Considerations on how to integrate different transport model schemes together

Dr. Ralph Gambetta
Head of Promotion
Calypso Networks Association (CNA) – Belgium
Kranjska Gora, Slovenia, 27.02.2013
• Calypso’s Introduction
• Transport Operator eco system
• Necessary evolutions for smart ticketing
• CNA Calypso applet presentation
• Java world
• NFC world
• Interoperability
CALYPSO NETWORKS ASSOCIATION is not a supplier

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

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

**as full members:** All operators or operator associations including organising authorities, using calypso technology

**as associate partners:** Industrial licensees, distributors, consultants, and other operators & organising authorities

- Main Objective is to maintain a set of open specifications addressing transit business needs in the context of developing contactless systems.
Calypso = Multi-application Interoperability Intermodality

Customer area

(1) Terminals
   - Issuing
   - sales & reloading
   - Validation

(2) Concentrators

(3) Central system

(4) Clearing

AFC system

INDEX
Calypso isn’t an AFC system, but a set of specifications for the card/terminal transaction, providing:

- **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 industrialists
  - to avoid supplier monopoly thanks to an open competition
  - to assure durability of investment (multi sourcing)

- **The basis for the technical interoperability**
  - between Transportation networks
  - between various services providers

- **Possibility for each T.O to build his own system**
  - Suitable for all PT environment: Scalable, flexible, intermodal

- **A real multi-application management:**
  - Park, access control, e-purse, city card, tourism, stadium etc
1) Contactless technology + exchange security protocols
   ISO 14443 A&B + Session / Ratification protocol+ keys diversified
   Ease access  Protect rights

2) Smart card µprocessor only able to secure off-line
   Fraud-proof +secured transaction (cryptography up to 3DES + Hash ISO )
   Protect rights  Customise  Adapt offer  seamless Travel  New Services

3) Tools for a generic transaction
   Common rules, commands, files data structure
   compliance with ISO 7816-4
   Compliant products  seamless Travel

Providing a range of numerous compliant cards & terminals
Transport Operator eco system
Transport Operator eco system

**Political framework:** laws making process, policy, opinion leaders, mainstream, ..... 

**Legal framework:** dedicated laws, company forms,...

**Economical framework:** financial instruments, funding,...

**Societal framework:** demographic development, change of values,...

**Technical framework:** product maturity, development time, R&D, spirit of innovation,...
Many European and non European transport companies find themselves inside of such an eco system:

- Municipal company
- Low political support
- Decrease of usage
- Old rolling stock, vehicles
- High maintenance costs
- Insufficient service orientation
- No company culture
Transport Operator eco system

- Technical guidance of management processes
- No integration of transport modes and transport networks
- Deregulated competition
- Private operators
- No fare integration
- Lack of any form interoperability

- Necessity of investment funds
But there are restrictions for transport operators:

- Low eligibility for credits for transport operators
- Municipalities are as well of low trustworthiness
- Legal framework
- Low visionary competency
- Business model is unclear
Action plan for transport operators

Structural set up of actions:

• Development of a coherent „policy“

• Create the necessary minimal legal framework

• Sector relevant regulations

• Development of a sustainable business orientation

• Set up of competence

• Customer orientation

➢ Realisation of these actions will strengthen the position of transport operators in their negotiation of the choice of financial and business models
Most wide spread approaches:

- Full financing of projects through supranational, national, regional or/and municipal funding mechanisms,…

- Partial financing: own resources and investment from third parties, PPP, creation of new shared companies,…

- Outsourcing,…
strategic plan

1. Consolidate and enhance the ticketing system’s **contribution** to company performance
2. Improve **ease of use** for clients and develop new payment and recharging methods
3. Increase the **accessibility** of ticketing systems
4. Expand the **opportunities** offered by a scheme
5. Develop an **evolution** program
6. Strengthen **collaboration** with partners
7. Improve **internal work** methods
Necessary evolution with smart ticketing
Cost of sales via internal personnel: **11 to 15 %**

- Very high cost and restrictive as to methods of payment, hours and locations

Cost of sales via equipment: **4 to 6 %**

- Rather high cost and restrictive as to hours and locations

Cost of sales via outside agencies: **2 %**

- Very low cost but restrictive as to hours and locations

Cost of sales via Internet, mobile phone: **1 to 2 %** (when mature)

- Very low cost and clients can purchase fares anytime, anywhere and on the device of their choice
Better accessibility for clients
- « Where, when and how I want it »
  - At home, at the office, on the road
  - Reduction in waiting time

Decrease in costs for operators
- External recharging terminals
- Electronic payments

Evolution: Develop remote sales & recharging system
My telephone becomes my card and allows me to consult, select and buy my transit fares.

My telephone becomes a hand-held fare vending machine. I can recharge my children’s cards or transfer a ticket to another card user.
Occasional clients could use their contactless payment cards instead of traditional fare cards.

Following registration with transit operators, regular clients could also use their contactless payment cards as identifiers for access to « best price » fare calculations.
My card also enables me:
- to use BIXI and car-sharing and to access parking at a reduced rate

My card also provides a link to city, cultural, recreational services …
Calypso going to Java Card way multi application platforms
From native card centric to S-W application centric

1) Calypso decided to take the Java Card™ way

- **Java Card**: A powerful tool from the Java concept running environment based on a virtual machine

- **API GlobalPlatform GP™** (Application Programming Interface)
  - Indispensable for the concept
  - The most disseminate as possible

2) Calypso: an easy Java Card/ GP approach
Thanks to the Calypso specifications respecting the standards (ISO 7816 in particular)

`‘Calypso generic Applet’ fully GP compliant & ready to run on Java cards`
The Common platform

Java card™+ Global Platform:

- Several “Security Domains”
- Identical interface to download various applications (GP)
- Dynamic application management
- Actors & scenarii administration
- Large dissemination (2 billions devices)

The target: the Platform implemented in a lot of usual devices of clients
CNA has the full property of a ‘Reference Calypso Applet’

- CNA will deliver its applet free of charge and in a non discriminatory manner to any PTO / TSM
- CNA taking in charge its distribution, maintenance and management.

CNA applet fully compliant GP

- Delivered under several different compilations compliant with the different extant versions of Java Card and GP
- Downloaded, installed and instantiated under the different versions of Java Card / GP specifications.

CNA applet compliant with Calypso rev 3.1 & rev 2.4

- instantiated and activated under the types files structures defined by rev2.4 & rev 3.1 of Calypso
- pre-personalisation, and personalisation under the existing Calypso protocols are the same as with native cards
Ticketing standards

Selection of standards:

- Media Interface: ISO 14443
- Secure element file structure: ISO 7816-4
- Protocols for smart ticketing appl.: CEN TC278 WI 278344
- Secure element security: ISO 15408
- Data commands: Global Platform
- Operating systems: Java, Android, ...
- Security algorithms: Global Platform (3DES, AES, RSA)
- Smart ticketing roles: EN ISO 24014-1
- Transport data elements: EN 1545
Java world
For some time in a lot of e-ticketing projects a new magic word is born:

**EMVco / Credit card payment**
- presented as the paradigm solution for ticketing
- Answer to all complex ticketing requirements

Can ticketing be reduced to a simple payment act?

- Can bank & payment networks be substituted for a ticketing system?

What is hidden behind?
Public transport IS a MARKET of SERVICES

- raising the perception, awareness and image of this service
- Increasing usage & customer numbers
- selling more and more services to potential customers
- satisfying customers to make them buy again and again

a Marketing approach to the clients by T.O is essential
& The “Ticket” is the best marketing vector

Mobile citizens.....
prefer to
are able to
wish to
have to
Coexistence scenarios

Payment transaction “accepted” as a ticket for a single trip in flat fare
  • more dedicated for “occasional”

Transport and Payment applications on one “Portable object (mobile, USB sticks, etc)
  • T.O save support & distribution cost

Payment medium used for ID
  • Into a virtual transport account

Transport products stored on payment media.
  • To be agreed, defined & provided
Separate applications
the most realistic & generic scenario

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

only some technical convergence

Transport application coupled with Payment application offers
the real convergence of business
RAVENNA
Co – Branded Card

Poste, Mastercard and PT – operator

A.T.M.
Azienda Trasporti e Mobilità S.p.A.
Banking Card

The Banking card is a multi-application JavaCard with an EMV application and a Calypso Rev3 Cardlet thus combining both Worlds without compromising the system performance and requiring the transport equipments to comply with EMV requirements.

The card is used in the transport system almost like an anonymous card with the client being charged the value of the trip *a posteriori*. The system allows each operator to have their specific tariffs when handling this type of product.
Every sector keeps his competence:
- Bank for payment
- Transport for specificity of ticketing aspect

Definitely to avoid:
Mixing the competency areas because e-Ticketing infrastructure is more than a banking POS.

➡️ Multi-application cards emitted by whoever is an additional distribution channel (with multiple advantages) but a cheapest distribution channel as it is, will NOT replace any loaded application.
NFC world
- Tools
- State of art in France - -
- Nice
NFC in France: Industry Sectors engaged to date

Payment

PEGASUS

Specifications for interoperable mobile payment schemes

Transport

ULYSSE

Functional requirements for public transport application

Retail/Distribution

ERGOSUM

Joint definition of a coherent mobile shopper experience

End-to-end technical specifications for all types of services and interoperability/compatibility mark.
Applications range

- Smart posters
- Loyalty
- Transport
- Payment

Thousands of paying customers equipped with NFC handsets

A wealth of services, stored in the SIM

New sales & support processes
Nice: a NFC show case in France
Reading NFC tag or 2D barcode

Envoyez par sms:
azur xxxx
au n° 31000
NICE : NFC Customers feeling

- Purchase/ validation transport ticketing
- Shopping: Purchase & payment
- Real time ‘Travel information’
Interoperability in Europe
• Payment processes are no longer a barrier to the use of Public Transport across EU

• Seamless accessibility to different Public Transport Networks using the same Portable Media

• Smartcards will have migrated to a Secure Element on a Portable Object (Mobile Phone, PDA, USB device etc)

• Individual IFM Applications can co-reside in a multi-application environment

• An EU-IFM Application usable across many Networks?
IFM Customer media demonstration
VDV-ITSO-Calypso ‘On demand’

Java card JCoP 31 82K
Standard product on the shelves
Interoperability in Belgium
MOBIB becomes Belgian

- Brussels started in June 2008 and is about to complete its smart ticketing system this year
- National railways will start with seasons tickets during 2013 and expects to finish in 2014
- Flanders and Walloon forecast a complete deployment in 2014

So, mag stripe tickets will be history end of 2014!
Brand management of MOBIB
Brussels scheme open to multiapplication contexts

- Brussels PTA
- Interoperability with other PTAs
- Transport stored value
- Car parks

Mobility Brussels scheme

Operations
Other domains

- TRANSP.
- TRIANGLE
- PARKING
- SERVICE
- MULTI-APP
- RESERVE

- Master File
  - Customer ID Number

- Transp Products
- Story File
- Stored Value
  - Operator ID
  - Transp Products

- Interparking application
- Operator's staff domestic applications
- Contract (8)
- Story File (10)

- Future applications
TRIANGLE 2: A strong way forward to realise easily interoperability

• TRIANGLE 2 interoperability allows to load locally a transport contract on a media non locally issued

• TRIANGLE 2 interoperability allows also to load locally on a locally issued media a transport contract that can be validated somewhere else

• Triangle 2 application to be implemented after the local one will use shared secret keys and some operational common rules

So combining the local application and the TRIANGLE 2, such media appears to be UNIVERSAL!
Calypso is already running on:

- G &D
- Calmell
- Gemalto
- TOP
- Oberthur BMS 2
- Atmel
- Type B
- Infineon SLE 77 CL xx
- Type A&B
- NXP Smart Mx
- Type A
- Atmel
- Type B
- Samsung
- Type B
- NXP
- JCOP
- Gemalto
- OPTELIO
- G&D Sm@rtCafé
- Oberthur COSMO Fly
- Athena IDProtect
- KEBT KONA 27
- Gemalto City 4K
- Oberthur City go
- Athena
- IDProtect
- NXP Smart Mx
- Type A
- Oberthur
- COSMO Fly
- G&D Sm@rtCafé
- Calypso Application / mask
- ASK Calypso applications
- Morpho BMS2
- ASK
- Watchdata
- G&D CD21
- Calmell
- G&D
- Morpho
- Oberthur
- Gemalto
- NFC World
- Javacard / GP
- UICC (SIM)
- SWP
- Java Card / GP Domain
- NFC
Calypso Networks Association
Promotion Group
Dr. Ralph Gambetta
Rue Royale 76
B-1000 Brussels

Tel.: +49-172-7146234
wg3leader@calypsonet-asso.org
www.calypsonet-asso.org