v1.0
Frederic LEVY
frederic.levy@spirtech.c

# Securing Multi-Application Multi-Operator Ticketing Systems

- Security Principles
- Central Systems: SAM Management and Fraud Detector
- Multi Application: Classic and Improved Solution
- Example of Use: Multiple Tourist Services Management

# Ticketing Security Principles

## Goals

- Ensure that the transport titles have been paid for
- Do not make the ticketing system too expensive or too complex to manage

## Conditions

- Validation: ensure the title authenticity and a correct debit
- Reloading: prevent fraudulent title creation
- To have detection and correction means at disposal

## Interoperability Security Constraints

- Responsibility sharing
- Need for a common secure policy

## Method

- Identification of the goods, threats, attacks, requirements and means
- Definition of the security under the control of the transport operators
- Implementation in the equipments

# Portable Objects

## Types of Authentication

- Card / Terminal authentication
- Data authentication

## Card / Terminal authentication

- Secret keys to access to the card data: Authentication, Read, Write
- Keys may be different for different types of data (contract, event...)
- Used mainly with microprocessor cards

## Data authentication

- Signature associated with the data to authenticate the data
- Example: contract signature issued when selling the contract, and verified when validating.
- Used mainly with contactless tickets

## Symmetric Algorithms

- High transaction speed, small amount of data, lower card cost
- 128 bit keys allowing a high security level (DES, DESX, Triple DES)
- Keys are never present outside of a secure environment (card, SAM)

# SAM

## SAM

- Secure Application Module
- Comply with the smartcard standard (ISO 7816, ID000 format)

## Safe Box for the cryptographic keys

- Contains one to many secret keys
- Authorizes some operations, according to each key parameters
- Forbids any other operation

## Secure the dialogue with the cards

- Mutual Authentication. Authentication of the data exchanged
- Different SAM for validation, selling, personalization…

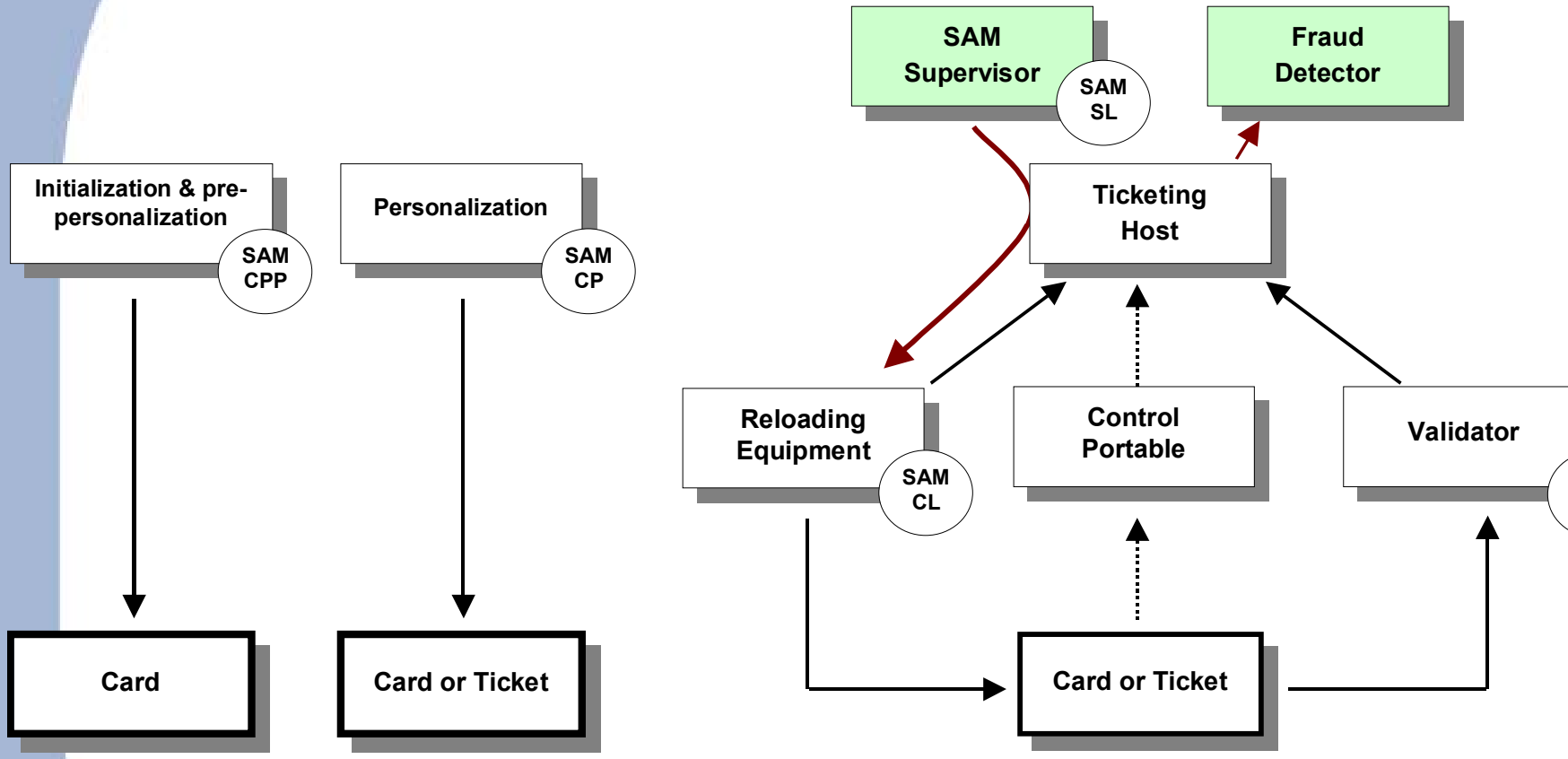
## Secure the dialogue with the tickets

- Data signature computation and verification

## Secure the dialogue with other SAMs

- Data collection
- Configuration update

# SAM Usage




Note: to increase security, the different kinds of SAM are limited to their function (e.g. a Validation SAM cannot personalize a card)

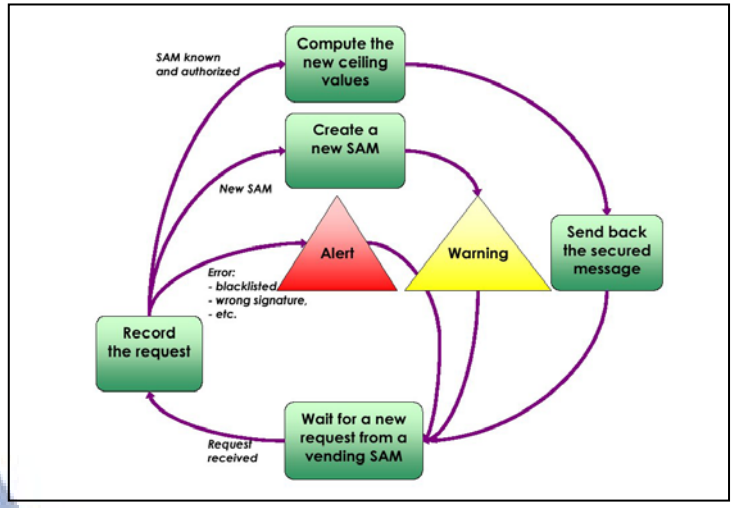
# Central System: SAM Supervisor

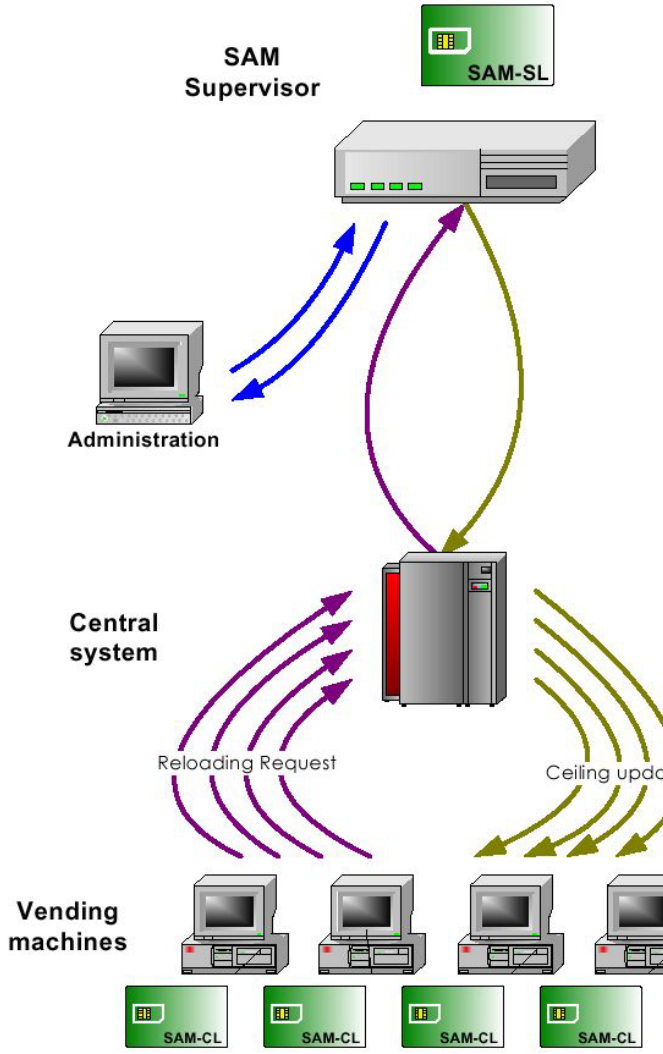
## SAM Supervisor

- Database of all authorized SAM
- Use of a Supervision SAM (SAM-SL)
- Alert if ceiling reached or unknown SAM

## Functions

- SAM Reloading (Ceiling update)
- New Key Loading
- SAM Supervision



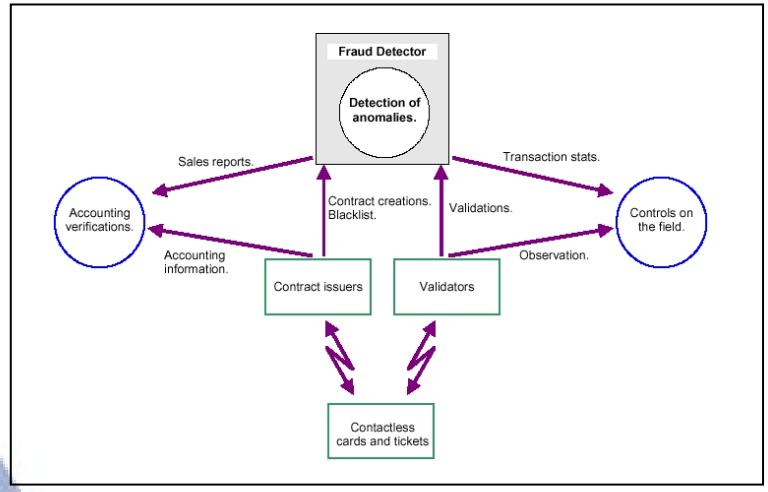
# Central System: Fraud Detector

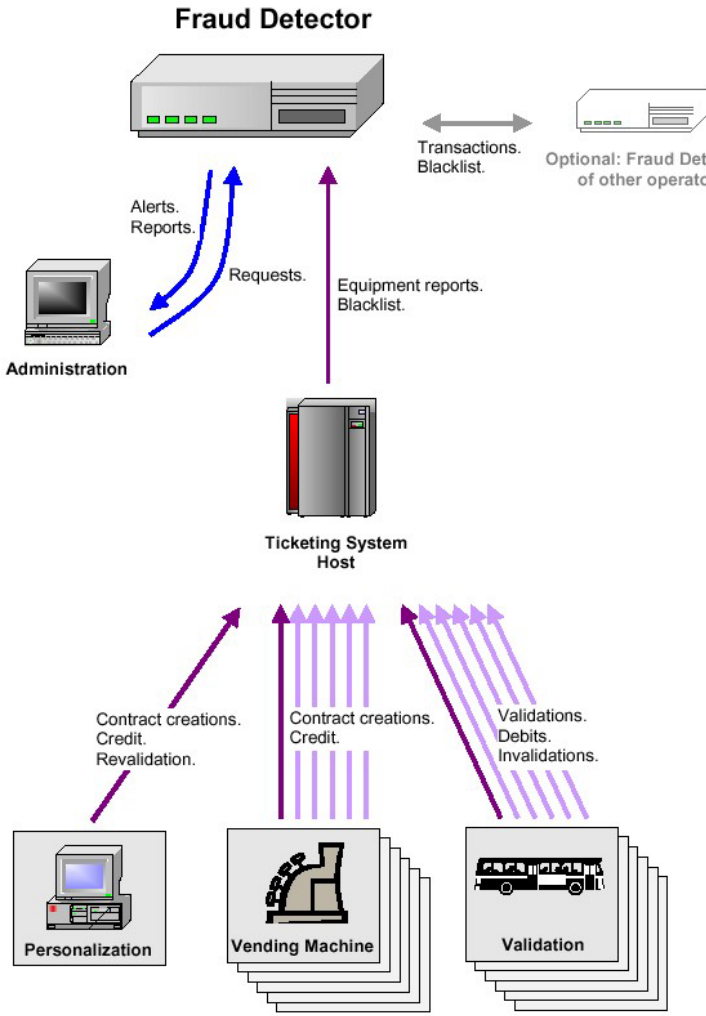
## Fraud Detector

- Database of all cards and tickets
- Automatic transactions analysis
- Alerts if fraud is suspected

## Transaction Analysis

- Unknown cards or tickets
- Unsold contracts
- Same card used "too often"
- Cryptographic signatures



# Multi-Application Management

## Applications

- Transit Network
- Electronic Purse
- Many Services: Museums, Exhibitions, Shows, Swimming Pool, Parking, Children Services, etc.

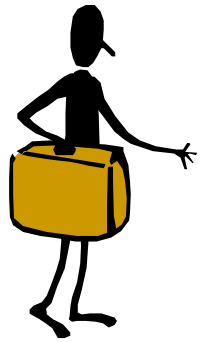
## Services Classic Solution

- Many independent operators
- One card directory for each operator? for each application?
- One security environment for each
- Interoperability is complex (independent applications, key distribution...)

## Improved Solution

- One card environment for all services
- The SAM secures the data and valuables of each operator independently
- Easier interoperability (all data in the same application)

# Example of use: Presentation



## Paris Tourist Cards

- Public Transport (Navigo)
- Museums.
- Guided Tours.
- Exhibitions.
- Shows.
- Others (hotel access control, vouchers...)

## Solution

- Calypso card and SAM-S1 version E1
- Two card Applications: Public Transport and “Services”
- Public Transport: one common security environment
- Services: one environment, but **no trust** between operators

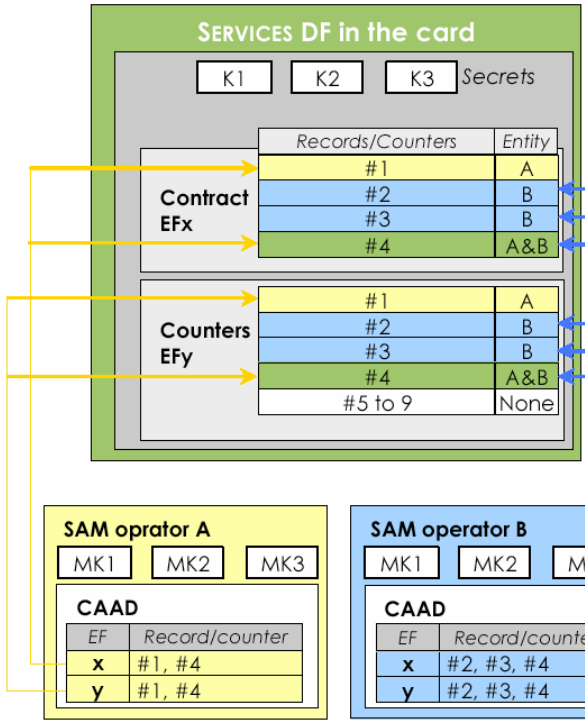
# Example of use: Management

## Security Management

- Unique identifier for each operator
- SAM of each operator has limited authorizations

## SAM Authorizes Only

- Access to some file records
- Creating / Modifying data including operator ID
- Modifying the counters attached to this data



# Further References

## Internet Resources

- European Project SINCE:http://www.eurosmart.com/since
- Calypso Networks Association: http://www.calypsonet-asso.org
- Technical Calypso Site: http://www.CalypsoTechnology.net
- Spirtech: http://spirtech.com

## Contact

- spirtech@spirtech.com