CALYPSO
FUNCTIONAL PRESENTATION

FP01 SAM and Key Management

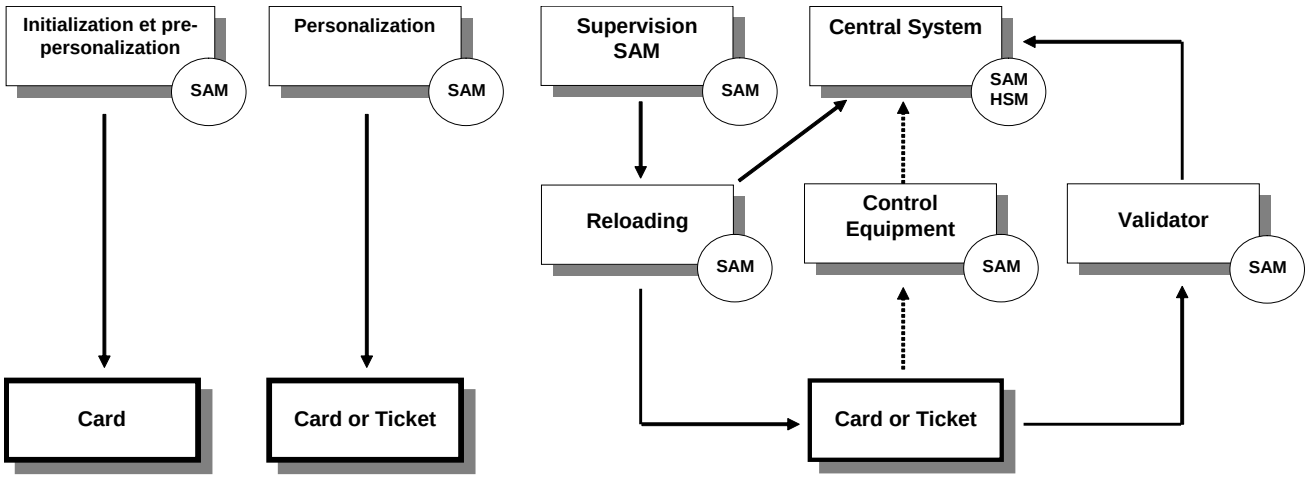
Written by: Frederic Levy 7 March 2014

This document contains an introduction to the Calypso SAM functionalities and to the recommended management of the ticketing secret keys.

Introduction

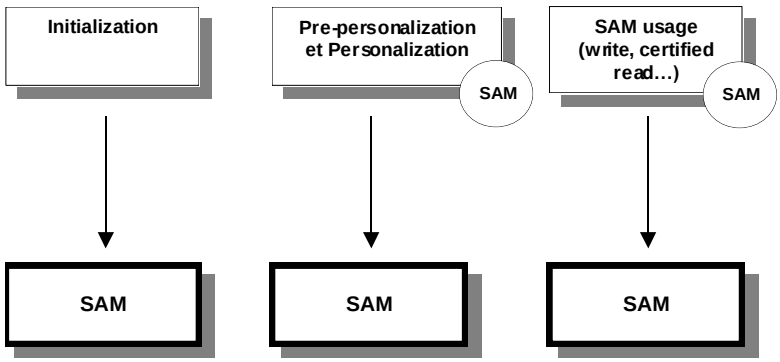
The Calypso ticketing system security is partly based upon the use of secret keys, stored into microprocessor cards and into Secure Application Modules (SAM), which act as a real safe for these data. The knowledge of the keys allows to authenticate the cards or ticket content, and to modify it.

The terminals that dialog with a card or a ticket, at any of their lifecycle phase (manufacturing, initialization, personalization, use, end of life) must therefore be equipped with a secure module that allows and limits their possible actions upon the cards and tickets.



Actually, the secure modules (SAM) are also microprocessor smart cards. The information that they contain are protected by SAM system secret keys (called “SAM keys”). For on-line operations such as remote loading, an HSM (Hardware Security Module) may be used instead of a SAM.

As for the cards, the personalization, authentication, and modification of the modules requires the presence, in the terminals processing the modules, of another module ensuring the confidentiality of the operations.



Furthermore, in order to increase the system security, the modules are not all identical. A module only contains the keys necessary for its use, each of the key being limited only to the necessary actions (ciphering, personalization, etc.).

The Calypso SAM

A Calypso SAM is a secure module working with Calypso cards and tickets:

- It is a microprocessor based smartcard that is usually packaged in a smartcard credit size format, with a removable “mini-SIM” format (format ID000).
- It works according to the ISO/IEC 7816-3 T=0 standard, including PPS mode, and to the HSP mode.
- Its data are organized in files, according to the ISO/IEC 7816-4 standard.
- It allows the use of the Calypso AES, triple DES and DESX cryptography, with 128 bits secret keys.
- It uses the latest generation of microchip and implements the latest algorithms, providing state of the art hardware and software protection.

A Calypso SAM manages up to 126 independent cryptographic keys.

Each key has parameters defining and limiting its usage. Some keys may be used for verification only, or may be subject to a limited number of operations until a “reload” of the SAM by a central supervision system.

A key may be used:

- To manage Calypso card transactions (e.g. reloading a card, validation of a card).
- To manage data signatures used in contactless tickets (such as the CTM512 from ASK, the SRT512 from STMicroelectronics, etc.).
- To manage other SAMs (e.g. to reload a SAM used in a selling equipment).

The number of usages of any key may be traced with a counter, which maximum value (its “ceiling”) may be securely managed to limit the key usage.

The SAM does not interpret the data exchanged with the card, but only authorizes the card modification, or generates and verifies the data signatures.

However, a configurable mechanism called “CAAD” allows controlling the card data modification according to the data location in the card, or to markers at the beginning of the card data.

The Key Management: the Security Architecture

The security architecture defines the different keys used in a specific network, the different SAM configurations and the use of each configuration of SAM.

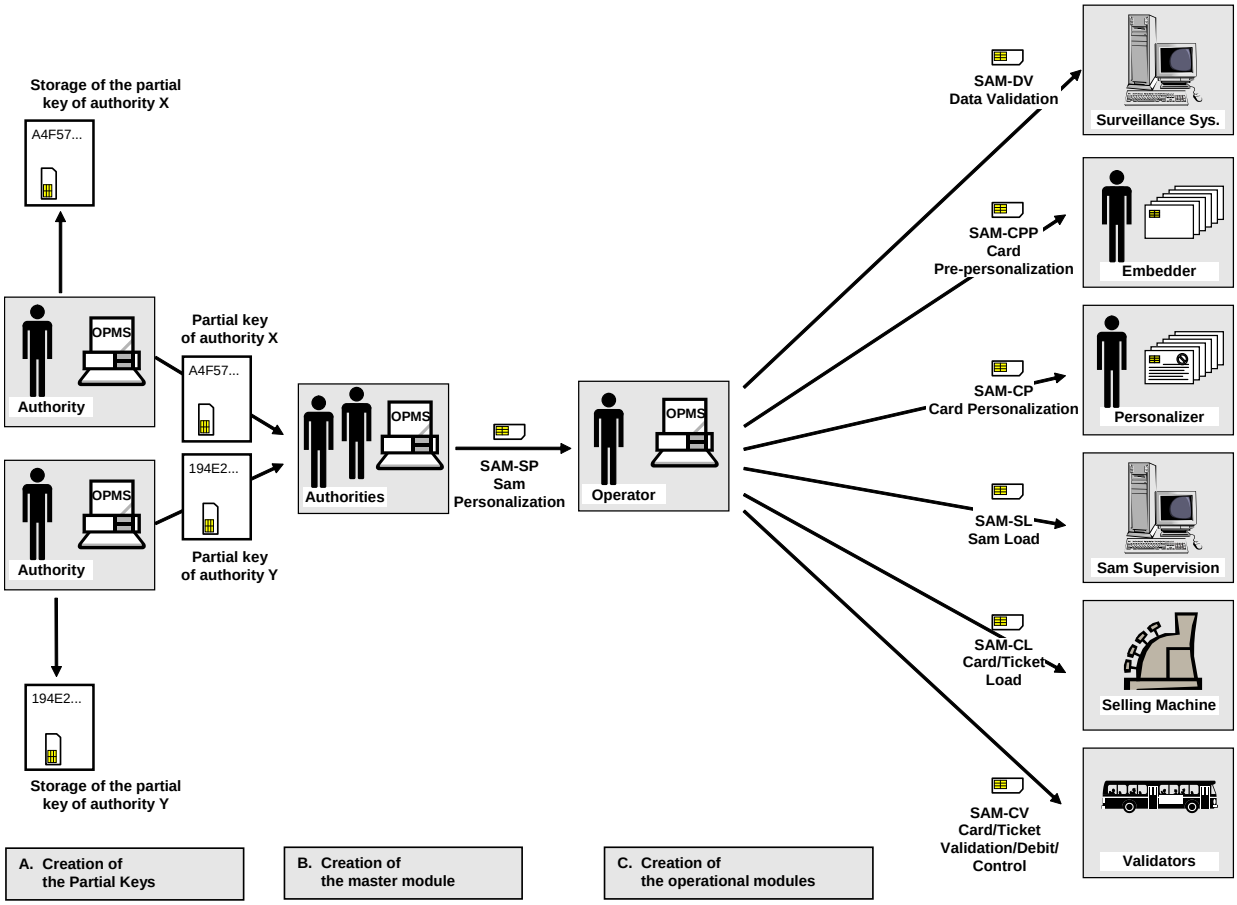
For example, the following SAM configurations may be defined:

- Pre-Personalization: to load the keys in the card during the card manufacturing.
- Personalization: to load the initial card and ticket data, and possibly to load a first contract.
- Reloading: to reload a new contract in the cards or tickets.
- Validation: to verify the authenticity of a card or ticket when entering the network.
- Master: to manufacture in a secure way the SAM of the system.

The security architecture may need to be adapted to the requirements of a specific network.

The Key Creation: the Key Ceremony

The key creation and the SAM manufacturing must be organized to ensure the security of the secret keys and the physical management of the SAMs. For example, the following organization is typically used:



The Key Ceremony allows the initial key creation:

- Create the partial secret keys (one for every entity responsible for a partial key).
- Create the ticketing keys, by combining the partial keys.
- Create the SAM-SP, which allows the creation of the other SAM of the system.
- Execute these operations with the assurance that the keys created remain confidential.

After manufacturing the SAM must be managed according to their level of importance. For example, the master SAM, which allows manufacturing of other SAM must always be protected and kept in a secure safe.

References

Calypso Functional Specification for Ticketing, Card Application, v1.5 *010608-NT-CalypsoGenSpecs*
Public presentation of the Calypso card application.

For access to the detailed Calypso specification, please register at http://www.CalypsoStandard.net.

Modifications History

7-03-2014	Added: AES, counters and ceilings, CAAD, and www.CalypsoStandard.net registration. Editorial improvements.
8-12-2010	Added: HSM and triple DES. Removed DES (deprecated). Updated ceremony diagram. Editorial improvements.
15-01-2003	Creation

Calypso Technical Contact

Spirtech
29 rue du Louvre • 75002 PARIS • FRANCE
spirtech@spirtech.com