Calypso

Networks Association

CALYPSO & ECLIPSE KEYPLE

CALYPSO & CNA

Overview

WHAT IS CALYPSO?

Calypso®

A SET OF SPECIFICATIONS THAT DESCRIBE A CONTACTLESS,

OFF-LINE, FAST AND SECURE TRANSACTION

BETWEEN A PORTABLE OBJECT AND A TERMINAL

◆ Born in the 90s – partnership RATP Innovatron
◆ To not depend on a unique manufacturer
◆ To foster competition

Not an AFC System !

European projects ICARE and CALYPSO

CALYPSO NETWORKS ASSOCIATION created in 2003

MAIN FEATURES OF CALYPSO

- **A high security level for all contactless transactions**
    - High Security Level for revenue protection
    - Trust in multi-application contexts

- **A large range of compliant products from various manufacturers**
    - To avoid supplier monopoly thanks to an open competition
    - To ensure the durability of the investments (multi sourcing)

- **The basis for the technical interoperability**
    - Between transportation networks
    - Between various services providers

- **Possibility for each Transport Operator to build his own system**
    - Suitable for all public transport environment: scalable, flexible, intermodal

CALYPSO 3 PILLARS

Calypso®

1) Contactless technology + exchange security protocols

ISO 14443 A&B (included in NFC standard) + Session / Ratification protocol+ keys diversified

Protect rights   **Ease access**

2) Secure Element microprocessor able to secure off-line

Fraud-proof +secured transaction (cryptography up to AES + Hash ISO)

Protect rights   **Customise**   **Adapt offer**   **seamless Travel**   **New Services**

3) Tools for a generic transaction

Compliant products   Common rules, commands, files data structure

seamless Travel   compliance with ISO 7816-4

Providing a range of numerous compliant cards & terminals

WORLDWIDE DEPLOYMENT

◆ **25 countries**

◆ **125 cities & regions**

◆ **About 1 billion patented objects**

A MULTIPROVIDER ECOSYSTEM

Supplier	Morpho	Gemalto	Any embedder (Oberthur, etc.)	Watchdata	Oberthur Technologies	ASK	Many embedders including unlicensed (Alios Card, ASK, Gemalto, Morpho Oberthur, etc.)
Product	Calypso MoneoPass	Celego Calypso G1	CDS3 by Innovatron	Calypso TimeCOS	cityGo Calypso	tanGo for Calypso	CD21 by STMicro
Revision	REV 2.4	REV 2.4/ 3.1 / 3.2	REV 2.4 / 3.1	REV 2.4 / 3.1	REV 2.4 / 3.1	REV 1/ 2.4 / 3.1 / 3.2	REV 1/ 2.4 / 3.1 / 3.2
Chip	Atmel	Infineon				Samsung	STMicroelectronics
RF	ISO 14443 B	ISO 14443 A &B				ISO 14443 B	B', ISO 14443 A & B

Supplier	Athena	Gemalto	Oberthur Technologie	Any embedder	KEBT		Giesecke & Devrient	Morpho	Oberthur Technologies	Gemalto
Product	IDProject	Optelio	Cosmo Fly	JCOP by NXP	Kona 27		SkySIM CX	SIMply NFC Evolution	dragonFly NFC SIM	UpTeq NFC SIM
Chip	Atmel	Infineon		NXP	Samesung		SWP link to NFC mobile CLF			
RF	ISO 14443 B	ISO 14443 A &B		ISO 14443 A	ISO 14443 A & B		(ISO 14443 A & B)			

CALYPSO NETWORKS ASSOCIATION

MAIN OBJECTIVE

◆ To maintain **a set of open specifications** addressing transit business needs in the context of developing contactless systems

CALYPSO NETWORKS ASSOCIATION

Not a supplier

◆ Established in Brussels as a non for profit association by the stakeholders of a European research program
◆ Founded by public transport operators
◆ To **promote** the Calypso standard
◆ Open to other businesses and to suppliers

In 2018

89 members

CALYPSO NETWORKS ASSOCIATION

- **Business model**
  - Revenues of licenses based on patents (payed by card manufacturers)
  - Membership fees
  - Sales of services (certification, support for NFC mobile ..)

- **Patents**
  - Contactless communication ISO 14443 B, no more mandatory for Calypso.
  - The Calypso applicative patents, or « Session » and « Ratification », patents.

- **Technical support and technical working group**
  - To ensure a constant improvement of the security features of Calypso.
  - To set up and to maintain a policy of certification
  - To facilitate the emergence of new technologies and services in the Calypso environment

THE CALYPSO ASSOCIATION
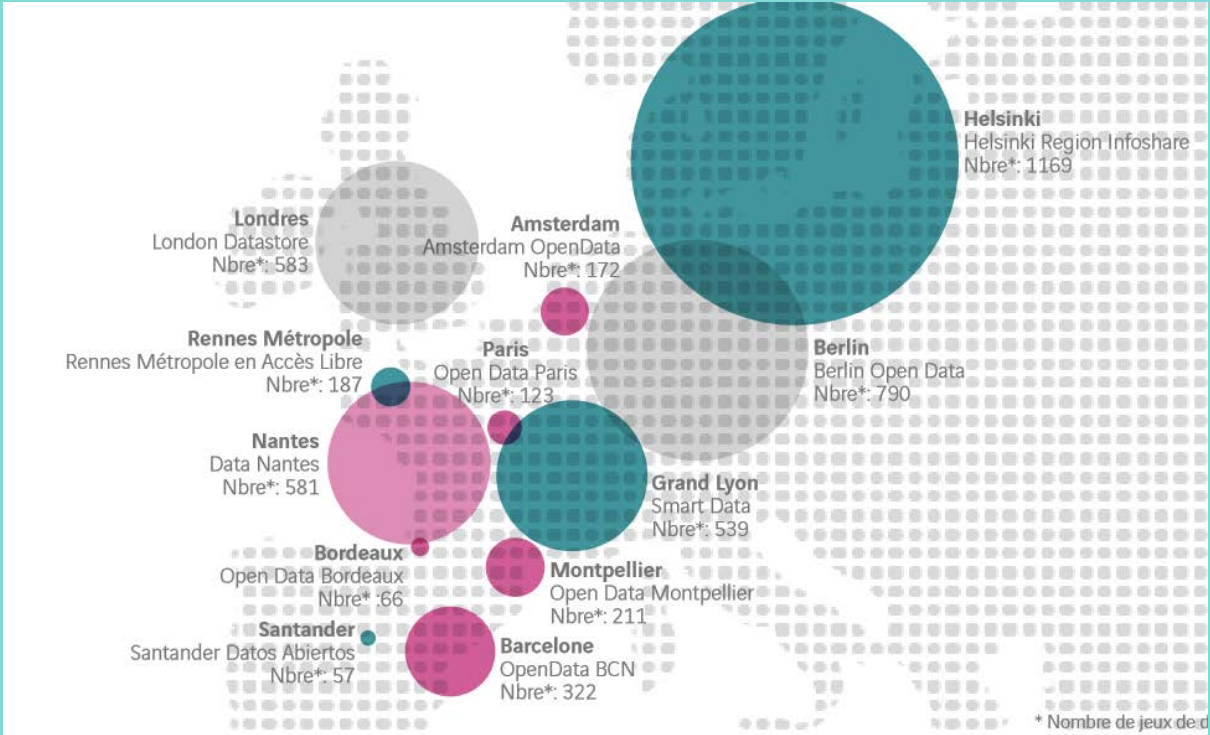
Calypso®

2003

2018
89
members

**FROM AN OPEN
TICKETING STANDARD …**

Calypso®

TRANSPORT SERVICES ARE MORE AND MORE OPEN

HOW IS TICKETING OPEN TODAY?

Calypso®

Achieved **for cards and portable objects** with the Calypso standard: a large choice of products and providers and a real competition

Supplier	Morpho	Gemalto	Any embedder (Oberthur, etc.)	Watchdata	Oberthur Technologies	ASK	Many embedders including unlicensed (Alios Card, ASK, Gemalto, Morpho Oberthur, etc.)
Product	Calypso MoneoPass	Celego Calypso G1	CDS3 by Innovatron	Calypso TimeCOS	cityGo Calypso	tanGo for Calypso	CD21 by STMicro
Revision	REV 2.4	REV 2.4/3.1/3.2	REV 2.4/3.1	REV 2.4/3.1	REV 2.4/3.1	REV 1/2.4/3.1/3.2	REV 1/2.4/3.1/3.2
Chip	Atmel	Infineon			Samsung	STMicroelectronics	
RF	ISO 14443 B	ISO 14443 A &B			ISO 14443 B	B', ISO 14443 A & B	

Supplier	Athena	Gemalto	Oberthur Technologie	Any embedder	KEBT		Giesecke & Devrient	Morpho	Oberthur Technologies	Gemalto
Product	IDProject	Optelio	Cosmo Fly	JCOP by NXP	Kona 27		SkySIM CX	SIMply NFC Evolution	dragonFly NFC SIM	UpTeq NFC SIM
Chip	Atmel	Infineon		NXP	Samesung		SWP link to NFC mobile CLF			
RF	ISO 14443 B	ISO 14443 A &B		ISO 14443 A	ISO 14443 A & B		(ISO 14443 A & B)			

BUT FOR TICKETING EQUIPMENT?

- Terminal applications operating ticketing data (contracts, pricing, user profile) have to be implemented on top of a smartcard management layer.

- Today, implementing a ticketing solution often requires a big investment.

- Only few big transport networks have the control of their solution by requiring the support of specific API to terminal manufacturers, in order to manage themselves their ticketing application.

- But most of networks are linked to a ticketing integrator/manufacturer and evolutions may only be managed in a "purchase by agreement" manner, with a direct impact on the price.

HOW TO FACILITATE NEW MOBILITY & MULTISERVICE APPLICATIONS IN THIS CONTEXT?

- **How integrating new mobility actors ?**

- **How these emerging actors can benefit of the highly secured Calypso transaction "as a service" ?**

- **How Calypso could become the reference in the secured authentication field "Secure Element based" ?**

LEADING TICKETING TO OPEN SOURCE: A NEW CHALLENGE FOR CALYPSO

- It is now time that Ticketing follows the way opened by Passenger Information!

  - By opening up to new principles

  - By facilitating its access to new actors

  - And so facilitating integration of Public Transport ticketing with new mobility services, multiservice in the City

- But in respect of security and interoperability

- **OPEN SOURCE is the way that Calypso intends to follow.**

**TO AN OPEN SOURCE
TICKETING SOLUTION.**

ECLIPSE KEYPLE : A SDK TO BECOME THE REFERENCE IN OPEN SOURCE TICKETING

Q3 2018

First Java SDK Application

- Communicating with a Calypso SE & integrating readers
- Calypso Secured Identification

Next Step

A full ticketing tools kit

- Managing a Calypso portable object
- High level service API

Authentication as a service

Account Based Ticketing

Multiservice

ECLIPSE KEYPLE : A REFERENCE LIBRARY

To facilitate the implementation of Calypso for an as exhaustive as possible range of terminals:

- An open source library available in Java, C++ & C:

- Designed on a mutual Object-Oriented Model

- Compatible with any terminal architecture: mobile/embedded/server

- Interoperable with any smart card reader solution: standard/proprietary, local/remote

- Managing the advanced security features of Calypso

- But also able to manage non-Calypso smartcard solutions, for ticketing or payment
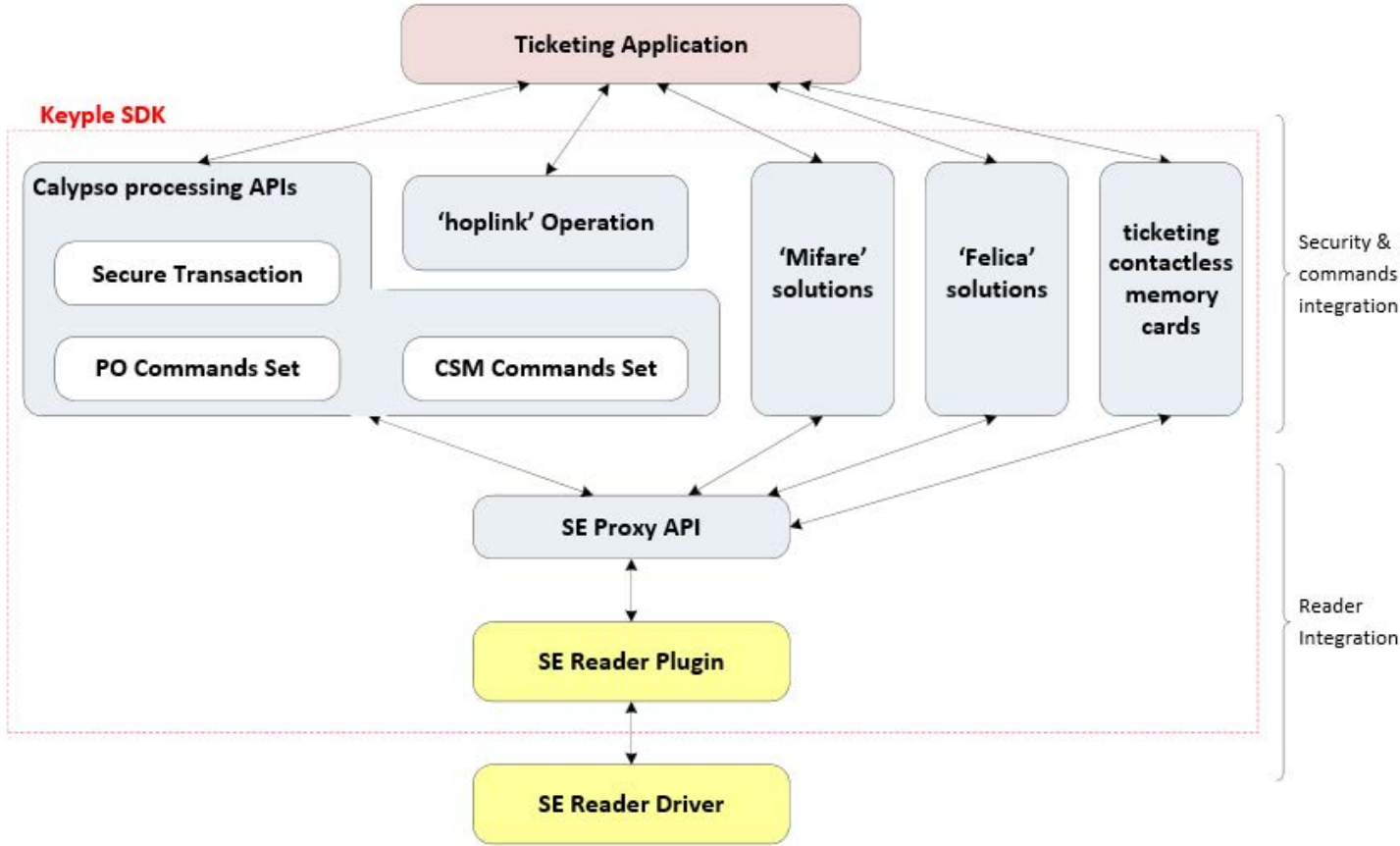
A SDK ANSWERING TO ALL NEEDS

Calypso®

keyple

Calypso Processing API

Universal Secure Element Interface

Eclipse Keyple can be extended at any level: above the SE Proxy, at generic commands' set layer, or higher,

to add Calypso processing,

or to manage other kinds of SE solutions.

A promise:

Ticketing processing implementations independent from the terminal architecture

Eclipse Keyple can be extended at any level: above the SE Proxy, at generic commands' set layer, or higher,

to add Calypso processing,

or to manage other kinds of SE solutions.

SOFTWARE INTEGRATION

HARDWARE INTEGRATION (1/2)

- **Local / Remote** Secure Element optimization:

  Cards or SAM's commands are grouped to limit network exchanges for mobile, embedded terminal or server solution.

- **Standard / Proprietary** SE reader driver:

  Eclipse Keyple will be packaged with plugins to manage standard Secure Element interfaces: Android NFC Reader, Android SmartCard interface, Windows/Linux PC/SC, Java SmartCard IO PC/SC interface.

  Keyple Eclipse can also be extended with plugins implementation to manage proprietary drivers, by smartcard reader manufacturers.
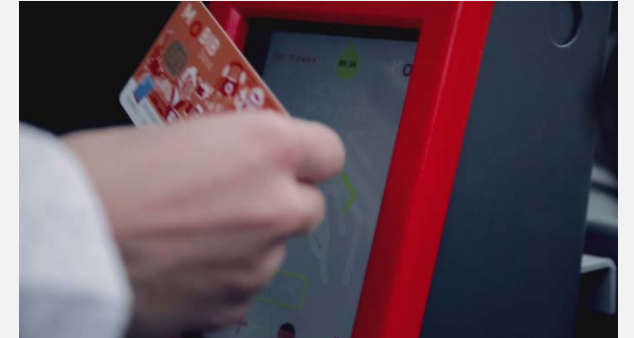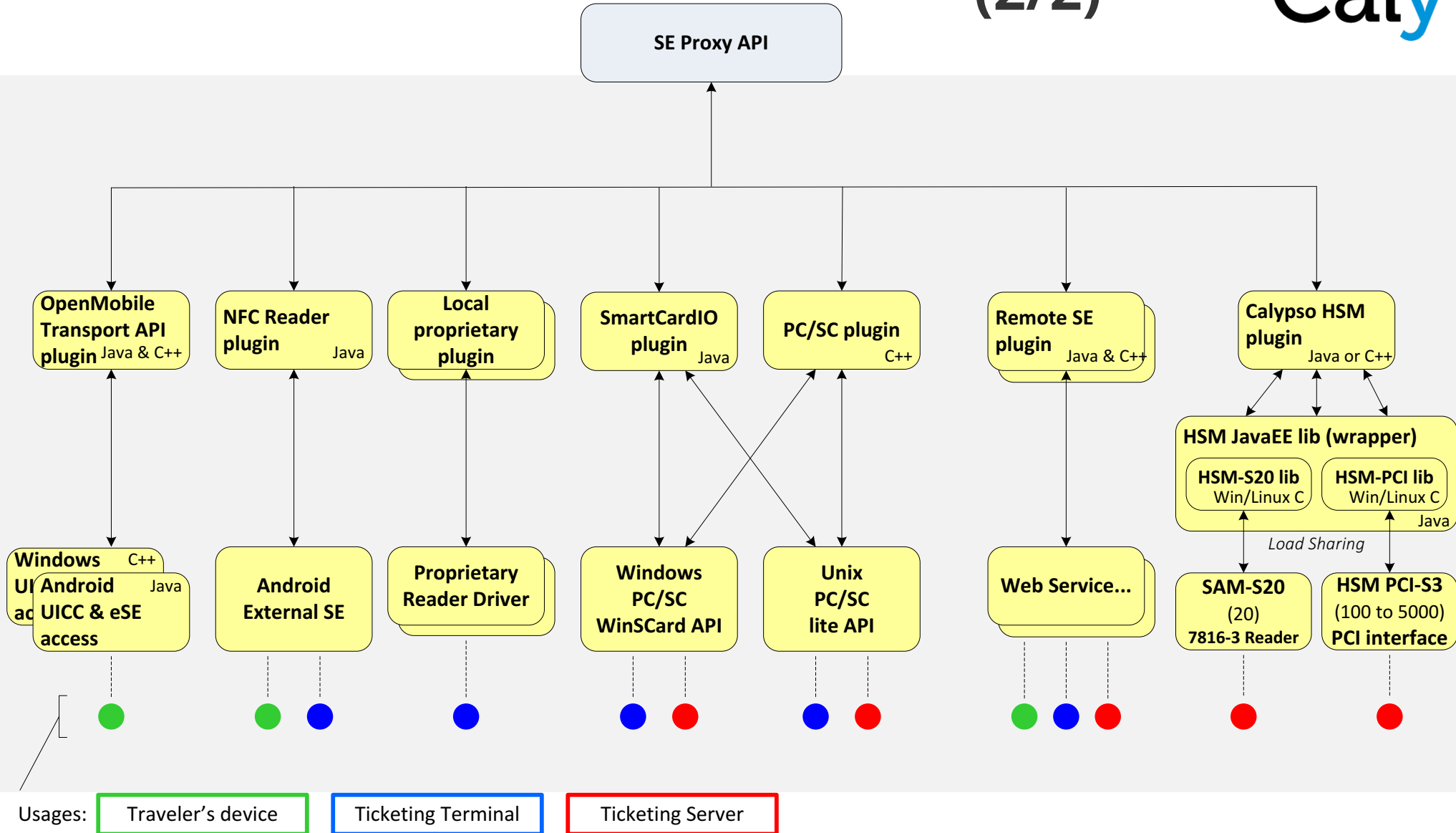
FIRST INTERESTED PARTIES

THANK YOU !

Calypso®