Spirtech

SECURE & SMART

Security in the contactless smart card systems

April 2012

Focus On...

Key issues

Distribution channels diversification: with the deployment of NFC-enabled handsets and the remote loading of contactless smartcards, transit operators improve their services to customers.

Security: use of the Calypso application for Java Card provides a high level of security, based on the session and Calypso on strong cryptographic standards.

Multi-actors project: Java Card portable objects offer to many service providers to share the same platform. Thus, transport, access control or payment applications can be loaded into the same SIM for NFC transactions. In this case, agreements should be found between the owner of the platform (mobile operator) and the service providers.

More information

Relevant information related to the Calypso standard:

calypsonet-asso.org

The Calypso specifications are available on the Calypso technical website:

CalypsoStandard.net

More information about Calypso and Java Card be found on the Spirtech website:

spirtech.com

Calypso Applet and remote loading

An ***NFC phone***, a ***Java Card*** or an ***USB NFC fob*** allow multiple service providers to share a same portable object.

Indeed, the standard environment called ***Java Card**** enables an application (transport, payment, university services, etc.) to be dynamically installed, even after the issuance of the object, without compromising the security of the other applications already installed.

The application of each provider (***CAP file****) is loaded into a firewalled secure domain (SD). This domain protects the access to the provider's data by requiring the use of its secret cryptographic keys. These keys ensure the ***authenticity***, ***integrity*** and ***confidentiality*** of the data.

GlobalPlatform* is the set of specifications that standardizes and secures the lifecycle management of the portable object in an environment with multiple providers and different types of actors: portable object issuers, application providers, service providers (called TSM for *Trusted Service Managers*). GlobalPlatform specifies how to load, install, personalize, and , if necessary, remove an application in a Java Card. These operations may be done remotely, via Internet or GSM (in which case, it is called "OTA" : *Over The Air*).

From a ***central system****, administered either by the portable object issuer, or by a TSM, a GlobalPlatform software allows to *load* an application, to *create* an ***instance****, to *personalize* it, and, if necessary, to *remove* it.

Calypso Networks Association (CNA) published the rules to ensure the secure loading of a Calypso application, in accordance with GlobalPlatform and Calypso Revision 3.

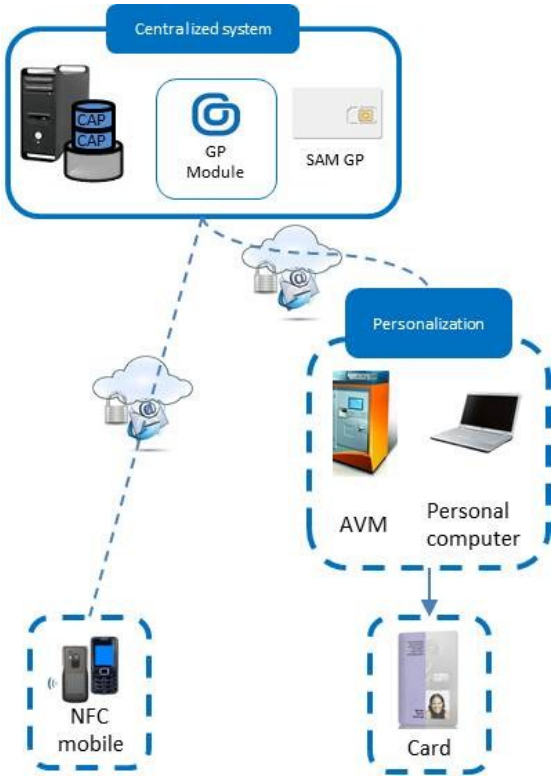
Once certified by CNA, the Calypso software can be transmitted as a CAP file to a trusted service manager or to the issuer of the portable object. The ***secure loading*** into the object is performed locally or remotely, using the necessary GlobalPlatform keys.

The Calypso software is then ***instantiated and activated***: the Calypso application is created with its keys, its files and possible specific data (e.g. a book of tickets for a specific transport network). It is possible to create several independent applications in a portable object from the same Calypso software.

This instantiation and activation are secured with a ***Calypso activation module****.

The activation module, embedded in the central system, secures the loading of the Calypso cryptographic keys (personalization, vending, and validation.

Spirtech can provide the Calypso Java Card application, the ***GP Module****, and testing tools.



CAP File: contains the Java Card application software. For instance a Calypso application software.

GlobalPlatform: specifications allowing the management of applications in Java Card and Multos smartcards. Initially based on OpenPlatform designed by Visa, they are now managed by the GlobalPlatform association.

Instance: data related to a specific application in a card. Several instances may use the same CAP file (eg several Calypso applications).

Java Card: language and operating system allowing the design of card embedded software for smart cards. A Java Card software ("applet") can theoretically run in any Java Card.

Calypso activation module: security module required to activate a Calypso applet.

GP Module : software library allowing the central system to manage the security and cryptography of the secure domains, applications and instances.

SAM GP: security module containing the GlobalPlatform keys which allow managing the Java portable objects. The SAM secures the GlobalPlatform operations.

Central card management system: centralized management system of the portable objects. The central system allows, remotely or locally, to load software, create instances, and modify or remove the applications and instances present in the object.

More information

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

Spirtech Consulting offers consulting and expertise services to authorities and operators. Its experts may also advise industrials during the design and implementation phases. They carry out interoperability tests on portable objects and teleticketing facilities.

spirtech.com

Spirtech Consulting. RUNN, Java Card and GlobalPlatform.

The ***RUNN*** project —*Réseau Universitaire Numérique Normand* or Normandy Digital University Network— invloves the main universities of the French Basse and Haute Normandie, as well as the university restaurants and regional authorities.

Driven by the engineering school ***ENSICAEN*** and initiated by Marc Pasquet, this project prepares a ***digital student workspace*** which will offer a centralized access to the ***university services***, ***digital network hubs*** and a ***multiservice smartcard***.

The multiservice card for universities is an ambitious initiative which will lead to the deployment of 65.000 contactless smartcards to all students of both regions, as well as to university staff.

The multiservice smartcard is a Java Card complying with the ***Java Card*** and ***GlobalPlatform*** standards. These standards allows the secure deployment of applications from different providers in the same portable object. For example for public transport, access control, electronic payment, library access.

With the company Monecarte, Spirtech participates in the design, specifications and implementation of the centralized system RUNN.

Thanks to its in-depth expertise in Java Card and GlobalPlatform , Spirtech assists ENSICAEN in the integration of these technologies in their project.

Spirtech has also designed and developed a ***GlobalPlatform software module*** (called GP Module) which eases the management of the Java cards to add software packages and applications, to update them and, if necessary, to remove them. This module is embedded in the central system supplied by Monecarte.

Spirtech also supplies the Calypso Java Card application which enables public transport applications in the card.

This application implements the Calypso security system in contactless portable objects, particularly in the sim cards of NFC mobile phones, USB fobs and Java cards.

This application is compatible with the Calypso SAM and HSM, and therefore offers a high level of performance and security.

More information

The Calypso technical website contains all the Calypso specifications:

CalypsoStandard.net

Latest versions of our products

Product	Version	Specification
SAM-S1 Type D	v1.11	000522-SE-SDI-SAMS1D v2.4
SAM-S1 Type E	v0025	041115SDI-SE-SAMS1E v1.5
SAM-C1	v0003	101010-SAM Calypso v1.1
HSM/SAM S20 Librairies	v63	090225-MU-LibCsm v1.9
CAS/DAM Librairies	v79	110620CHY-MU-LibCas v1.2

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

Events

CNA - Technical visit
3 May 2012, visit the LRT of Jerusalem (Israel) to learn how the Calypso standard meets the Israeli needs for national interoperability of public

www.calypsonet-asso.org

NFC World Congress
19-21 September 2012, the NFC actors meet in Nice (France) during the exhibition dedicated to this technology

www.nfcworldcongress.com

Cartes & Identification
6-8 November 2012, Paris (France) the world renowned congress gathers all players in digital security, smart technologies, payment and contactless.

www.cartes.com

Contact and subscription

Spirtech
1, rue Danton
75006 PARIS - France

spirtech.com

Useful Links

www.spirtech.com

www.calypsonet-asso.org

www.calypsotechnology.net

www.unr-runn.fr

www.adcet.com

Spirtech

The smart card and teleticketing experts.

Secure & Smart - April 2012
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