



## CALYPSO open specifications

for secure & interoperable transactions

Gilles de Chantérac  
President of Calypso Networks Association



## Who we are

**CALYPSO NETWORKS ASSOCIATION**  
is not a supplier

Established in Brussels as a non profit association  
by the stakeholders of a European research program,

Founded by public transport business,  
open to other businesses and to suppliers

Objective is to maintain a set of specifications  
addressing transit business needs  
in the context of developing contactless systems.



contactless media specifications  
basically designed from public transport needs  
can address other businesses

- off-line transactions for fast transactions
  - active data inside the card
  - high real-time decentralised security  
can be backed by back office verifications
- possible coupling with payment or other services



## Highlines

- **Secure** transaction for off line transactions
  - High Security Level for revenue protection
  - Trust in multi-application contexts
- **Open and flexible** solution
  - multiple vendors
  - compatible with international standards
  - adaptable to technological progresses :
    - new chips,
    - new form factors (not only cards)
    - new transmissions (NFC)
    - new application management (Global Platform)
- **Compatible with existing organisation**
  - of PTA, transit agencies or operators & associated commercial operators
  - other businesses (banks, telephone, etc.)



## Current implementation

8% of public transit cards

85% of microprocessor cards in transport schemes  
(outside SONY FELICA)

mainly in Europe

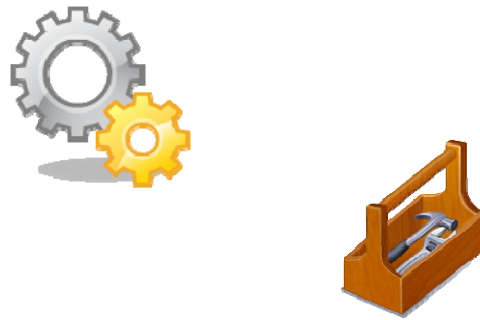
- France, Belgium, Portugal, Italy, Greece, Switzerland ...
- Compliant to the British ITSO national scheme

Chosen for the national scheme in Israel

Chosen by some transport agencies in America



## Technical highlights



## Customer media interface for user oriented interoperability.

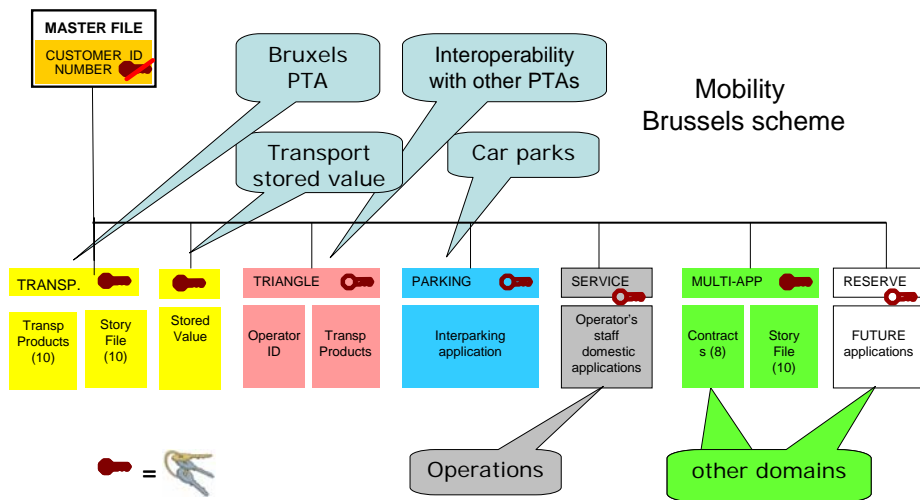




- High Security Level for the media
  - Microprocessor media for off line security
  - Standard cryptography (up to 3DES)
  - Keys per functions (personalisation, load, unload) for each application domain
  - Diversified keys per media for authentication
  - Stakeholders decide if they share the keys
- Set of commands
- Transactions are controlled to be complete



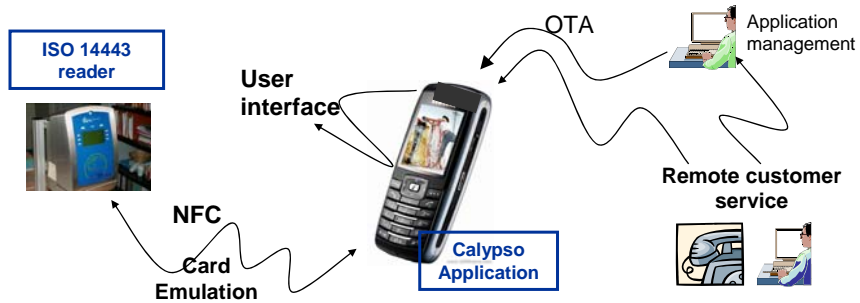
## Open to multiapplication contexts





## from the concept of card to the concept of application

- the same specs can be adapted to global platform contexts
- interoperable process to load and use ticketing products in the application (under definition)



## About payment and transport

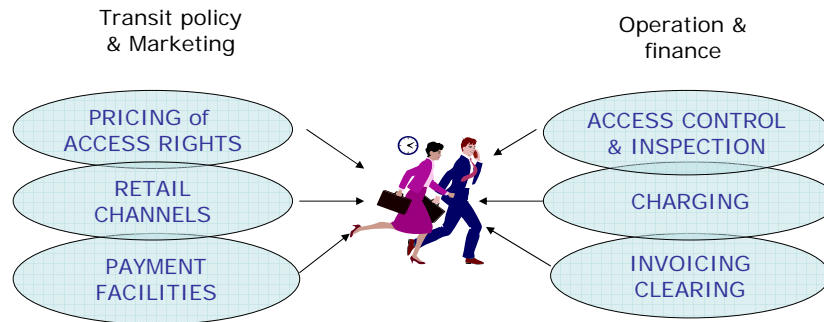


- Transit industry to move people
- Financial payment industry to move money



## Fare collection is not only payment

Contactless AFC makes Transit Agencies think commercial organisation all new & customer oriented



Managing products and policies is their strategic issue.



## For transit industry, products are access rights and related fares

- In the ISO business framework, (ISO24014-1)  
transit products are access rights & associated fares (what you sell)  
vehicles, services, etc are the production (how you produce)
- Payment means are not products.  
They move the money from travellers to transit agencies
- Stored value is a transit product.  
Loading a stored value is paying a product  
whatever payment means is chosen by the customer  
Debiting a stored value is using a product.  
no money moves, no payment
- Electronic purse is a payment means

## Scenarios for integration

(ISO meeting – Munich – April 2008)

- Payment medium used for ID
- Payment transaction accepted as a ticket
- PT products stored in payment application
- PT and Payment applications on one chip

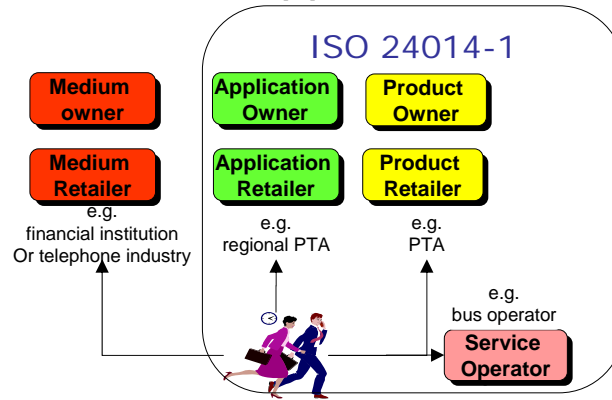


Separate applications  
the most realistic generic scenario

Policies will be different for long

- *≠ institutions & business organisation*
- *≠ political choices to fund PT*
- *≠ geographical scales*

## Products < Application < medium



- *Need for a common technical base*
- *Need for an organisation framework*

## Open specs

for technical and business acceptance

- **STANDARD SECURITY ALGORITHMS**  
The larger the interoperability,  
the more secure the medium must be.
- **FLEXIBLE PROCUREMENT**  
The larger the interoperability,  
the more open and flexible procurement
- **NEUTRAL TO BUSINESS ORGANISATIONS**  
The larger the interoperability,  
the more neutral towards fare policies
- **NEUTRAL TO SYSTEM ARCHITECTURE**  
The larger the interoperability,  
The more different systems you meet



Similitude / difference  
between Calypso and contactless EMV  
to be examined

- Internal work package recently decided by CNA
- Common work to be an opportunity for progress for both transit and financial payment industries



Thank you for your attention

Let's work together



Calypso Networks association  
[contact@calypsonet-asso.org](mailto:contact@calypsonet-asso.org)  
<http://www.calypsonet-asso.org/>

