Abstract

Today, transport operators have to rise to the dual challenge of improving service quality and maximizing their income.

Until recently, passengers were anonymous. They have now become customers and require a seamless access to transport. Related services should simplify their daily life while fostering their loyalty and maximizing their relationship with the transport network.

Transport operators also have to improve corporate management by avoiding fare evasion and by adapting the supply to the demand.

The new system of electronic ticketing is now playing a major role throughout the whole transport system. It is for this reason that it must be secure and reliable.

Calypso was designed to meet these challenges. It offers the best solution, suited to all transport needs: open, widespread, secure and proven. Moreover, Calypso is not simply restricted to transport applications but also offers the perfect opportunity to enable access to third-party services, using the same device within a multi-applications scheme.
Contents

- **Introduction** ................................................................................................................. 6
  - Definition of Calypso ............................................................................................... 6
  - History ....................................................................................................................... 6

**PART I: Using Calypso** ................................................................................................. 8

- **Main Calypso references** ......................................................................................... 9
  - Calypso in Belgium .................................................................................................... 9
  - Calypso in Canada ..................................................................................................... 9
  - Calypso in France ...................................................................................................... 10
  - Calypso in Israel ....................................................................................................... 10
  - Calypso in Italy ......................................................................................................... 10
  - Calypso in Portugal ................................................................................................. 10
  - Calypso in the United Kingdom .............................................................................. 11
  - Calypso in other regions ......................................................................................... 11

- **Calypso main assets** ................................................................................................. 12
  - User driven ................................................................................................................ 12
  - Fast and secure ......................................................................................................... 12
  - Ready for new trends ............................................................................................... 12
  - Open to new services .............................................................................................. 13
  - Facilitating back-office integration ......................................................................... 13
  - Encouraging competition ....................................................................................... 13
  - Fully interoperable .................................................................................................. 14
  - Adaptable and flexible ............................................................................................. 14
  - Adapting the supply to the demand ....................................................................... 14

- **Calypso faces mass transport new challenges** ......................................................... 15
  - Interoperability ........................................................................................................ 15
    - At the administrative level ...................................................................................... 15
    - At the customer level .............................................................................................. 15
    - At the fare management level ................................................................................ 15
    - At the technical level ............................................................................................. 16
    - Calypso interoperability through the Triangle application .................................. 17
  - Calypso open to new technologies .......................................................................... 18
    - A main step towards Java Card technology .......................................................... 18
    - Convergence with contactless bank cards ............................................................. 18
  - Multi-application ....................................................................................................... 18
• **Which business model for operators?** ..................................................... 20
  Card and infrastructure costs ................................................................. 20
  Customer relationship management ......................................................... 20
  New sales channels .............................................................................. 21
  Multi-application medium ....................................................................... 21
  Fare evasion reduction ........................................................................... 21

• **Practical guideline to getting started with Calypso** .............................. 22
  Elements of a Calypso ticketing system .................................................. 22
  ▪ Microprocessor smart cards .................................................................. 22
  ▪ CNA Calypso applet .............................................................................. 22
  ▪ Terminals ............................................................................................... 22
  ▪ SAM / CSM ............................................................................................ 22
  ▪ Secret keys ............................................................................................ 23
  ▪ Back-office integration .......................................................................... 23

  Recommendations for the practical implementation of a Calypso ticketing system .................................................. 24
  ▪ Introduction .............................................................................................. 24
  ▪ Calypso interoperability basis ................................................................. 24
  ▪ Data models ............................................................................................ 26
  ▪ Cryptographic keys ................................................................................ 26
  ▪ Conclusion ............................................................................................... 26

PART II: The Calypso technology .................................................................. 28

• **The Calypso technical framework** ......................................................... 29
  Ticketing transaction layers ...................................................................... 29
  The communication interface layer .......................................................... 30

  The memory organisation .......................................................................... 31
  ▪ Master File (MF) ................................................................................... 32
  ▪ Transport files ....................................................................................... 32
  ▪ Stored value files .................................................................................. 32
  ▪ Citizenship files ..................................................................................... 32

  The secure transaction layer ...................................................................... 33
  ▪ The Secure Application Module (SAM) .................................................. 33
  ▪ The secret keys ....................................................................................... 33
  ▪ Secret key sharing .................................................................................. 34
  ▪ Key creation ceremonies ....................................................................... 34
  ▪ The cryptographic algorithms ............................................................... 35

  The Calypso Secure Session & Ratification .............................................. 35

  The data model .......................................................................................... 36
  A terminal API .......................................................................................... 36
  The security architecture .......................................................................... 36

• **Calypso versus other technologies** ....................................................... 38
  Standard compliance ................................................................................ 38
  Transaction completion ............................................................................. 39
  Security ...................................................................................................... 39
PART III: The Calypso ecosystem

- **A glimpse of other Calypso features**

  Enhancements to the specifications

Certification

- Specification of portable objects
- Portable objects and applets
- SAM
- Terminal registration
- Complete terminal certification

Calypso license policy

- License main objectives
- A license for the benefit of Calypso’s users
- License conditions

Smartcard durability

Calypso and users privacy

- **Calypso organisations**

  Calypso Networks Association

  - Calypso Networks Association membership
  - Present Members (2014)
  - CNA Activities
  - CNA Funding

- **Glossary**
Introduction

Definition of Calypso

This Handbook gives an outline of the Calypso technology, including its history and its recent developments. Its aim is to better explain the strength of the Calypso concept and to discover the range of its possible applications.

Before going into details, it is important to define exactly what Calypso is. A good definition would be:

*Calypso is a set of technical specifications describing a fast and secure contactless transaction between a terminal and a portable device.*

A *Calypso portable device* (or Portable Object in the Calypso terminology) was historically a microprocessor smart card, but, as technology moves on, it could now be one of the following devices:

- Traditional contactless smart cards
- JAVA contactless cards
- NFC mobile phones
- USB key with a contactless communication interface (smart key)
- Any other contactless customer media

Beyond this simple definition, Calypso is the appropriate solution suited to transport and mobility needs. It stems from an approach that transport operators introduced in the nineties. It is an open technology, free from any manufacturing monopoly making it both economical and adaptable to evolving future technology changes.

The Calypso vision is to meet the current and future demands and requirements of all the transport providers in the world.

Calypso offers a standardized and multi-application solution while preserving individual data protection.

Calypso technology is a bespoke and progressive solution for all transport operators.

History

In the early nineties, several transport operators and authorities in Europe were facing the issue to renew their existing ticketing system, based on paper or magnetic ticket technologies. They were aware of the huge possibilities that the emerging smart card could bring in their business, both in economic terms and possibilities to offer new services to their customers.

Some experimentations using contact smart cards had been realized, but unsuccessfully because, if the functionalities were really promising, the time of transaction of contact smart cards was completely incompatible with the requirement of access in transport networks, whether bus or metro.
It appeared clearly that the transaction had to be contactless to be enough quick, and facing a total lack of industrial solutions in this field, several transport operators in Europe undertook initiatives to develop a solution fitting their requirements.

Among them, RATP built a partnership with INNOVATRON, the company owned by Roland Moreno, inventor of the smart card, partnership joined by SNCF, to create a smart card contactless technology adapted to many markets, including public transport, the Contactless Pass. The principle of the partnership was to open the results to as many manufacturers as possible, through a license policy, in order to ensure a seamless compatibility between products and a true and attractive market competition for the tenders to come. The main goal was to avoid any kind of industrial monopoly, given the important investment that represents a ticketing system in 1990, a group of European transport operators from Belgium, France, Germany, Italy and Portugal decided to develop an open technology for all portable objects that was required to operate secure, fast and reliable public transport ticketing systems.

On the basis of the Contactless Pass, in 1995, a group of European transport operators from Belgium, France, Germany, Italy and Portugal decided to join their efforts to develop on a larger scale this solution, in different environments and for different needs, and with the same philosophy of an open technology for all portable devices that was required to operate secure, fast and reliable public transport ticketing systems.

It results of this cooperation the successive Icare (1996-1997) and Calypso (1998-2000) European projects, financed by the EU programs of R&D, including Brussels, Lisbon, Konstanz, Paris and Venice, and complementary developments that have leaded to the CALYPSO technology, today largely deployed globally. These programs showed through several trials that this technology could be adapted to many public transport environments (big metropolis area, medium size capitals, mixed urban and rural area, touristic city) , and could be combined with other services, such as electronic purses, loyalty, access control, and so on. In the continuity of Calypso, the Triangle project proposed an inventive solution for interoperability at international level.

These European projects brought many advances, recognized by the European Commission as main contributions, to the development of smart ticketing in Europe and to the emergence of standards, such as, particularly, the contactless ISO 14443 and the EN 1545 ticketing data standard.

To better identify the technology, it was renamed Calypso in the year 2000.

Following the large success of the Calypso concept and its widespread use across the world, Calypso Networks Association (CNA) was created in 2003 to federate Calypso users enabling them to drive and manage the future enhancement of the technology.
PART I: Using Calypso
With more than 110 million Calypso cards and 400 000 readers at the beginning of 2014, Calypso is the largest microprocessor based smart card technology ticketing system. The number of Calypso users is constantly increasing all over the world.

**Calypso in Belgium**

STIB, the main transport operator in Brussels, deployed its electronic fare management system in 2008, and chose Calypso as the contactless technology.

A working group has been created at national level to build an interoperable transport application involving all operators in Belgium. The working group has access to the Brussels application and benefits from the STIB experience creating the Belgian national transport application based on Calypso. 3 million Calypso cards are currently active on the Belgian networks.

This national interoperable ticketing application may reside in the same support than other applications, enabling the management of other services in addition to public transport, such as: parking, park and ride, access to theatres and museums. This support also includes a Triangle 2 application to manage cross border interoperability with cities of the north of France.

**Calypso in Canada**

The towns of Quebec, Gatineau, Laval and Montreal have also chosen Calypso for their contactless ticketing system.

The greater Montreal region deployed the OPUS contactless smart card in April 2008 and modernized all the related transport equipment with the purpose of setting up a true Customer Relationship Management tool and multiplying the ticket sales channels. OPUS now federates
more than 20 transport operators of Montreal region. Over 6 million OPUS cards have been delivered since the launch of the system, 3 million are active.

**Calypso in France**

The different challenges faced by interoperable ticketing applications led to France choosing a highly secured system based on microprocessor smart cards, with interoperability at the regional level.

Calypso open specifications perfectly met those requirements. All regional applications are now based on Calypso, the most important being Navigo (Paris region), with more than 1.5 million cards delivered each year, 4.7 million active, and OùRA (Rhône-Alpes region), more than 1 million cards already delivered.

At the same time, a standardization working group has created a set of specifications concerning ticketing data management (which is not imposed by Calypso). They are:

- **Intercode** concerning data stored inside the portable device (customer media),
- **Interbob**, relating to data exchanges between back-office systems.

The French ministry of Transport is promoting Triangle 2, the Calypso interoperable application and the CNA Calypso applet for a common ticketing application on mobile phones.

**Calypso in Israel**

Israel was the first state to implement Calypso at a national level. Ten years after, all the public transport operators (buses, trains, Jerusalem LRT, Haifa BRT) are operating the same Calypso, with a full interoperability between them for more than 3 million active Calypso cards.

KIF, the Calypso-Israel Forum, is now pushing for upgrading the Calypso version in Israel, for enlarging the national interoperability to Calypso contracts, and also for integrating Calypso with mobiles and with the banking world.

**Calypso in Italy**

Numerous transport networks use Calypso technology, including Milan, Torino and Venice.

Many regions are now developing the interoperable transport technology, based on Calypso. This is now the case in the Emilia-Romagna, Campania, Veneto, and Piemonte regions.

**Calypso in Portugal**

The country’s transport networks made the choice of Calypso, among which Lisbon, Porto, Madeira, Coimbra and some private transport operators of the surrounding regions.

Interoperability is a watchword, already a reality in central regions like Lisbon, Porto and Madeira. National interoperability is under study, in particular in the scope of the Triangle project.

OTLIS, gathering Lisbon’s transit operators, has benefited from the openness of Calypso to maximize the number of points of sale in order to reduce the cards delivery costs (bank ATM, on-line sale through Internet, etc.). More than 4 million cards have been delivered, 1.7 million are active.

Calypso allowed for the creation of the dual purpose banking card (Caixa Viva) that is also accepted in the transport network.
The Lisbon parking municipal company is now accepting Calypso cards (Viva Parking) in their parking meters and closed parks.

TIP, in Porto, has successfully integrated and modernized the region fare system thanks to Calypso.

Several applications different from transport ones are in roll-out phases. Calypso was adopted to unblock car sharing vehicles and to authorize vehicles access to old typical districts.

**Calypso in the United Kingdom**

The United Kingdom has issued a set of functional specifications (*ITSO*) enabling the compatibility of ticketing back-office applications, despite the large number of operators.

Calypso is one of the ITSO certified front end technologies (the *ITSO* specifications state that every *ITSO* member shall accept any portable object of another operator).

**Calypso in other regions**

Calypso is used or being deployed in many other countries, among which are:

- Algeria (Algiers).
- Morocco.
- Columbia (Pereira).
- Latvia (Riga).
- Mexico (Mexico City).
- Venezuela (Caracas).
- Switzerland.
Calypso main assets

Among the different ticketing systems on the market available at the moment, Calypso ranks as an attractive and innovative solution, made for transport operators and driven by transport operators. Here are a few good reasons why customers choose Calypso technology:

User driven

Considering the budget investment involved with the overall set-up of the technologies, operators have to be frontline players to guarantee the durability and profitability of their investment.

Operators choosing Calypso become actively involved in the developments of this technology through their involvement in CNA.

Fast and secure

Calypso uses up-to-date contactless technology to ensure a complete transaction in less than 200 milliseconds.

All ticketing transactions are run through a secure session that guarantees the integrity of the data written onto the card, even if the card is withdrawn too quickly. The Ratification anti-tearing function leaves the card in a safe state if the communication link is broken between the terminal and the card.

To avoid possible fraud or forgery, the secure session ensures that the card, the terminal, and the data are genuine, thanks to mutual authentication. Calypso’s high level of security is reached using microprocessor cards, Security Modules on terminals, and proven fast symmetric cryptographic algorithms (DESX, TDES, AES) using hardware accelerators.

- The card, the terminal and all data exchanged between them are authenticated. These operations are carried out with a high-speed algorithm resulting in the shortest possible transaction time.
- In addition of AES, the latest release introduced the confidentiality access mode in order to dynamically encrypt the communication between the reader and the portable object.

There are three main secret keys which perform a specific function: personalisation, loading and debit. The secret keys inside the cards are uniquely diversified by the card serial number and the corresponding SAM master key: If a card’s secret keys are cracked, only the security of the attacked card is jeopardized, and will be invalidated by the system.

Calypso guaranties the uniqueness of the Calypso application serial number, for all types of Portable Objects.

Ready for new trends

Today, transport operators wish to deliver the best services and simplify people’s daily lives. Future tools may help them in reaching that goal: NFC phones will certainly become more widely used and stand out as the inevitable multi applicative media. Meanwhile contactless USB keys may increase home usage services, such as the reloading of transport data.

Calypso is ready to accept those new challenges: a generic applet is already available, fully compliant with the GlobalPlatform API specifications, and is today widely used by SIM
providers and bank card manufacturers. The applet is downloadable onto a Secure Element based on the Java Card environment and implemented in an NFC mobile phone or a contactless USB key. This enables new facilities for customers and retailers.

Open to new services

Rolling out an electronic ticketing project over time, requires the ability to integrate new upgrade and technological capabilities on an ongoing basis.

Modern urban living is rapidly changing with new technological innovations, one of which is the possibility to integrate different electronic “on demand” services into one single medium. Therefore different applications can be brought together into one single device for the citizens of tomorrow in Europe: The "Urban Pass", will have the ability to integrate mobility and banking applications, local authority and public administration service access.

Calypso security technology and memory storage are tailored to meet multi functional requirements. A transport application and a dedicated city application may, for example, safely reside on the same Secure Element of a portable object, moreover they may live alongside third party applications, opening the road to the ideal urban pass.

Facilitating back-office integration

Calypso implemented in front-end of AFC system, frees the back office from an important number of administrative tasks regarding control and recovery of failed transaction: thanks to the Calypso secure session, all transactions performed off-line by the terminals are successfully completed and optimized and can later on be collected by the central system.

The high security level and the specified rules simplify greatly the design and development of all back offices and further assure the interoperability between ticketing systems from different suppliers.

Encouraging competition

The Calypso technology enables ticketing schemes to be really independent from industry suppliers.

License and non-license holder companies (via the purchase of OEM licensed components) can promote the technology through tendering. The conditions are clearly non discriminatory, allowing a fair competition between those who already possess the necessary licenses and those who would have to acquire them if awarded the contract.

The technology is distributed through numerous licenses, offering a wide range of multi-source compliant cards and terminals.

Moreover, because of the huge variety of licensed companies in the market, this allows different parts of the ticketing system to be assigned to different suppliers. This competition leads to a significant drop in investment costs within the tendering procedures and also enables the possibility to tender for only single elements and components of a ticketing system.

If there is an unfortunate case of a licensed component manufacturer not performing efficiently, it is possible to take on a new supplier who will acquire the license and manufacture the component.
Fully interoperable
Calypso technology is able to satisfy the demands of interoperability while offering freedom and independence to each operator. Wide Calypso interoperable networks have now proved it, gathering operators within a city or within regions: Lisbon: 22 operators, Paris: 3 major operators, Grand Montreal 20, French Rhône-Alpes region: 32 operators and authorities, and so on.

Interoperability between suppliers increases the need for security, confidentiality and integrity. The key to an efficient interoperable system is technical compatibility by adhering to international standards and the sharing of data model implementation.

Calypso follows this basic concept and is compliant with many international standards. (See § “Ticketing transaction layers”, page 29.)

Adaptable and flexible
Calypso can complement or ease the migration from any existing ticketing systems by using paper tickets, magnetic stripe tickets and allowing a seamless move from one technology to a fully contactless system on a step by step basis.

There is no requirement to have a central system, a GPS-system or an existing data collection system.

Adapting the supply to the demand
Calypso is a fundamental step towards a Customer Relationship Management application. Transport operators may draw-up and store precise usage statistics on their network by storing “events” from entrance and exit gates. They could then tailor the network activity according to the user demand. The statistics will remain strictly anonymous, thus preserving the user privacy and adhering to data protection laws.
Calypso faces mass transport new challenges

Calypso, as a new vision of transport, ideally addresses the modern challenges of Mass Transport:

- Interoperability is the response to the need for mass transport networks to work together within countries, regions or cities at the European level.
- New technologies, new tools: Transport operators should adapt their services to the increasing demand of travellers by enabling them to use Internet and mobile phones when buying tickets, downloading applications or accessing transport networks.
- Multi-applicative context: Local government, bank and university projects highlight the fact that there is an attractive possibility to share one medium with different service providers, among them transport operators.

Interoperability

*Interoperability is the ability of a system or a product to work with other systems or products without any extra effort required from the customer.*

Interoperability has now become a major issue for ticketing systems since a growing number of passengers both inside and outside European borders like to travel in comfort and appreciate coherent services, simplified fare management and seamless transport changes without involving any special effort.

Transport authorities and operators willing to set up an interoperable transport area, should it be at a city, at a region or at nation level, need to agree on many rules and regulations of their systems:

- **At the administrative level**

  Transport authorities, operators and, eventually other public or private stakeholders must define the exact scope of their relationship, accept a common liability, agree on shared services and fares and on financial issues (financial flows, money clearing, subsidy expectation, and so on.)

  Choosing Calypso helps them to ease the process of reaching these agreements by giving access to a wide range of products and suppliers and by a clear separation between the technical layers of the application and its commercial content.

- **At the customer level**

  It is a marketing issue which should make a passenger feel as if s/he is local everywhere: how does s/he buy a transport contract?, how does s/he board a bus and validate the contract?, what management is expected?, are important questions allowing for a seamless travel experience whilst also leaving some room for individual operator requirements?

  Calypso applications and media provide a consistent environment for the customers.

- **At the fare management level**

  Fare management is also a marketing issue with two identifiable interoperability levels:
• The range of transport options available (multi-operator season tickets, integrated fares, etc...).

• The setting of rates and pricings (based on the distance - zones, sections - or on time - variable according to the period, etc.).

The creation of transport options common to several operators leads to fare integration, which may remain limited by some transport options, by some operators and in some areas.

Calypso applications give the product owner the possibility to share products or not.

### At the technical level

The technical interoperability concerns a wide range of devices: smart cards, vending machines, validators, control equipment.

The key factors for building a successful technical interoperability platform are:

- Any portable object (PO) is compatible with any application depending on its owner’s choice and decision.
- One medium is sufficient to cover all the services offered by all operators concerned, and should respond to the request for “services on demand”.
- “Service contracts” are not linked to a dedicated medium.

To respect those rules, interoperability providers need to apply these major steps:

- Development of common technical specifications and security requirements.
- Management of secret keys.
- Standardization of the system interfaces and processes.
- Agreement on a common Data model.
- Development of joint certification requirements, accreditation of test houses and processes for testing system components.

Among all parameters that will make interoperability easier, international standardization is an essential step towards a mutual understanding of differing heterogeneous systems.

The development of Calypso was a decisive step towards defining the basis of this technical interoperability. It also led to the complementary development in European and international standards (EN1545, ISO 14443).

In Europe, the development of standards such as EN 1545 for data elements is completed by the incoming international standard for an Interoperable Fare Management System architecture (ISO 24014-1, also known as “IFMS”) which was additionally jointly developed with US and Japanese experts.

These standards are used in each country within regional interoperable applications such as VDV-Kernapplikation (Germany), Intercode (France), ITSO (UK), MOBIB (Belgium), Translink (Netherlands).

All these standards aim at defining a common Trust and Privacy model which could be shared by many transport authorities and operators with the ultimate objective of setting up a future European Status application.

Calypso is well on the path to meeting this normative approach and meanwhile supplies all the requirements to a real interoperability through the seven layers of its transaction framework:

- The strict application of standards to layers 1, 2 and 4 (ISO 14443, ISO 7816-4, EN1545).
- The use of the secured transaction on layer 3 (card commands).
The use of the same data implementation on layer 5 (strictly the same adaptation of the generic data model for all system partners).

- The bringing into play of a common security architecture on layer 7.
- The definition of an API on layer 6 is not strictly necessary for interoperability, but it certainly gives a better assurance that all terminals will process the cards in the same way, and facilitate common upgrades and enhancements.

Calypso therefore offers a time proven, open interoperability technical standard.

### Calypso interoperability through the Triangle application

The market for cross-region and cross borders mobility knows a rapid development. It mainly has to do with short, even one-day round trips between cities and calls for a combination of middle to long distance and urban travel, and the access to related services.

The Triangle application addresses this market. It creates a unique contactless “Tool for Access” to long, medium or short distance transport facilities or to other services, without any necessity of a common back-office. The Triangle application is a Calypso application compliant with Rev. 3.1 which can be present in any contactless portable object compliant with ISO 14443.

Triangle vision of interoperability relies on three major principles:

- The shared use of a specific Triangle set of Keys by Triangle media issuers and product owners.
- The absolute respect of a standardised environment
  - accessible from all operators,
  - defining the handling, interpretation and coding of the application data,
  - defining the security system and the encryption for a secure accessibility of the application and the application data.
- The (re-)use of available technologies and existing (or under deployment) systems
  - Accepting only marginal and minor evolutions,
  - Leaving the back-office untouched,
  - Paving the way to bilateral and multilateral commercial agreements.

Through some adaptation at card structure level and at terminal level (additional set of Keys in Security Access Module), Triangle interoperability scheme creates a unique and universal mean of access to urban transport services and medium or long distance railways transport services associated to the possibility to buy other services or purchases.

![Diagram of Triangle application interoperability](image-url)

**Figure 2: Validation Outside Issuance Network - Typical Use Case**
Calypso open to new technologies

Today, trials are constantly taking place all over the world with use of new devices to access daily living services: NFC mobile phones, Java cards, contactless USB keys are the foreseen medium that will be present tomorrow in everyone’s pockets to access a wide range of services. Among them, transport access plays a major role since the customer’s media (portable object) will be frequently used by the user, and will allow him/her to load and validate a transport application, buy some contracts and renew them independently.

A main step towards Java Card technology

Calypso secures contactless transactions by being independent from the communication layer, it is well suited to those new multi-applicative devices where one-time programmable applications may well disappear and give way to ‘on-demand’ downloadable applets. This is why Calypso uses the description “portable objects” instead of smart cards.

A set of Calypso specifications describe the way a Calypso applet may be securely downloaded, activated and customised within a portable object, according to the standard GlobalPlatform specifications, and detail how remote services (such as reloading of contracts and rights) may be accessed directly by the portable object.

Thanks to the Calypso compliance to international standard 7816-4, a download remote infrastructure compliant with Global Platform may be used seamlessly.

Furthermore, the use of Java compatible portable devices does not require any change in the existing terminal and SAM of an operator. The portable object behaves as a native smart card rev 3.1 (except for a slight increase in transaction time).

Convergence with contactless bank cards

The technical convergence between contactless bank cards and Calypso portable devices is being studied by a CNA work group.

EMVCo specifies the banking cards / terminals contactless communication interface (level 1), based on ISO 14443, and completes various lacks of the standard. A different interpretation of these lacks has been already implemented in Calypso portable devices.

New card readers, tuned to both Calypso and EMVCo could become generic terminals, able to handle both bank and transport cards. The main goal being to have a universal certification for all POs and terminals, independent of activity’s sector.

This convergence could help operators to solve the problem raised by occasional passengers who may not have the suitable pass. They could access the transport network, paying the fare with their contactless credit card directly using network validators.

Multi-application

Today, Calypso provides a range of technical solutions able to enhance urban mobility systems, requiring the multi-application management in an interoperable environment.

City Life smart cards may allow citizens to use and pay for leisure, local e-Government and transport services without using cash.

As shown in the technical framework, the dedicated citizenship Calypso application and e-Purse application (Stored Value) may simultaneously reside with the transport application
inside the same portable object, widening the field of applications to multi-service environments:

- **Mobility**: parking, park & ride, car and bike rental.
- **e-Government**: access to on-line services from public multimedia kiosks.
- **University**: student cards, university canteens, entry access control.
- **Leisure**: library access, stadiums, museums, etc.
- **Commerce**: private payments, loyalty schemes.

Depending on the smart card memory size, one or several citizenship applications may be added to the transport application. Each application holds its own private keys and remains securely separated from the other. Moreover, a common area related to holder information and profile may be shared between the applications. If needed, personal information may be protected by a PIN to preserve the holder’s personal data.

One interesting feature is that city life projects using native Calypso smart cards may easily switch to a Java Card multi-applicative environment (by using a mobile phone for example), since all individual applications inside the Secure Element may become downloadable applets onto the Java platform, keeping the same behaviour without any change to the existing terminal infrastructure.
Which business model for operators?

Mass transport operators who have not yet migrated to a ticketing system may wonder about the opportunities and the reliability of the business model before acquiring such a system.

Card and infrastructure costs

New ticketing operators may consider the card cost as one of the main pitfalls, however, when choosing a ticketing technology; many factors must be taken into consideration:

- Addition of new services or functions may be very costly depending on the technology required for the customer media. Extra cost can be induced by non open or non standard systems, limiting the functionalities and the ticketing system durability.
- Before making a choice, operators should keep in mind that some system integrators, terminal or card manufacturers may try to promote closed systems, making it more difficult to include any competition between suppliers over the system's lifetime.
- This is one of the main goals of Calypso: to ensure healthy competition, so that transport operators are not tied with one supplier in the future, and so that they may enjoy lower costs of systems and easily integrated enhancements, as well as benefitting from innovations introduced from a diverse range of suppliers.
- When migrating from a full magnetic system, the card costs increase heavily, but the equipment maintenance costs drop dramatically (to one fourth of what it is when using magnetic stripe readers), which leads to a return on investment after five years.
- The cost of the cards alone is not the only relevant criterion when choosing the correct technology. Operators introducing a ticketing system are not only buying cards but also the capability to offer their customers and their company the service they want. The cost of the whole system during its lifetime must therefore be considered, including: future update and enhancement costs, security management costs, and so on. For example, will the system allow an easy use of new technologies such as using NFC mobile phones, or using contactless USB keys?

Customer relationship management

Beyond pure expense considerations, the management of the relationship with transport network users, for the modern day passenger is very important.

Calypso is a true CRM tool. The analysis of validation events collected by the back-office systems gives transport operators a precise picture of the customer’s daily travel practices and behaviour and can adapt the transport supply to the demand, thus increasing customers’ satisfaction. This feature is not only quantifiable in terms of money but highly improves the network’s efficiency and the operator’s image.

Loyalty programs can aid fare management, and even if rarely used at the moment, specific tariff rates according to time slots, destinations and user profiles can easily be implemented in a ticketing system, thus adapting the commercial benefit to the customer.
New sales channels

Linked to CRM, the emerging NFC mobile technologies, new USB keys and internet developments make it possible to use remote vending facilities, on automatic vending servers or at home.

Many passengers dream to avoid the queue lines when reloading season tickets and contracts. Calypso enables different experimentations for buying and reloading contracts remotely:

- Over the Internet:
  - At home with a contactless USB key: in France, RATP has launched a pilot to test the use of smart keys. Passengers connect to a Web site where they can purchase and pay on-line the transport contract which is thereafter downloaded onto the contactless USB key.
  - With contactless smart cards: in Belgium, STIB enables to buy, renew and pay on-line transport contracts. The contract is disseminated through specific lists to all automatic vending kiosks and validators. When the passenger checks the transport card against one of those, the new contract is loaded onto it.
  - Anywhere with a card reader: in Portugal, OTLIS developed a website that allows purchase and load transport contracts of 22 operators. Through this website it is also possible the request and pay of custom cards.

- Over the Air with NFC phones:
  - NFC phones are probably the ideal medium to host transport contracts, which can be loaded remotely “Over the Air” onto the mobile phone, according to Global Platform specifications. Their user interface is very convenient for passengers willing to check and activate their transport contracts.

As already mentioned, in some countries, like Portugal, passengers may also benefit from the existing ATM infrastructure to buy and re-load travel tickets from their bank account.

Calypso is well suited to those new sales channels which on the one hand aids the customers’ daily life and on the other hand reduce the operator’s tickets distribution costs.

Multi-application medium

Multi-application projects, bank, city and university card projects have the opportunity to avoid specific travel ticket distribution. Java cards with a GlobalPlatform interface can be dissociated from the card issuer and the application providers, meaning that only one medium may be shared by different application providers, reducing cards and distribution costs.

Fare evasion reduction

The use of microprocessor cards and Calypso’s high level of security make forgery and system violations extremely unlikely.

Calypso’s fast contactless technology ensures systematic ticket validation at each boarding or network entrance, reducing the number of fare-dodgers. Transport operators should be aware that before imposing a compulsory validation, they need to prepare their customers to accept this new technology through a massive communication campaign.
Elements of a Calypso ticketing system

This section presents some of the main elements of a ticketing system.

▪ Microprocessor smart cards

Transport operators can obtain Calypso microprocessor smart cards from numerous suppliers, and buy the most suitable card at the best price.

Most cards offer an optional dual communication interface, a memory size of 2 to 16k bytes, cryptographic algorithms DESX, TDES or AES.

Calypso is supporting both ISO 14443 type A and type B, even if, for historical reasons, most of the cards in the field are in Type B.

The most recent have been certified by CNA on the basis of its certification process launched in 2014.

More information on the suppliers and their products are available on the CNA web site (http://www.calypsonet-asso.org).

▪ CNA Calypso applet

Java oriented products, though not yet massively delivered to transport network users, will be an important trend over the forthcoming years.

CNA developed a generic Calypso applet and propose it for free to operators. The CAN Calypso applet offers them the possibility to accept mobile phones, credit cards, all Java Card portable objects.

The Calypso applet, of course, strictly respects all the standards (see the technical description of the applet), and can be used with all existing Java Card hardware platforms, provided that this platform strictly respects these standards: it is the only way to guarantee interoperability.

▪ Terminals

The market diversity of Calypso terminal suppliers is a very real one, manufacture card readers or OEM readers, as well as transport validators or automatic ticket machines.

Please visit the page “Products/suppliers” on the Calypso web site: http://www.calypsonet-asso.org.

▪ SAM / CSM

The SAM technical specifications are owned and managed by CNA. There are presently two manufacturers for the SAM: ASK and SPIRTECH, who may also directly supply SAM components.

Additionally, SPIRTECH supplies the Calypso HSM, which may be used in central database systems, for example for the remote selling of transport contracts (a HSM may replace up to 5000 SAM’s).
Other ticketing systems, that have their own security management and SAM, may integrate Calypso cards handling functions into their SAM. This is the case with ITSO (Great Britain), whose SAM is able to handle Calypso cards.

- **Secret keys**
  
  Secret key generation is a rather technical process which impacts heavily and for a long time on the global security of a system.

  The process can be conducted independently by the transport operator, if he wishes to be totally independent of any equipment supplier, or may be entrusted to the system integrator.

  In the first case, it is possible to make the necessary key creation tools from scratch or to require help from ASK or SPIRTECH who offer a complete range of relevant services:

  - Key ceremony organisation, under control of the operator,
  - Technical documentation and training, enabling the operator thereafter to be autonomous
  - The creation of Key loading tools.

- **Back-office integration**

  Calypso only deals with the security of the contactless interface subsystem, not with the management of data exchanges between independent terminals and the central management system.

  CNA will act as a facilitator to implement the ticketing system but it is the operator’s responsibility to integrate Calypso fare collections within their existing IT infra-structure or use an existing integrator’s AFC system.
Recommendations for the practical implementation of a Calypso ticketing system

When installing an electronic fare management system, operators may choose:

- To select a system integrator who delivers the central system (level 1), the different elements (points of sales, ATM, validators, etc… - level 2 and 3) and the contactless interface devices (card readers, mediums, SAMs – level 4, Calypso elements).
- To manage the project integration independently.

Calypso is not tied to any supplier, consultancy firm or research department. This means that operators are free to choose the level, cost and quality of service according to their needs.

Numerous suppliers around the world market Calypso products, including the main electronic fare management system suppliers.

Introduction

Managers of ticketing systems need their system to be open to competition. In addition to the basic requirements of rapidity and security, concerns about the longevity and cost reduction over the system’s lifetime require competition among several manufacturers.

Effectively:

- Ticketing systems will evolve during their life span (network extensions, additional operators, tariff modifications, etc.).
- Some suppliers may leave this field.
- New solutions become available (e.g. renewing of season tickets on ATM, mobile phones with contactless interface) and are sometimes designed by new players that may have difficulties in obtaining technical information from historical suppliers.

Calypso was designed by a group of transport networks operators to answer these concerns with a modern ticketing system based upon contactless smartcards.

Calypso is the only open solution among all the available and time proven technical standards. This explains its large success. Indeed, more than 110 transport networks have selected Calypso and more than 30 suppliers around the world can already provide it.

Nevertheless, a manufacturer is always looking for ways to "close" the systems delivered, even when they are based on Calypso. This section highlights some technical issues to watch closely when implementing a Calypso system to avoid such pitfalls.

Calypso interoperability basis

The communication between a smartcard and a reader requires the clarification of several technical rules to guarantee the technical interoperability between different sources of cards and readers.

When these rules are applied, they become a de facto standard, supported by a group of users, and may become a normative standard if they are accepted by a bigger body (national such as AFNOR or DIN, or international such as CEN in Europe or ISO for the world). As already mentioned Calypso is deeply involved in this normative process and is based upon all relevant standard of its field.
When designing a ticketing system, the main technical rules apply:

- **The physical transmission.**
  Calypso uses the international standard ISO 14443, which it has partly defined. Up to now, both for technical and industrial reasons, Calypso cards have mainly used the type B of the standard, but since the Calypso rev 3.1, type A is allowed as well. (See § “The communication interface layer”, page 30)

- **The set of commands to control the cards.**
  Calypso extends the international standard ISO 7816 (contact smartcards) to the contactless and ticketing requirements (to avoid being locked with a command set proprietary of one supplier).

- **The security functions.**
  Calypso uses microprocessor smartcards and standard cryptographic algorithms with private keys securely stored in a SAM. (See § “The secure transaction layer”, page 33)

  Nevertheless, the keys are specific to each transport network to secure the access to its data. The key creation process must be controlled to avoid being limited by the rules of one supplier.

- **The data model** (the definition of the data stored in the card, or "mapping").
  Calypso uses the ISO 7816 file structures and recommends using the European standard EN 1545 to encode transport related data.(See § “The data model”, page 36)

  Nevertheless, these standards must be adapted to fit each application (Calypso cannot define the details of all possible applications). The data model is thus the most sensitive point to watch because:

  *If it is normal - but not always necessary - that the data model be specific to a network, it must not be solely dominated by one supplier, making its use difficult by competitors. This is what some manufacturers are tempted to do to simplify their applications (avoid adapting the data processing to a specific network) but also to control the solution, making any competition very difficult.*

Furthermore, Calypso is often complemented by contactless tickets (using wired logic instead of microprocessors), reducing the costs for infrequent passengers. The best solutions are designed to be as close as possible in design to the Calypso solutions, in order to blend harmoniously with them:

*Their physical transmission is similar (low layers of ISO 14443, to offer the best response times and simplifying the physical architecture of the system and its global reliability). The security of these tickets is simplified but also uses the Calypso SAM. The data model is also simplified, but remains close to the Calypso data model.*
### Data models

The system manager must have the rights to freely use, adapt and communicate with third parties in its data model. The manager may be the transport network operator, an association of operators, the regional authority, the buyer or, more generally, the person in charge of the continuity and interoperability of the ticketing system.

**Recommendation 1: Control of the data models.**
The transport network must understand their data models. They must have the right to modify them and to transmit them to their suppliers without limitations.

Calypso recommends using existing data models, adapted by an experienced third party, independent from the suppliers of cards, terminals or systems.

The cost of this independence is small compared to the high risks at stake concerning the short or medium term issues relating to the interoperability and longevity of the ticketing system.

In practice, a supplier sometimes refuses to communicate their data model, and in some cases, even if the supplier accepts this communication, they continue to have a competitive advantage. More importantly, experience has proven that differences may exist between the current version of the data model used in its equipment compared to the version delivered, which generates incompatibilities between different versions that can be very difficult to deal with.

If this problem is not addressed early, it is at the very least recommended that the client demands the data model from their supplier, with serious penalties if there are any differences observed between the original specification and the implemented system.

### Cryptographic keys

The system manager must own the cryptographic keys, and must be able to use them freely, within the limits set by the agreed regional rules of security.

**Recommendation 2: Control the cryptographic keys.**
The transport network must own the keys which control access to its cards.

As for the data model, Calypso recommends using standard security architecture and, for the key creation process, using an experienced third party, independent from the suppliers of cards, terminals or system.

In any case, it is necessary to ask for the specification of the security architecture and initial keys, allowing a possible independent reproduction of the keys if necessary.

### Conclusion

The preceding recommendations are simple to put into practice and not costly (less than 10 to 30k euros). They help to ensure the required openness and longevity of the ticketing system that Calypso promotes.

The control of the data model and of the cryptographic keys within a Calypso system also guarantees the technical interoperability and the best conditions for the enhancements of the installed system.
Nevertheless, the technical interoperability is but one of the issues of a practical implementation of a ticketing system; as described previously in the § Interoperability p 15. Implementing a ticketing system requires a global approach to all these subjects. The transport networks using the Calypso technology are automatically included in the Calypso Networks Association. Other members of the association may help with the practical implementation by imparting their own experience. This is the essence of Calypso.
PART II: The Calypso technology
The Calypso technical framework

The Calypso specifications are designed to improve and enhance any existing electronic ticketing application. They are used in fact, as part of a secure contactless system including: a central system, different front end terminals (reloading or re-charging appliances, validators, control devices, etc...), and portable devices (smart cards, mobile phones, USB keys). Calypso focuses essentially on the ticketing transaction between a terminal and a portable object.

Calypso has been designed to meet multi-modality, interoperability and multi-application requirements.

Ticketing transaction layers

The ticketing transaction is organized into layers, as illustrated in this table:

<table>
<thead>
<tr>
<th>Security Architecture and Mechanisms</th>
</tr>
</thead>
<tbody>
<tr>
<td>Application Programmable Interface for readers</td>
</tr>
<tr>
<td>Data model (Instantiation)</td>
</tr>
<tr>
<td>Card Data Structure: EN 1545</td>
</tr>
<tr>
<td>Card-reader Transaction Commands (including Session and ratification)</td>
</tr>
<tr>
<td>Card Mapping and file Organisation: ISO 7816-4</td>
</tr>
<tr>
<td>Communication Interface: Contact ISO 7816 1-3 contactless : ISO 14443</td>
</tr>
</tbody>
</table>

The development of the Calypso ticketing application is based on international standards:

- **Communication interface:** ISO / IEC 14443 (Type A&B), defines the radio signal and protocol for an induction transmission at 13.56 MHz. For dual interface cards, ISO 7816 (1-3) describes the physical characteristics and the electronic signals and transmission protocols of Integrated Circuit Cards. It is also compatible with NFC (Type 4 Tag).
- The **Card mapping and file organisation:** ISO/IEC 7816-4 defines the card data organisation in a file structure’s basic card commands.
- **Card-reader transaction commands:** Calypso specifies the PO, SAM commands and files used during the ticketing transaction. These functions are optimized for ticketing (fast, secure) and include innovative patented technology such as the Secure Session and Ratification functions.
- **Card data structure**: EN 1545, defines the coding of data elements used for public transport (such as: date, time, validation event, transport contract, etc.).
- **Data model**: describes the definition and the interpretation of the data in the files of the card.
- **Application Programmable Interface for readers**: Application Software ensures that the cards are managed in the same way by all terminals, and allows an easier enhancement of all kinds of terminals.
- **Security architecture and mechanisms** describes the management of the security for a ticketing system, and recommends good practices and all available choices for transport providers.

**The communication interface layer**

The Contactless technology is nowadays widely incorporated by transport providers and has superseded magnetic stripes and paper ticket use.

Contactless technology is based on inductive transmission operating at 13.56 MHz frequency in close proximity of a reader antenna, allowing data transfer up to 848 Kbps.

The ISO 14443 standard defines two types of contactless communication protocols: Type B and Type A. Calypso specifications are indifferent regarding this option: as being a set of functional specifications; they are independent from the communication layer.

Historically, Calypso cards were available using the type B, which is very well suited to microprocessor products and which offered more possibilities for enhancements than type A. (For example, higher communication speed rates can be reached with type B). All recent Calypso readers are now fully A&B compliant. Calypso chips for portable devices exist in each type of protocol.

Calypso portable devices may be implemented in any form, for example, as native cards or Java cards:

- Dual smart cards, contactless only smart cards.
- USB contactless keys.
- NFC mobile phones, other format…

![Figure 3: Smart card layers and components](image-url)
The memory organisation

The Calypso application data is organized into files structures, according to the ISO 7816-4 standard. For public transport applications, the file structure is fully compliant with the EN 1545 standard, allowing any dual Calypso PO (contact and contactless) to communicate easily with numerous existing terminal networks.

The Calypso specification does not advocate just one specific file structure, it however defines several generic examples of file structures that may be used directly or customized. The specification makes it possible to re-define a complete new file structure.

Each Calypso application owner (transport network, regional Authorities, etc…) may choose the best file structure to fulfil its needs among the existing generic examples, or alternatively may define a new file structure. The file structure and data model stored within the Calypso application are key factors for successful network interoperability.

The file structure is defined before the activation of the Calypso application (personalization phase). The type of file structure used by the PO is installed on the terminal at startup time.

The picture below depicts the memory organisation of an example PO used in a multi-applicative environment and holding three Calypso applications: transport, stored value (electronic purse) and city application.

The file access is ruled by access conditions: access mode (Always, Never, Session, PIN) with a key number associated to the command executed. Two additional access modes have been added in Revision 3.2: Confidential and Confidential & PIN.

A file may contain one or more records (each record may contain 1 to 255 bytes).

![Calypso file structure example](image)

*Figure 4: Calypso file structure example*
Master File (MF)

Many Calypso portable devices contain the following files:

- ICC: Manufacturing information (1 record), contains the serial number of the application as well as several manufacturing data records.
- ID: Holder Identify (1 record), contains Holder sensitive information, whose access is protected by the presentation of a PIN code.
- FREE: (4 records), free for use during implementation.

Note that in a Java Card environment, the notion of MF and underlying files might not exist or be slightly different. In this case, these files may be files from the Calypso DF, shared by other DF.

Transport files

The green files illustrated in the picture above represent the minimum file structure for a transport ticketing application. The transport files access is managed using the transport network secret keys.

An application may contain additional files, with a variable number of records.

A simple application may be limited for example to:

- Environment (1 record): contains information about the transport network application and information about the holder.
- Contract list (1 record): contains the list of active contracts in the PO, with a priority indicator.
- Contracts (4 records): contains the transport contracts.
- Counters (1 record): contains the values of 9 counters, associated to the contracts or handled independently.
- Events log (3 records): contains the last entrance and exit validation events.
- Special event (1 record): contains unusual events or errors detected when accessing the transport network.

Stored value files

The Stored Value is a Calypso application implementing an electronic purse, working with its own secret keys.

- Load log: contains the reload transactions of the electronic purse.
- Purchase log: contains the debit transactions of the electronic purse.

Citizenship files

This is an example of the implementation of a city life application, with its own secret keys. This application may contain the following files:

- Environment: contains information related to the city life project identification and holder identification and profiles.
- History: contains the list of validation events generated by the bank of terminals installed for the city life project.
- Contracts: contains the contracts and access rights of the city life project (parking, library, swimming pool, …)
- Contract extension: may contain numbers relating to contracts or other information connected to access rights.
The secure transaction layer

The Calypso secure transaction has to pass through a range of security measures allowing a Portable Object (PO) and a terminal to communicate (layer 4 of the Framework).

The security measures are activated during Calypso personalization and activation, and are then used during the three main phases of PO activity:

- **Loading:** the PO is loaded for one or more transport providers, at a network point of sale, any expired contracts may be removed.
- **Validation:** when entering/exiting the network, the PO is checked and validated. Contracts are debited, events recorded, and any other files can also be modified.
- **Control:** the card validity and contracts may be checked by a handheld control terminal.

![Calypso ticketing system components and their associated security](image)

The main security measures involve:

- **The Secure Application Module (SAM)**
  - The SAM authenticates the PO, the terminal and all data exchanged between them. It is historically a smart card, but, as remote services are nowadays delivered by distant servers, it can also be a hardware device plugged into a server (HSM).
  - Calypso uses the new term of Calypso Secure Module (CSM) to cover both the SAM and HSM.

- **The secret keys**
  A Calypso application within a PO contains three diversified keys:
  - **Issuer key:** used to modify personal data.
  - **Load key:** used to modify reload data.
  - **Debit key:** used to modify validation data.
Any key may be used to authenticate the card content.
All secret keys within a PO are uniquely identified from the SAM master keys with the Calypso serial number of the PO application. This protects the system against PO secret key attacks. The secret keys are only present in highly secure devices such as the PO and the SAM.

### Secret key sharing

The Application Data Control function of the SAM allows a number of operators to share the same Calypso application in a PO with the same set of keys, while ensuring the security of each operator’s data. The SAM application contains a list of Control Access Authorization Descriptors (CAAD) to enable this feature.

The access control to the records of the application is managed by the SAM itself through 2 modes:

- the *static allocation mode*, where records and counters are allocated by their number to each entity.
- the *dynamic allocation mode*, where records and counters are allocated to each entity according to the values of the first bytes of the records.

In order to enforce the CAAD security, the SAM restricts the commands that may be used in a transaction.

This function is well suited to multi-services application and avoids having to define an application and a set of keys for every service. It is a fundamental element of the security of the Triangle application (see page 17)

### Key creation ceremonies

Formal key creation ceremonies are used to ensure the confidentiality of the system keys and their loading inside the SAMs. Below is an example of a key ceremony:

**Figure 6: Key ceremony example**
The cryptographic algorithms

Cryptographic algorithms are used to authenticate the PO, the SAM and the data exchanged between them.

A Calypso PO application may support the standard symmetric cryptographic algorithm: DESX, TDES or AES (this one since Rev.3.2)

The Calypso Secure Session & Ratification

The secure session performs:

- The authentication of the card,
- The authentication of the terminal.
- The authentication of all data exchanged during the session, proof that the card modifications have been correctly performed and applied.

These operations are carried out with a high-speed algorithm designed to perform in the shortest transaction time, essential, when using the card for access control.

All data modification requests given during the session are automatically cancelled if the final authentication fails, or is interrupted for some reason.

Thus, the session function ensures that either the modification made during the session is correctly carried out completely, or no change takes place at all. If the session is not successfully closed (because of a bad signature, a card error, an unexpected shut down, etc.), then all the modifications carried out during the session are cancelled.

Moreover, a special feature, called the “Ratification”, allows the ground terminal to handle without problem, any final communication link problems. During any communication, a break in the link may occur unexpectedly. This is particularly true in the case of contactless communication, where the card may be taken out of the terminal radio field during normal use, and before completion of the transaction.

The secure session is very efficient at solving this problem, as an interruption before closing the session, will cancel all the modifications made to the card, leaving it in the same state it was in before the session. For example, if a counter is decreased, an “allow” entrance event must be recorded at the same time on the card, the session mechanism will ensure that either both are completed or that neither is executed.

At the end of the session when any changes have been validated, an acknowledgement (including the card signature) must always reach the terminal. If the communication link is broken between the session closing, and the receipt of the acknowledgement, the terminal has no proof that the card is legitimate and that the transaction has succeeded. In this case, the customer might have already paid, or have had his access rights decreased, and may not be allowed future access.

The usual solution to this problem involves a complex function in the terminal, which must register the cards that fall into this case, and handle them as normal, if they are presented again soon after.

The problem is even more complex for transport providers, where many different validators may control the same network entrance gate, and where the user might be tempted to try another validator if the previous one failed. To allow the user to enter without paying twice, while avoiding this very complex and costly management in the entrance terminal, a mechanism was designed, known as: the Ratification.
The Ratification works as follows:

- Step 1: On session closing, the PO records the session as “not ratified”. The PO then sends the session closing acknowledgement to the terminal.
- Step 2: On receipt of the acknowledgement, the terminal needs to allow access to the transport network, and sends a new message to the PO, issuing also a session closing acknowledgement.
- Step 3: On receipt of this new message, the PO changes the state of the recorded session to “ratified”.

When a new session is opened, the PO sends back the state of the previous session.

The session remains in the “not ratified” state only if the communication is broken during Step 1 before the PO changed the state of the recorded session to “ratified”. The probability of this occurrence is small, because the corresponding time duration is very short.

The function with ratification allows a second terminal to take the following actions:

- If the previous transaction happened at the same entrance and is recent, according to the ratification state:
  - Ratified: The terminal forbids access, without rejecting a legitimate user, as it has registered that the previous terminal completely processed the transaction.
  - Not ratified: The terminal grants the access, without debiting the PO again, letting all legitimate users enter the network.
- If the previous transaction was at another entrance or is old, the terminal assumes that it is a new transaction and debits the Calypso application granting network access.

The data model

The data model describes in detail, the coding, position and rules for handling all data elements in order to establish the basis of an interoperable card and ticket management system.

A terminal API

In order to avoid inconsistencies between different implementations of the Calypso Data model, it is necessary to outline the terminal implementation in greater detail.

A Terminal API defines a common software interface for Calypso card application management.

When possible, the terminal library managing the cards may be shared among various different interfaces to make the card management more homogeneous. This is particularly useful on multi-applicative environments that include numerous players (city card, banks, tourism, resort, etc…) or on large multi-modal or interoperable networks, when the same cards are shared among many different operators.

The security architecture

Calypso offers security recommendations for a ticketing system together with an organisation model and tested security procedures. (level 7 of the Calypso transaction framework)

These recommendations aim to make Calypso the most secure existing ticketing system.

The security architecture covers all technical functions ensuring that all access to the networks are fully and authentically charged.
Calypso has a pre-defined risk analysis and security recommendations for an Electronic ticketing system, based on the following principles:

- At the time of validation, the authenticity of the customer’s medium must be checked.
- All sales equipment must be strictly monitored to prevent the creation of an authentic transport title onto a card without payment.
- Means of fraud detection must be set up to prevent any possible forgery.

They include the Calypso security functions found in terminals and PO (already described in this document), organisational rules (responsibilities, handling procedures for components, etc.) and central security function (fare collection analysis, fraud detection, SAM manufacturing, key creation process, application personalization and activation, etc…).

These recommendations make Calypso the most secure existing ticketing system on the market.
Calypso versus other technologies

The use of microprocessors which has formed the basis of Calypso since the beginning of the 1990s (high security, roll back function to manage interrupted transactions, compliance with ISO 14443), now appears, after several cases of fraud, to be essential, to ensure a sufficient level of security for contactless transactions.

The main rival technology now uses the guiding principles promoted by Calypso as a migration path of their proprietary solutions towards higher security and performance.

But as it is often the case in many industries, the followers are not able to reach the same as the original and most comparisons prefer Calypso.

Standard compliance

Figure 7: Contactless technologies vs. international standards

😊 The CNA Calypso applet is fully compatible with the GlobalPlatform specification from v1.0 to 2.2.

😊 Calypso’s rival technology companies offer proprietary solutions, only partially compliant to ISO 14443. Their command set being not fully compliant with ISO 7816, blocks the way to a direct & open application management on multi application platforms as SIM can be in mobiles, and require adding a supplementary layer in a special SIM supplied by the solution provider.
**Transaction completion**

😊 The Calypso secure session includes a BEGINNING and END, ensuring that the transaction is done and entirely done securely. (See § “The Calypso Secure Session & Ratification”, p35)

😊 Competing technology doesn’t include either secure closing of the transaction (possible hacker attack), nor graceful management at the end of the transaction (the state might be unknown to the terminal if the communication link is broken at the very end).

**Security**

😊 Calypso specifications are for different forms of media based upon microprocessor technologies, the security part is available to manufacturers (signing NDA).

Calypso uses the most secure and time proven cryptographic algorithms existing in the smartcard industry.

😊 Some Calypso rival technologies offer no security or only proprietary security including proprietary cryptographic algorithms

**Open procurement**

😊 Calypso opens up true competition in the market place. The set of specifications is available to suppliers under RAND conditions (Reasonable And Non Discriminatory), so that different compatible products can be supplied by different manufacturers. (See § “Elements of a Calypso ticketing system”, p22). Any new manufacturer is also free to join.

As Calypso is an application, it can be put onto any platform, whatever the protocol used, whatever the chip manufacturer, and whatever the form factor.

Calypso specifications have always been thought, to cover the needs of any ticketing system, to last a long time and to cater for a range of compatible products.

Schemes can therefore choose the most appropriate product for their needs and be guaranteed the migration to new generations or to new suppliers without disproportionate efforts as the industry goes forward.

Calypso specifications are owned, managed and maintained by a group of users in Calypso Networks Association (CNA). Any scheme can join CNA to enable them to be kept informed and offer their input in any future modifications of the specifications.

😊 In comparison, other technologies are completely controlled by one chip manufacturer which may impose its views onto the whole market.

Family products of rival technologies are often completely incompatible one with another: (Different and incompatible sets of commands).

**Card cost**

The lower cost of memory cards compared to Calypso microprocessor cards used to be considered as an argument to accept a lower level of security and a higher risk due to possible hacker attacks.

😊 Calypso products are now much more competitive with prices at market value. They also offer the extra-value of the flexible range of products and of their full portability in JAVA & GlobalPlatform environments as described above.
PART III: The Calypso ecosystem
A glimpse of other Calypso features

Enhancements to the specifications

As for any technical specification, the set of Calypso specifications are always evolving to meet new operator and/or user needs, to handle new products and to benefit from any new technological innovations.

The Calypso Revision 3.1 specifications were published at the end of 2008. Calypso Revision 2 is still widely used.

The two versions are largely compatible however, Rev 3.1 is much stricter in order to avoid incompatibilities.

- By moving from a native smart card specification to a multi applicative platform specification. (The platform may be hosted by various form factor applications).
- By moving to an “on demand” application management.
- By taking into account multi-applicative standardized platforms (such as Java Card).
- By controlling optional functionalities in order to increase technical interoperability.

Revision 3.1 allows for the deployment of ISO 14443 type A contactless products and ensures compliance with standardized NFC products, widening the availability of the Calypso products range.

The Calypso Networks Association (CNA) will continue to add new functions to the portable devices and SAM, according to its members’ requirements, as well as being watchful of the availability of older versions and ensuring upward compatibility.

The Revision 3.2 specification published in 2013 added security features: AES cryptography, quick mutual authentication between the PO and the equipment, mechanisms for privacy data protection, etc.

Calypso Revision 3 is becoming the main point of reference as operators and transport authorities get ready to do the migration.

The Calypso specifications are available on the Calypso technical web site: http://www.calypsostandard.net
Certification

- **Specification of portable objects**
  For Calypso Revision 2.4 portable objects, CNA granted a conformity stamp to the portable object specifications issued by the manufacturers. An independent laboratory mandated by CNA checked the submitted specification and charged the certification cost to the manufacturer. It however only concerned the external paper specifications and did not guarantee the intrinsic quality of a product made and marketed by a card manufacturer.

- **Portable objects and applets**
  Regarding the Portable Objects rev 3, due to the request of a strict adherence to the specification, CNA created a Calypso reference test to ensure this compatibility, built a test tool based on this functional test plan, and defined a certification process relying on a technical evaluation made by an independent laboratory.
  This process was brought in practice at the beginning of 2014. Detailed information and conditions are available on the CNA website.
  The certification of applets is a little more complicated, since one applet itself may be certified on a given platform, which may increase the number of tests sessions. However, when an applet is already certified on a platform, the certification process on another platform is lighter and less expensive.

- **SAM**
  On the terminal and central system side, the security of Calypso is ensured by SAM (Secure Application Module) and HSM (Hardware Secure Module).
  These elements ensure the use of the secret keys within a Calypso system and prevent them from being copied or fraudulently used.
  Since the SAM has an important role in the interoperability of Calypso systems, and due to the small market for SAM, CNA has authorized two sources of SAM (SPIRTECH and ASK) for now.
  When fully tested, Calypso security may also be embedded in the secure elements of other systems. For example, the ITSO SAM in the United Kingdom already includes Calypso security management.

- **Terminal registration**
  CNA has launched a process of registering all new terminals and OEM readers whose Calypso software application is compliant with rev 3.1. The registration is fully functional since the beginning of 2010. The goal is to register the terminals that are currently able to process Calypso portable objects application, according to rev 3.1 requirements.
  A typical manufacturer audit involves a one day visit from a Calypso technical expert to the manufacturer’s premises, investigation of the terminal in question, a set of elementary tests are run, and finally a compliance report is written.
  This registration can include any existing Calypso terminal or any new industrial products, manufactured by industrial partners wishing to access Calypso technology. In the case of new industrial products, additional technical assistance can be provided along with the terminal registration service.
Complete terminal certification

The feedback from the first registered audits will lead thereafter to the creation of a more comprehensive certification framework for terminals.

CNA will probably split the complete certification in two parts:

- *The low level communication part*, referring to ISO 14443, could be capitalized from an existing PCD type approval (e.g. EMVCo PCD type approval Level 1) and completed with specific Calypso tests for the analog part.

- *The application part*, which could enhance the registration audit with complementary tests (performances, cross tests with different cards and SAM, etc.).
Calypso license policy

Setting-up a Calypso ticketing system requires using two patents:

- Session patent, which guarantees the data integrity within the card in all possible situations, even if the card is put off the transaction area during the exchanges of information with the reader.
- Ratification, which allows ending correctly a transaction even if any problem occurs during the final acknowledge of data transmission.

The fees resulting from the use of these two Calypso patents are known under the wording “Calypso license”.

The users of Calypso (transit authorities, transport operators) have nothing to achieve about this license, neither to negotiate nor to buy. They only have to benefit, through really opened tenders, from the large industrial offer of Calypso products, which is the direct result of the strong willingness of the Calypso founders to avoid any monopoly.

Calypso license addresses manufacturers, both for terminal equipment (readers) and portables objects (cards, SIM, USB keys …).

In order to simplify the license policy, given the huge number of terminal manufacturers and given the diversification of portable objects (cards, mobile phones, USB keys), today the license addresses only:

- The SAM (Secure Application Module), mandatory in a Calypso terminal or a system; the SAM is today provided by two vendors (Spirtech and ASK). The manufacturers of terminal have no license to acquire; they only have to integrate these SAM.
- IC components used in the portable objects; the related fees are generally paid by IC manufacturers, or card embedders.

Calypso license answers to the rules imposed by the standardization bodies at European and global levels, which very often establish standards integrating patents and fees: the license has to be “reasonable and non-discriminatory”. As such, Calypso license is recognized compliant with this rule. Like whatever industrial product which always integrates some fees resulting from patents, it concerns only manufacturers and not final users (transport operators for example).

License main objectives

The Calypso license answers to two objectives:

- It ensures, as it is usual in the industrial world, a return on investment for the expenses of Research and Development that have been achieved by the inventors, particularly the private partner, Innovatron in this case.
- It ensures the main income for CNA, which represents the operators/users of Calypso, in order to allow them to keep control on Calypso specifications and security. It finances the development of complementary evolutions of Calypso, which are required to ensure the sustainability of this solution. So the incomes from licenses benefit directly to all the community of users of Calypso.

A license for the benefice of Calypso’s users

Calypso license management is ensured by Innovatron, who co-financed in the nineties the R&D development of the Calypso solution. RATP, the proprietary of the Calypso patents, has delegated an exclusive mandate of gesture of Calypso license to Innovatron, who is consequently the only one able to negotiate and sale a license to a manufacturer. In counterpart of this exclusivity, Innovatron has no authorization to manufacture whatever
Calypso product. In consequence, for Innovatron, the return on investment is ensured only through the selling of license, which guarantees to the users that they will benefit from the maximum of manufacturers in competition for buying their Calypso products. All the Calypso licensees benefit from the same conditions and fees, ensuring a true and loyal competition between them in tendering process.

Regarding the costs of the Calypso products, the fees linked to the Calypso license have no impact, or a favourable one: in whatever product, one part of the selling cost is always dedicated to the return on investment of the R&D program of the manufacturer who designed this product. For a Calypso product, this part of the cost is shared between all the licensees through the Calypso fee, which represent an amount less important than in the case of a product of a single manufacturer (there is only one R&D cost for all manufacturers selling Calypso products).

- **License conditions**

For specific information about license conditions and application patents, please contact INNOVATRON [http://www.innovatron.fr](http://www.innovatron.fr).
Smartcard durability

When building a ticketing system, one important economic aspect to consider is the expected life span of the card and durability, meaning how long a card can work without significant deterioration.

The durability is a direct function of the card’s physical characteristics and the frequency of its usage. Transport usage is considered as “heavy”, as the card may be used several times during the same day and over 200 days per year.

The way the card is protected also strongly influences its durability: a bank card is generally in a wallet, whereas a travel card is in a pocket!

Transport operators expect a minimum card life span of 4-5 years, the feedback from European countries using Calypso contactless technology for nearly ten years now, clearly shows that a requirement of 5 years is realistic, as long as the card manufacturing process maintains a high level of quality.

The card’s physical characteristics such as the embedded chip and the manufacturing process of the card all play an important part in the durability of that card. Many factors (heat, bending, chemical attacks, and abrasion) might impact or significantly reduce the card’s life span.
Calypso and users privacy

Protecting privacy has always been a major issue for smart card based IT systems, whether they concern national ID, health, passport or e-tickets.

The main paradox highlights the need for identification/authentication to access networks in a secure way and the temptation to store and/or broadcast or distribute any stored personal information for marketing and commercial purposes.

Calypso allows application owners to deal with that paradox, it being a fundamental element in a transport operator’s CRM toolbox.

The need for careful handling of personal information comes when specific special offers only apply to a certain demography (junior, senior, student, disabled person, etc.). Since the ticket holding the fare is nominative, personal information may reside inside the card to enable further ID and ticket controls by the network agents.

Calypso specifications only deal with the contactless transaction between a terminal and a portable object, they don’t include information about the back-office management system and the collection of transaction data. The transaction is designed to run off-line, that way, there is no need for a constant data exchange over the IT network, limiting the risk of eavesdropping. The data collection and storage falls under the total responsibility of the operator.

The Calypso data model can be tailored to protect individual privacy: a Calypso application holds an Environment/Holder file with fields related to the cardholder’s personal information (name, birthday, etc.) and ID number (ID for the transport network only). Only this holder identification number may be exchanged within data transaction logs, associated to the holder profile, responding to the CRM request of identifying a customer thus preserving his privacy.

In a multi-applicative context, a user’s personal information may be recorded into an ID file that can be shared by several applications (transport, citizen application). Calypso specifies that the read file access may be governed by a PIN code presentation, thus protecting the user’s privacy.

So, CNA, in the Rev 3.2 the portable object, added new features related to privacy protection, mainly additional reading access rules for Calypso files in a Portable Object

In fact, Calypso is privacy-neutral, meaning that its secure e-transaction uniquely requires systems that use it to comply with the recommended privacy guidelines currently in use. It is thereafter the operators’ responsibility to maximize protection of personal information, by limiting them to the appropriate time period and increasing confidence among users by explaining how private information is protected.
Calypso organisations

Calypso Networks Association

The association created in 2003 continues to promote the co-operation and “Know How” sharing philosophy which existed at the beginnings of the Calypso project between different technology founders:

- LANDRATSAMT KONSTANZ (public authority in Germany)
- OTLIS (seven transport operators in Lisbon in Portugal)
- RATP (transport operator in Paris region, France)
- SNCF (national railway company, France)
- STIB (transport operator in Brussels region, Belgium)
- VELA S.p.A (sales entity of the ACTV transport operator in Venice, Italy)

Brussels was chosen to establish the Association as a non-for profit entity, formed under the Belgian statute (called ‘ASBL’).

The main objectives of the Calypso Networks Association are to:

- Define and improve the reference specifications, within all evolving technologies.
- Set up a certification scheme guaranteeing product compatibility.
- Contribute to the international standardization process.
- Promote Calypso to operators and manufacturers in order to maximise its distribution.
- Meet transport operator needs guaranteeing the success of their investment.
- Establish long lasting relationships between all partners using the Calypso specifications, particularly between operators and industry.
- Define and improve the reference specifications, throughout all technology enhancements.
- Set up a certification scheme guaranteeing product compatibility.
- Facilitate and amalgamate different members' needs and experiences.
- Encourage mutual user assistance in the implementation of Calypso e-ticketing systems.

Calypso Networks Association membership

The association is by rights open to:

- All operators or transport operator associations that use certified Calypso media.
- Calypso prescribers, including Transport authorities.

The association welcomes as associated members, without any active voting rights:

- Industrial license holders or distributors of the technology’s components and consultants who contribute in the promotion of Calypso.
- Operators, Operator associations, Organizing Authorities not currently using Calypso cards.
- All organisations with interests in this field and supporting Calypso.
### Present Members (2014)

#### Founders
- LANDKREIS KONSTANZ: Germany
- OTLIS: Portugal
- RATP: France
- SNCF: France
- STIB: Belgium
- VELA: Italy

#### Operators and Transport Authorities
- BMC: Belgium
- INTERPARKING: Belgium
- KEOLIS: France
- MINISTRY of TRANSPORT ISRAEL: Israel
- POSTEMOBILE: Italy
- SIA RIGAS KARTE: Latvia
- SOCIETE DE TRANSPORT MONTREAL: Canada
- START ROMAGNA: Italy
- TRANSDEV: France
- TSP: Italy

#### Industrial Partners
- AEP: Italy
- ASK: France
- GEMALTO: France
- GEP S.p.A.: Italy
- HB TECHNOLOGIES: Algeria
- INTO IT: Belgium
- MORPHO: France
- NOVABASE: Portugal
- OBERTHUR: France
- PARKEON: France
- PRODATA: Belgium
- SCHEIDT & BACHMANN: Germany
- SIEMENS Portugal: Portugal
- ST MICROELECTRONICS: France
- THALES: France
- VIX TECHNOLOGY: France
- WATCHDATA SYSTEM Co Ltd: France

#### Consultants & Experts
- CARD4B: Portugal
- CARD PROJECT: Italy
- DIGIMOBEE: France
- ELITT: France
- FIME: France
- HIGHQ PROFESSIONAL SERVICES: Germany
- LINK Consulting S.A.: Portugal
- MTA – Mobility, Ticketing & Applications Sprl: Belgium
- ORT: Israel
- PHAYMOBILE: Turkey
- SPIRTECH: France
CNA Activities

CNA activities take shape through the creation of task forces; currently, the main working groups are:

- **WG1**: improving and developing Calypso reference specification, to provide an appropriate solution to transport operator needs.
- **WG2**: favouring interoperability between transport networks, and amongst networks, to ensure that any Calypso Portable Object can work with any Calypso terminal.
- **WG3**: promoting Calypso technology worldwide and participating in national and international standardization initiatives so that Calypso's good practices will spread throughout the community.

The technical working groups welcome all contributors who are willing to participate and bring their own expertise: operators, industry vendors and manufacturers, consultants, software houses, and so on.

Each working group is managed by a company leader, chosen by CNA and paid accordingly. An internet collaborative forum federates the working groups: [http://www.cnawg.net](http://www.cnawg.net).

To complete its members' contributions, CNA calls for specific skills from external companies.

CNA Funding

The funding of CNA comes from different sources:

- **Membership dues**
  - Effective members contributions are very low (250€/year), suppliers contribution is slightly higher (from 2500 to 5000€/year).
- **Patents incomes**
  - CNA statutes specify that every member protecting a "know-how", necessary to the implementation of the Calypso specification must refund half of the royalties to CNA, in order to sponsor the working groups' activities. The other half subsidises its R&D investment costs.
  - This is the case for the incomes from the patents related to the Calypso Session and Ratification (marketed by INNOVATRON).
- **Certification services**
  - Specification certification/validation, and in the future the complete certification of all products, is a charged service.

CNA expenses are mainly charges which relate directly to Calypso promotion and communication activities, as well as any specification enhancements.
## Glossary

<table>
<thead>
<tr>
<th>Abbreviation</th>
<th>Full Form</th>
</tr>
</thead>
<tbody>
<tr>
<td>AFC</td>
<td>Automatic Fare Collection</td>
</tr>
<tr>
<td>API</td>
<td>Application Program Interface</td>
</tr>
<tr>
<td>ATM</td>
<td>Automated Teller Machine</td>
</tr>
<tr>
<td>CLUB</td>
<td>Contactless Users Board</td>
</tr>
<tr>
<td>CAAD</td>
<td>Control Access Authorization Descriptors</td>
</tr>
<tr>
<td>CNA</td>
<td>Calypso Networks Association</td>
</tr>
<tr>
<td>CRM</td>
<td>Customer Relationship Management</td>
</tr>
<tr>
<td>CSM</td>
<td>Calypso Secure Module</td>
</tr>
<tr>
<td>DES</td>
<td>Data Encryption Standard</td>
</tr>
<tr>
<td>GP</td>
<td>GlobalPlatform</td>
</tr>
<tr>
<td>HSM</td>
<td>Hardware Secure Module</td>
</tr>
<tr>
<td>IOPTA</td>
<td>InterOperable Public Transport Application</td>
</tr>
<tr>
<td>ITSO</td>
<td>Integrated Transport Smartcard Organisation</td>
</tr>
<tr>
<td>NFC</td>
<td>Near Field Communication</td>
</tr>
<tr>
<td>OEM</td>
<td>Original Equipment Manufacturer</td>
</tr>
<tr>
<td>OTLIS</td>
<td>Operadores de Transportes da região de LISboa</td>
</tr>
<tr>
<td>PCD</td>
<td>Proximity Coupling Device</td>
</tr>
<tr>
<td>PIN</td>
<td>Personal Identification Number</td>
</tr>
<tr>
<td>PO</td>
<td>Portable Object</td>
</tr>
<tr>
<td>RATP</td>
<td>Régie Autonome des Transports Parisiens</td>
</tr>
<tr>
<td>SAM</td>
<td>Secure Application Module</td>
</tr>
<tr>
<td>SNCF</td>
<td>Société Nationale des Chemins de fer Français</td>
</tr>
<tr>
<td>STIB</td>
<td>Société des Transports Intercommunaux de Bruxelles</td>
</tr>
</tbody>
</table>