

## The New HSM Calypso PCI-S3 solution from Spirtech to Secure Remote Transport Ticketing Vending

The *Calypso HSM PCI-S3* is a PCI card securing internet vending transactions for transport ticketing. It is the effective solution to the new security challenges raised by the selling of public transport contracts through the Internet or remotely to NFC phones.

**Paris, 24 November 2009** - Spirtech, an independent engineering and design company, expert in the field of smart cards, teleticketing and cryptography, announced today a solution to the central management of the Calypso transactions.

The *Calypso HSM PCI-S3* meets the needs of modern public transports. Because they serve an larger number of passengers, transit operators have to face an increased number of classic remote transactions (between an internet server and vending machine or internet customers), but also due to the new nomad objects such as NFC phones. These new trends lead to new security challenges.

When a traveler wishes to load a new season ticket or a simple transport ticket in a contactless portable object – cards, phones, etc., what actually happens? This authorization to modify the data in a Calypso portable object is protected by a Secure Application Module (*SAM*) which is normally present in every terminal issuing transport contracts. This *SAM* contains the cryptographic keys of the transit network necessary for the vending operations to prevent any frauds. A *SAM* can only manage one operation at a time, whereas a server needs to manage many simultaneous transactions (for example at the beginning and ending of season ticket periods). The central management of numerous remote transactions would suppose as many *SAM* as there are simultaneous transactions.

**Spirtech designed the solution to this problem and proposes the *Calypso HSM PCI-S3*.** Compatible with the *Calypso SAM-S1* from Spirtech, the *Calypso HSM PCI-S3* can manage up to 10.000 simultaneous transactions (sales, personalization or key loading for cards and tickets). It is installed in a PCI slot of the Internet server PC processing the remote transactions. This technology eases the physical installation and can manage several independent applications (for example different transport networks). François GRIEU, CTO of Spirtech, explained that *“the technical stakes required developing a powerful, easy to use and standard system able to store the security cryptographic keys in a central server”*.

Several international transport operators have already acquired and deployed the Calypso HSM PCI-S3 developed by Spirtech. Users of the Calypso technology they wished to improve their services to their customers allowing them, for example, to securely load their season tickets from home.

Spirtech has chosen the Calypso technology to develop its first version of the **Calypso HSM PCI-S3**. Calypso is the teleticketing standard created by the transport operators and promoted by industrialists. The *Calypso HSM PCI-S3* includes the Calypso license and can therefore be used with any terminal, even if not licensed by Calypso. The integration of a *Calypso HSM PCI-S3* in a teleticketing system is therefore very easy.

Frederic LEVY, CEO of Spirtech, said: *“Complementing the SAM-S1 and the SAM-S20, the Calypso HSM is an important innovation to secure and manage numerous simultaneous transactions. We are glad to contribute one more to simplify the daily life of the passengers of public transport networks”.*

#### **About the Calypso HSM PCI-S3.**

The software library of the HSM Calypso PCI-S3 offers the following functions:

- Opening of a channel (equivalent to reserving a SAM-S1).
- Exchanging commands (using the 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.

HSM Calypso 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 the access functions to the PCI-S3 (available under Linux and Windows).
- A PCI-S3 replaces from 100 to 10,000 SAM-S1, according to the configuration chosen.

#### **About Spirtech.**

Spirtech is an independent engineering and design company, expert in the fields of smart cards, teleticketing and cryptography. Its experts participated to the creation of significant innovations such as the ISO14443 standard and the teleticketing standard Calypso. They also designed the SAM-S1 which is used to secure Calypso transactions all over the world. Spirtech advises transport operators and Calypso-licensed companies when they wish to implement Calypso foster interoperability and multimodality in their teleticketing systems. Spirtech is also the technical assistant of Calypso Networks Association.

[www.spirtech.com](http://www.spirtech.com)

#### **Press Contact:**

email : [contact@spirtech.com](mailto:contact@spirtech.com)

phone : + 33 1 40 46 36 20