Spirtech

SECURE & SMART

Security in the contactless smart card systems

May 2011

Focus On...

Key issues

Triangle 2 : Calypso application allowing the seamless use of ticketing media between regions and countries.

Calypso Revision 3 : latest release of the specifications of the open ticketing standard Calypso. Triangle 2 is compliant with these specifications.

Key management : the Triangle keys must be written in the master SAM (SAM-SP) of the local interoperable area during the key creation ceremony.

Triangle 2: The Trans-Regional and Cross Border Interoperability

Initiated by *Belgium Mobility Card, managed by Calypso Networks Association (CNA)* with the support of the European Union, ***Triangle*** allows transit networks interoperability for travels, between regions and countries.

In order to meet the growing market for interregional and cross-border mobility, Triangle defines common rules for managing **security keys**, a **file structure** and a **data model**.

Triangle is protected by ***DESX*** and ***Triples DES*** security keys, managed by CNA, and present in the SAM of the ticketing equipments. The data model allows loading public transport contracts of any type and duration. These contracts are secured by a signature: the unique identifier of the contract issuer is written into the contract; it cannot be forged and is secured by a SAM.

Triangle is a **Calypso Revision 3** ticketing application implemented in a portable object (smartcard, NFC phone, USB fob, etc.). It can be used independently, or in complement to a local application.

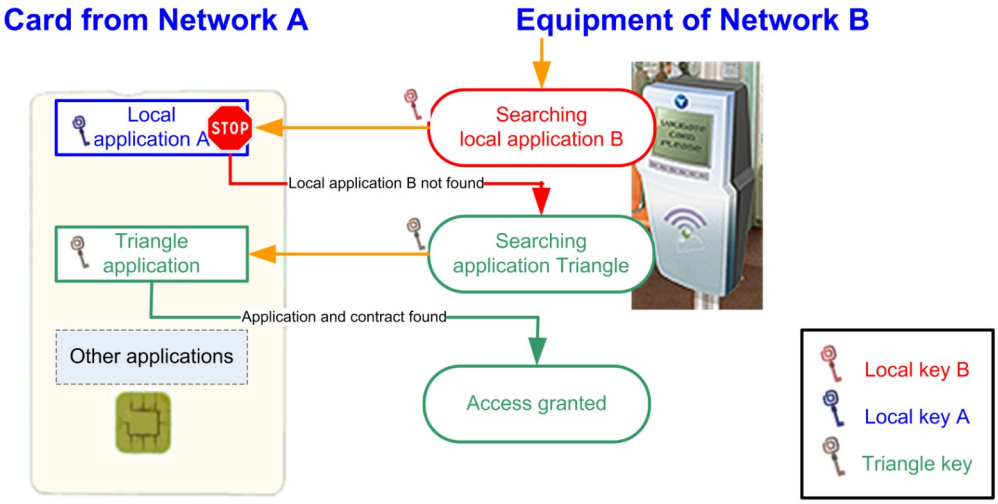
Outside the portable object issuance area, partner operators can directly use the Triangle application to manage local and interregional contracts.

Within the issuance area, the Calypso ***shared files mechanism*** accelerates the validation duration by allowing to validate a Triangle contract from the local application: when a portable object is presented to a ticketing equipment, the local application selected and the equipment may validate either a local contract or a Triangle contract, using the local keys.

Writing a new contract into a portable object require the Triangle keys. This operation is only limited by the memory capacity of the portable object. When available memory becomes scarce, the traveller may decide to erase contracts which are not needed anymore.

Triangle does not require a common back office. Thus, transport authorities can easily extend their interoperable and multimodal range of services and address interregional and cross border mobility needs. Networks wishing to manage interregional fares only need to define these common fares and agree on the corresponding commercial agreements.

The Triangle application is available free-of-charge from CNA.



Validation Outside the Issuance Area

More information

Triangle and the Calypso Standard :

Calypsonet-asso.org

The Triangle specifications are available on the Calypso technical website:

CalypsoTechnology.net

Calypso Networks Association (CNA) : ticketing operators and authorities supporting the Calypso open standard for their interoperable and multimodal teleticketing system.

Data Model : detailed coding description of the data written in the portable object.

DESX : Ciphering algorithm using a 120 bits key and a security equivalent to Triple-DES.

File structure : description of the files (number, identifier, size, security) present in a Calypso portable object application.

Keys : cf. Secure & Smart February 2011.

Local keys : keys securing the application of the issuance area. They are shared by all the partners of the local interoperability area.

SAM (Secure Application Module) : cf. Secure & Smart February 2011.

Shared files : mechanism specified by Calypso allowing the secure and controlled sharing of data between different applications of the same portable object.

Signature : cryptographic data added to the contract information in order to authenticate it and securely identify its issuer

Triangle keys : keys securing the Triangle interoperability ticketing application. These keys, shared by all Triangle partners, are managed by CNA.

Triple DES : Ciphering algorithm made of three successive DES operations, using a double DES key (112 bits).

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.

www.spirtech.com

Spirtech Consulting. Belgian interoperability and Beyond.

The Brussels transport operator MIVB/STIB has initiated the Belgian interoperable teleticketing project ***MOBIB***.

By choosing ***Calypso***, the open standard for ticketing, for their MOBIB system, the four Belgian public transport operators (De Lijn, NMBS/SNCB, MIVB/STIB and TEC) proved their willingness to ensure their independence from any manufacturer as well as their commitment for a strong interoperability of their systems. Grouped within the **Belgian Mobility Card** (BMC) organization, they are fostering the emergence of a common national mobility service.

Furthermore, MOBIB is a **multiservice card**. In addition to public transport, it can be used for car parks, access to museums and exhibitions, bike rental and is open to new services.

MOBIB offers innovative services. Any traveller may buy a contract by phone, internet or other means. When validating, the contract bought is automatically written into the card.

MOBIB can manage numerous transport contracts (ticket book, season ticket), as well as special fares (school, student, senior, etc.), which may also vary according to the location of residence for example.

BMC has decided to include the ***Triangle*** keys in the MOBIB SAMs. Transport authorities of Belgium and those from the north of France are working on using Triangle to facilitate cross border mobility.

Spirtech Consulting assists MIVB/STIB and the Belgian operators since the beginning of the national ticketing project to help them manage its complexity. Spirtech has designed the key and SAM security architecture, written technical documents, carried out test and qualification processes, and helped optimize the card transaction speed.

This experience helps us to successfully assist BMC in the design of the national interoperability framework.

More information

The Calypso technical website contains all the Calypso specifications

CalypsoTechnology.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 v1.4
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 available under NDA on: www.CalypsoTechnology.net.

Events

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

Cartes & Identification
15-17 November 2011, Paris (France) Famous congress bringing together all the players in digital security, smart technologies, payment and contactless.

www.cartes.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.stib.be

www.adcet.com

Spirtech

The smart card and teleticketing experts.

Secure & Smart - May 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