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 - anonymous
- 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
- Equipped 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 subsidiary of the purse provider or the purse provider

Card Issuer

- Responsible for the personalization of EP
- Manage and maintain card personalization system
- Receives personalization input data from purse provider
- Provides personalization 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 e.g. 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

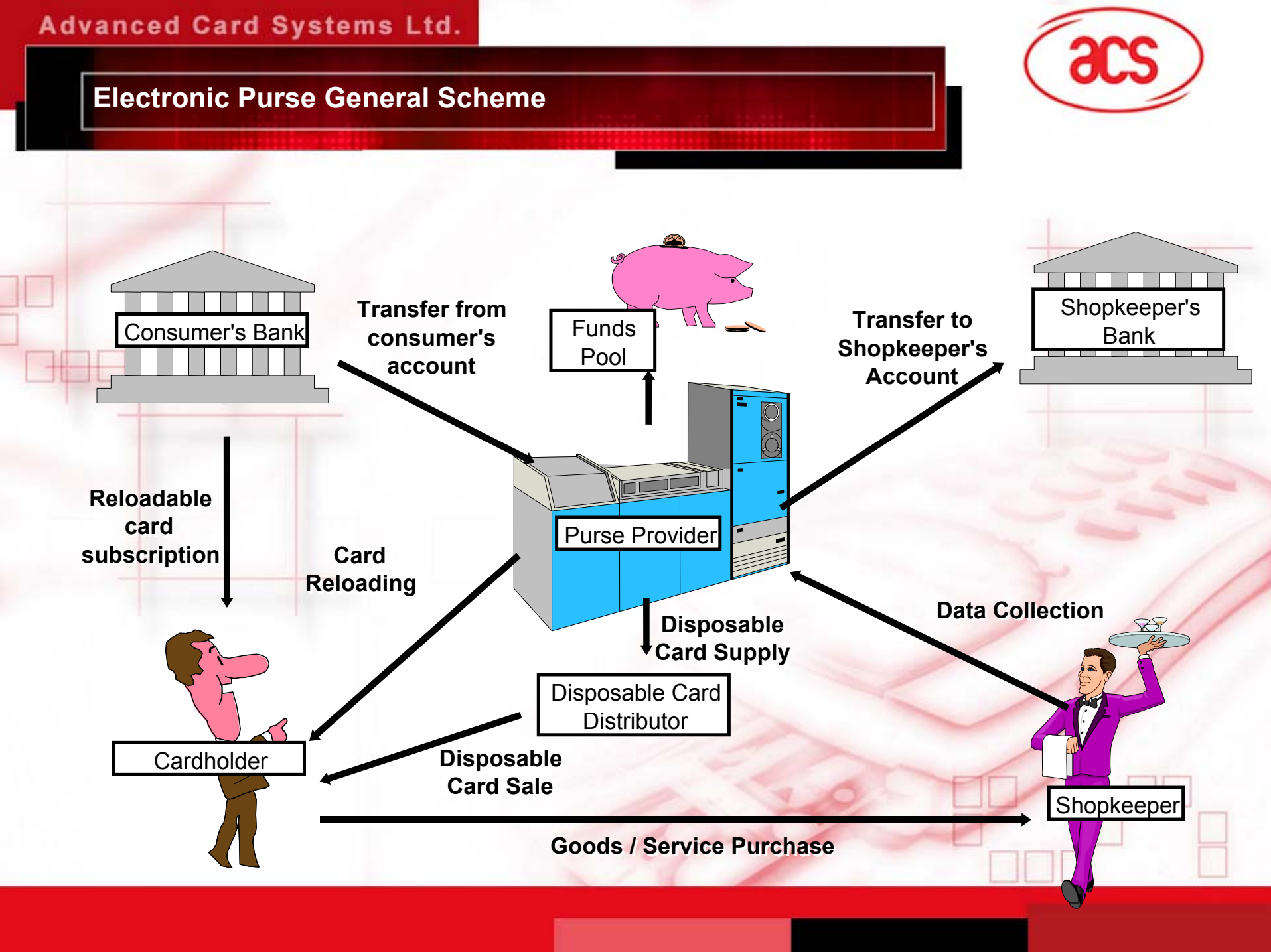
Service Provider's Concerns

- Correct amount shown and debited
- Reliability 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-friendliness
  - 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 (personalization 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

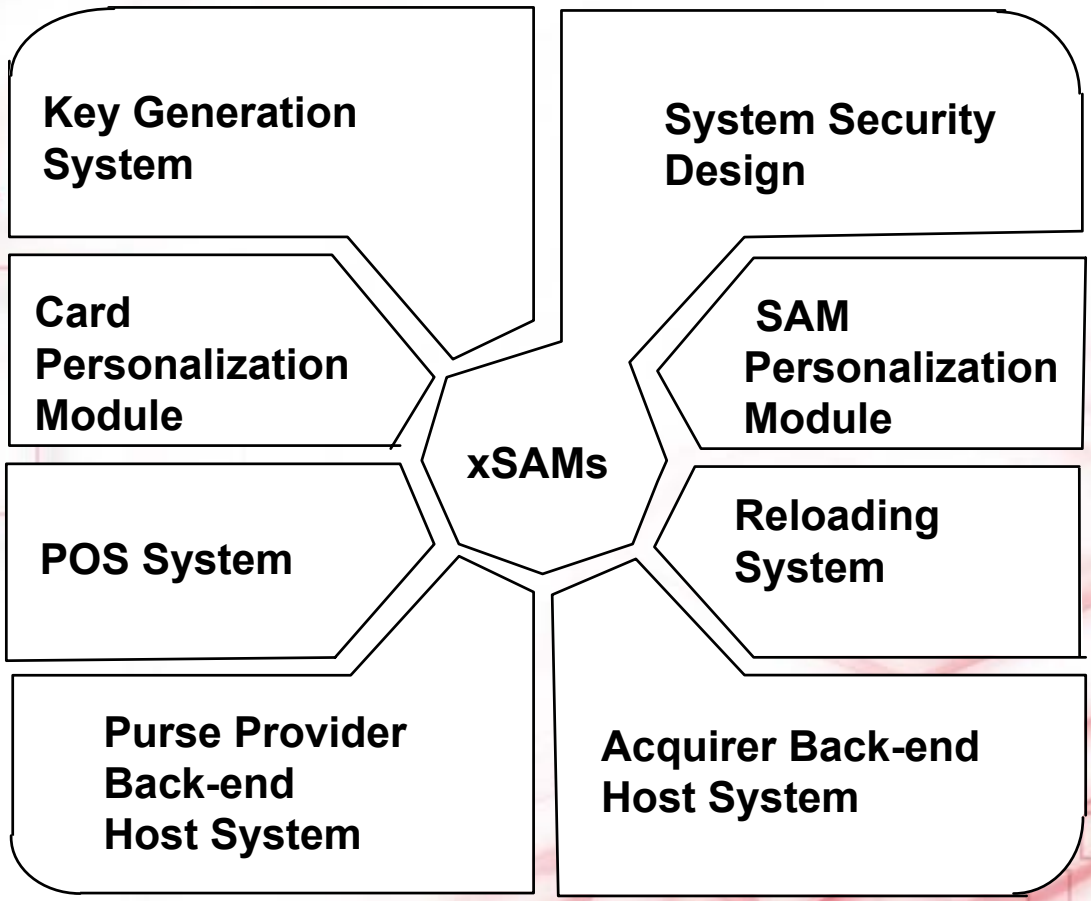
- Micro-payment not cost-effective for processing
- Nevertheless very important for the acceptance of cards & success of the system e.g. payphone, vending, copier
- Micro-payment can be accumulated after debit verification by PSAM and credit to the respective purse providers
- At the end of the day, 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

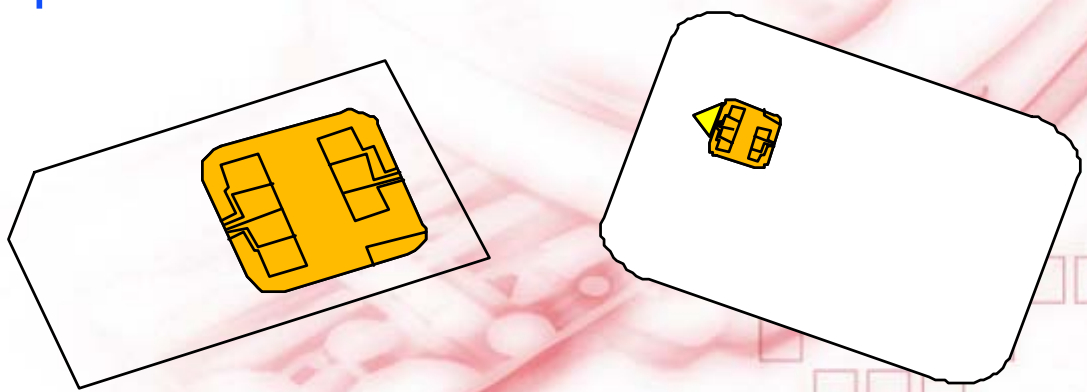
- Maximum cumulative micro-payment amount parameter stored in PSAM
- Cumulative micro-payment amount transacted by the card captured in card
- When the limit is reached, POS converts cumulative amount in the EP to a audit transaction for the purse provider
- POS resets the cumulative amount
- Transaction 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

Define lists of IEP commands:

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

Define lists of IEP commands:

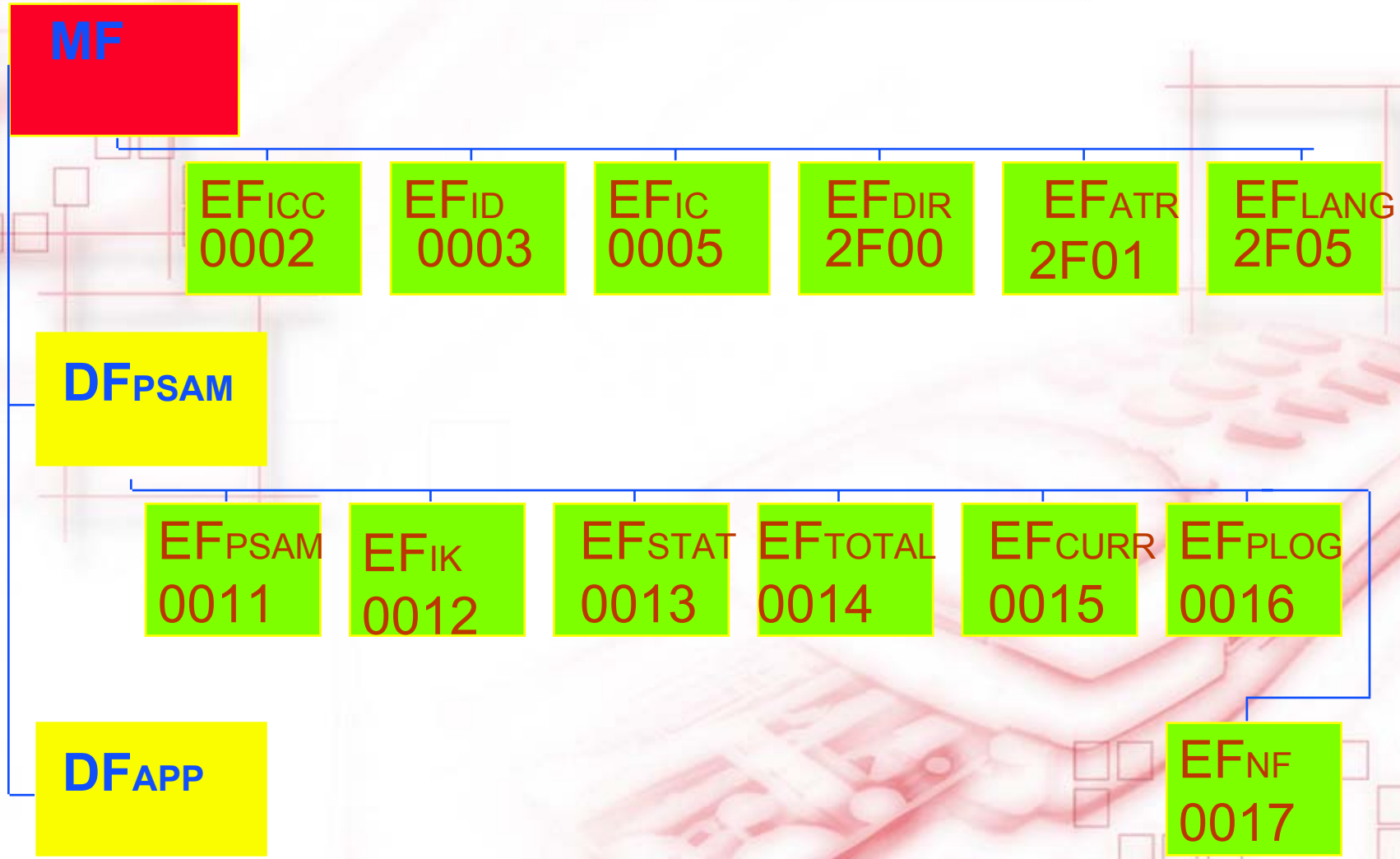
- Debit IEP
  - First step
  - Subsequent step
  - Acknowledge
- Convert IEP Currency
- Update IEP Parameter
- Get Previous IEP Signature

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

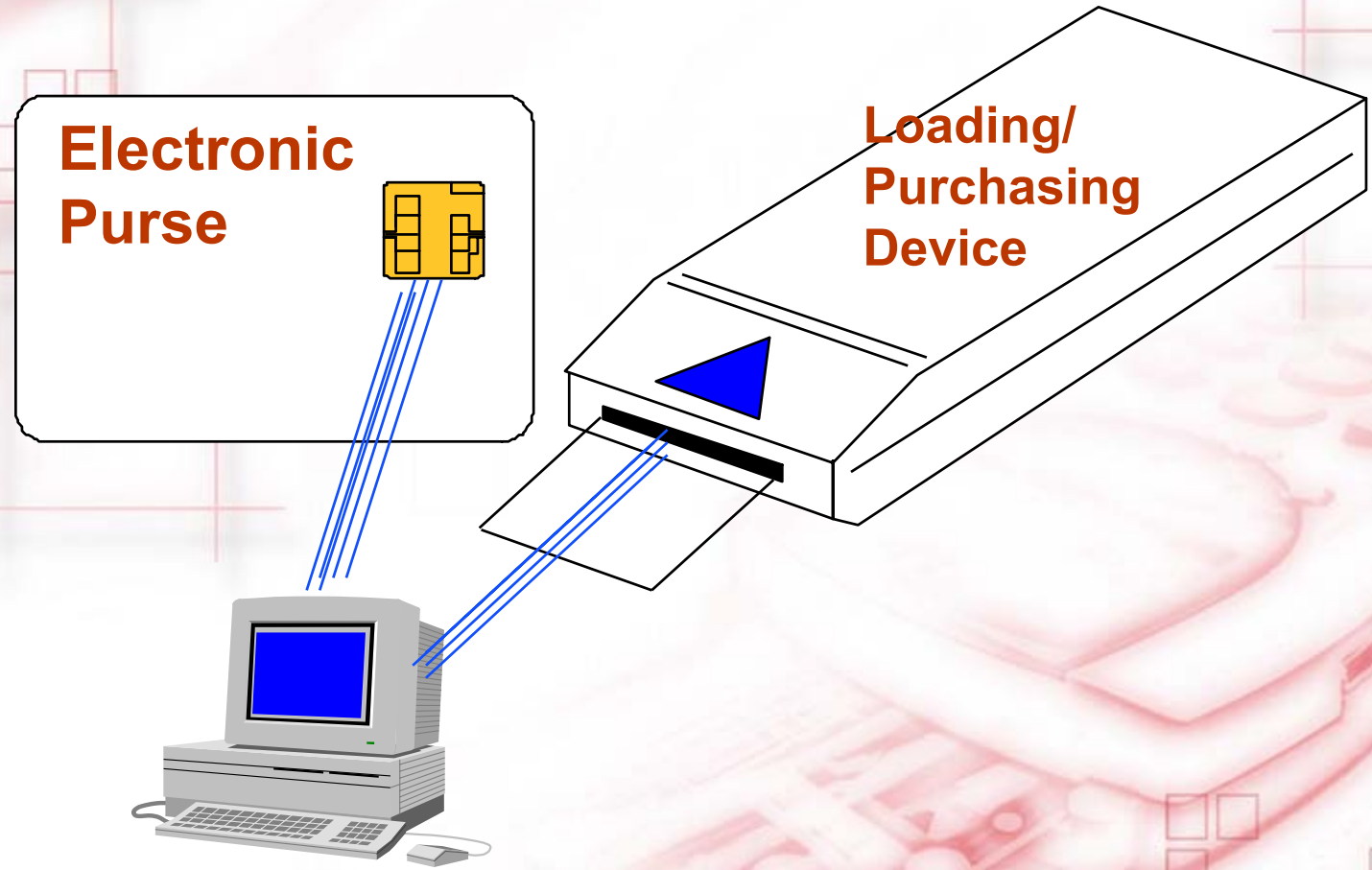
Define lists of IEP PSAM commands:

- Initialize 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 beginning of txn
  - Error recovery
  - Multi-currency
- Standardized command set
- Upgradeable to public key algorithm
- Compatible with EMV,ETSI

Attack On Electronic Purse System



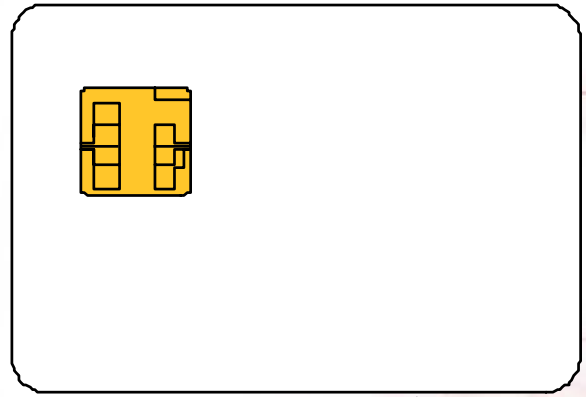
Type Of Attack

- 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
  - Transferring 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



Ask Random

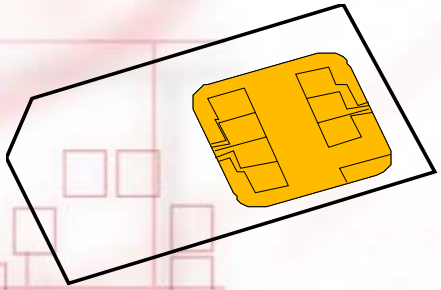
R1

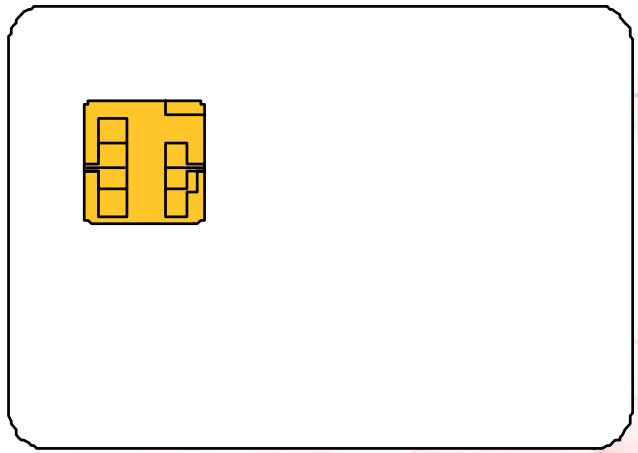
Terminal generates
random number R2

SelKey(@K,R2)

generate random # R2
SK=DES(K,R1xor R2)

Chip OS Design Weakness





ask random

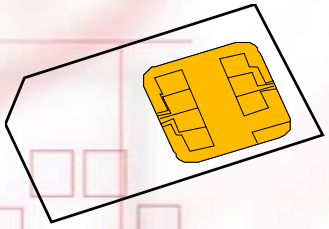
random #, R1

SelKey(@K,R1)

generate random # R2
SK=DES(K,R1xor R2)

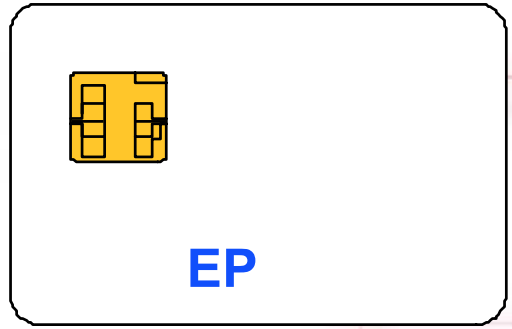
R2

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

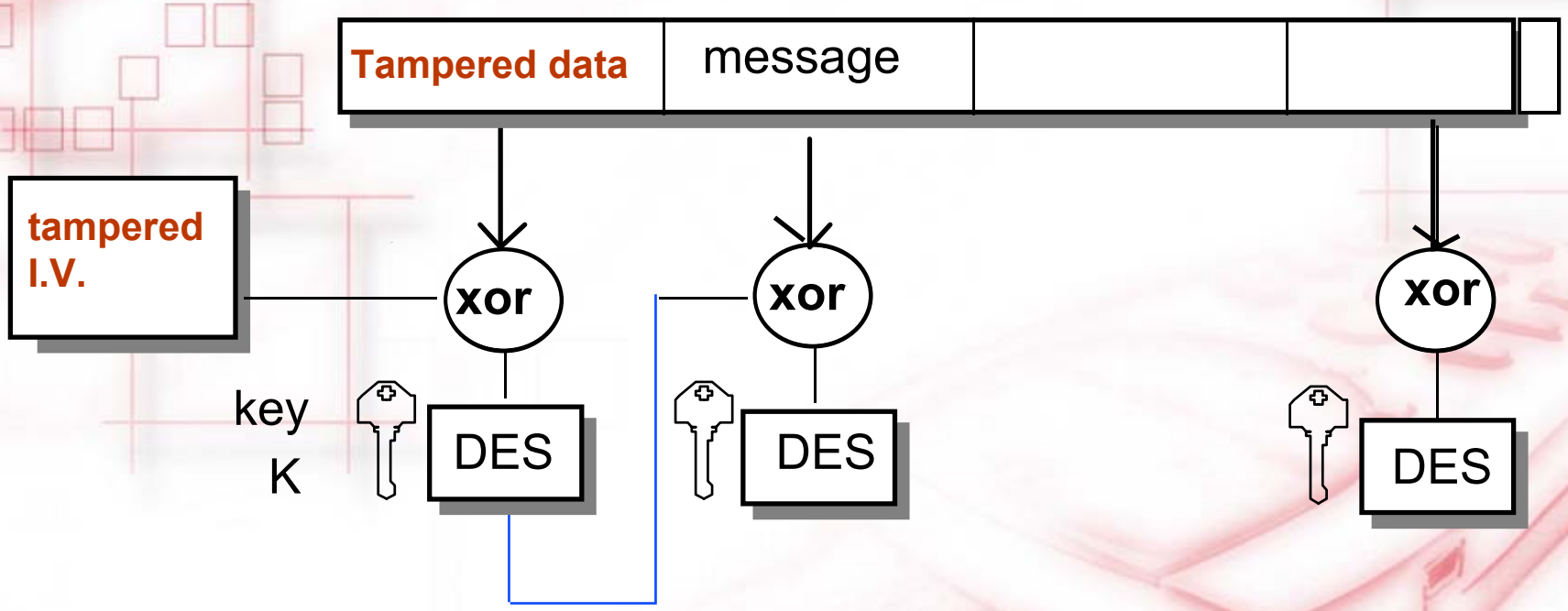
SK=DES(Ki,R1 xor R2)

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

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

SK=DES(Ki,R1 xor R2)

Pitfall in Using XOR



Purchase Transactions

PSAM	POS	IEP
	Init_IEP_Purchase →	expiry date,balance, txn#
		← IEP Id,currency code..S1
verify parameters & S1 (IEP authentication) terminal cert S2 →	← **Init_PSAM_Purchase**(..)	
	Debit_IEP(amt..S2) →	
		← debit cert, S3=f(K,S2)
verify S3,credit amount, update purchase log, return S2→	← **Credit_PSAM**(amount,S3)	
	Debit_IEP_Ack(S2) →	repeat verify S2, update purchase log
update&sign PSAM total,update purchase log...Stotal	← **Complete_PSAM_Purchase** Store Txn In POS	

Load Transactions

PPSAM /LSAM	Reload Terminal	IEP
amount,currency code..random number ← **Init_SAM_Credit**(..)		
	Init_IEP_Load →	IEP Id,txn#,expiry date ←..S1
verify parameters & S1 (IEP authentication) compute credit cert S2 →		
	Credit_IEP(amt..S2) →	
		← verify cert S2, update load log S3=f(K,S2)
verify S3,debit amount, update credit log, total return S2 ← **SAM_Credit_Verify**(amount,S3)		
	→ Store Txn In LDA	