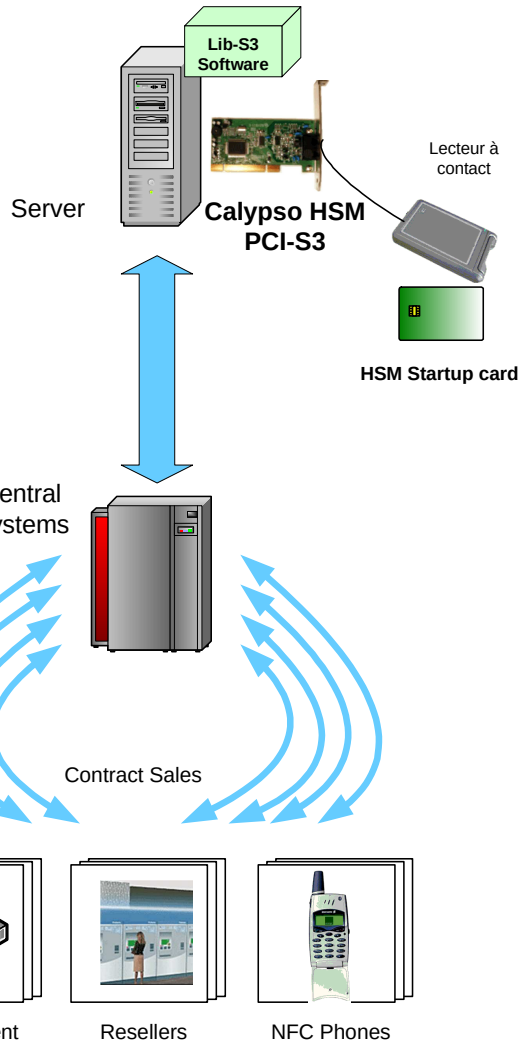
CALYPSO HSM PCI-S3

Remote management of CALYPSO transactions

The ***Calypso HSM PCI-S3*** manages the security of a large number of simultaneous Calypso transactions.

A PCI-S3 advantageously replaces a batch of SAM used for remote vending and personalization operations.



REMOTE CALYPSO TRANSACTIONS: SECURITY MANAGEMENT

Contactless ticketing enables the owner or a portable object (contactless smartcard, NFC mobile phone, etc.) to enter and travel in the transit networks.

In order to do this, the proper rights (transport contracts) are previously loaded in the portable objects by a vending machine or at a vending booth.

This loading is protected by a secure application module (SAM-CL) usually present in each terminal issuing transport contracts. This SAM contains the cryptographic keys necessary for the vending operations.

A SAM is inexpensive, but it is relatively slow and can only manage one operation at a time.

A remote vending server may have to deal with numerous simultaneous reloading requests (for example during the beginning and ending of season ticket periods).

The central management of these vending operations would then require the presence of a large number of SAM connected to the server, which would not be practical.

Furthermore, the SAM lifetime is limited to less than 17 millions operations.

The HSM Calypso PCI-S3 is a powerful secure module which advantageously replaces 100 to 5000 SAM (according to the configuration).

Main functions

- Compatible with the SAM-S1.
- Up to 5.000 simultaneous transactions: vending, personalization or key loading for cards and tickets
- Secure management of the cryptographic keys.
- Internal counters allow to securely audit the key uses.
- Calypso cryptography management.
- Management of the specific security functions of the CD21, Tango and CD97 Calypso products.

Spirtech

CARACTERISTIQUES TECHNIQUES

The Calypso Secure Session

The authorization to modify the data in a Calypso portable object, and its authentication, is done by a session mechanism which comprises:

1) The session opening, that transmits a random value generated by the SAM to the portable object.
2) The readings and writings toward the portable object.
3) The session closing, which transmits a certificate generated by the SAM to the portable object in order to authenticate the terminal and the data written.
4) The transmission of a certificate by the portable object to the terminal in order to authenticate the data read and to prove that the writings have been made.

Central Management of the Calypso Secure Session

During all a session between a portable object and a Calypso SAM (SAM-S1), the SAM remains dedicated to this session.

The central management of multiple Calypso sessions (for example to sell a contract through the Internet or to remotely reload an NFC mobile phone) would require therefore as many SAM-S1 as simultaneous transactions.

The remote sessions may last more than 10 seconds (depending on the network delays), the number of SAM to manage becomes too large when the system becomes popular.

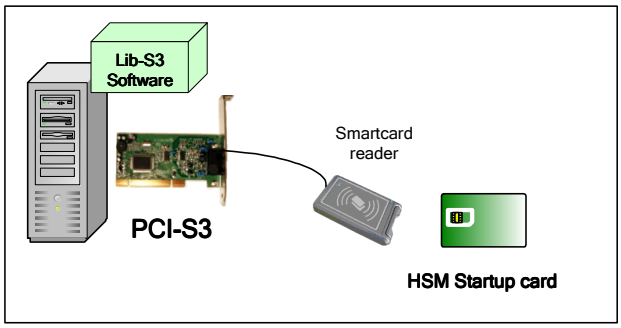
A Calypso HSM PCI-S3, replaces this batch of SAM and allows managing many simultaneous Calypso transactions, thus simplifying the Calypso security management on the central systems.

A light version (SAM-S20), well suited to tests, pilots and small systems, offers the same functions for a reduced number of simultaneous transactions (20).

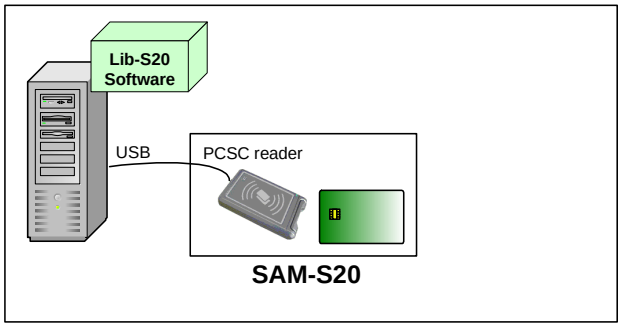
Both configurations include a software library (Windows or Linux) offering the following functions:

- Opening of a channel (equivalent to reserving a SAM-S1).
- Exchanging commands (SAM-S1 APDU format).
- Closing the channel (freeing the reserved SAM-S1).
- Management of independent key groups.
- Key management (transfer, deletion, invalidation).
- Startup secured with a smartcard (possibly installed permanently in a safe box).

PCI-S3 Configuration



SAM-S20 Configuration



Product Range

The Calypso HSM functions are available in two configurations:
- PCI-S3: PCI card for PC
- SAM-S20: ISO 7816 smartcard to be used in a PCSC reader.

PCI-S3 CONFIGURATION

- PCI-S3: HSM card in PCI format (or PCI Express), evaluated FIPS 140-2 Level 3, to be installed in a PC compatible.
- Lib-S3: Software offering all access functions to the PCI-S3 (available under Linux and Windows).
- A PCI-S3 replaces 100 to 5000 SAM-S1, according to the configuration chosen (to be evaluated according to the forecasted load and to the network delays):
  - PCI-S3/100
  - PCI-S3/500
  - PCI-S3/1000
  - PCI-S3/5000

SAM-S20 CONFIGURATION

Simpler to install and less expensive than a PCI-S3 configuration, the SAM-S20 configuration is compatible for the PC software and allow the management of up to 20 simultaneous transactions. Warning: the SAM-S20 lifetime requires changing the SAM-S20 after 16 millions operations.

- SAM-S20: ISO7816 smartcard (ID000 format), based on an EAL 5+ component, the SAM-S20 manages up to 20 simultaneous transactions, connected with a PCSC reader to the PC.
- Lib-S20: Software library giving access to the SAM-S20 (Linux, Windows). The library API is compatible with the S3-Lib API.
- Each SAM-S20 replaces up to 20 SAM-S1.

Practical Information

Available.
Price: contact us.

Usage Rights

The Calypso HSM is marketed under a Calypso license.
You are therefore free to use it with any terminal to do the portable object transactions, including terminals not manufactured under a Calypso license.

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