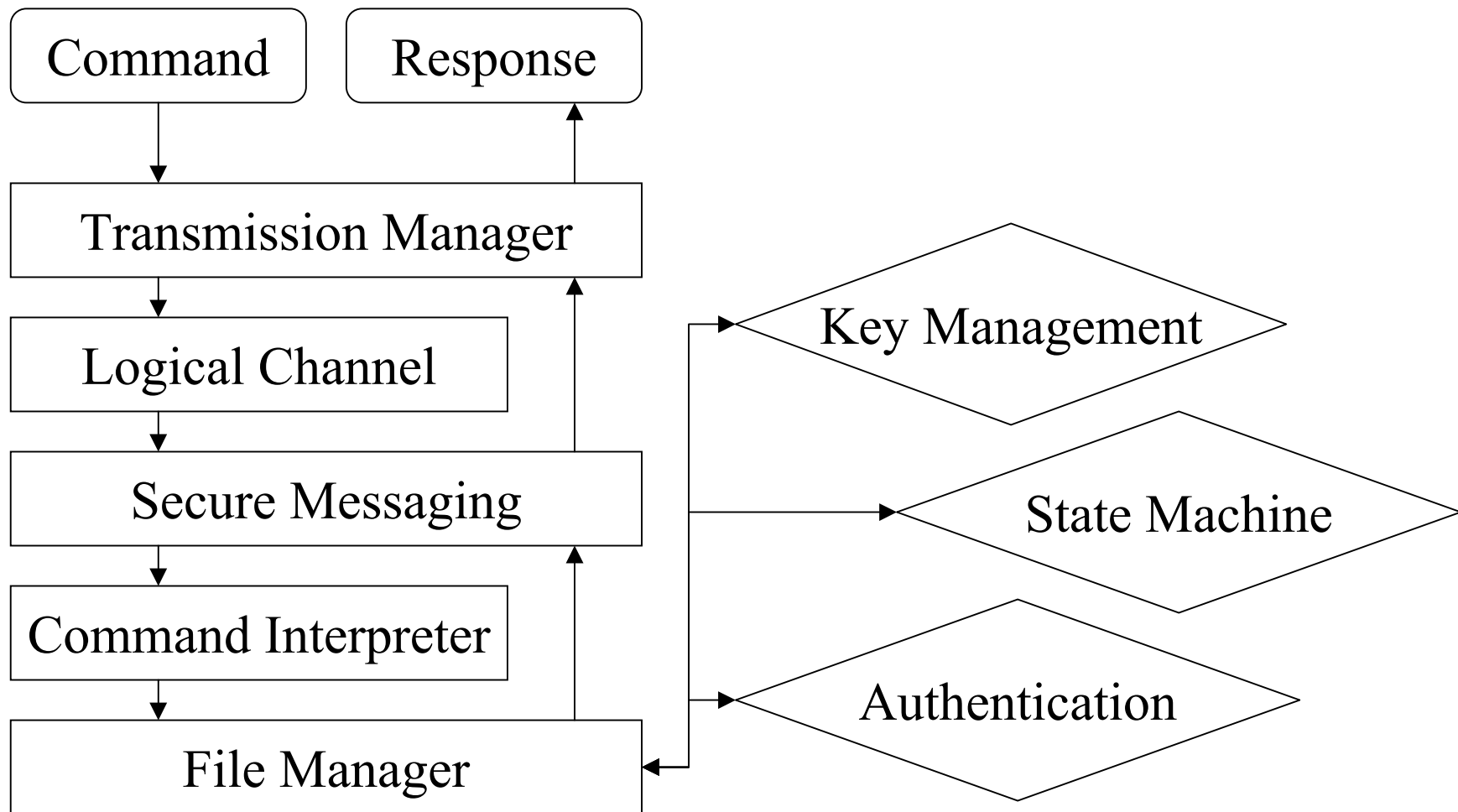
Ondřej Těthal

tethal@coprosys.cz

# Hlavní úkoly OS

- Dohled nad vykonáváním příkazů
- Přenos dat na kartu / z karty
- Správa souborů
- Správa a vykonávání kryptografických algoritmů

# Zpracování příkazu

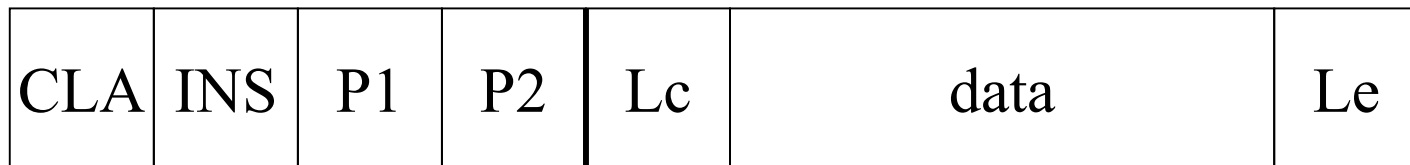


# Přenos dat

- Protokoly pro přenos dat
  - Kontaktní (podle ISO/IEC 7816-3)
    - Bytový přenosový protokol T=0
    - Blokový přenosový protokol T=1
  - Bezkontaktní (podle ISO/IEC 14443)
    - Blokový přenosový protokol T=CL
- Data se přenášejí ve formě APDU (Application Protocol Data Unit)

# Přenos dat - APDU

- Command APDU:



- Response APDU:

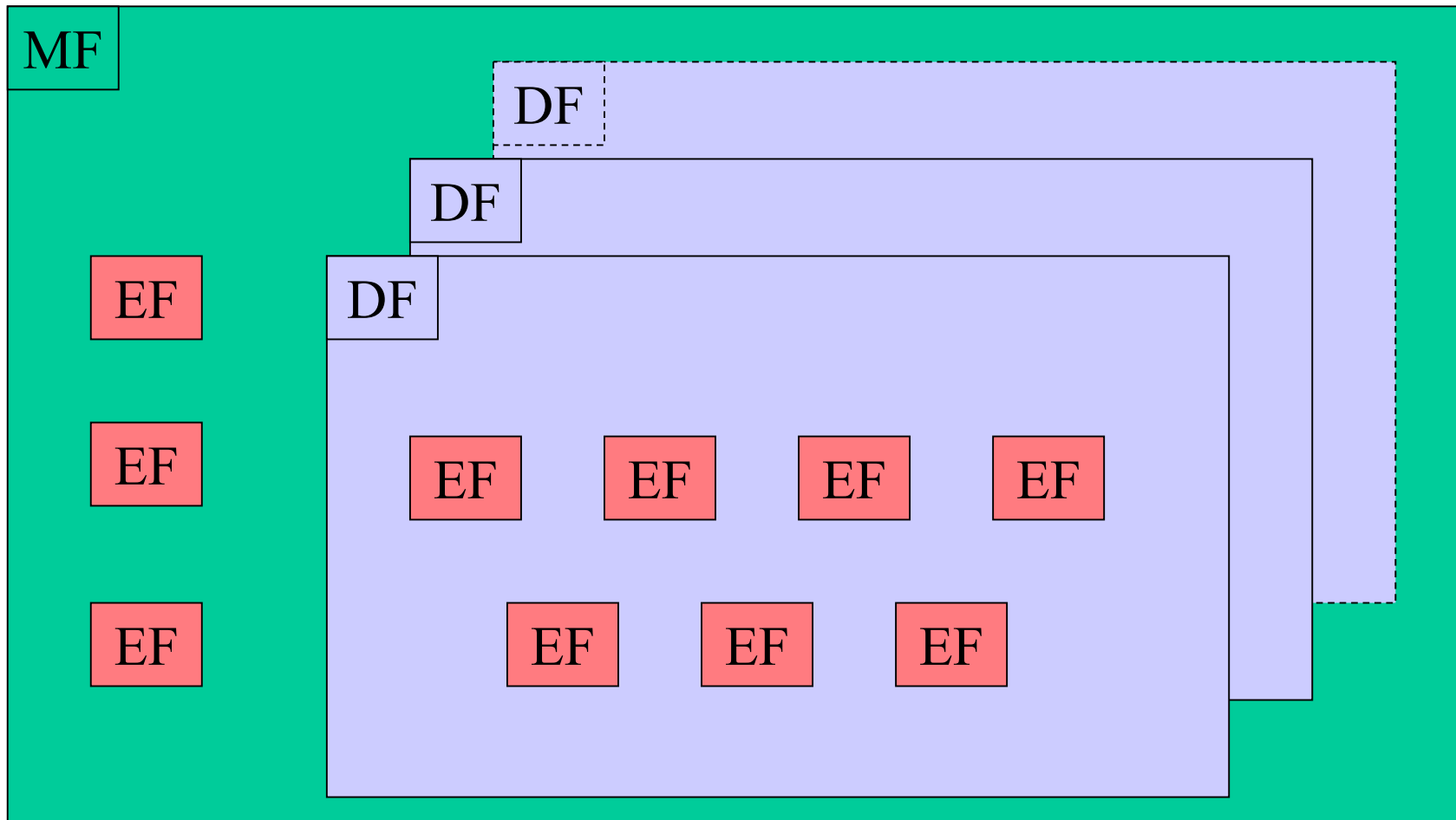


- CLAss
- INStruction
- Parameter 1-2
- Length Command
- Length Executed
- Status Word

# Správa souborů

- Typy souborů podle ISO/IEC 7816-4
  - MF (Master File)
  - DF (Dedicated Files)
  - EF (Elementary Files)
    - Internal EF
    - Working EF

# Hierarchie souborů



# Názvy souborů (1)

- Každý soubor má FID (File IDentifier)
  - 2 byty dlouhý
  - MF má vždy 3F00
  - 3FFF a FFFF jsou rezervované
- Short FID
  - Pouze EF
  - 5 bitů
  - Umožňují tzv. implicitní výběr souboru

# Názvy souborů (2)

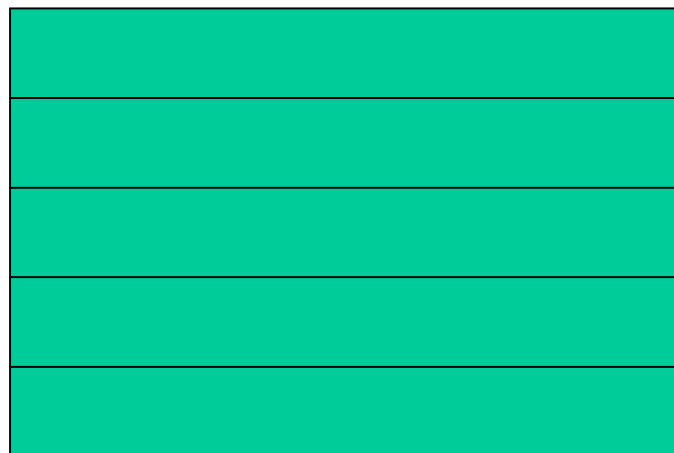
- DF Name
  - Pouze DF
  - 1 – 16 bytů
  - Typicky obsahují AID (Application IDentifier)
- AID (ISO/IEC 7816-5)
  - 5 bytů RID (Registered IDentifier), povinný
  - 0 – 11 bytů PIX (Proprietary application Identifier eXtension)

# Struktura EF souboru

- Linear fixed
- Cyclic
- Compute
- Transparent
- Object
- Linear variable
- Execute

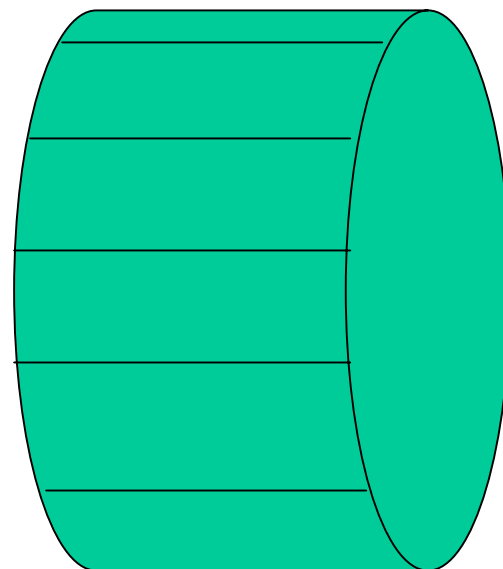
# Struktura EF – linear fixed

- Všechny záznamy stejně dlouhé (až 254 bytů)
- Se záznamem se pracuje jako s celkem
- Záznamy se číslují 1-254
- READ RECORD,  
UPDATE RECORD
- Př.: telefonní seznam



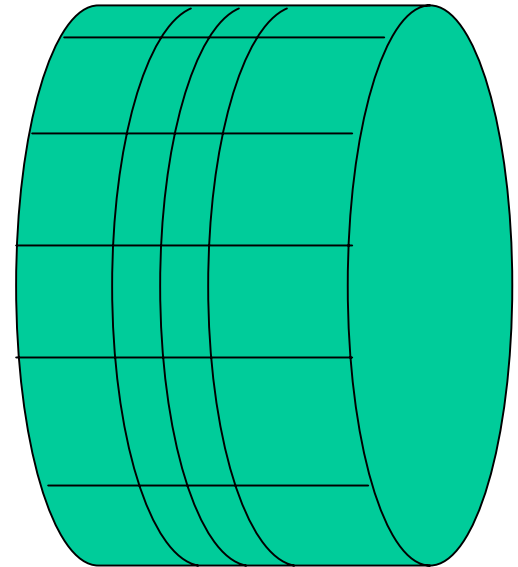
# Struktura EF – cyclic

- Všechny záznamy stejně dlouhé
- Zápis pouze na aktuální pozici
- Čtení libovolného záznamu
- READ RECORD, UPDATE RECORD
- Př.: seznam volaných čísel



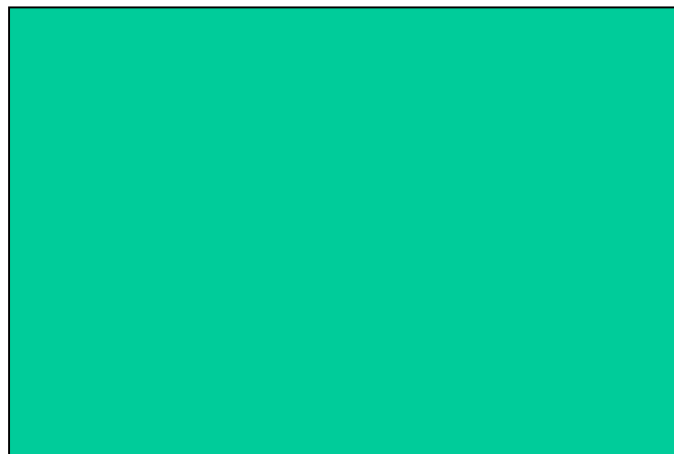
# Struktura EF – compute

- Všechny záznamy mají stejnou vnitřní strukturu – čítač, kontrolní součet, data
- Čtení jako u ‘cyclic’
- READ RECORD, INCREASE, DECREASE
- Př.: elektronická peněženka



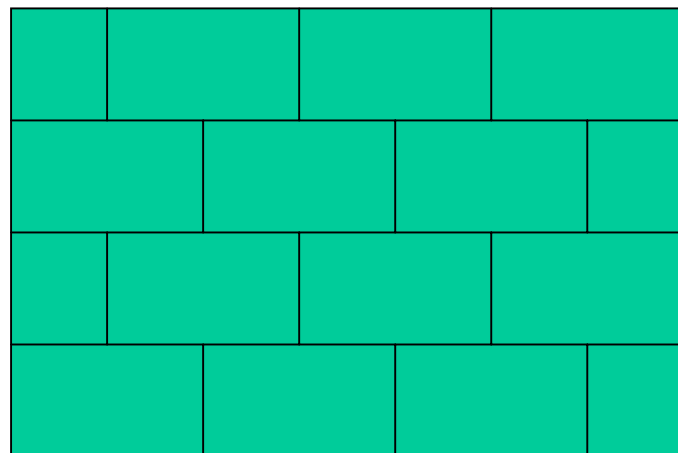
# Struktura EF – transparent

- Až 32.768 bytů
- Přímý přístup k datům
- READ BINARY,  
UPDATE BINARY
- Př.: fotografie



# Struktura EF – object

- Nejvýše jeden v každém DF
- Data uložena jako TLV objekty
- GET DATA, PUT DATA, ERASE OBJECT FILE
- READ BINARY, UPDATE BINARY



# Vytváření souborů

- Parametry příkazu CREATE FILE
  - Velikost souboru (po vytvoření nelze měnit)
  - Název (identifikátor) souboru
  - Struktura souboru (pouze pro EF)
  - Pravidla pro přístup k souboru (Access Conditions)
    - Pro každou operaci nad souborem zvlášť určují, za jakých okolností lze se souborem danou operaci provést
    - Lze stanovit přísnější podmínky pro T=CL

# Výběr souborů

- Vždy je vybrán právě jeden soubor
- Explicitní výběr
  - Příkaz SELECT FILE
  - Pomocí FID, příp. DF name
- Implicitní výběr
  - Pouze pomocí Short FID (tj. pouze EF), který je součástí jednotlivých příkazů pro přístup k souboru

# Autentizace

- Autentizace držitele – PIN (PUK)
  - Příkaz VERIFY
- Autentizace zařízení – 3DES, RSA
  - EXTERNAL AUTHENTICATE
- Autentizace karty – 3DES, RSA
  - INTERNAL AUTHENTICATE
- Vzájemná autentizace
  - MUTUAL AUTHENTICATE

# Stavový automat

- Různé stavové automaty pro MF a DF
- 16 stavů (0-15)
- Přejechod mezi stavy pomocí autentizačních příkazů
  - Definiuje se při ukládání klíčů na kartu
- Stav určuje, které operace lze provádět
  - Definiuje se při vytváření souborů (Access Conditions)

# Key Management (1)

- Globální klíč
  - Uložen v MF
  - Např. společný PIN pro všechny aplikace
- Default klíč – v případě více klíčů stejného typu lze jeden klíč nastavit jako default
  - Pokud prostředky mimo kartu neurčí specifický klíč, karta použije default

# Key Management (2)

- Derivované klíče
  - odvozené od master klíče a sériového čísla karty
- Session klíče
  - Jedinečné pro každou transakci
- Blokování klíče
  - Key Fault Presentation Counter (KFPC)

# Příklad (1)

- Aplikace pro menzy (jednoduchá elektronická peněženka)
- Na kartě jsou:
  - Stav účtu
  - Uživatelský PIN, který je vyžadován pro nákup
  - Administrátorský PIN, který je vyžadován při nabíjení
  - Symetrický klíč pro ověření pravosti terminálu pro dobíjení

# Příklad (2)

- Tabulka přechodů mezi stavy:

	0	1	2	3
Uživatelský PIN	1	1	1	1
Administrátorský PIN	-	-	3	-
EXT. AUTH.	2	2	-	-

# Příklad (3)

- Stav účtu je uložen v EF souboru se strukturou compute
- Přístupová práva:

	0	1	2	3
INCREASE	-	-	-	0
DECREASE	-	0	-	-
Změna uživatelského PIN bez znalosti předchozí hodnoty	-	-	0	0
Čtení stavu účtu	0	0	0	0

# Karetní aplikace

- Definice souborové struktury
  - Typy a velikosti souborů
- Obsah souborů
- Definice stavového automatu
  - Počet stavů a přechody mezi nimi
- Nastavení přístupových práv (AC)
  - k datům a klíčům

# OS s možností spouštění kódu

- Nativní kód
  - Rychlý, možnost změn (oprav) OS
  - Závislý na procesoru karty
  - Potenciálně nebezpečný
- Interpretovaný kód (Java Card)
  - Přenositelný kód
  - Nároky na paměť (6-8 kB)
  - Rychlost (20 – 40x pomalejší)

# Zdroje a odkazy

- Rankl, W., Effing, W.: Smart Card Handbook, Second Edition, John Wiley & Sons, Ltd, 2000
- StarCOS 2.5DI Reference Manual, Giesecke & Devrient GmbH
- David B. Everett: Smart Card Technology: Introduction to Smart Cards, Smart Card News Ltd, 1999
  - <http://www.smartcard.co.uk/resources/tutorials/sct-itsc.pdf>

Diskuse