SAM-S1
Type E

Secure Application Module

the solution for CALYPSO transit applications

The *SAM-S1* module manages the security of the smart cards and tickets complying with the CALYPSO Specification.

Its new CAAD system allows the secure sharing of the same card application by different operators.

SAM USAGE IN A TICKETING SYSTEM

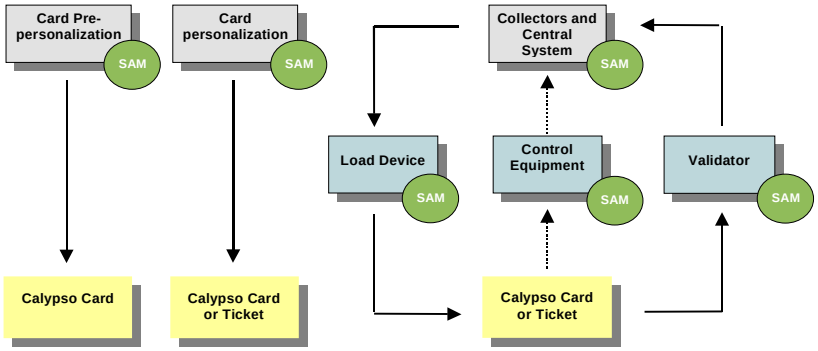
The CALYPSO cards are contactless smartcards for payment of public transport.

The authentication and modification of the cards are subject to the use of secret keys, allowing the terminals to ensure the card authenticity and forbidding an unauthorized modification of the card content.

To remain secret, these keys are always kept secure inside the cards or inside the SAM.

The CALYPSO compliant SAM-S1 is used as part of a secure system including a central system, reloading equipments, validators, and possible other equipments :

- The central system keeps track of the transactions, makes statistics and verifies the system security and integrity. It may use a SAM to check certificates of transactions.
- The reloading equipment loads value and tickets (one-way tickets, season tickets, etc.) into the cards. It uses a SAM to secure the transaction with the cards.
- The validator validates entrance in (and optionally exit from) the transit network. It uses a SAM to secure the transaction with the cards.
- Hand-held controlling equipment, personalization machines, etc., may also use a SAM to secure the card transactions.



SAM-S1 supported cards and tickets

- CD21, CD97, CD97-BX, CD Light.
- Tango for CALYPSO, CT2000, CT4000 …
- GTML, GTML2, GTML+.
- BMS-2 (except MONEO electronic purse).
- DES*Fire* (option).
- CTS256, CTS512, SRIX, Mifare Ultralight …

Main functions

- Management of the cryptographic keys.
- CALYPSO cryptograms computation.
- CD21, Tango, CD97 and DES*Fire* specific functions.
- Card Access Authorization Descriptor (CAAD) mechanism for multi-applications.
- Sum management and counters.
- Functions to manage other SAM: ciphering of SAM data, SAM signature verification.
- Arbitrary message signature.

Spirtech

* calypso is a registered trademark.

TECHNICAL FEATURES

Detailed Characteristics of the SAM-S1

STANDARDS

- ISO 7816-3 T=0
- ISO 7816-4
- ISO 9797 MAC
- Calypso compliant

CRYPTOGRAPHIC FEATURES

- Triple DES
- DESX and DES
- Variable signature size
- Up to 126 work keys

COMMUNICATION PROTOCOL

- ISO/IEC 7816 PPS protocol.
- HSP protocol (Calypso fast serial mode).
- Automatic protocol selection at reset.
- Explicit protocol selection with the Change Speed command.

PHYSICAL CHARACTERISTICS

- Credit card size, with a removable "mini-SIM" format (ID000).
- Extended voltage range : 2.7 to 5.5 volts.
- Temperatures: Storage -65°C to +60°C; Working: -25°C to +60°C.

OTHER FUNCTIONS

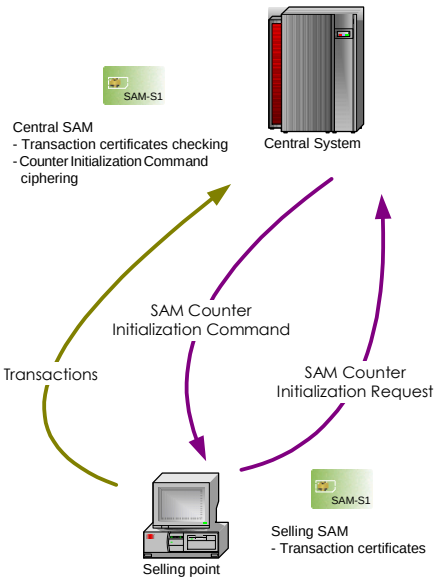
- 27 *Event Counters*, and associated *Ceilings*.
- Any work key may be disabled.
- DES*Fire* compatible (option)
- Possibility to verify on a central system the transaction reported by terminals.

Central Security Management

The SAM are key elements of the security architecture: based on a smart card component, they protect the secrets of the system. However, when in non physically secured environment, on a selling point, for example, they could be stolen and misused.

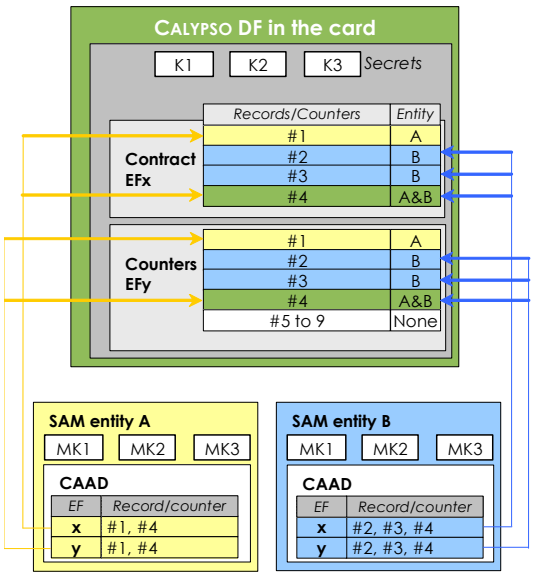
Therefore, the SAM-S1 includes a mechanism that limits the use of its keys : each key can be linked to an *Event Counters* and associated *Ceiling*. Each time the key is used, its *Event Counter* is incremented, and once this *Event Counter* has reached the *Ceiling* value, the SAM rejects any command which would increment the *Event Counter*.

The selling machine needs to connect to the Central System in order to reset the *Event Counter* of its SAM : this operation is secured with an upper level SAM managed by the Central System.



Example of secure transactions

CAAD Mechanism for Multi-services Application Secure Sharing



CAAD : example of static allocation mode

The **Card Access Authorization Descriptors** (CAAD) is a new feature of the SAM-S1 that simplifies the management of the card security among different entities (e.g. parking, library, sport center, show booth): it allows to securely share the same application (DF) of a card with a unique set of key.

The access control to the records of the application is managed by the SAM itself through 2 modes :

- the *static allocation mode*, where records and counters are allocated by their number to each entity.
- the *dynamic allocation mode*, where records and counters are allocated to each entity according to the values of the first bytes of the records.

In order to enforce the CAAD security, the SAM-S1 restricts the commands that may be used in a transaction.

Some **case studies** of the CAAD system:

- **Cities** manage services available to their inhabitants, for example swimming pools, libraries, car park, access control in schools, etc. The keys are shared by all services of the cities, but each service is managed independently. Thanks to the CAAD, it is possible to ensure that the data of a given service can be modified only by the service terminals.
- **Tourism Vouchers :** when selling a trip, tour operators often pre-sell tickets (called vouchers) for various services, each services being operated by an independent service provider. Thanks to the dynamic CAAD allocation, it is possible to use only one key set for all tour operators and all service providers.

Spirtech
1, Rue Danton - 75006 Paris - FRANCE
tel : +33 1 40 46 36 20 fax : +33 1 40 46 36 29
email : mail@spirtech.com
web : www.spirtech.com

All rights reserved. This document is not binding and the specifications here above can be modified without prior consent.
For more information about Calypso, contact http://www.calypsonet-asso.org.

Version 1.6 - December 2006.