ELECTRONIC PURSE APPLICATION REQUIREMENTS

Participants In An EP System

- purse providers
- purse holders
- load agents
- acquirers
- card issuers
- SAM issuers
- clearing house

Purse Provider

- provides & guarantees electronic value in card because it receives the amount from the purse holder
- responsible for the liability of the system
- responsible for the security of the system
  - purse
  - SAMs-PSAM, LSAM, PPSAM, perso SAM
- responsible for load and purchase devices
- responsible for activation & de-activation of purse & SAMs

Example of Purse Provider:
bank, telephone company, public transport company

Purse Holder

- a person that possesses the EP
- card not associated with a particular person - ananoymous
- card lost or stolen, EP can be used by others
- PIN not required

Question :

What if the card is not lost but not functional ?

Service Provider / Merchant

- sells goods or services to purse holder
- accept EP for payment
- equiped with purchase devices
- transactions stored in purchase devices
- sends transactions to purse provider
- receives payment in return
- pays a fee for the service provided

Load Agent

- a trusted agent of the purse provider
- enables load transaction with the holder’ s purse
- collects funds from purse holder on behalf of the purse provider
- typically a bank, a subsidary of the purse provider or the purse provider

Card Issuer

- responsible for the personalisation of EP
- manage and maintain card personalisation system
- receives personalisation input data from purse provider
- provides personalisation output data to purse provider
- can be a banking association, currency printing company or the purse provider himself

Acquirer

- provides the service of handling the transactions on behalf of the service provider / merchant
- provides and maintain the purchase devices
- charge a fee for the service
- usually a bank or the purse operator himself
- in same cases can also be a service provider eg telephone company

Purse Holder’ s Concerns

- is money debited according to transaction
- is money refundable if card is lost, non-functional or he no longer wants to use
- is money in the EP bearing interest
- anonymity
- is the EP user friendly
  - ease of use
  - universal usage
  - fast transaction

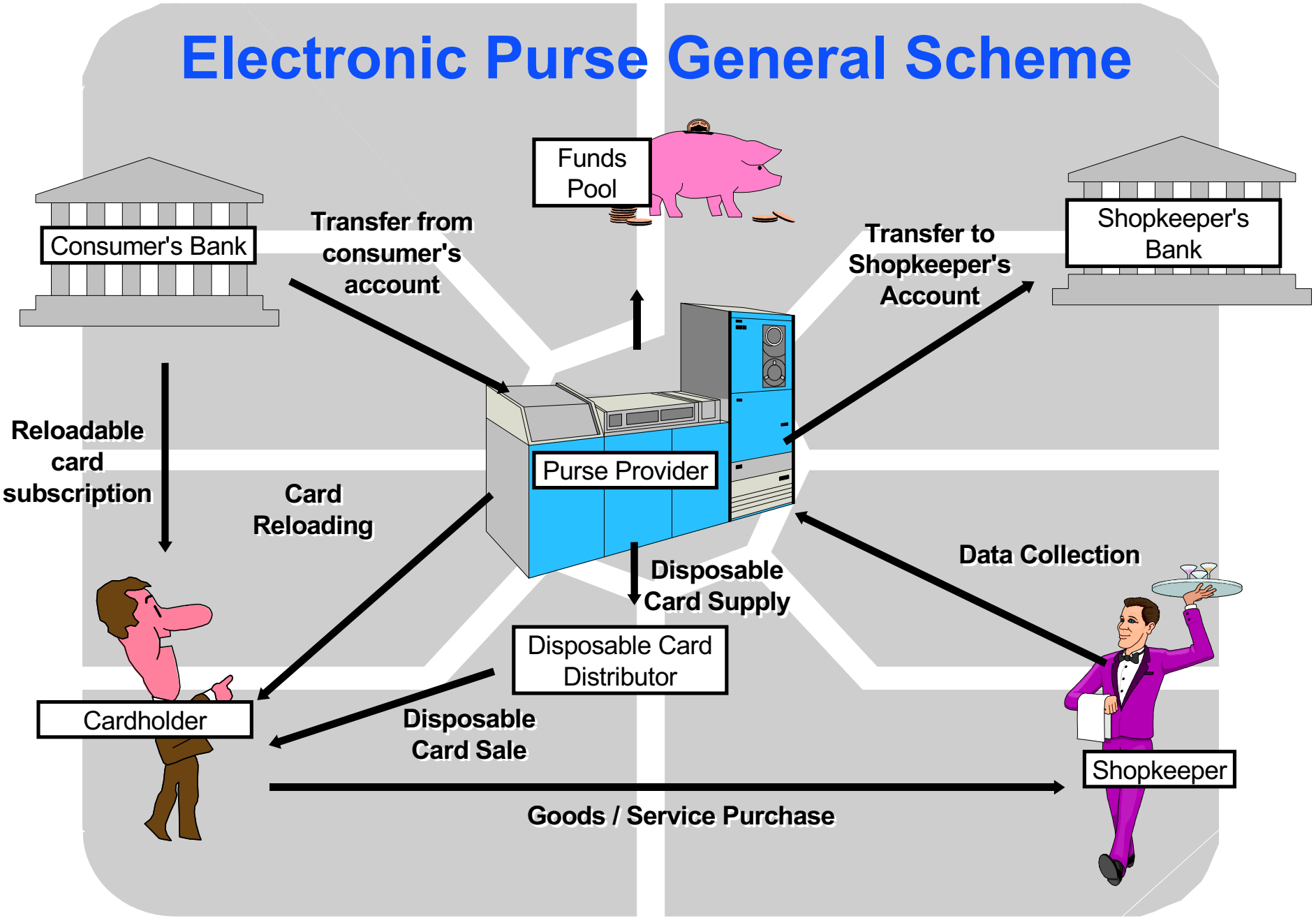
Service Provider’ s Concerns

- correct amount shown and debited
- reliablity of purchasing devices
- is payment guaranteed
- what is the cost and commission
- how long is the payment period
- how big is the card holder base
- user-friendlyness
  - ease of use
  - fast transaction
  - summary reports

Purse Provider’ s Concerns

- only pays for genuine transaction and only once per transaction
- not possible to create false value in the system
- money is indeed debited from the card for a debit transaction
- money is collected for credit / cancel debit transaction
- able to detect and control fraud if it happens
- is the system open
- cost of the system

Electronic Purse General Scheme



EP System Operational Flow

- purse holder buys card from load agent
- purse holder pays for services at service provider / merchant POS
- POS upload transaction to clearing house
- clearing house sorts & sends transactions according to purse providers & acquirers
- purse providers and acquirer acknowledges clearing house
- clearing house performs clearance for purse providers and acquirers

EP System Security Flow

- POS security init
  - merchant activation
  - blacklist validity
- POS authenticates EP
- EP authenticates POS
- POS checks EP validity
- POS checks blacklist
- POS checks purse holder (optional)
- POS computes terminal signature (S2)
- POS debits EP & log transaction automatically
- EP returns debit signature (S3)
- POS verifies that money is indeed debited
- PSAM accumulates transaction amount
- POS logs transaction records

Transaction Collection

- transaction collection can be on-line
  - via telephone line
- Transaction collection can be off-line
  - via merchant card
- POS sends transaction records & de-activated blacklisted EP IDs
- host download secured updated blacklist

Transaction Record Information

- POS transaction number
- POS ID & merchant ID
- transaction type
- transaction date / time
- transaction amount
- purse balance
- EP transaction number
- EP ID
- PDA signature
- EP debit signature
- other data required for audit

Acquirer Host Functions

- verify terminal merchant ID
- verify POS transaction number
- verify transaction date / time
- verify POS signature
- acknowledges clearing house
- settlement with merchants

Purse Provider Host Functions

- verify EP ID
- verify EP transaction number
- verify EP transaction date
- verify EP transaction type
- verify EP debit signature
- verify new balance = old balance + amount
- blacklist management
- acknowledges clearing house
- interfacing with card issuer (personalisation system)

Clearing House Functions

- collects transaction logs from POS
- blacklist management
  - consolidates blacklists from purse providers
  - download blacklists to POS
- sorting of transaction records
- upload purse provider’ s transaction & acquirer’ s transaction
- performs clearance after acknowledgement from purse providers & acquirers

How To Handle Micro-payment Transaction

- Micro-payment not cost-effective for processing
- nevertheless very important for the acceptance of cards & success of the system eg payphone, vending, copier
- micro-payment can be accumulated after debit verification by PSAM and credit to the respective purse providers
- at the end of the day, no longer a tiny amount

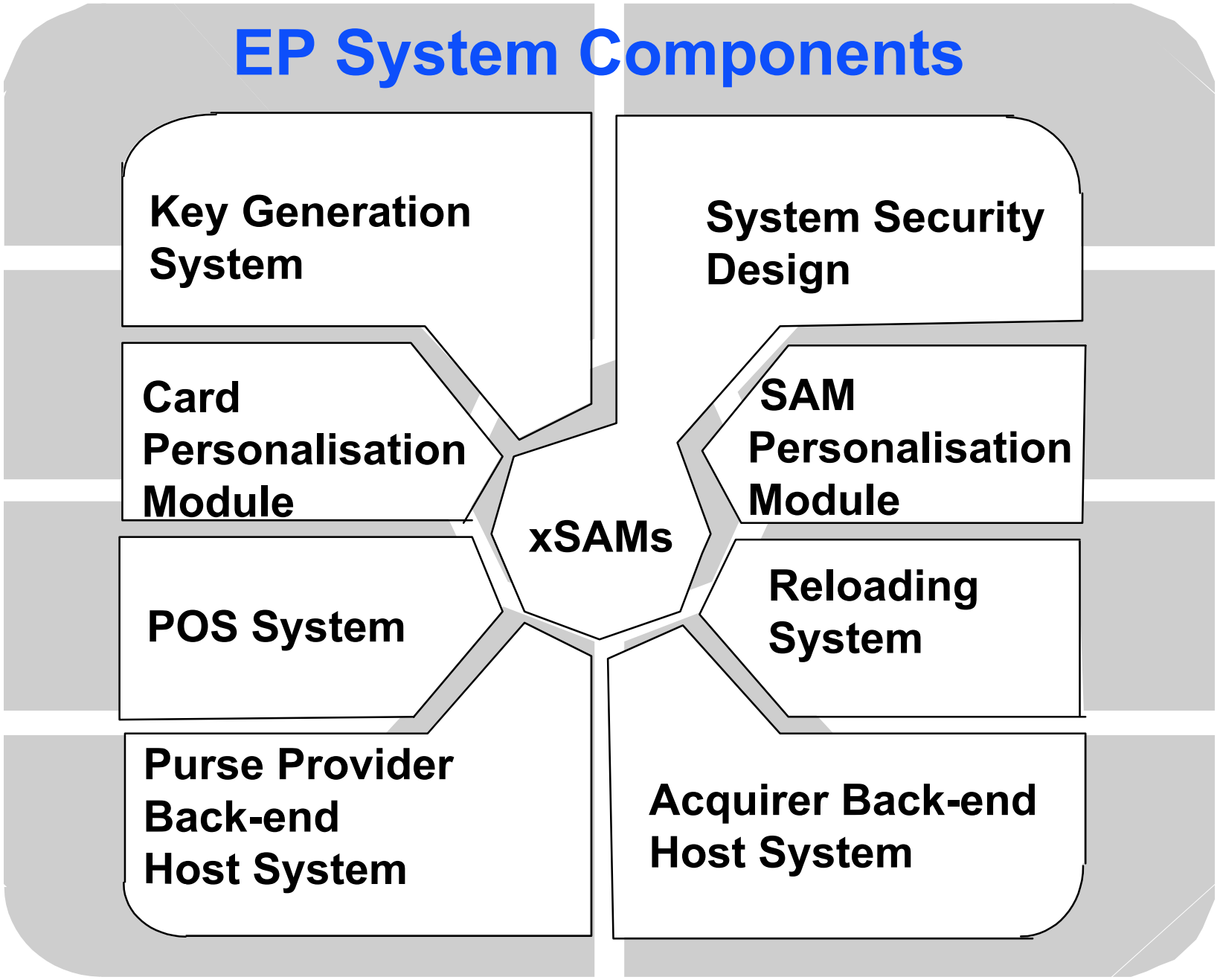
Question:

How to solve the problem of purse holder finishing the value, electronically destroy the card and claims from the purse provider ?

Micro-payment Transaction Security

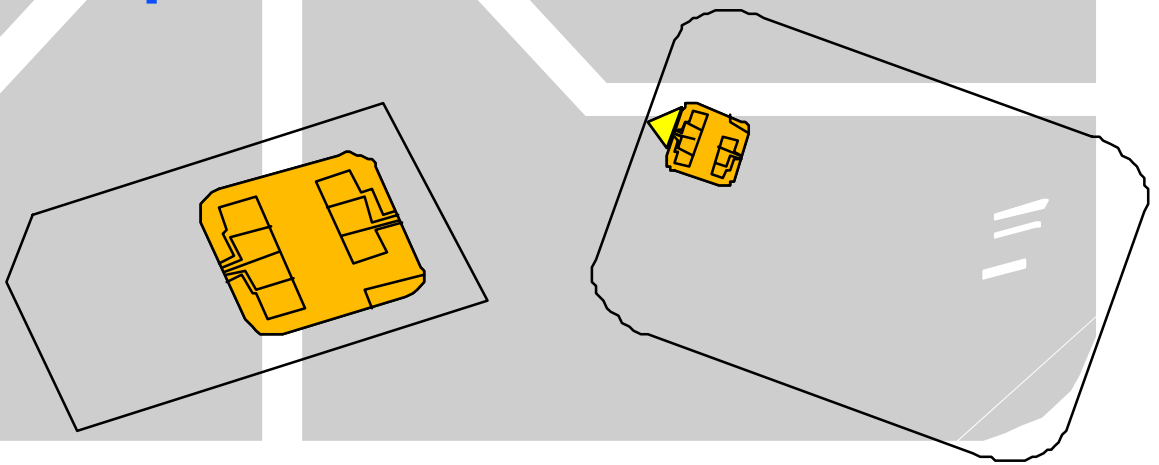
- maximum cumulative micro-payment amount parameter stored in PSAM
- cumulative micro-payment amount transacted by the card captured in card ...
- when the limit is reached, POS converts cumulative amount in the EP to a audit transaction for the purse provider
- POS resets the cumulative amount
- transaction amount handled by the POS cumulated in the PSAM
- PSAM provides signature on amount cumulated for clearance

EP System Components



Security Application Module - SAM

- an autonomous intelligent device
- a secured storage of keys / master keys
- keys once loaded never leave the SAM
- uses keys to generate/verify certificates
- needs to be activated before its function
- self-destruct if tampered
- security not compromised even if lost or stolen



Inter-Sector Electronic Purse (IEP)

- prepared by TC224, WG-10
- specification named EN-1546
- EN-1546 comprises of 4 parts:
  - part 1: Definitions, concepts & structures
  - part 2: Security Architecture
  - part 3: Data elements and interchanges
  - part 4: Devices
- the least card manufacturer specific solution to electronic purse application

EN-1546 Part 1
Definitions, Concepts & Structures

- definitions of terms used in IEP systems
- concepts & structures of an IEP systems
  - logical model of an IEP system
  - participants & responsibilities
  - special considerations
  - IEP transactions
  - SAM transactions
  - system functions

EN-1546 Part 2
Security Architecture

- describes security architecture of the IEP
  - security requirements & characteristics
  - error handling
  - security relevant data elements
  - security procedure
    - IEP transactions
    - SAM transactions

EN-1546 Part 3
Data Elements & Interchanges

Define lists of IEP commands:

- Initialise IEP
  - Load
  - Purchase
  - Purchase Cancellation/Error Recovery
  - Currency Conversion
  - Parameter Update
- Credit IEP
  - Load
  - Purchase Cancellation/Error Recovery

EN-1546 Part 3
Data Elements & Interchanges

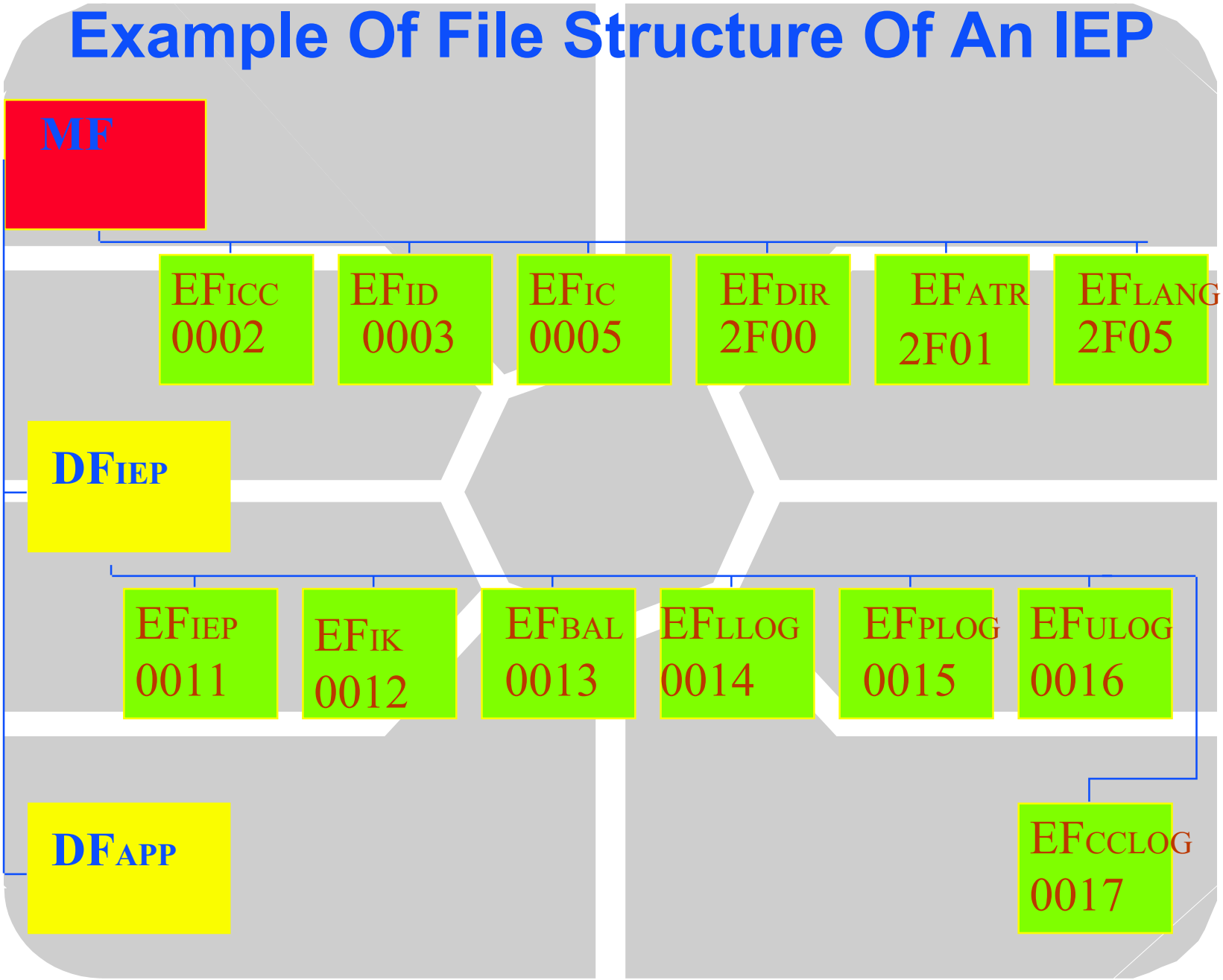
Define lists of IEP commands:

- Debit IEP
  - first step
  - subsequent step
  - acknowledge
- Convert IEP Currency
- Update IEP Parameter
- Get Previous IEP Signature

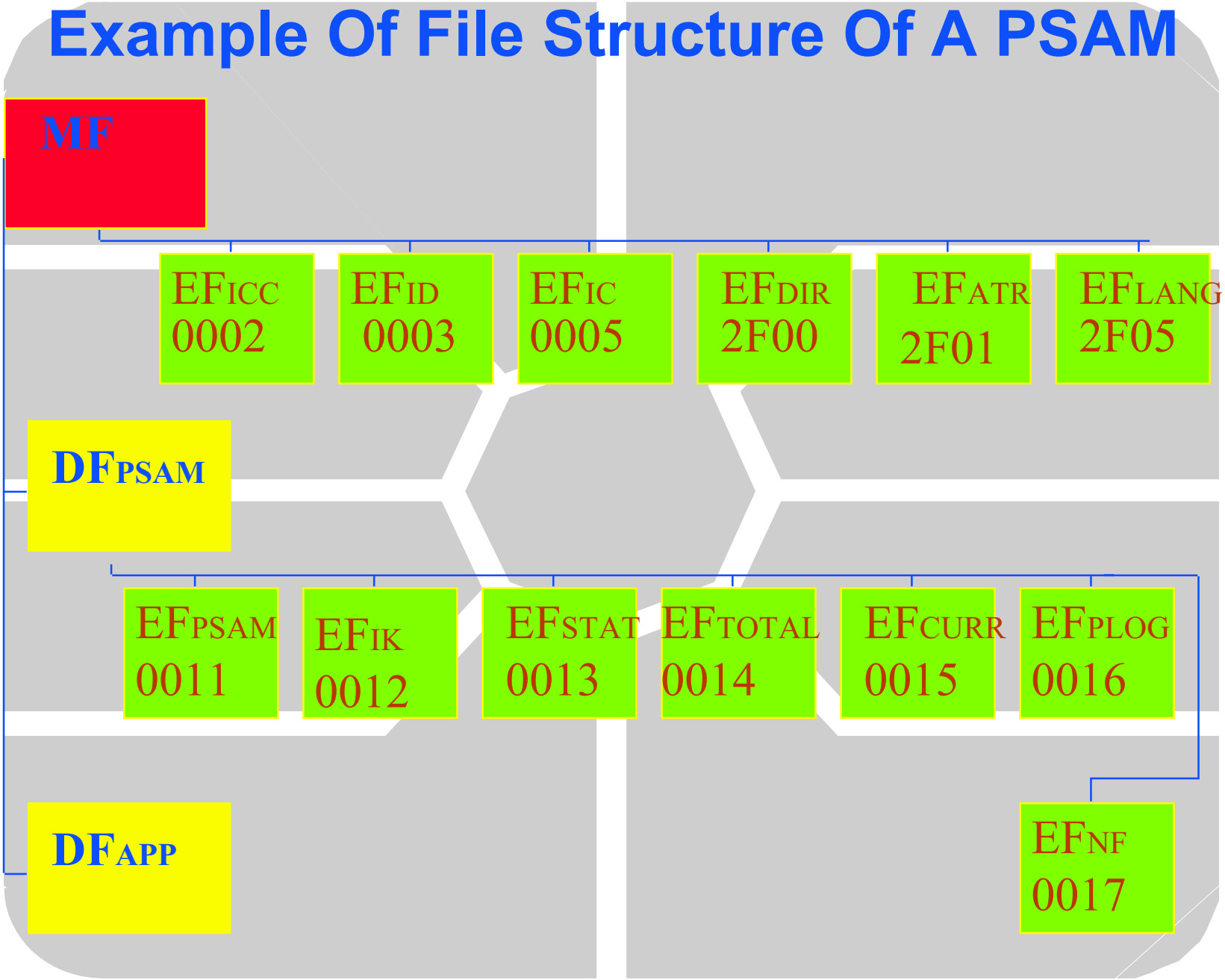
EN-1546 Part 3
Data Elements & Interchanges

- conformance to ISO-7816 part 3,4,5,6
- example of IEP file structure
- PSAM commands
- PSAM file structure

Example Of File Structure Of An IEP



Example Of File Structure Of A PSAM



WG10 Part 3 PSAM Commands

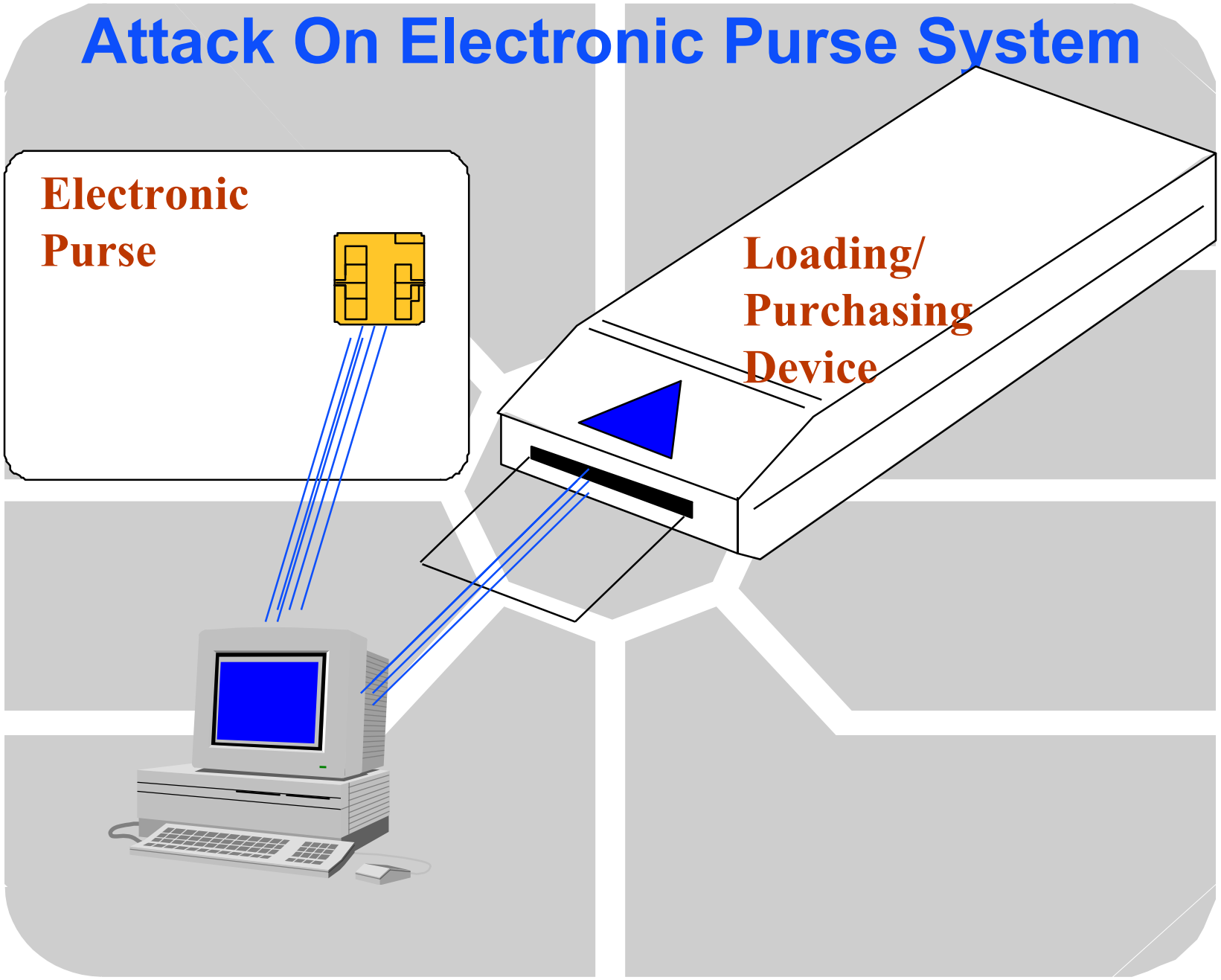
Define lists of IEP PSAM commands:

- Initialise PSAM for
  - purchase, cancellation /error recovery
  - on-line & off-line collection
  - on-line update
- Credit PSAM for purchase
- PSAM Complete Purchase
- PSAM Collect On-line, Off-line
- PSAM On-line Ack, Off-line Collection Ack
- Update On-line, Off-line
- Get Previous Signature

Why Follow WG-10

- Well thought out security scheme
  - IEP,PSAM,PPSAM,LSAM
  - chip controlled transaction logging
- Well thought out application scenario
  - amount not known at begining of txn
  - error recovery
  - multi-currency
- Standarised command set
- Upgradable to public key algorithm
- Compatible with EMV,ETSI

Attack On Electronic Purse System



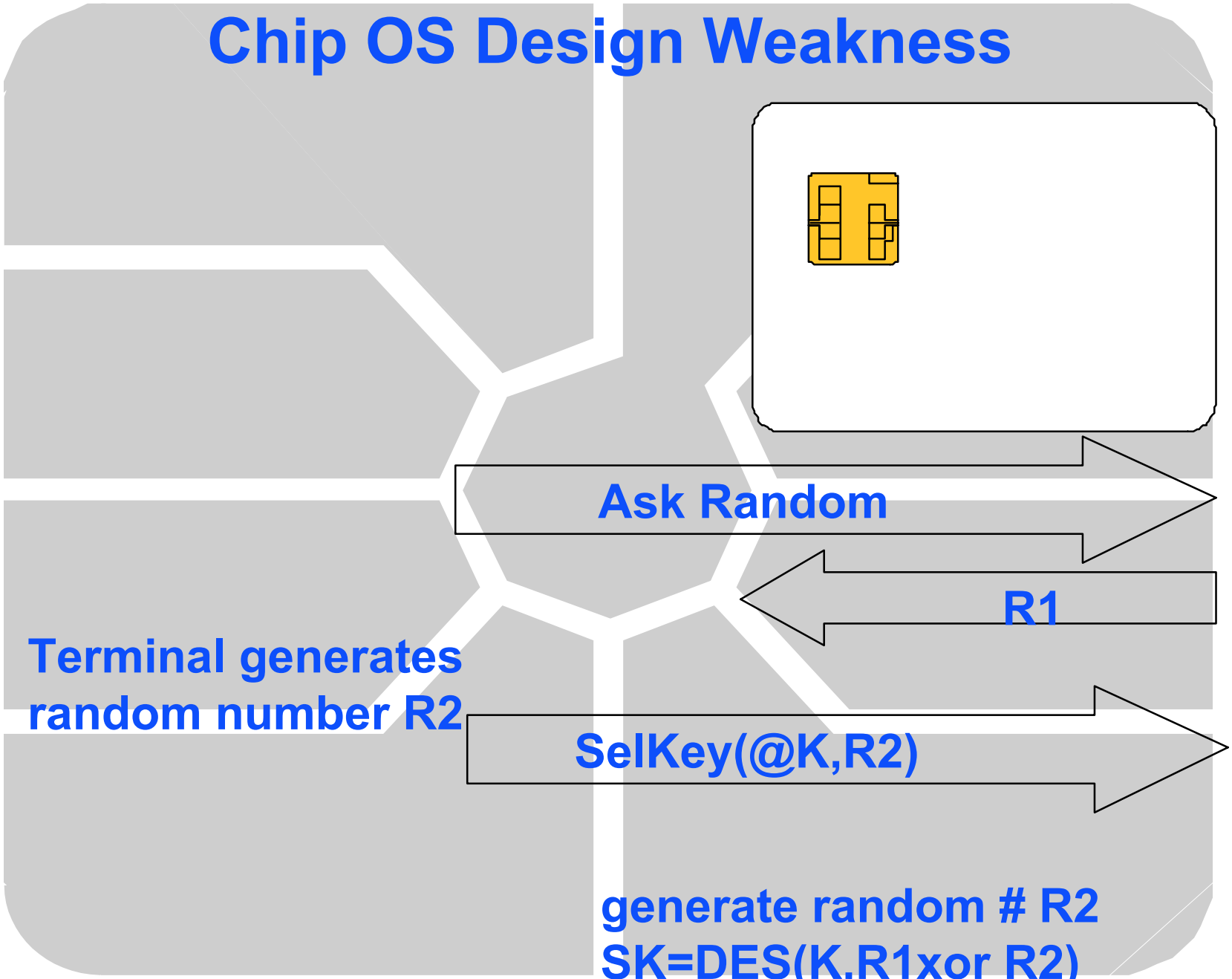
Type Of Attack

- Emulation
  - emulation of EP to generate fake txn
- Replay
  - replay of reloading transaction
  - replay of debit transaction
- Disruption
  - disruption of debit cancellation
- Tampering of Data
  - transfering of genuine transaction into another terminal
- etc

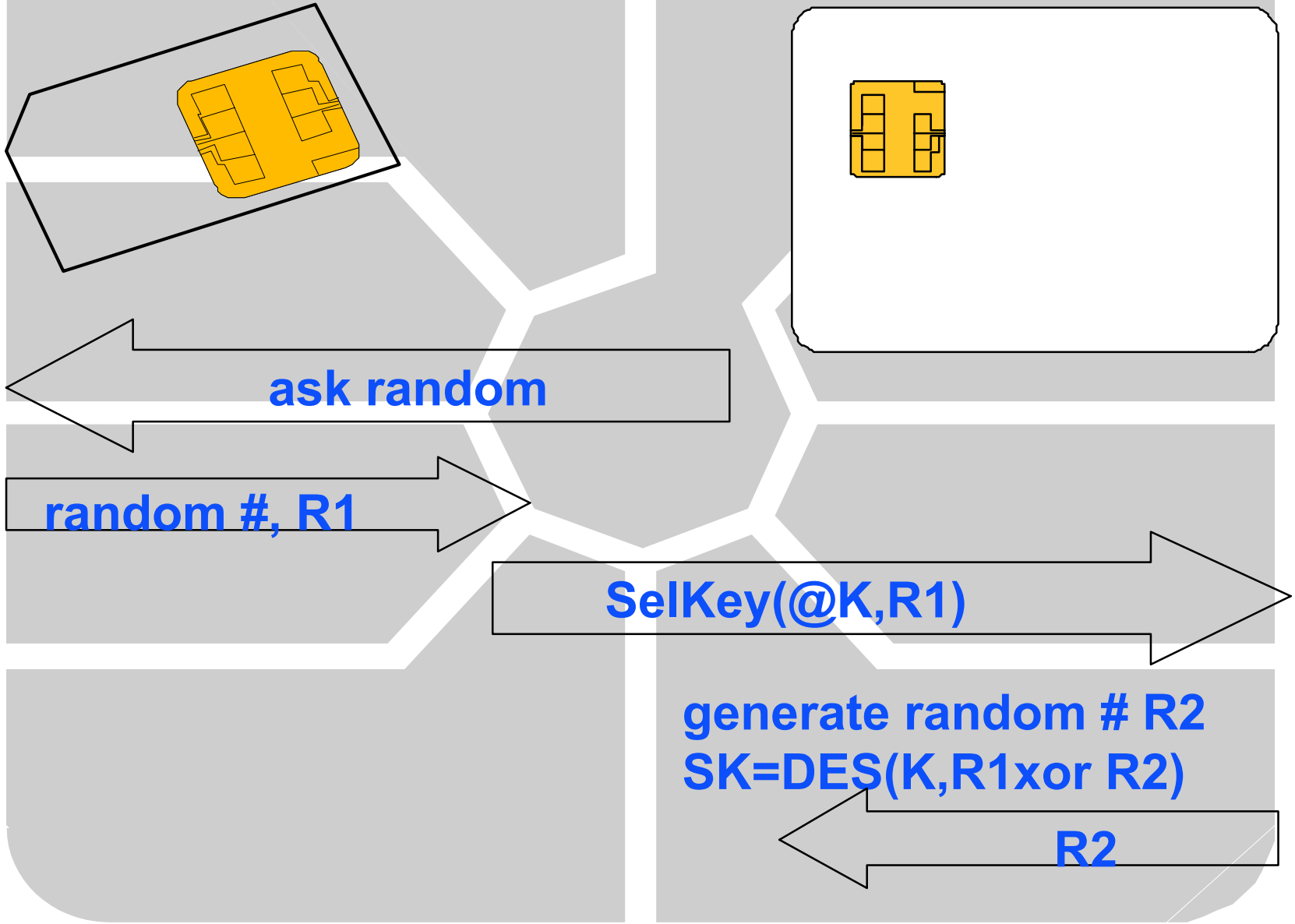
Causes of Security Weakness

- weakness in smart card
  - weakness in chip operating system
  - weakness in command set
- weakness in SAM design
  - secrets leaking module instead of security application module
- weakness in application implementation
- weakness in design
- weakness in system key management

Chip OS Design Weakness



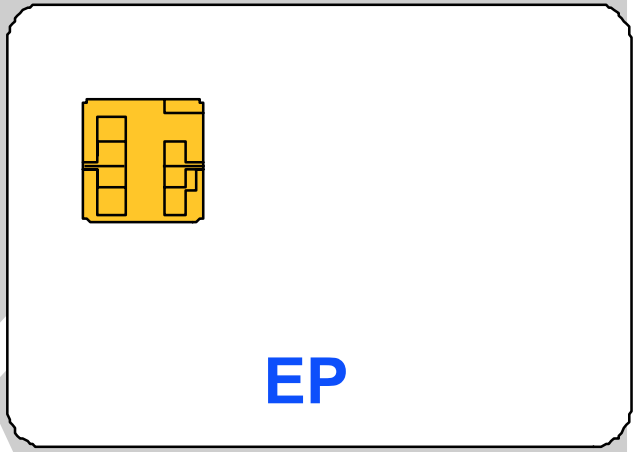
Chip OS Design Weakness



Chip OS Design Weakness

SAM

Terminal Application



EP

Read File---------->

<---------S/No

<----------Ask Random

R1---------->

<----Diversify Key(@Km,s/no)

Ki=DES(Km,s/no)

SelKey(@Ki,R1---------->

generate random, R2

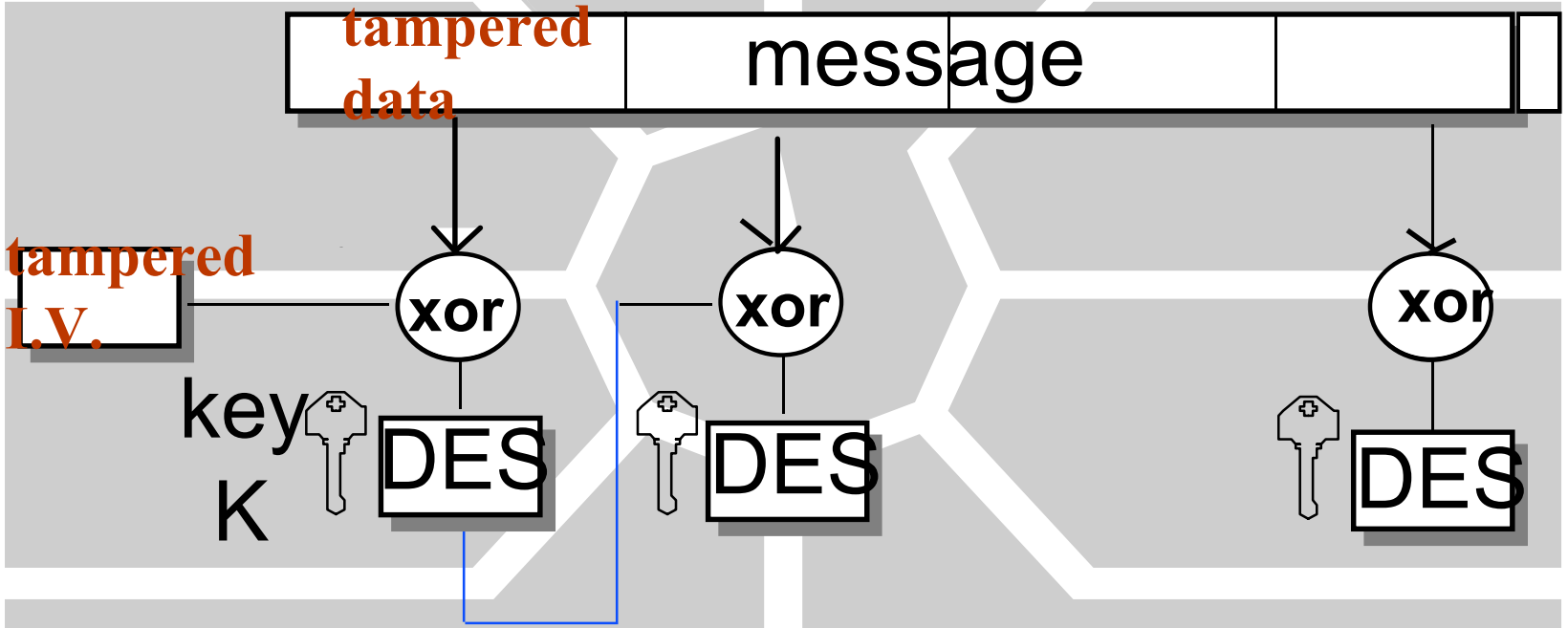
SK=DES(Ki,R1 xor R2)

<----------R2

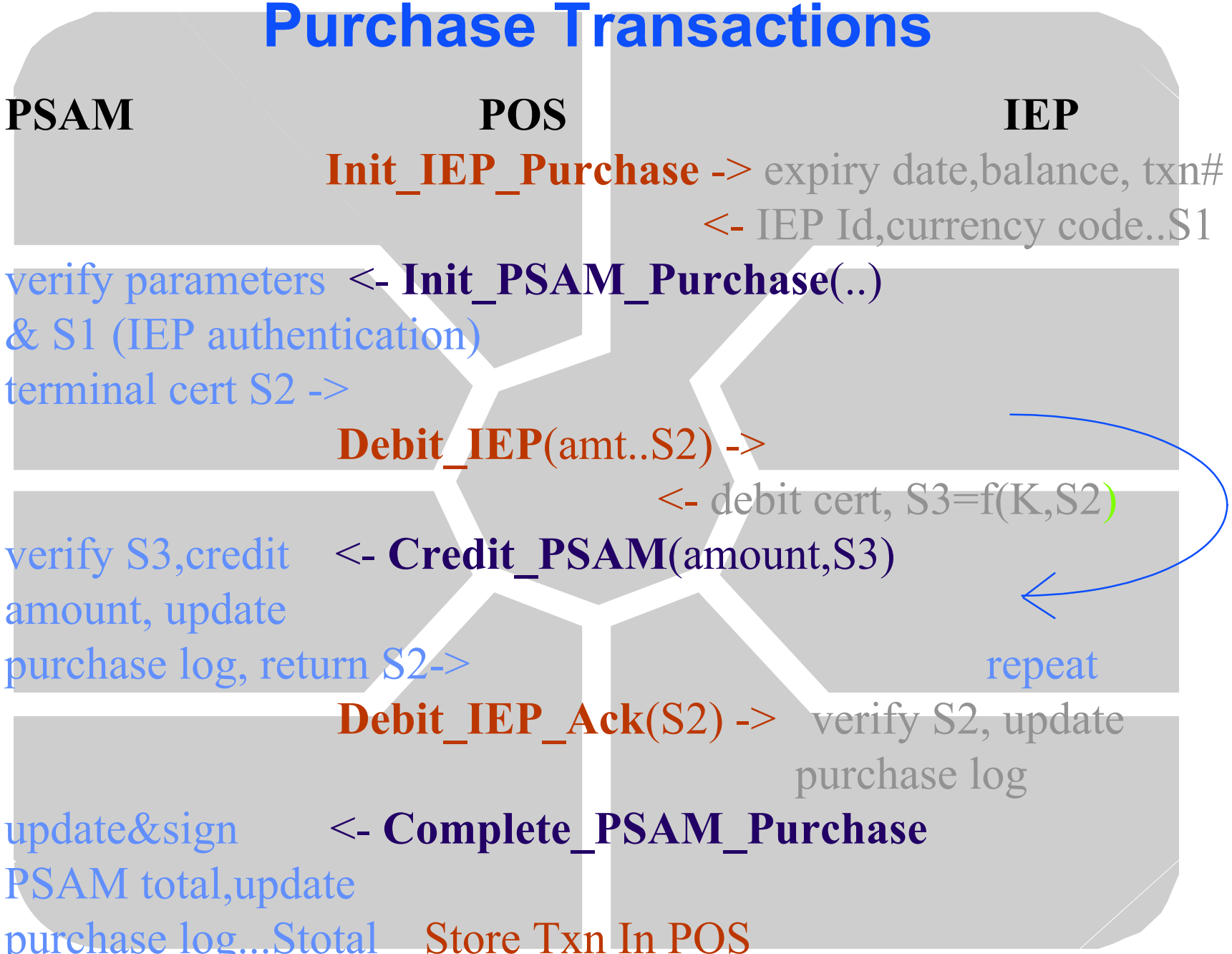
<----------SetSK(R2)

SK=DES(Ki,R1 xor R2)

Pitfall In Using Xor



Purchase Transactions



Load Transactions