Spirtech

SECURE & SMART

Security in the contactless smart card systems

February 2011

Focus On...

Key issues:

Independence : the company responsible for the security architecture design and supply must be independent from the industrialists, particularly card manufacturers and integrators. The authorities and owners thereby remain in control of the security of their ticketing system.

Master SAM (SAM-SP): Organizing authorities should demand the creation of a SAM-SP remaining under their possession. This ensures the authorities' independence from any SAM supplier.

More information:

The vending channels increase (internet, portable terminals, NFC phones, etc.) may require using a centralized security module HSM (not presented in the illustration).

spirtech.com

The general specifications of Calypso security modules are downloadable on the Calypso technical support website.

CalypsoTechnology.net

The Calypso Security Architecture

Calypso is the international standard for ticketing applications: public transports, multi-services and other daily life services. For these uses, the security of the system is a major concern.

The ***security architecture*** defines the process for authenticating and securing Calypso portable objects (smartcards, NFC mobile phones, etc.) and their content. It relies on *secret keys* specific to each application or interoperability area. These keys prevent the use of unauthorized portable objects in the ticketing system.

To remain secret, these keys are securely kept and used inside *secure application modules* (SAM). Configured according to each type of equipment, the SAMs secure the transactions and authentication of the portables objects.

The keys are created during the ***key creation ceremony*** and are stored in a Master SAM, named **SAM-SP**, used to securely produce the other SAMs of the system.

During ***pre-personalization***, the keys are loaded into the contactless portable objects with the **SAM -CPP**.

During ***personalization***, the **SAM -CP** secures the network and holder data writing in the portable objects.

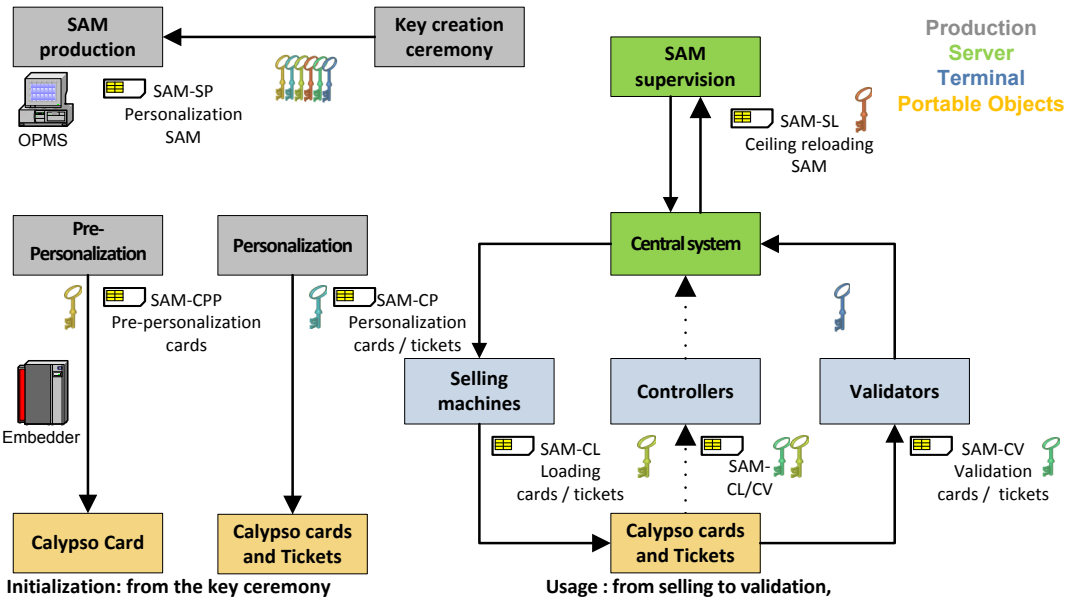
A ***vending equipment*** (automatic vending machine, booth, etc.) uses a **SAM-CL**. Without its secret keys, it is impossible to issue a new contract.

A ***validator*** offers specific services (passenger entrance, goods delivery, etc.). It uses a **SAM-CV** which authorizes the control, the debit and the validation of the coupons.

A ***control equipment*** also uses a **SAM-CV** to ensure the authenticity of the rights stored in the portable objects as well as to provide a proof of control.

Finally, in the central system, the ***SAM Supervisor*** and its **SAM-SL** authorize the SAM-CL of the vending equipments to continue their sales transactions. Therefore, a stolen SAM-CL would be blocked and would only issue a limited number of contracts.

All these transactions are critical since they are subject to high security and performance stakes. The Calypso architecture guarantees the system integrity and improves the customer's experience. The independence of the designer and supplier of the security architecture ensures the autonomy of the system owner.



Initialization: from the key ceremony to the Calypso cards.

Usage : from selling to validation, a secured teleticketing system

Glossary

Calypso: interoperable and multi-suppliers teleticketing standard, designed and managed by its users (Calypso Networks Association).

Key creation ceremony: moment of creation of the cryptographic keys which secure the whole ticketing system. The keys are written in the SAM-SP.

Keys: secret elements protected in the SAMs and cards. They ensure the authenticity of the SAMs, of the portable objects and of their contents. They can also authorize content modifications.

OPMS: SAM personalization tool.

SAM (Secure Application Module): electronic component present in the ticketing equipments (personalization, sales, validation, control, etc.) and which securely contain the secret keys.

SAM-CV: SAM for validation, debit and control operations. Used by the validation and control equipments.

SAM-CL: SAM for loading the contracts (rights). Used by vending equipments.

SAM-CP: SAM for personalization. Used by the portable object production equipments to load the network data and possibly a first contract.

SAM-CPP: SAM for pre-personalization. Used by card manufacturers during production to load the keys into the portable objects.

SAM-SP: SAM for personalization of other SAMs. Used by the OPMS to produce the other SAMs.

More information:

Spirtech Consulting helps the actors of the teleticketing industry in the success of their projects.

Spirtech Consulting offers consulting and expertise services to authorities and operators. Its experts may also advise industrialists during the designing and implementation stages of their Calypso solutions. They carry out interoperability tests on portable objects and teleticketing facilities.

spirtechconsulting.com

Spirtech Consulting : LMCU teleticketing project and ticketing interoperability

In the context of its public debate about mobility initiated in 2008, Lille Métropole Communauté Urbaine launched a modernization plan of its transportation system. The ambitious goal of the project is to ensure interoperability between all urban transit and mobility operators of the Lille area.

Whatever the public transport (metro, bicycle, bus, tram, train) and whoever the operator, a traveller should be able to use the same *Transpole* transport title. The system must be *interoperable* and *multimodal*. *The Calypso standard was therefore the only solution*, furthermore ensuring high security and performances to improve the service to the users.

Security is a priority issue in the implementation of LMCU ambitious goals. Reducing fraud and improving the reliability of the usage statistics are essential to enhance the quality of services of these new teleticketing technologies.

The regional interoperability being a prerequisite, the security must comply with the standards defined by the Nord-Pas-de-Calais Region. Each partner of the interoperability area has to guarantee its system integrity to the other partners.

One of the main ambitions of this project is to allow for *cross-border interoperability* with Belgium (which already uses the Calypso standard for its national interoperability).

The Transpole cards will be used also for *daily life services* (libraries, swimming pools, help to the persons, etc.) facilitating the access of its users to public services.

Spirtech Consulting helps LMCU in the success of this project. Technical and security expertise, multi-application management, remote transactions and multi-modality are the main topics of our collaboration in order to design the best solution between performances and security.

More information:

The Calypso technical website contains all the Calypso specifications

CalypsoTechnology.net

Last versions of our products

Product	Version	Spécification
SAM-S1 Type D	v1.11	000522-SE-SDI-SAMS1D v2.4
SAM-S1 Type E	v0024	041115SDI-SE-SAMS1E v1.3
SAM-S20	v0104	081110FGR-SE-SAM-S20 v1.1
Librairies HSM/SAM S20	v5.1	090225-MU-LibCsm v1.8

The SAM specifications are confidential; they are nevertheless available under NDA on: www.CalypsoTechnology.net.

Events

UITP Mobility & City
10-14 April 2011 : Dubai (Qatar) welcomes an international mobility congress with the participation of Calypso Networks Association.

www.uitp.org

NFC World Congress
19-21 September 2011: the NFC actors meet in Sophia-Antipolis (France).

www.nfcworldcongress.com

6th Assises des TECT
6-7 October 2011: ADCET holds its annual congress on teleticketing and electronic transactions in Lyon (France).

www.adcet.com

Contact and subscription

Spirtech
1, rue Danton
75006 PARIS - France

www.spirtech.com

Links

www.spirtech.com

www.calypsonet-asso.org

www.CalypsoTechnology.net

www.lillemetropole.fr

www.adcet.com

Spirtech

The smart card and teleticketing experts.

Secure & Smart - February 2011
Newsletter by Spirtech - 1, rue Danton - 75006 Paris - France.

Founded in 2000, Spirtech is an independent engineering company, expert in smart cards, cryptography and contactless technology