Fraud Detector

Ticketing System Supervision

The **Fraud Detector** is central to the security of ticketing systems.

The *Fraud Detector* supervises the use of ticketing cards and tickets.

It generates alerts and reports in case of possible fraud, allowing the system manager to assess the threat and react in time.

SECURITY MANAGEMENT OF A CONTACTLESS TICKETING SYSTEM

Contactless ticketing systems, based on Calypso, Mifare or other technologies, allow the owner of a contactless smartcard with the proper rights (transport contracts) to enter and travel in the transit networks.
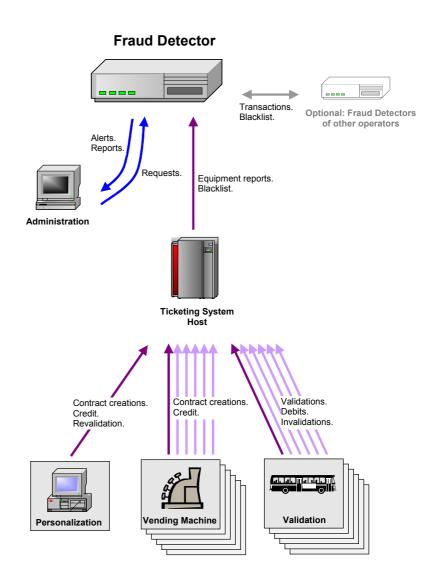
These contracts have previously been bought, or in specific cases are granted without payment.

These contracts are protected in the cards and tickets by the use of cryptographic keys, which are normally necessary for all operations.

Since a technical process cannot be completely secure, in a ticketing system as well, several types of *technological frauds* are theoretically possible, in the different places where cards are processed: personalization, sales and validation.

Therefore, transit networks setup a monitoring system able to detect and investigate the possible technological frauds, should they appear.
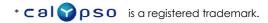
The core of this system is a central equipment processing the reports of the operations done in the transit network: the **Fraud Detector**.

Fraud Detector

Transactions. Blacklist.

Optional: Fraud Detectors of other operators

Alerts. Reports.

Requests.

Administration

Equipment reports. Blacklist.

Ticketing System Host

Contract creations. Credit. Revalidation.

Contract creations. Credit.

Validations. Debits. Invalidations.

Personalization

Vending Machine

Validation

Main functions

- Management of a database of all cards, tickets and last transactions.
- Automatic analysis of the transactions.
- Verification of the cryptographic signatures.
- Generation of alerts if a fraud is suspected.
- Interactive analysis of the data in case of suspected fraud.
- Reports to fraud detectors of other operators (if they exist).
- Recording of all the operations performed.
- Secured remote administration through a web browser.
- Alerts (email, RSS, SMS).

Spirtech

* calypso is a registered trademark.

Fraud Detector Environment

The Detector is indirectly connected to:

The **personalization and vending equipments** (equipments able to load a transport contract in the cards) which report the following transactions:

- Creation of a contract in a card or ticket.
- Removal of a contract in a card or ticket (refund).
- Blacklisting of a card or ticket.
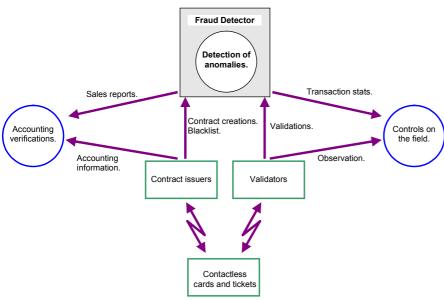- Removal from blacklist.

The **validators** which transmit the reports of validation transactions:

- Validations on entrance of the transit network.
- Invalidation report of blacklisted cards.

If they exist: **Fraud Detectors of other transport operators**.

The Detector manages a database of all cards and tickets contents, associated with their last transactions. To protect the privacy of the customers, the Detector erases the transactions after a short time period (two or three days), and never associates a card with a person.

Operations Synoptic

The Detector:

- Sends reports to the accounting department allowing comparisons with the accounting information supplied by the contract issuers.
- Carries out the coherence controls with the data received from the contract issuers and from the validators.
- Sends statistics reports for possible coherence verifications with manual controls on the field.

Administration Functions

All administrative tasks are managed with a web browser using HTTPS.

Various parameters ease the initial creation of the data and allow a large flexibility in the system management.

For such a system, where it may happen that no fraud appears before several years (if at all), it is important that the number of alerts does not become too frequent or never appear. Therefore, many parameters allow to filter the alerts easily.

When an alert if first encountered, the Detector generates a precise report detailing its source and the data associated with the problem. Care is taken to avoid the multiplication of many alerts of the same type to ease controlling the system (for example in case of erroneous or missing information received).

Product Range

The Fraud Detector is available in three forms: stand-alone network appliance, software package or as a web service:

NETWORK APPLIANCE

- Rack mountable appliance
- Fully automated and stand-alone
- Plug and Play

SOFTWARE PACKAGE

- Windows XP application
- The package includes MySQL and all the software tools necessary for operation

WEB SERVICE

- Remote server operated by Spirtech
- Located on a secure site
- Lowers installation and maintenance costs

Detailed Characteristics

INTERFACES

- USB: PC/SC smartcard reader(s)
- TCP/IP, HTTPS, XML or native

VOLUMETRY

- Up to 2,000,000 cards
- Up to 20,000,000 tickets
- Up to 5,000,000 daily transactions

DATA BASE CONTENT

- All the cards and tickets with their last transactions
- Alerts and Fraud Detector parameters
- All operations are logged

ASSOCIATED PRODUCTS

- SAM Supervisor
- SAM-S1 Secure Application Module

Spirtech